

## Data Processing Agreement

Effective as of September 29, 2023 | [See a previous version of Data Processing Agreement](#) | [Compare changes](#)

According to the requirements of Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the Protection of natural persons with regard to the processing of personal data and on the free movement of such data, repealing Directive 95/46/EC (hereinafter referred to as the "GDPR"), Provider (hereinafter referred to as the "Processor") and You (hereinafter referred to as the "Controller") are entering into the data processing contractual relationship in order to define the terms and conditions for the processing of personal data, the manner of its protection, as well as to define other rights and obligations of both parties in the processing of personal data of data subjects on behalf of the Controller during the course of performing the subject matter of these Terms as the main contract.

1. **Personal Data Processing.** The services provided in compliance with these Terms include processing information relating to an identified or identifiable natural person listed in the [Privacy Policy](#) (hereinafter referred to as the "Personal Data").
2. **Authorization.** The Controller authorizes the Processor to process Personal Data, including the following instructions:
  - (i) Purpose of Processing shall mean the provision of services in compliance with these Terms. The Processor is only allowed to process Personal Data on behalf of the Controller regarding the provision of services requested by the Controller. All information collected for additional purposes is processed outside of Controller-Processor contractual relationship.
  - (ii) Processing Period shall mean the period from entering cooperation under these Terms to termination of services,
  - (iii) Scope and Categories of Personal Data. The Services are intended for the processing of general personal data only. However, the Controller is solely responsible for the personal data scope determination.
  - (iv) Data Subject shall mean a natural person as an authorized user of Controller's devices,
  - (v) Processing Activities shall mean every and all operation necessary for processing,
  - (vi) Documented Instructions shall mean instructions described in these Terms, its Annexes, Privacy Policy, and service documentation. The Controller shall be responsible for the legal admissibility of the processing of Personal Data by the Processor regarding the respectively applicable provisions of data protection law.
3. **Obligations of Processor.** The Processor shall be obliged to:

- (i) process Personal Data only on the grounds of Documented instructions and for the purpose defined in Terms, its Annexes, Privacy Policy, and service documentation,
- (ii) to instruct the persons authorized to process the Personal Data (hereinafter referred to as the "Authorized Persons") about their rights and duties according to the GDPR, on their liability in case of breach and ensure that Authorized Persons have committed themselves to confidentiality and follow the Documented instructions,
- (iii) implement and follow the measures described in the Terms, its Annexes, Privacy Policy, and service documentation,
- (iv) assist the Controller with responding to requests from Data Subjects related to their rights. The Processor shall not correct, delete or restrict the processing of Personal Data without the instruction from the Controller. All requests from Data Subject related to Personal Data processed on behalf of the Controller shall be forwarded to the Controller without delay.
- (v) assist the Controller with notification of personal data breach to the supervisory authority and Data Subject. The Processor shall notify the Controller of any breach of Personal Data processing or personal data security immediately after the discovery. The Processor shall cooperate to a reasonable extent in an investigation and remediation of such breach, and take reasonable measures to limit further negative implications.
- (vi) at the choice of the Controller to delete or return all the Personal Data to the Controller after the end of the Processing Period. The Controller undertakes to inform the Processor about its decision within ten (10) days upon the end of the Processing Period. This provision shall not affect the Processor's right to keep the Personal Data to the necessary extent for archiving purposes in the public interest, scientific research purposes, statistical purposes or for the purpose of establishment, exercise or defense of legal claims.
- (vii) keep an up-to-date register of all the categories of Processing Activities carried out on behalf of the Controller,
- (viii) make all information necessary to demonstrate compliance as part of the Terms, its Annexes, Privacy Policy, and service documentation available to the Controller. In case of the audit or control of the Personal Data processing from the Controller's side, the Controller shall be obliged to inform the Processor in writing at least thirty (30) days before the planned audit or control.

**4. Engaging Another Processor.** The Processor is entitled to engage another processor for carrying out specific processing activities, such as the provision of cloud storage and infrastructure for the service in compliance with the Terms, its Annexes, Privacy Policy, and service documentation. Currently, Microsoft provides cloud storage and infrastructure as part of Azure Cloud Service. In such a case, the Processor shall remain the only point of contact

and the party responsible for compliance. The Processor hereby undertakes to inform the Controller about any addition or replacement of another processor for purposes of possibility to object such change.

**5. Territory of Processing.** The Processor ensures that processing takes place in the European Economic Area or a country designated as safe by the decision of the European Commission based on the decision of the Controller. Standard Contractual Clauses shall apply in case of transfers and processing located outside of the European Economic Area or a country designated as safe by the decision of the European Commission upon the request of the Controller.

**6. Security.** The Processor is ISO 27001:2013 certified and uses the ISO 27001 framework to implement a layered defense security strategy when applying security controls on the layer of the network, operating systems, databases, applications, personnel, and operating processes. Compliance with the regulatory and contractual requirements is regularly assessed and reviewed similarly to other infrastructure and operations of the Processor, and necessary steps are taken to provide compliance on a continuous basis. The Processor has organized the data security using ISMS based on ISO 27001. The security documentation includes mainly policy documents for information security, physical security, security of equipment, incident management, handling of data leaks and security incidents, etc.

**7. Technical and Organizational Measures.** The Processor shall protect the Personal Data against casual and unlawful damage and destruction, casual loss, change, unauthorized access and disclosure. For this purpose, the Processor shall adopt adequate technical and organizational measures corresponding to the mode of processing and to the risk presented by processing for the rights of the Data Subjects in compliance with the requirements of the GDPR. A detailed description of the technical and organizational measures is stated in the [Security Policy](#).

**8. Processor's Contact Information.** All notifications, requests, demands and other communication concerning personal data protection shall be addressed to ESET, spol. s.r.o., attention of: Data Protection Officer, Einsteinova 24, 85101 Bratislava, Slovak Republic, email: [dpo@eset.sk](mailto:dpo@eset.sk).