TLP: CLEAR

22HLAV

Guidelines

of 22HLAV s.r.o. and 22HLAV EDU s.r.o.

to ensure compliance with the obligations arising from Regulation (EU) 2016/679 of the European Parliament and of the Council 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, and under the Act on the processing of personal data No. 110/2019 Coll.

Version: 2.0 valid and effective on the date of signature by the statutory body Approved by:

Ing. Miroslava Nebuželská

Digitally signed by Ing. Miroslava Nebuželská
Date: 17 March 2026 10:06:11 +01:00

signature of the statutory body

Miroslava Nebuželská

Vít Vagner

Digitally signed by Ing. Vít Vagner
Date: 12 March 2026 16:57:30 +01'00'

signature of the statutory body

Vít Vagner

Contents

1. INTRODUCTORY PROVISIONS

1.1 Subject matter and purpose of the Directive:

This Policy serves to ensure compliance with the obligations arising from Regulation (EU) 2016/679 of the European Parliament and of the Council 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 (hereinafter referred to as the "General Data Protection Regulation").

22HLAV s.r.o. and 22HLAV EDU s.r.o. declare that they have assessed the potential obligations arising from Act No. 171/2023 Coll. on the protection of whistleblowers and that, as of the date of this policy's update, they meet the conditions for the implementation of an internal reporting system as set out in Section 8.

1.2 Definitions:

Datasets

- are groups of data comprising personal data of a similar scope, processed for the same purpose under the same legal basis.

Legitimate legal basis

- is the legal basis of the controller's legitimate interest, which applies to such processing of personal data where the legitimate interests or rights of the controller override the interests or rights of the data subject, taking into account the reasonable expectations of data subjects based on their relationship with the controller. This includes, for example, the protection of the controller's property, and the life and health of employees and persons entering the controller's premises.

The companies 22HLAV s.r.o. and 22HLAV EDU s.r.o.

- 22HLAV s.r.o. and 22HLAV EDU s.r.o. are data controllers, and their employees process personal data on behalf of their employer as part of their work duties; 22HLAV s.r.o. and 22HLAV EDU s.r.o. act as a Data Processor on the basis of a data processing agreement. They are also referred to as the Company or 22HLAV.

An authorised person

- is any employee of the controller who, in the course of their employment with the controller, comes into contact with personal data or processes it. Authorised persons must be instructed and made aware of the contents of this internal regulation. A written record is kept of the briefing and familiarisation. Authorised persons must be briefed again if there has been a change in their job classification or any other change resulting in a change to or the scope of the authorised person's duties in relation to the processing of personal data. Access to the personal data of data subjects is strictly limited to briefed authorised persons only.

The data protection officer

- is an employee of the company who has the relevant authorisations and access to personal data necessary for the performance of their duties.

Personal data

- is any information relating to an identified or identifiable natural person (data subject). An identifiable natural person is a natural person who can be identified, directly or indirectly.

A breach

- is a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Authorised person

- is an employee of the company who has been entrusted with a specific job or task that is not part of their main duties.

Profiling

- any form of automated processing of personal data evaluating personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's work performance, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her.

Shared drive

- is a shared email drive and network storage (Google Drive), administered by Google Ireland, VAT No.: IE6388047V, with its registered office at Gordon House, Barrow Street, Dublin 4, Ireland.

Shared storage on our own server

- is SeaFile shared storage on 22HLAV's own server, which is located at the registered office of 22HLAV, Všebořická 82/2, Bukov, 400 01 Ústí nad Labem.

Employee file

- is a set of documents relating to an employee, containing in particular: the employment contract, personal questionnaire, CV and handover report.

Consent of the data subject

- is any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of his or her personal data.

Data controller

- 22HLAV s.r.o., Company ID No. 64052907 and 22HLAV EDU s.r.o., Company ID No. 04333497, with its registered office at
  Všebořická 82/2, Bukov, 400 01 Ústí nad Labem, is the entity that determines the purposes and means of personal data processing and is responsible for such processing.
- The clients of 22HLAV s.r.o. and 22HLAV EDU s.r.o. who have entered into a personal data processing agreement with these companies also act as data controllers.

Data subject

- is a natural person to whom the processed personal data relates.

Turquoise organisation / Turquoise principles

- Turquoise organisations, as introduced by Frederic Laloux, are characterised by unique principles. Instead of a rigid hierarchy, they rely on autonomous teams that manage their own activities. The emphasis is on individuality, openness, flexibility and agility. These values enable employees to approach their work creatively and responsibly, leading to greater efficiency and innovation.

Recruitment process

- is the process of selecting and, where appropriate, recruiting a new employee.

Employee data

- refers to the personal data of the company's employees. A specific list is provided in Annex 1 to this policy.

Personal data processor

- is an entity that processes personal data on behalf of the controller on the basis of a signed personal data processing agreement.
- Under personal data processing agreements concluded between 22HLAV and its clients, 22HLAV acts as a personal data processor. The subject matter of these agreements is the processor's obligation to process, on behalf of the clients (as data controllers), personal data to which the processor gains access whilst providing services under the service provision agreement.
- Personal data processors also include persons who are in a contractual relationship with 22HLAV as external collaborators on the basis of an agreement on the involvement of a sub-processor in the processing of personal data; see Annex No. 7.
- **The contractual processors of personal data** for 22HLAV, as the data controller, are: Google Ireland, VAT No.: IE6388047V, with its registered office at Gordon House, Barrow Street, Dublin 4, Ireland (hereinafter also referred to as **"Google** Ireland"); ABRA Software a.s., Company ID No.: 25097653, with its registered office at Jeremiášova 1422/7b, Stodůlky, 155 00 Prague 5; KASTNER software s.r.o., Company ID No.: 25591169, with its registered office at Třebízského 508, 798 41, Kostelec na Hané; Web4U s.r.o., Company Registration Number: 17311501, with its registered office at Korunní 2569/108, Vinohrady, 101 00 Prague 10; 59codes s.r.o., Company ID No. 24331708, with its registered office at Nové sady 988/2, Staré Brno, 602 00 Brno; Direct Fidoo Payments s.r.o., Company ID No.: 02690446, registered office at Pod dráhou 1636/1, Holešovice, 170 00 Prague 7; the company Digitoo s.r.o., Company ID No.: 08494584, registered office at Pernerova 697/35, Karlín, 186 00 Prague 8; Dativery s.r.o., Company ID No.: 05574617, registered office at Olešná 51, 338 24 Němčovice; GIMMEDATA, s.r.o., Company ID No.: 26481782, registered office at Ječná 498/35, Čechovice, 796 04 Prostějov; INFLO GROUP LIMITED, with its registered office at Inflo Limited E.Volve Business Centre, Rainton Bridge South Business Park, Houghton Le Spring, Tyne and Wear, United Kingdom, DH4 5QY; Microsoft Corporation, with its registered office at Konrad-Zuse-Str. 1, 85716 Unterschleißheim, Germany; Docusign, Inc., with its registered office at 9-15 Rue Maurice Mallet, 92130 Issy-les-Moulineaux, France; the Drupal Association, z.s., Company ID No.: 05063701, registered office at Proboštovská 281/33, 417 12 Proboštov; Jan Polzer, Company ID No.: 75684411, Černého 45, 635 00 Brno; MSI Global Alliance, registered office at 10 Queen St Pl, London,

United Kingdom; FIRM ACADEMY LIMITED, with its registered office at The Mill Pury Hill Business Park, Alderton Road, Towcester, Northants, England; Amazon Web Services EMEA SARL, with its registered office at 38 Avenue John F. Kennedy, L-1855, Luxembourg (hereinafter also referred to as **the "contracted** processor").

1.3 Legislation:

- Act No. 110/2019 Coll., the Personal Data Processing Act
- Act No. 127/2005 Coll., the Electronic Communications Act, as amended
- Act No. 171/2023 Coll., Act on the Protection of Whistleblowers
- Act No. 253/2008 Coll., Act on Certain Measures against the Legalisation of Proceeds from Crime and the Financing of Terrorism, as amended
- Act No. 89/2012 Coll., the Civil Code, as amended
- Act No. 435/2004 Coll., the Employment Act, as amended
- Act No. 563/1991 Coll., the Accounting Act, as amended
- Act No. 582/1991 Coll., Act on the Organisation and Implementation of Social Security, as amended
- Act No. 592/1992 Coll., Act on Public Health Insurance Contributions, as amended
- Act No. 589/1992 Coll., Act on Social Security Contributions and Contributions to State Employment Policy, as amended
- Act No. 586/1992 Coll., the Income Tax Act, as amended
- Act No. 235/2004 Coll., the Value Added Tax Act, as amended
- Act No. 93/2009 Coll., the Act on Auditors, as amended
- Act No. 262/2006 Coll., Labour Code, as amended
- Act No. 187/2006 Coll., the Sickness Insurance Act, as amended
- Act No. 264/2025 Coll., the Cyber Security Act, as amended
- Act No. 250/2017 Coll., the Electronic Identification Act, as amended

1.4 Personal data processing process:

- A description of the individual personal data processing processes, broken down into individual datasets, is available in Annex 1.

2. RESPONSIBLE PERSONS

Responsibilities and responsibilities listed listed stem from the employee's employment contract or from their authorisation by the Company's management.

2.1 Data Protection Officer (DPO)

- This role is an appointed position. It is an employee who is responsible for overseeing the lawfulness of the processing of all personal data processed by the controller and for ensuring their proper protection and security.

2.2 All employees

- All employees of the Company who process the personal data of data subjects as part of their work.

3. EXERCISE OF THE RIGHTS AND OBLIGATIONS OF THE DATA CONTROLLER

3.1 Duties of data protection officers:

A. The responsible persons referred to in Chapter 2 are obliged to secure the personal data being processed.
B. When protecting data stored on personal computers, including laptops and servers, data controllers shall secure personal data in such a way as to prevent unauthorised or accidental access, alteration, destruction or loss, unauthorised transfer, processing, and any other misuse of such personal data.
C. The responsible persons referred to in Chapter 2 of this policy are authorised to handle only those personal data that they require to fulfil their work duties.
D. Authorised persons may process personal data only for the purpose of fulfilling their work duties, in accordance with the purpose of processing and on a legitimate legal basis.
E. The data controllers referred to in Chapter 2 of this policy are required to keep the personal data they process up to date and accurate.
F. Data controllers are required to provide the security manager with all information that affects the security, up-to-dateness and accuracy of records of personal data being processed.
G. Data controllers are required to keep proper records of all personal data processing in accordance with the scope of their responsibilities and duties.
H. Responsible persons are obliged to process personal data in accordance with the processing principles set out in Chapter 3.2. Responsible persons shall process personal data exclusively on the company's equipment. All responsible persons processing personal data in any capacity shall sign a confidentiality clause; see Annex No. 3.

3.2 Principles of personal data processing:

3.2.1 Lawfulness, fairness and transparency

A. For each purpose of processing, there is a legitimate legal basis under points (a) to (f):

A. the data subject has given consent to the processing of their personal data for one or more specific purposes; see the form on the website www.22hlav.cz and see Annex 2 and Annex 3;
B. processing is necessary for the performance of a contract to which the data subject is a party, or for the implementation of measures taken prior to entering into a contract at the request of that data subject;
C. processing is necessary for compliance with a legal obligation to which the controller is subject;
D. processing is necessary to protect the vital interests of the data subject or another natural person;
E. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
F. processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

3.2.2 Purpose limitation

- In accordance with Section 25 et seq. of Act No. 110/2019 on the processing of personal data, as amended, personal data must be collected for specific, explicitly stated and legitimate purposes and must not be further processed in a manner incompatible with those purposes.
- The purposes of processing for individual datasets of personal data are set out in Annex 1.

3.2.3 Minimisation

- The personal data processed is limited to the extent necessary in relation to the purpose of the processing.
- It is prohibited to process personal data that is not strictly necessary to fulfil the purpose, .

3.2.4 Accuracy

- Personal data is kept accurate and updated as necessary by the authorised person.
- Inaccurate data, taking into account the purpose of processing, shall be rectified without delay.
- If inaccurate personal data cannot be rectified, it must be erased without delay.

3.2.5 Storage limitation

- The storage of personal data in a form that allows the data subject to be identified for a period longer than is necessary for the fulfilment of the purpose for which it is processed is prohibited.

3.2.6 Integrity and confidentiality

- The processing of personal data by responsible persons is permitted only in accordance with this Directive.

4. PROCESSING OF PERSONAL DATA BY THE COMPANY

- A summary table of the Company's processed datasets and their content is available for inspection in Annex 1 to this policy.
- Employees are informed of the method of processing all their personal data by the Company prior to signing their employment contract via an internal policy. They shall confirm their acknowledgement of and consent to this internal policy by signing the record.

4.1 22HLAV in the role of data controller

4.1.1 Employee data

A. Documents proving the existence of an employment relationship, the legality of a foreign national's residence, the termination of an employment relationship and employees' pay slips are stored in electronic form on the cloud storage (Google Drive operated by Google Ireland) with restricted access for all Company employees, in accordance with the Turquoise Principles, for the purpose of complying with Act No. 435/2004 Coll. on the legal basis set out in Chapter 3.2.1, point A), letter c), for a period of 10 years from the termination of the employment relationship

B. Employee files are stored electronically on cloud storage (Google Drive operated by Google Ireland) and their outputs are stored in the internal system of the processor 59codes s.r.o. The data is accessible with restricted access to all employees or authorised employees of the Company, in accordance with the Turquoise Principles, for the purpose of complying with Act No. 435/2004 Coll. under the legal basis set out in Chapter 3.2.1, point A), letter b), until the termination of the employment relationship, after which it is deleted.

C. Payroll documentation processed for the purpose of complying with Act No. 582/1991 Coll., the Act of the Czech National Council on the Organisation and Implementation of Social Security, Act No. 586/1992 Coll., the Act of the Czech National Council on Income Tax, and Act No. 262/2006 Coll., the Labour Code, with legal grounds under Chapter 3.2.1, point A), letter c), for a period of 10 years, commencing on the first day of the calendar year following the year to which they relate.
    a. A specific list of personal data contained in payroll records is available for inspection in Annex 1 to this directive; see datasets PAYROLL RECORDS 1–4.
    b. The Company's employees' payroll records are stored in the FlexiBee accounting and payroll software of the contracted processor ABRA Software a.s.; any copies are stored in cloud storage (Google Drive operated by Google Ireland).
    c. Access to payroll documentation is restricted to authorised employees
    d. The 10-year retention period under Section 4.1.1(C) does not apply to record sheets, which are disposed of after 3 years, starting from the first day of the calendar year following the year to which they relate.
    e. The 10-year retention period under Section 4.1.1(c) does not apply to payslips, which are retained for 45 years, starting from the first day of the calendar year following the year to which they relate.

D. Employees' personal data published on the websites https://www.22hlav.cz/ and for the purpose of presenting the team are

processed on the legal basis set out in Chapter 3.2.1(A)(a) until the termination of the employment relationship or until consent to the processing of personal data for this purpose is withdrawn, with consents being updated at least once every 12 months.

E. If the Company processes documents containing personal data of current employees other than those specified in Chapter 4.1.1, points A) to D), such data is processed exclusively for the purpose of managing personnel matters on the legal basis set out in Chapter 3.2.1, point A), letter b), until the termination of the employment relationship.

F. During the recruitment process, the Company receives CVs from job applicants. These are stored in the email accounts of authorised persons. Once assessed, they are deleted from the email inbox. The processing of personal data within the recruitment process is as follows:
   a. CVs of job applicants who attended a face-to-face interview and were hired are governed by Chapter 4.1.1, point B).
   b. Job applicants' CVs are processed in electronic form for a limited period during the recruitment process, with access restricted to authorised persons on cloud storage (Google Drive operated by Google Ireland); they are deleted once the recruitment process has ended.
   c. CVs of job applicants who attended a face-to-face interview but were not hired are processed as follows:
      i. Retention of data relating to unsuccessful candidates: In the event that no employment relationship is established with the candidate, the Company retains their CV and a record of the entrance test result for a period of 12 months from the formal conclusion of the relevant recruitment process.
      ii. Legal basis and purpose of retention: This retention is based on the Company's legitimate interest [Article 6(1)(f) of the GDPR]. The purpose is to protect the integrity of the recruitment process, specifically to monitor the waiting periods for the possibility of repeating professional entrance tests, to verify the consistency of stated work experience in the event of repeated applications, and to ensure the effectiveness of the recruitment process.
      iii. Balance test and transparency: The demonstrability of this legitimate interest is documented in the Balance Test (see Annex 10), which is a separate annex to this documentation. Each applicant must be demonstrably informed of this processing and of their right to object to it no later than before submitting their CV (e.g. via text in the recruitment form).
      iv. Deletion of data: After a period of 12 months has elapsed, or immediately following a valid objection raised by the applicant, the relevant authorised person shall ensure the permanent and secure deletion of this personal data from all the Company's systems, provided there is no other legal basis for its further retention.

4.1.2 Internal data

A. Accounting documents, accounting ledgers, depreciation schedules, inventory lists, chart of accounts and the Company's reports for the purpose of fulfilling obligations arising from Act No. 563/1991 Coll., the Accounting Act, with the legal basis set out in Chapter 3.2.1, point A), letter c), are retained for 10 years following the year to which they relate, with restricted access for

the contract processor; any copies are stored on the processor's shared server.

B. Accounting records used by the Company to demonstrate the keeping of accounts for the purpose of fulfilling obligations arising from Act No. 563/1991 Coll., the Accounting Act (§33) with legal title pursuant to Chapter 3.2.1, point A), letter c), are retained for 5 years following the year to which they relate, with restricted access for the contractual processor; any copies are stored on the processor's shared server.

C. The Company's financial statements are prepared in accordance with Act No. 563/1991 Coll., the Accounting Act, and are retained for 10 years following the year to which they relate.
    a. The financial statements are published in the public register.

D. Service agreements and cooperation agreements are recorded:
    a. For the purpose of fulfilling the subject matter of the contract with legal title pursuant to 3.2.1(A)(b) until the expiry of the contract.
    b. For the purpose of accounting records with legal title pursuant to Chapter 3.2.1, point A) letter c), for 10 years following the year to which they relate.
    c. Records are stored on cloud storage (Google Drive operated by Google Ireland). The data processor performs daily backups of the drive and deletes them after 30 days.
    d. The first name and surname of the sender/recipient of the postal item and its contents are processed for the purpose of recording mail with a legal basis under Chapter 3.2.1, point A) letter f) for 3 years from the first day of the calendar year following the year of receipt/dispatch of the postal item and are stored on cloud storage (Google Drive operated by Google Ireland) with access for all employees.

4.1.3 Partner data

A. For the purpose of sending out electronic newsletters and invitations to training courses, the following personal data is processed: first name, surname and email address are processed electronically in cloud storage (Google Drive operated by Google Ireland) and in the internal system of the processor 59codes s.r.o. on the legal basis set out in Section 3.2.1(A)(a) and (f) until the purpose of processing ceases to apply or consent is withdrawn.

B. For the purpose of sending New Year's cards, the following personal data is processed: first name, surname and email address of data subjects on cloud storage (Google Drive operated by Google Ireland) and in the internal system of the processor 59codes s.r.o., on the legal basis set out in Chapter 3.2.1, point A), letters f).
    a. New Year's cards are sent exclusively to clients and associates who are in demonstrable contact with the Company.

C. For the purpose of processing enquiries submitted via the web form on the website https://www.22hlav.cz/, the following personal data is processed: first name, surname, email address on cloud storage (Google Drive operated by Google Ireland) with a legal basis in accordance with Chapter 3.2.1, point A), letter a), until the purpose of processing ceases to apply or consent is withdrawn.

D. For the purpose of cooperating with authorities in the performance of their statutory duties, including inspections and investigations, the following personal data is processed: first name, surname, email address on cloud storage (Google Drive operated by Google Ireland) on the legal basis set out in Chapter 3.2.1, point A), letter c), until the purpose of processing ceases to apply.

E. For the purpose of cooperating with external partners on the basis of cooperation agreements and agreements on the involvement of a sub-processor in the processing of personal data, see Annex No. 7

The following personal data is processed: first name, surname, maiden name, date of birth, town and district of birth, nationality, permanent address, temporary address, telephone number, email address, bank account number, education, and photographs of external collaborators.

F. For the purpose of processing data arising from supplier-customer relationships, personal data is recorded in the internal system of the processor 59codes s.r.o. and on cloud storage (Google Drive operated by Google Ireland) with a legal basis in accordance with , Chapter 3.2.1, point A), letters b) to f).

4.1.4 Client data

Legal entities

A. For the purpose of client identification, personal data is processed on the legal basis set out in Chapter 3.2.1, point A), letters b) and c). The controller is an AML-obligated entity under Act No. 253/2008 Coll.; the process and scope of identification are subject to PART TWO, TITLE I (§ 7 -
Section 15a of the Act. The retention of information is governed by TITLE II (Sections 16–17a) of the Act. The controller retains the data for 10 years following the conclusion of a transaction outside a business relationship or the termination of a business relationship.
B. Customer identification process:
    a. is carried out in accordance with European Union Regulation No 910/2014 on electronic identification and trust services for electronic transactions in the internal market (eIDAS) and in accordance with Act No 250/2017 Coll. via the contracted personal data processor Docusign, Inc., with restricted access for authorised persons of the Controller. Any copies are stored in the Controller's cloud storage (Google Drive operated by Google Ireland). The contracted processor performs daily disk backups and deletes them after 30 days.
    b. This is also carried out through the client's personal identification. The data is stored on the Controller's cloud storage (Google Drive operated by Google Ireland). The contractual processor performs daily disk backups and deletes them after 30 days.
C. Contractual documentation:
    a. is stored on the Controller's cloud storage (Google Drive operated by Google Ireland). The Contracted Processor performs daily disk backups and deletes them after 30 days.

Natural persons

A. For the purpose of providing services purchased via the e-shop (website https://www.22hlav.cz/), data such as first name, surname, email address, billing and contact details are processed on cloud storage (Google Drive operated by Google Ireland) on the legal basis set out in Chapter 3.2.1, point A), sub-points b), c) and f) for the duration of the service provision and for the duration of the statutory obligation arising from the Accounting Act No. 563/1991 Coll., and are retained for up to 10 years after the year to which they relate.
B. For the purpose of creating a profile, personal data entered when creating an account on the website https://www.22hlav.cz/ (pre-filled data to facilitate the purchase of services) is processed on the legal basis set out in Section 3.2.1(A)(b), (c) and (f) until the account is deleted by the user. Personal data provided for accounting purposes arising

from the purchase of services by the data subject are retained for 10 years following the year to which they relate, pursuant to the Accounting Act No. 563/1991 Coll.

C. For the purpose of making a donation via the Dobrofond charity project through the website https://www.22hlav.cz/, such data is processed on the legal basis set out in Chapter 3.2.1, point A), letter f), for a period of 3 years from the last interaction with the donor.
D. The lawfulness of the processing of personal data on the legal basis set out in Chapter 3.2.1, point A), letter f) was assessed by the Controller through a balancing test, which is Annex No. 8 to this policy.

4.1.5 Sources of personal data

A. Website: https://www.22hlav.cz/
    a. as a result of automated processing when visiting the website, see Annex 6
    b. Web form
B. Telephone/audio-visual interviews or email or any other written communication
C. Other public or private legal entities with or without legal personality (e.g. contractual processors of personal data or authorities in the performance of their statutory duties, including inspections and investigations, e.g. the Financial Analytical Office, the Czech National Bank or the Chamber of Auditors of the Czech Republic)
D. Economic sources, e.g.: contractual documentation, assignment of receivables, acquisitions, mergers, acquisition of assets
E. Third parties
    a. In the event of the transfer of personal data by a Third Party, the Company acknowledges the following:
        i. the data subject has given prior consent to the use of their personal data and the Third Party was therefore authorised to process it for this purpose (transfer and disclosure of personal data)
        ii. in the event of the processing of personal data transferred by a Third Party, that party is obliged to provide the data subject with the necessary information regarding the processing of personal data, even if it has transferred the data

4.1.6 Conditions for disclosure

The Controller is authorised to disclose personal data on the basis of a lawful purpose, see Chapter 3.2.1, point A), letters b) to f), in the event of transfer:

A. to the data subject themselves and persons authorised by them
B. contractual processors of personal data
C. institutions in connection with the conclusion of a transaction (e.g. banks)
D. business partners / assignees of rights
E. to state institutions on the basis of fulfilling legislative obligations arising from from the overview of legal regulations, see section 1.3.

4.1.7 Third-party websites

The Data Controller bears no responsibility for the content and operation of third-party websites which the data subject may access via the Data Controller's website. The data subject acknowledges that by clicking through to an external website, data such as the IP address, time of access or type of browser used by the user (data subject) may be processed by a third party; see Appendix 6.

4.1.8 Rights of the data subject

A. The right of access means the right to obtain confirmation from the data controller as to whether or not personal data are being processed, and if so, the right of access to personal data and information regarding the processing;

B. The right to rectification means the right to have inaccurate personal data rectified and/or incomplete personal data completed without undue delay, including by means of a supplementary statement;

C. The right to erasure / the right to be forgotten means the right to have personal data erased without undue delay where the personal data no longer needs to be retained in relation to the purposes for which it was collected or otherwise processed, or where there is no other legal basis for processing; or the data subject objects to the processing and there are no overriding legitimate grounds for further processing; or the personal data must be erased following the fulfilment of a legal obligation to which the data controller is subject. The above grounds shall not apply if the processing of personal data is necessary: for the exercise of the right to freedom of expression
and information; or to comply with a legal obligation which requires the processing of personal data under the law to which the data controller is subject, or to perform a task carried out in the public interest or in the exercise of official authority vested in the data controller; or for reasons of public interest in the area of public health; or for archiving purposes in the public interest, for scientific or historical research purposes or for statistical purposes, where the right to erasure/the right to be forgotten is likely to render impossible or seriously impair the achievement of the objectives of such processing of personal data; or for the establishment, exercise or defence of legal claims;

D. The right to restrict the processing of personal data means restricting processing where the data subject contests the accuracy of their personal data, for a period enabling the data controller to verify the accuracy of the data subject's personal data; or where the processing is unlawful and the data subject agrees to the erasure of their personal data
and you request the restriction of their use instead; or the data controller no longer needs the personal data for the purposes of processing, but the data subject needs it for the establishment, exercise or defence of legal claims; or the data subject has objected to the processing of personal data pending verification of whether the legitimate interests of the data controller override those of the data subject;

E. The right to data portability means the right to receive the personal data that the data subject has provided to the data controller in a structured, commonly used
and machine-readable format, and the right to transmit those personal data to another data controller, where technically feasible and where the processing is based on consent or on the performance of a contract and the processing is carried out by automated means;

F. The right to object means the right to object at any time, on grounds relating to the specific situation of the data subject, to the processing of their personal data which is based on the performance of a task carried out in the public interest or in the exercise of official authority vested in us, or against processing based on legitimate interests, including profiling based on such interests, which results in the cessation of the processing of your personal data, unless we demonstrate compelling legitimate grounds for the processing which override your interests, rights and freedoms, or for the establishment, exercise or defence of legal claims;

G. The right to withdraw your consent at any time without affecting the lawfulness of processing based on consent given prior to its withdrawal, where the legal basis for the data controller's processing is the data subject's explicit consent;
H. the right to lodge a complaint with the Office for Personal Data Protection at Pplk. Sochora 27, 170 00, Prague 7, by email:posta@uoou.cz or via data box ID: qkbaa2n;
I. The right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning the data subject or similarly significantly affects the data subject, except where such processing is necessary for the conclusion or performance of a contract between the data controller or is permitted by law to which the data controller is subject, and which also provides for appropriate measures to safeguard the data subject's rights and freedoms and legitimate interests, or is based on explicit consent. With the exception of the right to lodge a complaint with the Office for Personal Data Protection, as stated above, these rights may be exercised by sending a request by email to:dpo@22hlav.cz , via data box: bfus9w4, or to the registered office of 22HLAV s.r.o., Všebořická 82/2, 40001 Ústí nad Labem. The data controller is obliged to inform the data subject, within one month of receiving the request, of the specific steps it will take in response to the request. This period may be extended by up to two months if necessary. In such a case, the data controller will inform the data subject of any extension within one month of receiving the request, including the reasons for the delay in processing the request.

4.2 22HLAV in the role of data processor / recipient

A. The rights and obligations regarding the protection of personal data between the Company (Processor) and the client (Controller) are governed by the personal data processing agreement , see Annex No. 4, signed by both parties.

4.2.1 Client data

A. Client data includes the datasets set out in Annex 1, in particular: Management of payroll and HR administration for the client, Management of accounting administration for the client, Management of tax administration for the client, Management of audit files for the client, and is
    A. processed for the purpose of fulfilling the subject matter of the contract and invoicing on the legal basis set out in Chapter 3.2.1, point A), letters b) and c)
    B. stored on the processor's shared storage (Seafile); in the case of audit file management, the data is also stored on the Inflo digital audit platform (INFLO GROUP LIMITED) and on Google Drive, a shared cloud storage service provided by Google Ireland, for the periods specified by law; see Annex No. 1
    C. Upon termination of the business relationship, documents of which the Company is the originator are retained for archiving purposes in the event of a potential legal dispute regarding liability for damages under the legal basis set out in Chapter 3.2.1, point A), sub-points b), for a period of 10 years from the end of the calendar year to which they relate, after which they are deleted. The period of liability for damages is determined by the Civil Code.
    D. Personal data processed during the organisation of a tender for a client (the data controller) is processed exclusively for the purpose of collecting

information for the evaluation of the tender procedure with a legal basis in accordance with Chapter 3.2.1, point A), letter b), and following its evaluation, all documents containing personal data are handed over to the controller

5. SECURITY OF MANAGED DATA

5.1 System security:

5.1.1 Mobile phone

A. Telephone contacts stored on a mobile phone are processed by authorised persons for the purpose of communicating with employees and partners, on the legal basis set out in Chapter 3.2.1, point A), letters a) to f), until the termination of the employment or partnership relationship or until consent is withdrawn.
B. For the purposes of this policy, a mobile phone is a mobile device used for the performance of work duties.
C. Employees are obliged to:
    a. secure the phone and protect it against access by unauthorised persons,
    b. ensure that every mobile device (phone, tablet, laptop) on which personal data is processed is secured against unauthorised access (PIN, biometrics, password) and has active data storage encryption (in accordance with Annex 5). In the event of the loss or theft of a device, the employee is obliged to report this immediately (within 30 minutes of discovery) to the IT department to initiate security procedures.
    c. set the visibility of incoming notifications so that they are only visible after the phone screen is unlocked,
    d. update the device regularly
D. Employees are prohibited from:
    a. Take photographs, make recordings or otherwise record personal data of natural persons, with the exception of storing telephone contacts in the usual manner.
    b. Send personal data of individuals via mobile applications, SMS/MMS, with the exception of sending telephone contacts via SMS or mobile business cards.

5.1.2 Email

A. All email attachments must be scanned for viruses.
B. Potentially dangerous attachments must be blocked.
C. It is prohibited to use email in a manner that endangers the data subject.
D. It is prohibited to send personal data of natural persons via email, with the exception of contact details commonly provided on business cards.
E. Point D) does not apply if the email is encrypted or if personal data is sent in a password-protected email attachment.

5.1.3 Computers and laptops

Company employees use a Company computer or laptop to perform their work. In the case of external collaborators, this is governed by the BYOD policy; see Appendix No. 5

A. Employees are required to secure the Company's computer or laptop and protect it against access by unauthorised persons.
B. Company computers or laptops must be password-protected for access to the active user account and secured with a screen saver.
C. Passwords must comply with the security requirements (length, complexity, expiry) set out in the currently applicable Minimum Security Standard (Appendix 5). Employees are required to use an approved password manager to manage their passwords, and sharing passwords with others is prohibited.
D. It is mandatory to have antivirus software installed on company computers or laptops and to update the software regularly.
E. Any external storage media connected to the device must be scanned by antivirus software.
F. It is prohibited to send personal data of individuals via online storage services.

5.1.4 Shared drive

A. Company employees use a shared drive located on an external server for storing and sharing data. The shared drive is properly secured both in terms of the stored data and in terms of communication with the drive – uploading and downloading data.

5.2 Data and physical security

A. Upon joining the company, employees are given keys or access details for their workplace.
    a. The last employee to leave their workplace checks it, secures it and closes/locks it (closes and checks the windows, turns off the lights and locks the door).
    b. The last employee to leave the workplace premises checks that the lights are off before leaving and closes/locks the main entrance door to the building.
B. Employees are required to adhere to the clean desk policy; in their absence, no freely accessible documents, portable media or devices not locked via software (computer, laptop, mobile phone) may be left at the workplace.
C. Paper documents containing personal data must not be left freely accessible on a desk when the employee is absent (Clean Desk Policy). Paper documents must be disposed of exclusively using **a shredder** (minimum security level P-4). It is prohibited to dispose of unshredded documents containing personal data in ordinary household waste (bins).
D. The company uses approved cloud services (Google Workspace) for the processing of personal data, which comply with GDPR requirements and have a Data Processing Agreement (DPA) in place. It is strictly prohibited to store files containing personal data on unauthorised private storage services (e.g. private Google Drive, WeTransfer).
E. The processing of personal data using generative AI tools is governed by the rules set out in **the Minimum Security Standard** (Annex 5). The inclusion of clients' and employees' personal data in public versions of AI tools is prohibited.

Point 5.2 is further governed in accordance with Annex 5, the Minimum Security Standard.

5.3 Monitoring compliance with the policy

A. The Compliance and IT team shall ensure that all Company employees to whom this policy applies receive training at least once during a calendar year.
B. The content of the training referred to in Chapter 5.3, point A) covers, in particular, the rights and obligations of persons responsible for the processing of personal data, the Company in its role as a controller
and processor of personal data, and the secure use of the Company's technologies and systems.
C. The Compliance and IT team shall update this policy during the year to ensure that complies with the Company's obligations under the General Data Protection Regulation.

5.4 Final provisions

A. The disposal of documents containing personal data in accordance with this policy, in particular the deletion or shredding of documents containing employee or partner data, shall not apply in the event of ongoing legal or other proceedings in which the documents would be used as evidence. In such cases, the documents shall be archived for the purpose of providing evidence with legal standing in accordance with Chapter 3.2.1, point A), sub-point f) until the conclusion of the proceedings, and then destroyed.
B. A breach of the duties of responsible persons arising from this directive is considered a serious breach of the duties arising from the legal regulations relating to the work performed by the employee and may constitute grounds for termination of employment.
C. If a responsible person causes damage to the employer due to a breach of the obligations arising from this directive, the employee is obliged to compensate the employer for the damage caused through their own fault.
D. The scope and method of compensation for damage are governed by Act No. 262/2006 Coll.

List of annexes according to the TLP

classification TLP:CLEAR

- Annex No. 1 Records of processing activities
- Annex No. 4 TEMPLATE 22HLAV Data Processing Agreement (Czech and English versions)
- Annex No. 6 Cookies
- Annex No. 7 TEMPLATE 22HLAV Sub-processor Agreement
- Appendix 8: Data Protection Impact Assessment – Communication with clients, donors and employees for marketing and fundraising purposes
- Appendix 10: Balancing test – legitimate interest in retaining CVs of unsuccessful applicants

TLP:GREEN

- Appendix 5 Minimum security standard
- Appendix 9: Balancing test – Assessment of legitimate interest in auditing company facilities, monitoring compliance with security rules and accessing employee accounts
- Appendix 11: GDPR and Cybersecurity Documentation Map

TLP:AMBER

- Appendix 2 Consent to the processing of employees' personal data
- Appendix 3 Declaration on confidentiality, information protection and the use of company devices