telelink
BUSINESS SERVICES

General policy for personal data processing of Telelink business Services

Table of Contents

1. Introduction

TELELINK BUSINESS SERVICES EAD (TBS or the Company), UIC: 130545438, with registered office and address of management: Sofia 1766, Vitosha region, v.z. Malinova Dolina, 6 Panorama Sofia Str., Richhill Business Center, Block B, represented by Ivan Zhitiyanov - Executive Director, is an administrator or processor of personal data in relation to personal data processed in the implementation of activities falling within the scope of this Policy.

This policy (" the Policy") aims to define the rules that TBS employees follow with regard to personal data and documents that contain personal data in the performance of their duties to Telelink Business Services EAD. The Company ").

2. Scope

The activities covered by this Policy are:

- The processing of personal data and documents containing personal data in the course of the usual commercial activity of TBS;
- The processing of personal data and documents containing personal data by TBS employees in the performance of their duties.

The policy follows the principles and requirements regarding the processing of personal data under Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of individuals with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46 / EC ("General Data Protection Regulation", "DPO", "Regulation"), the Personal Data Protection Act (PDPA), the guidelines of the European Data Protection Board (EDPS) , The Commission for Personal Data Protection (CPDP) and good practices in the field of personal data protection.

3. Basic concepts

TBS employees are familiar with the basic concepts introduced by the Regulation and the LPPD, namely:

"Personal data" means any information relating to an identified or identifiable natural person ('data subject').

"Special categories of personal data" means personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.

"Data concerning health" means personal data related to the physical or mental health of a natural person, including the provision of health care services, which reveal information about his or her health status.

"Data subject" means an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number,

location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Controller" means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

"Processor" means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

"Processing" means any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

"Third party" means a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

"Recipient" means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not. However, public authorities which may receive personal data in the framework of a particular inquiry in accordance with Union or Member State law shall not be regarded as recipients; the processing of those data by those public authorities shall be in compliance with the applicable data protection rules according to the purposes of the processing.

"Restriction of processing" means the marking of stored personal data with the aim of limiting their processing in the future.

"Profiling" means any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

"Pseudonymisation" means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

"Register of personal data" means a register of processing activities within the meaning of Art. 30 of the Regulation.

"Consent" of the data subject means 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 personal data relating to him or her.

"Personal data breach" means 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.

"Supervisory authority" means an independent public authority which is established by a Member State.

"Applicable law" means the law of the European Union and of the Republic of Bulgaria, which is relevant to the protection of personal data.

4. General principles when working with personal data

While performing their duties, TBS employees process and protect personal data in compliance with the following principles:

- Personal data are processed lawfully and in good faith and in a transparent manner for the data subjects;
- Personal data are collected for specific and lawful purposes and are not further processed in a way incompatible with those purposes;
- The personal data that are collected and processed are relevant, related to and not exceeding the purposes for which they are processed;
- Personal data is accurate and updated as necessary;
- Personal data are deleted or corrected when they are found to be inaccurate or disproportionate to the purposes for which they are processed;
- Personal data are maintained in a form that allows the identification of relevant individuals for a period not longer than necessary for the purposes for which these data are processed;
- Personal data is processed in a way that ensures an appropriate level of security, including protection against unauthorized or unlawful processing and against accidental loss, destruction or damage.

5. Confidentiality and security

TBS employees are obliged in writing to observe complete confidentiality in their work with personal data in the process of performing their work duties.

Each TBS employee has access only to those personal data and documents containing personal data that are related to the performance of his / her duties and responsibilities and the specific projects and tasks assigned to him / her (the principle of "need to know").

The personal data to which TBS employees have access in the performance of their duties and responsibilities are used solely for the purposes of performing their work duties. Employees

have no right to provide, disseminate or otherwise disclose personal data to third parties (individuals and legal entities), except in cases where:

- This is necessary for the fulfillment of the labor law obligations of the individuals whose data are provided.
- This is necessary for the normal course of business of the TBS or to protect the interests of the Company, provided that there is a valid basis for data disclosure.
- This is in implementation of an act of the judiciary (court, prosecutor's office, investigation) and the investigative bodies.
- This is in fulfillment of the legal obligations of TBS according to the provisions of the Bulgarian and European legislation.
- This is necessary for archiving purposes in the public interest, for scientific or historical research or for statistical purposes.
- This is by order or with the express consent of the person whose data is provided.

TBS employees are obliged to get acquainted with the internal policies and rules adopted by the Company in connection with the protection and security of personal data, as well as the procedures in case of breach of personal data security. The employees are obliged to apply the internal policies, rules and technical and organizational security measures approved by the Company when working with personal data.

In the event of a suspected breach of personal data security that could result in accidental or unlawful destruction, loss, alteration, unauthorized disclosure, or access to personal data transmitted, stored, or processed, staff shall immediately notify the Data Protection Officer and comply with the rules set out in the Personal Data Incident Management Procedure.

In case of questions and ambiguities regarding their scope and application, the employees turn to the Data Protection Officer for interpretations and make proposals for their change and / or supplementation.

6. Organisational measures

The employees are acquainted with and observe the technical and organizational measures regarding the security and protection of personal data, introduced by TBS and described in this section, during the processing and storage of personal data.

The organizational data protection measures introduced by TBS are the following:

- Improving the awareness of employees on the peculiarities of personal data processing in connection with the applicable regulations.
- Determining rules and deadlines for storage, archiving and destruction.
- Knowledge of internal policies and procedures for personal data protection.
- Knowledge of the policies and procedures introduced by TBS as an organization certified according to the following ISO standards:
    - ISO 9001: 2015 Quality management systems;
    - ISO / IEC 27001: 2013 Information security management systems;

- ISO / IEC 27701: 2019 Security methods. Addendum to ISO / IEC 27001 and ISO / IEC 27002 for information privacy management. Requirements and instructions;
- ISO / IEC 20000-1: 2018 Information technology. Service management. Requirements regarding the service management system;
- ISO 37001: 2016 Anti-bribery management systems. Requirements with instructions for use;
- ISO 14001: 2015 Environmental management systems. Requirements with instructions for application;
- ISO OHSAS 45001: 2018 Occupational health and safety management system.

Self-awareness when working with personal data

In their work with personal data and documents containing personal data, TBS employees are guided by the principles set out in this Policy.

Every newly appointed employee must go through onboarding meetings when entering a job at TBS. The introductory meetings of the new employees are led by the employees of the Talent team. During these meetings, new employees are introduced to the organization and its structure, the positioning of the employee in the structure, internal resources, internal organizational portals and spaces, policies, processes, and rules established in the TBS.

Upon entering the Company, the newly appointed employees are provided with all rules and policies for processing and protecting the security of personal data in the Company and employees are required to familiarize themselves with them.

At regular intervals, but not less than once a year, TBS organizes newsletters aimed at maintaining the knowledge and awareness of the company's employees regarding the basic requirements of the Regulation, basic concepts introduced by applicable law, risks that could arise from breaches of personal data security and their possible consequences.

In the case of the implementation of projects related to the processing of large volumes of personal data of TBS clients, the employees working on these projects undergo specialized training for processing and protection of personal data. This training includes in-depth acquaintance of employees with the requirements of the Regulation, rules and practices for personal data processing, examination of risks that may arise in the implementation of the project, technical and organizational measures, requirements, and practices for personal data protection relevant for the specific project.

The projects, the implementation of which requires specialized training, are determined jointly by the project manager and the Data Protection Officer.

7. Technical measures for data protection

Telelink Business Services has developed, implemented, and announced the necessary technical means for the protection of assets, information, and personal data.

Technical measures include, but are not limited to, control of physical access to the company's offices, control of logical access to network services, operating systems, applications, security of server infrastructure, security of information and personal data when working remotely, and etc.

The technical measures applied by Telelink Business Services are described in a number of documents - policies, processes and procedures in accordance with the international standard on information security ISO/IEC 27001: 2013 and its extension ISO/IEC 27701: 2019, related to the security of personal data that are available to all employees of the company and aim to ensure the three pillars of security of information and personal data - confidentiality, availability and integrity.

8. Roles and responsibilities

Every TBS employee is obliged to observe complete confidentiality when working with personal data in the process of performing their duties and responsibilities.

The Data Protection Officer (DPO) shall assist in the proper application and compliance with the rules of this Policy and the applicable legislation on personal data protection and shall fully assist the organization in fulfilling its obligations under the Regulation.