BORUSAN HOLDING GROUP
POLICY ON THE PROTECTION AND PROCESSING OF PERSONAL DATA

CONTENTS

INTRODUCTION

With this Policy, principles to adopt and take into consideration in practice by Borusan Group Companies regarding processing and protection of personal data are set forth. This principle also sets forth the matters to be carried out by the Group Companies and basic policies to comply with the regulations on the Law no. 6698 on Personal Data Protection ("**LPDP**").

PURPOSE

This Policy is prepared to ensure and provide top level management and coordination of activities specific to Group Companies in order to comply with the LPDP within a Group-Company-level for legitimate processing and protection of personal data.

Group Companies will make necessary regulations in accordance with principles determined by the Borusan Group in order to provide necessary internal operations for compliance and create necessary systems in order to create awareness for employees and business partners.

I. PRINCIPLES APPLICABLE TO PROCESSING OF PERSONAL DATA

This Policy shall be deemed as a guide to indicate how to practice rules asserted by LPDP and related legislation for Borusan Group Companies.

Group Companies will analyse their personal data processing activities guided by this Policy, will determine necessary actions in order to comply with this Policy and take any kind of technical and administrative precaution. Internal auditing mechanisms will run in order to continuation of compliance to this Policy after the determined actions are implemented.

Trainings and studies will be conducted in order to ensure employees' awareness to this Policy within the Group, necessary compliance processes will be operated for new employees and necessary regulations will be made regarding the commercial relations between group companies and their business partners.

In order to provide compliance with the LPDP, personal data must be processed in accordance with the general principle and provisions set forth in the said legislation. Within this scope, principles and conditions regarding all personal data processing activities by the Group Companies are addressed in this part.

Principles to take into consideration during processing of personal data are examined in the titles below.

1.1. Processing in Good Faith and in Accordance with the Law

Group Companies shall act in good faith and in accordance with the principles set forth under legal regulations during personal data processing activities. In this regard, Group Companies shall interpret and apply the principles of limited and proportional processing and process only necessary amount of data within appropriate levels for the purpose of processing.

1.2. Ensuring that Personal Data Are Accurate and Up-to-Date Where Necessary

Group Companies shall ensure that processed personal data are accurate and up-to-date and take necessary measures in this regard. For instance; Group Companies shall establish a system for data subjects to correct their personal data and verify their accuracy.

1.3. Processing for Specific, Explicit and Legitimate Purposes

Group Companies shall process personal data with specific, explicit and legitimate purposes. In this regard, Group Companies shall determine purposes for processing personal data in express and definite manners and declare such purposes for data subjects' information prior to processing of data. Personal Data should not be processed except for the specified purposes. The purposes to be determined by Group Companies must be legitimate and compliant with the law.

1.4. Relevant, Limited and Proportional to the Purposes for Which They Are Processed

Group Companies shall process personal data with regards to specified purposes and avoid processing where deemed irrelevant to the realization of the purpose or not required. For instance, personal data processing activity shall not be carried out by reason of meeting the needs that may arise in the future.

1.5. Keeping for Duration Necessary for The Purposes for Which the Data are Processed or Foreseen Under the Relevant Legislation

Group Companies shall keep personal data only for a duration stated under the applicable legislation or necessary for the purposes for which the data are processed. In this regard, if a duration is foreseen under the relevant legislation, such duration shall be complied with. If such duration is not determined, personal data shall be kept for the duration necessary for the purposes for which data are processed.

II. CONDITIONS OF PROCESSING PERSONAL DATA

As a rule, personal data shall be processed in compliance with one or more conditions set forth by Article 5 of the LPDP. In this regard, Group Companies shall determine whether personal data processing activities fall within the scope of these conditions or not and shall cease any processing activities which do not meet the said condition(s).

Special conditions are set forth for special categories of data within the LPDP. In order to meet these conditions, measures determined by the Data Protection Authority shall be taken into consideration while processing special categories of data.

With regards to personal data transfers to third parties within or outside the country, organisational systems that provide compliance with Articles 8 and 9 of the LPDP shall be established. All necessary security measures shall be taken prior to personal data transfers, which shall be in line with the purposes for processing.

Necessary systems shall be established and awareness shall be raised within the organisations in order to prevent unlawful processing of personal data.

III. OBLIGATIONS OF THE GROUP ASSOCIATIONS

3.1. Obligation to Provide Information for Data Subjects

Group Companies shall inform data subjects regarding how their data shall be processed, during the collection of personal data. LPDP determines the minimum scope of information notices; which are determined as follows:

(1) Identity of the personal data controller and of his representative, if any
(2) Purposes of personal data processing,
(3) Recipients to whom the personal data will be transferred,
(4) Method and legal grounds of the personal data collection,
(5) Rights of the data subjects.

In this regard, personal data collection spots shall be determined firstly, which shall be followed by determining the points for informing data subjects and preparing information notices, individually for each data collection spot.

3.2. Obligation of Data Controller to Respond to the Applications of Data Subjects

Personal data subjects have the right to make an application in writing or by the methods to be determined by the Data Protection Authority and to use their rights set forth in the LPDP.

In that regard, Group Companies shall take administrative and technical measures to fulfil their obligations mentioned in Article 13 of the LPDP and let data subjects exercise their rights.

Legal rights that may be exercised by data subjects with respect to their personal data are as follows:

- Learn whether data relating to him/her are being processed or not,
- Request further information if personal data relating to him have been processed,
- Learn the purpose of the processing of personal data and whether data are being processed in compliance with such purpose or not,
- Learn the third-party recipients to whom the data are disclosed within the country or abroad,
- Request rectification of the processed personal data which is incomplete or inaccurate and to request notification of third parties, to whom the personal data are transferred, about this process,
- Request erasure or destruction of in the event that the data is no longer necessary in relation to the purpose for which the personal data was collected, despite being processed in line with the LPDP or any other related law, and to request notification of third parties, to whom the personal data are transferred, about this process.
- Object to negative consequences about him/her that are concluded as a result of analysis of the processed personal data by solely automatic means,
- Demand compensation for the damages he/she has suffered as a result of an unlawful processing operation.

Only the applications made in writing shall be taken into examination by the Group Companies. However, other methods for application shall also be determined by the Data Protection Authority. Group

Companies shall respond to requests stated in the application, depending on the application's nature, as soon as possible and within 30 days the latest. Group Companies may either accept the requests and take necessary actions or reject the request by disclosing the reasons for rejection.

It is of high importance to state that, in cases where data subject's application is rejected or respond is found inadequate by data subjects or the application is not responded within the specified period; data subject may file a complaint to the Board within 30 days as of learning this situation. In order to prevent such complaints, it is important to give adequate responds to data subjects within the legal period.

3.3. Obligation to Ensure Security of Personal Data

Group Companies shall take all technical and administrative measures necessary to provide appropriate security level to prevent unlawful processing of and unlawful access to personal data and to provide preservation thereof.

Data Protection Board may determine detailed regulations regarding the obligations on data security. Therefore, in order to comply also with such obligations, reasonable effort shall be made and maximum amount of security shall already be established.

Group Companies shall establish necessary systems to make the audits or have audits made as required by law, as regards to the technical and administrative measures they shall take. These audits shall be examined by their relevant institutions and necessary actions shall be taken pursuantly.

In the event that personal data are obtained by third parties in an illegal manner, Group Companies shall inform the data subject and the Data Protection Board as soon as possible. In this regard, necessary organisations structure must be established.

In case of locating or spotting conditions that cause security risks, all necessary measures must be taken without delay in order to avoid prevent such risks.

3.3.1. Taking Technical and Administrative Measures to Ensure Lawful Processing of Personal Data

In order to process personal data legally, following measures shall be taken by the Group Companies:

- All procedures as regards to personal data processing within the Group Companies shall be analysed by relevant business units, mapping of "personal data processing" shall be conducted in this regard.
- Pursuant to the personal data processing map, necessary steps to provide compliance with the law shall be determined on a business unit basis.
- Personal data processing procedures shall be inspected by technical systems to be developed and reported to the relevant body or person.
- Employees of the Group Companies shall be informed and educated regarding legal processing and regarding the sanctions and penalties of unlawful processing of personal data.
- Periodical audits shall be conducted in order to raise awareness of employees and administrative measures shall be enforced by way of implementing the internal policies of the Group Companies and by setting educations on these policies.

- Clauses shall be inserted within relevant agreements and documents that lead and manage the employment relation between the employees and the Group Companies that cover privacy of personal data transferred and clauses that cover the manners of processing and storing thereof.
- Access to personal data shall be limited with the employees who are obliged to conduct relevant processing pursuant to the determined purposes. Any access irrelevant for other employees' work shall be blocked.

3.3.2. Taking Technical and Administrative Measures to Prevent Unlawful Access to Personal Data

Precautions below must be taken in order to prevent illegal access to the personal data by the Group Companies:

- Technical precautions suitable for technology must be taken in order to prevent access to systems and locations storing personal data, this precautions must be updated periodically.
- Access and authorization technical process must be designed and engaged in accordance with the legal compliance on business unit basis by the Group Companies
- Technical precautions taken must be reported to the related authority periodically, technological solutions must be created on subjects which has security risks.
- Software and hardware must be installed including virus protection systems and firewall software and hardware.
- Employees of the Group Companies must be trained regarding the technical precautions taken and knowledgeable personnel on technical subjects must be employed.
- Commitment for not disclosing personal data to third parties and for any other reason than process purpose must be taken from Group Company employees. This commitment will still apply after employee quits working.
- Provisions for necessary safety precautions in order to protect personal data must be added to the agreements made with the persons whose personal data is transferred by the Group Companies.

3.4. Obligation to Register with the Data Controllers Registry

Group Companies must register with the Data Controllers Registry by presenting information and documents stated in LPDP and within the timeline determined and declared by the Board before processing data. Documents to submit are stated below (It is possible to require additional information and documents with the secondary regulations by the Board):

(1) Identity and address information of the personal data controller and of his representative, if any, as a data controller,
(2) The purpose of the personal data processing for which the data are intended,
(3) Explanations on the entity, group and groups and data categories on these entities,
(4) Receiver or receiver groups to whom the personal data can be transferred,
(5) Personal data predicted to be transferred to foreign countries,
(6) Precautions on personal data security,
(7) Maximum time needed for processing personal data.

IV. ORGANISATIONAL STRUCTURING WITHIN THE GROUP COMPANIES

A ‘’Committee for Personal Data Protection’’ or an official must be assigned within the Group Companies who shall be responsible to ensure performance and adaptation of actions determined by executives, in order to manage the principles that are set forth herein this Policy and in other policies related to this Policy.

Within this scope, at least the following (minimum) actions must be taken by the Committee or assignee:

- Determine fundamental policies for processing and protection of personal data and actions to be taken in order to comply with the legislation.
- Present determined fundamental policies and actions to approval of the board; supervise its application and provide coordination,
- Determine how personal data processing and protection policies applied and in what way the supervision will be made, give necessary assignments after the approval from executives.
- Detect possible risks during data processing activity and provide necessary precautions, submit improvement suggestions to executive approval.
- Provide training about personal data protection and company policy to employees,
- Settle applications by the personal data possessor on highest level.
- Organize necessary regulations for company to fulfil its responsibilities in scope of LPDP within company.
- Follow developments on personal data protection; advise executives about things to do on these development
- Manage the relationship between the Institution and Board.

ANNEX-1 DEFINITIONS

Explicit Consent	**:**	Consent related to a specific subject which is given freely upon informing.
Anonymisation	**:**	Processing of personal data in such a way to make the linking of the data with another data of an identified or identifiable natural person impossible; i.e. techniques such as masking, aggregation, deterioration to prevent linking of data with a real person.
Personal Data Subject	**:**	Natural persons whose personal data are processed i.e. customers, employees.
Personal Data	**:**	Any information relating to an identified or identifiable natural person.; i.e. name-surname, ID number, e-mail, address, date of birth, credit card number. Hence processing of data relating to legal persons is not within the scope of the Law.
Special Categories of Personal Data	**:**	Data relating to an individual's racial or ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs; dress and appearance; memberships to any association, foundation or trade union; health or sex life; criminal conviction and security measures, biometric and genetic data.
Processing of Personal Data	**:**	Any operation which is performed upon personal data whether or partly by automatic means or otherwise than by automatic means which form part of a filing system, such as collection, recording, storage, retain, alteration, re-organization, disclosure, transfer, retrieval, making available, combination, or blocking.
Data Processor	**:**	Natural or legal persons who process personal data on behalf of and under the authority given by the data controller; i.e. an IT company that stores personal data that belong to customers of a company.
Data Controller	**:**	any natural and legal person which determines the purposes and means of processing personal data and is responsible for the establishment and management of the storage where data are kept (data register system).