

## **Directive 250103-S-03**

### **Processing and Protection of Personal Data**

#### **I. GENERAL PROVISIONS**

Regulation (EU) 2016/679 of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, hereinafter referred to as "GDPR") establishes uniform principles and rules for the protection of personal data across the EU. This directive is an internal standard of NEWTON University, a.s., which regulates procedures for the processing and protection of personal data within the organization.

#### **II. SCOPE OF VALIDITY**

Vysoká škola NEWTON, a.s. is the data controller within the meaning of the GDPR. This directive is binding for all employees and individuals in similar employment relationships (hereinafter collectively referred to as "users"). Each user is fully responsible for fulfilling the obligations imposed by legislation and internal documents in the area of personal data protection concerning the scope of personal data processed. The company Vysoká škola NEWTON, a.s. (hereinafter referred to as "Controller") is responsible for implementing measures and monitoring compliance with obligations.

#### **III. BASIC TERMS**

1. **Data Subject:** An identified or identifiable natural person.
2. **DPO, Data Protection Officer:** The person responsible for data protection (Data Protection Officer).
3. **Personal Data:** Any information relating to an identified or identifiable natural person.
4. **Record:** A record of individual personal data in relation to the purpose of processing.
5. **Processing:** Any operation or set of operations performed on personal data or sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

#### **IV. PROCESSING OF PERSONAL DATA**

1. Purpose and Scope of Personal Data Processing.  
The Controller processes personal data of natural persons to the extent necessary for fulfilling legal obligations, contractual relationships, and legitimate interests, particularly within the scope of human resources management.
2. Personal Data of Employees and Collaborators.

#### **Processed Data:**

- a) **Identification Data:** First name, surname, title, maiden name, date of birth, personal identification number, permanent address, contact address.
- b) **Employment Data:** Job position, classification, employment contract, agreements, salary, start/end date, attendance information, entitlement to benefits (e.g., home office), internal classification.
- c) **Data for Social and Health Insurance, Tax Identification, Payroll Calculation, and Contributions:** Data necessary for fulfilling obligations in these areas.
- d) **Contact Information:** Phone number, email address—particularly email addresses in the format created from first and last names (e.g., login@newton.university or login@sting), used for access to the NU information system (IS NU).
- e) **Processing of Employees' Private Phone Numbers:** Department heads and managers will have access to employees' private phone numbers. These numbers will be used exclusively for urgent work-related matters and in accordance with the GDPR. Employees will be informed that their private phone numbers may be processed for this purpose and have the right to the protection of their personal data. All users are obliged to ensure that unauthorized access to this data does not occur and that personal data protection rules are adhered to.

**Purpose of Processing:** Managing employment relationships, payroll administration, communication, fulfilling legal obligations towards the state and other institutions (e.g., Employment Office, Czech Social Security Administration, health insurance companies, tax authorities).

**Data Retention and Archiving:** Data is retained for the duration of the employment relationship and subsequently archived for at least 10 years in accordance with applicable legal regulations and the internal filing and disposal plan.

**Access to Data:** Access is granted only to authorized personnel in the human resources department, accounting department, and IT system administration, to the extent necessary for performing their duties.

### 3. Rules for data processing and security

All personal data is processed in accordance with applicable legal regulations, especially **GDPR (EU) 2016/679** and Act No. 110/2019 Coll., on the processing of personal data.

- Access to data is restricted to individuals authorized by the Controller.
- Data is processed electronically using secure systems.
- Archiving, disposal, and access rules are defined in the Controller's internal regulations.

4. In the event that a user creates a new record of personal data, the user is obliged to report this record, its purpose, and scope to the DPO.

**V. PROTECTION OF PERSONAL DATA**

1. Only authorized individuals have access to personal data.
2. Personal data must be secured against unauthorized or accidental access, alteration, destruction, loss, unauthorized transfers, or other unauthorized processing and misuse.
3. Security measures include storing written and electronic media containing personal data in locked cabinets, locking offices and other premises, and adhering to information security rules.
4. Personal data stored in internal information systems, data storage, or personal computers must be appropriately secured against unauthorized access, alteration, destruction, loss, unauthorized transfers, other unauthorized processing, and misuse.
5. Employees and other users are required to ensure the protection of personal data, especially against unauthorized access or viewing by others.
6. Upon finishing work on a computer, the user is obliged to lock the computer, log out, or turn off the computer.
7. No documents containing personal data should be left on the desktop (clean desk policy).
8. Documents containing personal data intended for disposal will be immediately deleted, shredded if in paper form, or handed over to the responsible employee for shredding.
9. Users are bound by confidentiality regarding processed personal data, even after the termination of the employment relationship or contract.

**VI. HANDLING REQUESTS AND INQUIRIES**

1. If a data subject contacts a user with a request to exercise rights related to the processing of personal data (e.g., a request for erasure or access to personal data), or if an employee of the Supervisory Authority or an auditor makes such a request, the employee shall always refer them to the DPO or to the Controller's website for submitting such requests. Contact details are always available in their current version on the Controller's website.
2. The user shall assist, if possible, in fulfilling the obligations of the DPO in handling data subjects' rights requests.

**VII. REPORTING PERSONAL DATA BREACHES**

1. Any suspicion of a breach of personal data security or other unauthorized access to personal data, or any suspected breach of GDPR or related data protection regulations, must be reported by the user without delay and no later than 24 hours after discovery to the DPO. The user must provide full cooperation and any information the DPO may need to fulfill legal obligations.
2. The reporting procedure is described on the Controller's website, including contact details, processes, and forms.

3. If the user becomes aware of or suspects a breach of their own personal data protection, they may inform the DPO or directly file an objection with the DPO. The DPO is bound by confidentiality and is required to handle such reports or objections.

#### **VIII. DOCUMENTATION AND TRAINING**

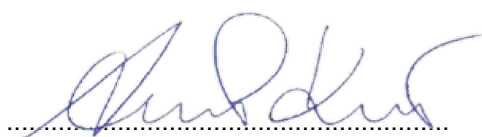
1. All documentation related to the processing and protection of personal data is always available from the DPO.
2. Employees are trained in the field of personal data protection upon entering into an employment relationship, as well as in the event of a change in job position or job description, if there is a significant change in duties and responsibilities regarding personal data protection at the Controller.

#### **IX. FINAL PROVISIONS**

With the entry into force of this directive, all previously issued directives or recommendations concerning the processing and protection of personal data at NEWTON University, a.s. shall be repealed.

This directive enters into force and becomes effective on June 1, 2025.

In Prague, on June 1, 2025.



**on behalf of Vysoká škola NEWTON, a.s.**

Anna Plechatá Krausová, DPhil.

Chair of the Board of Directors