# 1. INTRODUCTION

## 1.1. Purpose of the Document and Legal Definition

This document was elaborated on the basis of Act no. 18/2018 Coll. on personal data protection and amending and supplementing certain acts (the **"Act"**) and in accordance with the Regulation 2016/679 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of such personal data and on the free movement of such data (the **"GDPR"**).

The GDPR Act and Regulation applies to the processing of personal data carried out in whole or in part by automated means or other than automated means, if the personal data form part of an information system or are intended to form part of an information system.

The GDPR Handbook regulates the rules of personal data processing as well as the rights and obligations of the Data Subject, Controller or Processor in accordance with the Act and the Regulation.

GDPR Handbook:

**a.** constitutes the legal grounds for the personal data processing;
**b.** contains a list of prepared documentation related to the protection of personal reasons, which represents the legal basis for the processing of personal data;
**c.** describes organizational, technical, personnel and security measures;
**d.** determines the controls and accountability of persons who have access to and/or process personal data.

## 1.2. Definitions of some terms:

- **The Controller** is a non-profit organization EDYN, n.o., with its registered seat at Lermontovova 911/3, 811 05 Bratislava – Staré Mesto City District, Trade ID: 52 493 923 (hereinafter referred to as the "**Controller**" or "**EDYN**"), legal person who has defined the purpose and means of personal data processing and processes these on their own behalf;
- **Personal data** are data relating to an identified or identifiable natural person who can be identified directly or indirectly, in particular on the basis of a generally applicable identifier, another identifier, such as first name, last name, identification number, telephone number, e-mail, online identifiers, Cookies ID file, car brand, location data, or on the basis of one or more characteristics or traits that make up its physical, physiological, genetic, psychic, mental, economic, cultural or social identity;
- **The data subject** is any natural person to whom personal data relate;
- **The personal data processing** is a processing operation or set of processing operations involving personal data or personal data files, in particular the acquisition, recording, organization, structuring, storage, alteration, retrieval, browsing, use, provision by transmission, dissemination or in other manner, regrouping or combining, restriction, erasure, whether by automated means or non - automated means;

- **The data subject's consent** is any serious and **freely** given, specific, informed and unambiguous expression of the data subject's will in the form of a statement or unambiguous act by which the data subject consents to the processing of their personal data;
- **The Processor** is anyone who processes personal data on behalf of the Controller;
- **Employee means a person performing dependent work according to the Labor Code**, in some provisions of this GDPR Handbook for the purpose of uniform terminology, it may also mean a person cooperating on the basis of a different than employment contract.

The Controller, as well as the Processor, prepares and keeps **records of processing activities** - information systems in accordance with Article 30 of the GDPR and the Section 37 of the Act.

Records of processing activities form annexes no. 2 and 3 of the GDPR Handbook.

## 2. PRINCIPLES OF PERSONAL DATA PROCESSING

The Controller processes data according to the Article 5 et seq. of the GDPR, the provisions of the Section 6 et seq. of the Act:

**a.** lawfully, fairly and in a transparent manner;
**b**. for a specifically specified, explicitly stated and legitimate purpose;
**c.** in accordance with the principle of data minimization and retention time minimization;
**d.** with an emphasis on the accuracy and continuous updating of data;
**e.** guaranteeing adequate personal data security, integrity and confidentiality;
**f.** respecting the principle of responsibility for the application of the basic principles of personal data processing.

**The principle of data minimization** means the processing of only relevant data, the non-processing of redundant personal data and **the principle of minimizing the retention period** means the registration of data only for the necessary, reasonable period resulting from the valid legislation, or GDPR Handbook EDYN. After this time, the data must be shredded or otherwise safely disposed of.

**Adequate security** of personal data aims to ensure, through appropriate technical and organizational measures, protection against unauthorized and unlawful processing, accidental loss, misuse, erasure or damage of personal data.

### 2.1. Lawfulness of Personal Data Processing

The Controller processes personal data in accordance with the Article 6 of the GDPR and pursuant to the Section 13 (1) of the Act and on the basis of some of the following legal bases:

a. The data subject has given consent to the processing of his or her personal data for at least one purpose. The Controller is obliged to be able to prove at any time the provision of such consent;

b. Processing of personal data is necessary for the performance of a contract to which the data subject is a party or for the implementation of a pre-contractual measure at the request of the data subject;
c. Processing of personal data is necessary according to a special legal regulation or an international treaty binding upon the Slovak Republic;
d. Processing of personal data is necessary in order to protect the life, health or property of the data subject or of another natural person;
e. Processing of personal data is necessary for the purpose of the legitimate interests of the Controller or a third party, except in cases where such interests or rights of the data subject requiring the protection of personal data are overridden by those interests, such as ensuring the protection of property by monitoring the premises with a video surveillance system, recording visits to the building and more.

This legal basis requires the Controller to perform a proportionality test before starting to process the personal data. The proportionality test presupposes the three cumulative conditions are met, namely:

i. Monitoring the legitimate interest of the Controller or a third party;
ii. The necessity to process personal data in order to pursue this legitimate interest;
iii. Compare whether the fundamental rights and interests of the data subject are not overriding this legitimate interest.

### 2.2. Processing of Special Categories of Personal Data

Processing of a special category of personal data **is carried out in the framework of a legitimate activity as a non-profit organization** providing services of general interest and this processing concerns only their members or those natural persons who are in regular contact with them due to their objectives; personal data serve only for their internal needs and will not be provided to the recipient without the written or otherwise verifiable consent of the data subject. **For the processing of special categories of personal data, there is therefore an exception to the prohibition in accordance with the Section 16 (2) (d) of the Act and the Article 9 (2) (d) of the GDPR.**

The **Controller does not process other special categories of personal data**, such as data on health status, sexual orientation, criminal offenses, valid conviction of philosophical beliefs, genetic data.

### 2.3. EDYN Policies and Procedures within Personal Data Protection

EDYN stipulates the following rules of personal data protection in accordance with Article 24 of the GDPR and the Section 31 (2) of the Act:

a. Personal data is processed on the basis of the GDPR as well as the Act, in accordance with the adopted GDPR Handbook, on the basis of the specified legal basis and for a specific purpose;
b. The protection of personal data is one of the fundamental human rights and freedoms;



European Democracy Youth Network
+421 903 932 358 info@edyn.eu www.edyn.eu

c. Personal data are processed explicitly by authorized persons who are informed of the obligations associated with the personal data protection;
d. The persons authorized to process personal data are informed of the technical, personnel and security measures through which the protection of personal data is implemented;
e. Technical and security measures are taken to prevent the misuse, theft or loss of personal data.

### 2.4. EDYN recommendations on how to ensure the personal data protection

a. Access to the computer must be secured with access codes and password, while it is not allowed to create general passwords and access codes, or these to be communicated among the employees;
b. Personal data and characteristics of colleagues, job seekers, EDYN members, candidates for membership must not be provided during personal calls;
c. The printing of documents must be ensured in such a way that the contents of the document are not known to another person, the printed documents should be removed from the printer without undue delay and stored in a safe place;
d. Documents containing personal data must be shredded after the retention period or in case of their redundancy or error are to be handed over for disposal;
e. In the event of an employee leaving the workplace, whether for a meeting, during a lunch break or after working hours, documents containing personal data should be locked in a lockable cabinet and the individual offices should also be locked;
f. In the event of outgoing or reassigned employees, all access rights will be immediately revoked, and access to information systems containing personal data will be prevented.

## 3. OBLIGATIONS OF THE CONTROLLER

Among the most important obligations of the Controller, which are related to the protection of personal data, are the so-called information obligation and obligation to maintain the confidentiality of personal data.

### 3.1. Information Obligation

The information obligation of the Controller arises from the Section 19 et seq. of the Act and Article 13 of the GDPR and consists in the fact that the Controller provides the following information to the data subject during the personal data processing:

a. Name, legal form, Trade ID number, registered seat and contact details of the Controller;
b. Purposes of processing and legal basis of the processing (contract, legislation, legitimate interest or consent of the data subject);
c. Legitimate interests in such processing of personal data based on them - e.g. video surveillance system, entrances to buildings;
d. Categories of recipients (i.e. any external body other than public authorities, e.g. processor, recipient, third party);
e. Transfer to the third countries;

f. The period for which the personal data will be stored;
g. Further information on rights according to the Section 21 to the Section 27 of the Act, or Article 15 to 21 of the GDPR;
h. Information whether the provision of personal data is a legal or contractual requirement or a requirement necessary for the conclusion of the contract, whether the data subject is obliged to provide personal data, as well as the possible consequences of not providing the data.

Pursuant to Section 29 of the Act, the Controller shall provide the data subject with information and notifications concerning the processing of their personal data in a concise, transparent, comprehensible and easily accessible form, formulated clearly and simply, in principle free of charge, in paper or electronic form within one month. If it is a repeated request, manifestly unfounded or disproportionate, the Controller may charge a second reply.

### 3.2. Duty of Secrecy

The Controller's duty of secrecy about the personal data it processes follows from the Section 70 of the Act and Article 90 of the GDPR. The duty of secrecy continues even after the processing of personal data has ended. The Controller also obliges natural persons who come into contact with personal data with the Controller to remain confidential, not only during the duration, but also after the termination of the employment relationship or the termination of the contractual relationship. Employees show understanding and acceptance of the duty of secrecy by signing the attendance list from the training, or retraining on the Act and GDPR, by signing an employment contract or a contract on the basis of which a contractual relationship is concluded with the Controller, or by an online "click" or other confirmation, if the information was provided via electronic communication.

## 4. PROCESSOR

Processor is a natural or legal person or other entity that processes personal data on behalf of the Controller. According to Article 28 of the GDPR, the Controller is to use processors who provide sufficient guarantees of the adoption of appropriate technical, organizational measures, protection of the rights of the data subjects and compliance with the requirements of the GDPR. That is, the Controller will select a processor after a reasonable verification.

**The processing of personal data by the Processor is governed by:**

a. A special processing agreement or
b. Processor’s clause within the main contract

### 4.1. EDYN’s Processors

The Controller has a contract concluded with an accounting office: Ing. Monika Husenicová, IČO: 31743871, sídlo: Zámocká 7074/30, 811 01 Bratislava – Staré Mesto, which is autonomous, despite that has EDYN concluded a contract on personal data processing.

The Controller has concluded a Mandate Contract with: PRIKOPALEGAL s.r.o., ID: 56647417, with her registered seat at: Medzilaborecká 23, 821 01 Bratislava, executive director: JUDr. Michal Príkopa, attorney at law, who provides legal services for EDYN. Due to the fact that, in accordance with the law and the Advocacy Act, the lawyer is bound by secrecy about all facts (including personal data) of which the lawyer has learned in the exercise of her rights and obligations, EDYN does not have a separate processing agreement with her, but the obligation of secrecy is stated beyond the scope of the law within the Mandate Contract.

In carrying out its activities, EDYN sometimes finds itself in a situation where it does not have time to carry out all contractual activities through its internal employees. Regarding the performance of activities related to the processing of personal data, e.g. processing of technical documentation which also contains personal data, EDYN selects such natural, legal or other persons with reasonable seriousness and care, and the processing of personal data by these processors is governed by a specific contract, a Processor's clause in the main contract or secrecy provisions.

### 4.2. EDYN as a Processor

EDYN, within its scope, does not process any personal data for another controller, i.e. it does not have the status of a processor.

## 5. RIGHTS OF THE DATA SUBJECT

Articles 12 to 22 of the GDPR and Sections 21 to 30 and 38 of the Act define the rights of the data subjects. Data subjects have the following rights:

a. **Right of access to data.** The data subject is entitled to obtain confirmation from the Controller as to whether personal data concerning him or her are being processed. If so, the data subject has the right to access this data and information pursuant to Section 21 of the Act and Article 15 of the GDPR (comparable to the data provided when obtaining personal data). In this context, the data subject has:
   i. ***Passive right*** - the ability to find information on the web and/or in an internal document, etc.
   ii. ***Active right*** - request specific information. The Controller proceeds according to point 3.1: Information obligation of the Controller.

b. **Right of rectification and completion.** The data subject is entitled to have the Controller correct their incorrect personal data without undue delay or to complete them if incomplete.

c. **The right to erasure** (the right "**to be forgotten**") if certain reasons are met, e.g.: personal data are not necessary for the purposes for which they were obtained; the data subject has withdrawn their consent and there is no other legal basis for the processing; the data subject objects to the processing on grounds of legitimate interest, i.e. on the basis of Article 6 (1) (f) of the GDPR and in the situation the legitimate interest of the Controller does not prevail;

personal data were processed illegally; they must be deleted in order to comply with the legal obligation.

d. **The right to restriction of processing** applies if the data subject has challenged the accuracy of the data or the processing is illegal, but the data subject objects to the deletion and only requests their use to be restricted, unless the Controller no longer needs personal data but needs the data subject in connection with his or her legal claims. Processing is also limited until it is verified that the legitimate interests of the Controller are overridden by the legitimate reasons of the data subject.

e. **The right to data portability** between the Controller and another controller. The data subject is entitled to obtain personal data from the Controller in a structured, commonly used, machine-readable format and to transmit them to another controller without the original controller preventing him/her if:
i. processing is based on consent or contract;
ii. processing is carried out by automated means.

f. **The right to object** to processing on the basis of Article 6 (1) (f) of the GDPR (legitimate interest).

g. **The right to withdraw consent** if personal data are processed on the basis of Article 6 (1) (a) of the GDPR.

h. **Right to lodge a complaint / request to initiate proceedings** with the supervisory authority.

i. **Right to compensation**: any person who has suffered property or non-property damage as a result of a breach of the Act and/or the GDPR has the right to compensation from the Controller or the Processor.

## 6. PROCESSING ACTIVITY

### 6.1. Records of the Processing Activity

The Controller maintains and continuously updates the records of processing activities in the format recommended by the Office for Personal Data Protection, which according to Article 30 of the GDPR and the Section 37 of the Act contains:

a. Name, Trade ID and contact details of the Controller
b. Processing purposes
c. Legal basis of the processing
d. Categories of data subjects and categories of personal data
e. Categories of recipients to whom the personal data are provided
f. Transfer to the third countries
g. Time limit for erasure
h. Technical and organizational security measures



European Democracy Youth Network
+421 903 932 358 info@edyn.eu www.edyn.eu

EDYN's Processors maintain records of categories of processing activities with the following information:

a. Name, Trade ID and contact details of the Processor
b. Categories of personal data processing
c. Transfer to a third country or international organization and adequate transfer guarantees
d. Technical and organizational security measures

The Controller may register the following **information systems/processing activities** (their detailed records form Annex No. 2 to this organization standard):

1. Wages and human resources information system
2. Attendance information system
3. Accounting information system and accounting documents
4. G-suite information system (Google workspace)
5. Electronic mail
6. EDYN website
7. Information system of registration of business partners
8. Financial reporting information system - cash flow

Most of them may contain personal data in an electronic form, some in paper (e.g. personal questionnaires or copies of children's birth certificates) and some are combined.

### 6.2. Overview of the Personal Data

The Controller processes personal data of:

a. Job seekers,
b. Employees and family members of employees,
c. Members of the statutory body, members of the Board of Directors
d. Business partners, suppliers and their employees
e. EDYN members and those interested in EDYN membership
f. Visits and website visitors

In the case of **job seekers** and subsequently employees, the Controller processes the following personal data:

1. **Job application** - basic personal data: first name, last name, date of birth, permanent residence address, delivery address (if different), gender, contact details: e-mail, telephone number, data resulting from the motivation letter, curriculum vitae containing previous experience and education
2. **Employment contract** - basic personal data, contact details as well as data necessary for the employee to register with the relevant authorities (social, health insurance, tax office)



European Democracy Youth Network
+421 903 932 358 info@edyn.eu www.edyn.eu

3. **Wage agenda** - working hours (arrival and departure to work), vacation, overtime, salary, account number, attendance, business trips (in the case of business trips, as well as data on travel documents or identity cards (personal ID), evaluation
4. **Category of sensitive data**: political party affiliation, being part of a minority, information on personal professional development, information obtained on the basis of surveys and questionnaires

In relation to the employee's family members, the Controller processes the information necessary, for example: in the case of a tax credit for a child.

The Controller processes **personal data on members of the statutory body as well as members of the Board of Trustees and other bodies** to the extent necessary in accordance with the **Act no. 346/2018 Coll.** on the Register of Non-Governmental Non-Profit Organizations and on amending and supplementing certain acts, as well as in accordance with the Act no. 213/1997 Coll. on non-profit organizations providing services of general interest.

**Data on suppliers and business partners** appear mainly in accounting documents, e-mail, business cards, signed contracts and related documents. These are the data necessary for the conclusion of the contractual relationship, in particular: trade name, registered seat, Trade ID, VAT number, registration in the relevant register, bank account, IBAN, first name and last name of the person authorized to act on behalf of the business partner or supplier and are processed for the purpose of concluding the contractual relationship. In some cases, EDYN may also process personal data of employees of business partners, namely: title, first name, last name, address, date of birth, job position, ID card or other photo card to verify identity or job classification.

In the case of **EDYN members, persons interested in EDYN membership, EDYN** processes basic personal data: first name, last name, date of birth, address of permanent residence (delivery address if different), gender, job classification (information about job position and employer), information on personal professional development, information obtained from surveys and questionnaires on satisfaction with EDYN activities and information on activities organized by them as well as on the use of grants, scholarships and donations or mediated by EDYN. This data is processed primarily for the proper functioning of EDYN as a non-profit organization based on the provision of services of general interest.

EDYN may also process personal data about individual EDYN members, statutory bodies as well as employees in the form of photographs or audiovisual recordings. EDYN processes these primarily for the purpose of its promotion, advertising, marketing and proper acquaintance of candidates and job seekers with the personnel structure of EDYN as a non-profit organization and **with the provable consent of the data subjects who can withdraw them at any time.**

### 6.3. Proportionality test

To protect its property, the Controller has a written Agreement for the Lease of Non-Residential Premises, which guarantees a continuous security service and the use of a video surveillance

system, which interferes with the fundamental rights and freedoms of employees and other natural persons entering the Controller's premises or passing around the Controller's premises.

Nevertheless, the Controller also performed a proportionality test, on the basis of which it ascertained whether its legitimate interests exceeded the protection of the personal data of the data subjects.

Table No. 1: Proportionality test for the video surveillance system

| | **Legitimate interest** | **Risk** |
|---|---|---|
| **Controller** | Property protection<br>Overview of the movement of persons | Costs |
| **Data subject** | Protection of life and health,<br>Property protection (e.g. when a theft is recorder on camera) | Information on the movement of persons<br>Keeping a record of the face and figure |

There is an outdoor video surveillance system in the EDYN headquarters building. The cameras are marked with the appropriate pictogram before entering the place where the videos take place.

The Controller may record the entrance to the building in order to control the attendance of employees at work, permission to enter the premises, through the attendance system or the so-called "Pagers".

Table No. 2: Proportionality test for possible control of the entrance to the building

| | **Legitimate interest** | **Risk** |
|---|---|---|
| **Controller** | Property protection;<br>Overview of the movement of persons;<br>Employee attendance control | Costs |
| **Data subject** | Property protection,<br>Implementation of employees' right | Employees movement information; Consequences drawn by the employer in case of non-compliance with work discipline |

## 7. SPECIFICATION OF TECHNICAL, ORGANIZATIONAL AND PERSONNEL MEASURES TO ENSURE THE PROTECTION OF PERSONAL DATA

### 7.1. Technical measures

The technical measures are used for the creation, processing, storage, protection and archiving of personal data and must provide at least the following functions:

i. User identification and authentication on the technical device;
ii. Optional access control to objects (file, directory, peripheral device, services, etc.) based on the distinction and management of user access rights;
iii. Continuous keeping of a control record of technical means about its activities with the possibility of monitoring, re-examination of the technical means, as well as determining the responsibility of a particular user for the activities performed by him/her;
iv. Removal (disposal) of personal data that are not necessary for further processing, archiving or manipulation of memory elements after the end of work on the technical means so that it is impossible to find out their content.

**Technical measures consist of information, security, physical and object security.**

**The basic technical measures may include:**

a. **Building security system - security service and video surveillance system**
b. **Object designed to store documents containing personal data -** lockers
c. **Locking system** - patent lock, access control via assigned key
d. **Prevention of entry by unauthorized persons** - regime of visits, visits are accompanied by an authorized person
e. **Location of information systems in a protected area** - prevention of physical access by unauthorized persons and adverse environmental influences
f. **Physical protection** - during working hours by the Controller's employees, as well as IT support
g. **Regular backup of electrical documents**
h. **Hard disk passwording of laptops/computers and smartphones**
i. **Granting access to Google drive only to specific contractors in the form of sending access codes, usernames and passwords**
j. **Keeping systems up to date (software/firmware)**
k. **Electronic resource protection firewall -** Windows defender

## 7.2. Description of the technical means concerned

The Controller may process personal data in an automated and non-automated manner, for example:

Table no. 3: Examples of personal data processing methods

| Serial no. | Information System | Automated (semi-automated) information system - technical means | Non-automated information subsystem |
|---|---|---|---|
| 1. | IS wages and Human Resources | Software, data, files (Microsoft, software) | Personal cards, employment contracts, agreements on the |

| | | | |
|---|---|---|---|
| | | | performance of work, staff ledger, payroll documents, CVs, education documents, certificates of training, certificates of professional competence, |
| **2.** | IS Attendance | Attendance system | |
| **3.** | G - Suite | Software Hosting Google / Gmail | |
| **4.** | IS accounting documents | Software resources | Contracts, orders, acceptance documents, issued and received invoices |
| **5.** | IS records of business partners | Software resources | Contracts, orders and other documents |
| **6.** | IS Whistleblowing activity | Software resources | Evidence of suggestions |
| **7.** | Electronic mail | Domain: @edyn.eu | - |
| **8.** | Website edyn.eu | Software resources web hosting - Websupport | - |

### 7.3. Organizational measures

Organizational measures are used primarily to establish internal procedures and personnel management that will ensure the protection of personal data, including the appointment, dismissal and training of authorized persons, privileged authorized persons and responsible persons, investigation of security incidents, control activities and other measures to ensure personal data protection.

By issuing the GDPR Handbook, the Controller ensures the creation of an internal document describing the procedure and management of personal data protection. Every EDYN employee, member and other cooperating person is acquainted with the GDPR Handbook, as evidenced by a **handwritten signature** or by "**clicking**" consent in the emails if the GDPR Handbook was sent by electronic means.

The persons authorized by the Controller are obliged to become acquainted with the content of the GDPR Handbook and apply it in practice, i.e. follow the principles, policies and guidelines for the processing of personal data, whether they process information in electronic or paper form, in an automated or non-automated manner.

Authorized employees will get acquainted with Annex no. 2 of this standard entitled: *"Records of processing activities"*, which describes the purpose, legal basis, processing time, categories of data subjects, recipients, personal data and possible transfer of personal data to third countries. Upon termination of employment or similar, EDYN will ensure that all employees, access rights, documents and media containing personal data are duly demonstrably transferred by authorized employees and will inform the person of the consequences of a breach of legal or contractual confidentiality upon signature.

The Controller signs with all Processors a contract or a Processor's clause within the main contract governing further relations between the Controller and the Processor processors according to Article 28. (3) of the GDPR.

### 7.4. Personal security

Employees who will become acquainted with personal data must **be demonstrably** instructed on the protection of personal data in accordance with the GDPR n and the Act before processing personal data.

#### 7.4.1. Authorized persons:

a. they must have the appropriate education;
b. they have not caused a security incident in the processing of personal data in the last 2 years (affidavit);
c. they must have completed GDPR training.

**The authorized persons in the conditions of EDYN are**: persons instructed in accordance with the Act and the GDPR and bound by secrecy by expressing their demonstrable consent and access to EDYN's internal documents. These persons have the right to process personal data in full according to the assigned access rights, the instruction and acquaintance with the internal documents of these persons must be **demonstrable.**

When selecting employees, privileged authorized persons who will actively process personal data in the company's information system, they must be assessed, especially from the **point of view of personal and qualification preconditions**, before entrusting the processing of personal data or when hiring. **The Controller shall demonstrably acquaint** each employee, who is accepted into the employment relationship within which he/she comes or may come into contact with personal data, **with the security rules and measures, rights and obligations arising from the provisions of the Act.**

All authorized persons must be informed of the manner and internal rules concerning the reporting of various types of incidents in connection with the information system. Information system users must be instructed to report any events or indications of events that could affect the security of the system without delay.

Authorized persons must be especially careful when providing personal data, they must handle increased attention with paper and electronic documents containing personal data and avoid

providing personal data via email or telephone without encryption or passwording. In case of a request to provide **personal data, e. g. to credit, foreclosure companies, hotels an/or insurance companies, they shall request a written request for information.**

**Scope of responsibility of the authorized persons:**

a. Duty of Secrecy
b. Responsibility for the safety of personal data
c. Backup

### 7.4.2. Protection Officer

EDYN have an external authorized Protection Officer: **JUDr. Michal Príkopa, attorney at law** (hereinafter referred to as the "**DPO**"), contact email: **dpo@edyn.eu**.

Despite the fact that EDYN does not process special categories of personal data on a large scale, which is another reason why it does not have a designated Protection Officer under the Act and the GDPR, and the processing of special categories for EDYN is subject to the exception provided by the Act and the Regulation.

The Director entrusted the preparation of documentation in accordance with the Act and the GDPR, informing authorized employees to the contracted business partner, PRIKOPALEGAL s.r.o., ID: 56647417 with her registered seat at: Medzilaborecká 23, 821 01 Bratislava, executive director: JUDr. Michal Príkopa, attorney at law.

## 8. TRANSFER OF PERSONAL DATA OUTSIDE THE EU AND THE EEC (European Economic Area) ZONE

As a result, EDYN may be required to provide information about its activities, members, or employees and business partners. The information provided to these entities also contains personal data, and in accordance with the principle of minimization, this is the necessary scope of personal data: **first name, last name, date of birth, residence address, job title, political party affiliation and being part of an ethnic, gender or religious minority.** EDYN may have concluded standard contractual clauses with these entities recommended by the European Commission pursuant to Article 46 of the GDPR and their relationship represents a Controller – Controller relationship, as the processing of personal data is necessary for the proper functioning of the contractual relationship and for the fulfillment of obligations by EDYN.

The cross-border transfer of personal data to the third countries that does not guarantee an adequate level of personal data protection in the use of services of various recipients of personal data occurs mainly in the category: i) social network operators (Facebook, Instagram, LinkedIn, etc.), ii) security services (Windows defender), iii) web analytics and implementation in EDYN websites (cookies policy) iv) software services (Microsoft and Google) v) fulfillments of EDYN´s contractual obligation. In most of these cases, cross-border transfers of personal data to the USA take place on the basis of an exception for special situations within the meaning of Article 49 of the GDPR.

In general, we will always use standard contractual clauses approved by the Commission (EU) or require other reasonable safeguards to be required when making a cross-border transfer of personal data to the USA.

In the table below you can find a link to adequate or appropriate guarantees and means to exercise your rights under the GDPR:

| Supplier | Privacy Policy | Adequate guarantees within the meaning of Article 46 of the GDPR |
|---|---|---|
| Google | https://policies.google.com/privacy?hl=en-US | https://privacy.google.com/businesses/controllerterms/mccs/ |
| Facebook | https://www.facebook.com/policy.php | https://www.facebook.com/help/566994660333381?ref=dp |
| Instagram | https://help.instagram.com/519522125107875?helpref=page_content | https://www.facebook.com/help/566994660333381?ref=dp |
| Twitter | https://twitter.com/en/privacy | https://twitter.com/en/privacy |
| LinkedIn | https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy | https://www.linkedin.com/help/linkedin/answer/62533 |
| TikTok | https://www.tiktok.com/legal/privacy-policy-eea?lang=en | https://www.tiktok.com/legal/law-enforcement?lang=en |

## 9. SECURITY INCIDENT

The Controller performs and will do everything in order to avoid endangering or violating personal data during their processing. However, in the event that the personal data of the data subject is lost, destroyed or misused, the Controller will proceed in accordance with Article 33 and Article 34 of the GDPR as well as in accordance with Sections 40 and 41 of the Act.

A security incident could be, for example:

a. unauthorized access to personal data through a device for their processing, storage, reproduction, transmission;
b. unauthorized modification of personal data in facilities for their processing storage, reproduction, transmission;
c. loss of equipment containing personal data;
d. theft of equipment containing personal data;
e. destruction, unauthorized deletion of personal data;
f. unavailability (even temporary) due to loss of personal data;
g. unauthorized acquaintance with personal data, unauthorized disclosure of personal data;
h. provision of personal data to an unauthorized person (intentionally, unintentionally);
i. loss of control over personal data.

### 9.1. Notification of a personal data breach to the Office

The Controller is obliged to notify the Office of the personal data breach **no later than 72 hours** of after having become aware of it. The Controller does not have this obligation if the breach of personal data protection is not likely to lead to the risk of a natural person. The Controller must justify the delay of the 72-hour period. The form for reporting violations can be found on the website of the Office for the Protection of Personal Rights https://dataprotection.gov.sk/uoou/dp/dp-breach

In the case of personal data processing by the Processor, the Processor is obliged to notify the Controller of the personal data breach without undue delay after having become aware of it.

The notification to the Office is a mitigating circumstance in the case of an investigation of a security incident and in deciding on the amount of the imposed (possible) fine. According to the Section 40 (4) of the Act, the notification must contain:

a. a description of the nature of the personal data breach, including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;
b. contact details of the protection person or other contact point where more information can be obtained;
c. a description of the likely consequences of the personal data breach;
d. a description of the measures taken or proposed by the Controller to address the personal data breach, including measures to mitigate its potential adverse consequences, if necessary.

### 9.2. Notification of the personal data breach to the data subject

If a personal data breach is likely to result **in a high risk to the rights of a natural person**, the Controller is obliged to notify the data subject of such a breach of personal data protection. The notification shall contain a clear and simple description of the nature of the personal data breach and the information and measures referred to in points (b) to (d) in the Article 8.1 of the GDPR Handbook.

According to the Section 41 (3) of the Act, the communication shall not be required if:

a. the Controller has taken appropriate technical and organizational security measures and applied them to the personal data affected by the personal data breach, in particular encryption or other measures which make **the personal data unintelligible** to persons who are not authorized to have access to them;
b. the Controller has taken subsequent measures to avoid **a high risk** of infringing the rights of the data subject;
c. this would involve a **disproportionate effort**; the Controller is obliged to inform the public or take other measures to ensure that the data subject is informed in an equally effective manner.

**The Controller is obliged to document each case of a security incident, including the facts related to the breach of personal data protection, its consequences and the remedial measures taken.**

**Preparing for resolving a security incident by the Office:**

a. Taking into account the wording of Article 5 (2) of the GDPR, submit documentation that the person who was supposed to have caused the personal data breach has been informed of EDYN's instructions;
b. describe what specific safeguards were in place before the incident to prevent it;
c. according to the answer to point b. state the date and manner of implementation of these measures in practice, how the said employee was acquainted with these measures - submit documentation;
d. describe what specific measures were taken after the incident to prevent repeated breaches of personal data protection - date and method of implementation;
e. describe the specific measures put in place during the establishment and termination of employment relationships related to the protection of personal data, as well as the procedures for taking over and transferring personal data processed by the former employee - submit documentation.

**Annexes**:

1. The data subject's consent to the personal data processing
2. EDYN Processing Activities



European Democracy Youth Network
+421 903 932 358 info@edyn.eu www.edyn.eu