

# HR Directive No. 1/2022: Processing and protection of personal data

## I. GENERAL PROVISIONS

The General Data Protection 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 (GDPR) brings uniformity of principles and rules in the protection of personal data across the EU. This directive is an internal standard of NEWTON University (Vysoká škola NEWTON, a.s., hereinafter referred to as NU), which governs the procedures for processing and protecting personal data within the organization.

## II. SCOPE OF VALIDITY

1. NEWTON University is a data controller within the meaning of the GDPR. This Directive is binding on all employees, collaborators in a similar employment relationship and students (hereinafter collectively referred to as "Users"). Each user is responsible for fulfilling the obligations imposed by legislation and internal documents in the area of personal data protection to the full extent of the personal data processed. The statutory body of NEWTON University (hereinafter referred to as the "Controller") is responsible for the implementation of the measures and the control of compliance with the obligations.

## III. BASIC CONCEPTS

<b>Data subject:</b>	An identified or identifiable natural person.
<b>DPO:</b>	Data Protection Officer. Contact details for the DPO are always available on the website at <a href="https://www.newton.university/en/privacy-policy">https://www.newton.university/en/privacy-policy</a> .
<b>Personal data:</b>	Any information about an identified or identifiable natural person.
<b>Records:</b>	Records of individual personal data in relation to the purpose of processing.
<b>Processing:</b>	Any operation/set of operations on personal data or sets of personal data which are carried out with or without the aid of automated processes, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or any other disclosure, alignment or combination, restriction, erasure or destruction.

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

1. The User processes personal data solely on the basis of instructions for the fulfilment of a lawful purpose or legitimate interest of the Controller, and does not transfer or disclose personal data to any other person or recipient. The User shall not use the personal data processed for their own use or for any purpose other than the intended purpose.
2. In case that employee creates a new record of personal data, that employee shall notify the DPO of that record, its purpose and scope.

#### **V. PROTECTION OF PERSONAL DATA**

1. Only authorised persons have access to personal data. Personal data must be secured against unauthorised or accidental access, alteration, destruction or loss, unauthorised transfer, other unauthorised processing and other misuse of personal data.
2. When users are not present at the workplace, security consists in particular in keeping written and electronic media containing personal data in locked cabinets, in locking offices and other places, and in observing information security rules.
3. Personal data stored in internal information systems, data storage devices or personal computers must be appropriately secured against unauthorised access, alteration, destruction, loss, unauthorised transfer, other unauthorised processing and other misuse of personal data.
4. In the performance of their duties, staff members shall ensure the protection of personal data, in particular against unauthorised disclosure or access by others, where possible.
5. The user shall lock the computer or log off or switch off the computer when they have finished working on it.
6. There must be no documents containing personal data on the monitor screen (blank screen policy).
7. No paper documents containing personal information shall be stored on desks or in accessible locations (clean desk policy).
8. Any documents containing personal data to be disposed will be deleted immediately, shredded if in paper form, or forwarded by the user to the responsible staff member for shredding.
9. The user shall maintain confidentiality of the personal data processed, even after the termination of the employment relationship or contract.

## **VI. HANDLING REQUESTS AND ENQUIRIES**

1. If the User is contacted by a natural person (data subject) with a request to exercise rights in the area of personal data processing (for example, a request for erasure of personal data or access to personal data), or by an employee of the Supervisory Authority or an auditor, the employee will always refer the user to the DPO or to the website of the Controller for information. Contact information is always kept up-to-date on the website [www.newton.university/en/privacy-policy](http://www.newton.university/en/privacy-policy).
2. The User assists, as far as possible, in fulfilling the DPO's obligations for dealing with requests to exercise the rights of the data subject.

## **VII. REPORTING OF DATA BREACHES**

1. The User shall report any suspected breach of personal data security or other unauthorised access to personal data or suspected breach of the GDPR or other data protection regulations to the DPO without delay and no later than 24 hours after discovery, and shall provide the DPO with all assistance and information that the DPO may require to comply with their legal obligations.
2. The procedure for reporting is described on the Controller's website, including contacts, procedures and forms.
3. If a User discovers or suspects a breach of their own personal data protection, they may inform the DPO or lodge an objection with the DPO directly. The DPO is bound by confidentiality and is obliged to address such reports or objections, if any.

## **VIII. DOCUMENTATION AND TRAINING**

1. All documentation on the processing and protection of personal data is always available from the DPO.
2. Employees shall be trained in the area of data protection upon joining the employment relationship, as well as upon any change of position or change of job title if the employee's duties and responsibilities in relation to data processing and protection issues in the Controller's organisation change significantly.
3. Students are made aware of the data protection policies and guidelines when they start their studies.

## IX. FINAL PROVISIONS

1. Upon the effective date of this policy, any previously issued guidelines or recommendations regarding the processing and protection of personal data at NEWTON University are superseded.
2. This directive shall become effective and in force on March 1, 2022.

In Prague, February 28, 2022

.....  
on behalf of NEWTON University  
(Vysoká škola NEWTON)  
Anna Plechatá Krausová, DPhil.  
Chairperson of the Board of Directors