

BILGILI HOLDING GROUP
POLICY ON THE PROCESSING, PROTECTION, STORAGE
AND ANNIHILATION OF PERSONAL DATA
28.11.2019

Version: 2.0

INDEX

1.	INFORMATION REGARDING THE POLICY	4
1.1	INTRODUCTION.....	4
1.2.	PURPOSE.....	4
1.3.	SCOPE	4
1.4.	ABBREVIATIONS AND DEFINITIONS.....	4
2.	MATTERS RELATING TO THE PROCESSING OF PERSONAL DATA	6
2.1.	PROCESSING PERSONAL DATA IN COMPLIANCE WITH THE PRINCIPLES SET OUT IN THE LEGISLATION	6
2.1.1.	Personal Data are Processed Lawfully and in Conformity with Good Faith.....	6
2.1.2.	Personal Data is Accurate and Up-To-Date	6
2.1.3.	Personal Data is Being Processed for Specific, Explicit and Legitimate Purposes	6
2.1.4.	Personal Data Processing is Relevant with, Limited to and Proportionate to the Purposes for which they are Processed	6
2.1.5.	Keeping the Personal Data as Long as Necessiated by the Regulation or by the Purposes of Processing	6
2.2.	DATA SUBJECT CATEGORIES	6
2.3.	CONDITIONS OF PROCESSING PERSONAL DATA	7
2.3.	CONDITIONS OF PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA.....	9
2.4.	SPECIAL CASES WHEN PERSONAL DATA IS BEING PROCESSED	9
2.4.1.	Building Entries and Personal Data Processing Activities in the Building, Website and its Visitors ..	9
2.4.2.	Building Entrance and Camera Monitoring Activities.....	9
2.4.3.	Monitoring Entrances and Exits of Guests Entering into the Buildings and Other Facilities	9
2.5.	PURPOSES OF PROCESSING PERSONAL DATA.....	10
3.	MATTERS REGARDING PERSONAL DATA PROTECTION	11
2.2.	ENSURING PERSONAL DATA PROTECTION	11
3.1.1.	TECHNICAL MEASURES.....	11
3.1.2.	ADMINISTRATIVE MEASURES	12
2.3.	PROTECTION OF SPECIAL CATEGORIES OF PERSONAL DATA	12
2.4.	AWARENESS ACTIVITIES AND AUDITS WITHIN THE COMPANY	12
4.	RIGHTS OF THE DATA SUBJECT AND USING THESE RIGHTS.....	12
4.1.	RIGHTS OF THE DATA SUBJECT AND CONDUCTING THE APPLICATION PROCESS	12
4.2.	INFORMING THE DATA SUBJECT	13
5.	TRANSFER OF PERSONAL DATA	14
5.1.	TRANSFERRING PERSONAL DATA DOMESTICALLY	14
5.1.1.	Transferring Personal Data Domestically, Excluding Special Categories of Personal Data	14
5.1.2.	Transferring Special Categories of Personal Data Domestically.....	14
5.2.	TRANSFER OF PERSONAL DATA INTERNATIONALLY	15
5.1.2.	Having Adequate Protection.....	15
5.1.3.	Personal Data Transfer To Countries That Do Not Have Adequate Protection	16
5.2.	THIRD PARTIES THAT PERSONAL DATA MAY BE TRANSFERRED TO	17
6.	STORING AND ANNIHILATING PERSONAL DATA.....	17
6.1.	RECORDING MEDIUMS OF PERSONAL DATA	17

6.2.	REASONS TO STORE PERSONAL DATA	17
6.3.	REASONS.....	18
6.4.	STORAGE AND ANNIHILATION TERMS RELATING TO PERSONAL DATA	18
6.5.	ANNIHILATION PROCEDURES RELATING TO PERSONA DATA	19
6.5.1.	ERASURE AND DESTRUCTION TECHNIQUES RELATING TO PERSONAL DATA	19
6.5.2.	ANONYMIZING TECHNIQUES RELATING TO PERSONAL DATA:	20
6.6.	PERIODIC ANNIHILATION TERM REGARDING PERSONAL DATA.....	21
6.7.	DISTRIBUTION OF TASKS AND RESPONSIBILITY REGARDING THE STORAGE AND ANNIHILATION OF PERSONAL DATA 21	
7.	ENFORCEMENT DATA AND UPDATE OF THE POLICY	21
ANNEX-1.....		22
ANNEX-2.....		24
ANNEX-3.....		25

Warning. As Bilgili Holding Group, we believe that the confidentiality and security of your personal data is important. In this context, we would like to inform you about how we process, use and protect the personal data we collect from our customers, suppliers, business partners, their employees and officials and all other third parties while conducting our business relationships. Please note that if you do not accept this Policy, you should not pass on your personal data to us. If you choose not to provide us with your personal data, in some cases we will not be able to provide you with our services, nor we will be able to respond to your requests or provide full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data you submit to Bilgili Holding Group are accurate, complete and up-to-date. Furthermore, if you share other people's personal data with us, it is your responsibility to collect such data in accordance with local legal requirements. In such case, this means that you have obtained all necessary permissions to collect, process, use and disclose their information from that third party and our Company cannot be held responsible in this case.

BILGILI HOLDING A.S.

POLICY ON THE PROCESSING, PROTECTION, STORAGE AND ANNIHILATION OF PERSONAL DATA

1. INFORMATION REGARDING THE POLICY

1.1 INTRODUCTION

This Policy on the Processing, Protection, Storage and Annihilation of Personal Data (“**Policy**”), has been prepared by BILGILI HOLDING A.S. as the data controller pursuant to the Turkish Personal Data Protection Law numbered 6698 (“**PDPL**” or “**Law**”) and the Regulation Relating to the Erasure, Destruction or Anonymization of Personal Data (“**Regulation**”) enacted with its publication in the Turkish Official Gazette on October 28, 2017 (which acts as the secondary legislation of the Law) in order to fulfill our obligations and to inform the data subjects regarding the purpose of processing of their personal data, the determination of the maximum storage term needed for these purposes and the procedure regarding the protection, erasure, destruction and anonymization thereof.

The protection of personal data is one of the most important priorities of Bilgili Holding A.S. (hereby referred to as “**Bilgili Holding**”, “**Company**” or “**Bilgili Holding Group**” including its group companies) and thus, strives to comply with all applicable legislation relating to this. This Policy sets out the principles to be adopted by Bilgili Holding Group companies regarding the protection and processing of personal data. Unless stated otherwise, the Policy will also apply to Bilgili Holding Group companies. The list of Bilgili Holding Group companies may be found at <http://www.bilgiliholding.com/en/bilgili-group-companies.html>

1.2. PURPOSE

Bilgili Holding Group aims to determine the framework of the compliance activities to be carried out by the relevant companies and facilitate coordination thereof in order to comply with the PDPL relating to the protection and processing of personal data. Bilgili Holding Group has formed the structure necessary for the compliance with PDPL and has realized the necessary mechanisms in order to raise awareness with its employees and business partners. The policy is a guideline on how the Bilgili Holding Group applies the rules laid down by the KVKK and related legislation. Bilgili Holding Group periodically operates internal audit mechanisms to ensure compliance with the Policy.

Bilgili Holding Group takes all kinds of administrative and technical measures necessary for the processing and protection of personal data in line with the principles set out in the Policy, sets up training systems to ensure employee awareness, operates the necessary compliance processes for new employees as well as giving notices and warnings to the Company’s business partners regarding this.

1.3. SCOPE

This Policy is related to the personal data of Data Subjects processed fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.

The details of the personal data processing activities carried out by Bilgili Holding Group regarding Bilgili Holding Group employees and prospective employees can be found on Bilgili Holding Group Clarification Text Regarding Processing of Personal Data of Employees and Bilgili Holding Group Clarification Text Regarding Processing of Personal Data of Potential Employees published on www.bilgiliholding.com.

The personal data of the Company’s employees, employee candidates, service providers, visitors and other third parties are covered by this Policy and this Policy applies to all recording medium and activities relating processing personal data possessed or managed by the Company.

1.4. ABBREVIATIONS AND DEFINITIONS

ABBREVIATIONS	DEFINITIONS
Explicit Consent	Freely given, specific and informed consent
Application Form	The form prepared by Bilgili Holding that is published on the Website (which is also Annex-1 of this Policy) in order for the Data Subject to exercise his/her rights in accordance with Article 11 of the Law and to make an application to the Bilgili Holding Group for this purpose

Audit Firm	The firm where there are persons licensed as sworn-in certified public accountant or certified public accountant and authorized by the Public Surveillance, Accounting and Auditing Standards Board who independently audits and evaluates through the books, records and documents by applying the required independent audit techniques in order to obtain sufficient and appropriate independent audit evidence to provide reasonable assurance on the conformity and accuracy of the financial statements and other financial information of Bilgili Holding Group
Relevant User	Persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller, excluding the person or unit responsible for the technical storage, protection and back-up of personal data.
Annihilation	Erasure, destruction or anonymization of personal data
Recording Medium	Any kind of medium which contain personal data processed fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means.
Personal Data	Any kind of information relating to an identified or identifiable natural person
Processing of Personal Data	Any operation performed upon personal data such as collection, recording, storage, retention, alteration, re-organization, disclosure, transferring, taking over, making retrievable, classification or preventing the use thereof, fully or partially through automatic means or provided that the process is a part of any data registry system, through non-automatic means
Anonymizing Personal Data	Rendering personal data impossible to link with an identified or identifiable natural person, even through matching them with other data
Erasing Personal Data	Making personal data inaccessible to and not reusable for Relevant User.
Destroying Personal Data	The process of rendering personal data inaccessible and unusable for everyone
Board	Personal Data Protection Board
Special Categories of Personal Data	Personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature.
Periodic Annihilation	The process of erasing, destroying or anonymizing the personal data in accordance with the policy of storing and destroying personal data, which will be carried out at repetitive intervals in the event that all the conditions for processing personal data determined in the Law are no longer there
Data Subject / Relevant Person	The natural person whose personal data is processed

Data Controller	The natural or legal person who determines the purpose and means of processing personal data and is responsible for establishing and managing the data registry system
VERBIS	A registration system formed by the Department of the Board, accessed via the internet and where data controllers shall be registered to and shall be required record the data processing activities they are engaged with

2. MATTERS RELATING TO THE PROCESSING OF PERSONAL DATA

2.1. PROCESSING PERSONAL DATA IN COMPLIANCE WITH THE PRINCIPLES SET OUT IN THE LEGISLATION

All personal data processed by Bilgili Holding Group is processed in accordance with the PDPL and relevant legislation. The fundamental principles we are very on when processing your personal data and that are set out in Article 4 of the PDPL are explained below:

2.1.1. Personal Data are Processed Lawfully and in Conformity with Good Faith

Bilgili Holding Group acts in compliance with the principles conveyed by legal regulations, trust and good faith when processing personal data. Within this framework, Bilgili Holding Group processes personal data to the extent required by Bilgili Holding Group business activities and limited to these activities. Accordingly, Bilgili Holding Group does not collect or process personal data without the knowledge of the Data Subject. It is our basic principle to process Personal Data in accordance with the law, the PDPL and the relevant legislation.

2.1.2. Personal Data is Accurate and Up-To-Date

The Bilgili Holding Group makes every effort to ensure that personal data is accurate and up-to-date. In this context, in order to ensure the accuracy and up-to-dateness of the personal data, it keeps the channels that will provide this open and ensures their correction data upon the application of the Data Subject or ex-officio.

2.1.3. Personal Data is Being Processed for Specific, Explicit and Legitimate Purposes

The purposes that Bilgili Holding Group is processing personal data is clearly defined as a requirement of its illumination obligation. Bilgili Holding Group processes personal data for legitimate purposes in accordance with the Law, in connection with the works it performs and/or the services it provides.

2.1.4. Personal Data Processing is Relevant with, Limited to and Proportionate to the Purposes for which they are Processed

Bilgili Holding Group processes Personal Data for specific, clear and legitimate purposes, ensures that personal data is collected for the purposes set forth in this Policy or the approval of the Data Subject (Explicit Consent), stores them during the required period determined in line with the purpose and/or does not process personal data that is not needed. It is our basic principle to limit the processing of personal data to the necessity of realizing the purpose.

2.1.5. Keeping the Personal Data as Long as Necessiated by the Regulation or by the Purposes of Processing

If there is a certain period foreseen in the relevant legislation for the storage of personal data, Bilgili Holding Group complies with such period. If such a period is not specified therein, the Personal Data will be retained only for the period required for the purpose for which it was processed. In the event that the conditions for the processing of the personal data in Articles 5 and 6 of the Law no longer exist, the personal data is erased, destroyed or anonymized by Bilgili Holding Group upon the request of the relevant person or ex officio.

2.2. DATA SUBJECT CATEGORIES

The categories of data subjects whose personal data is processed by Bilgili Holding Group are listed in the table below. Persons who fall outside the following categories may also submit requests to our Company within the scope of PDPL and their requests will also be evaluated under the Policy.

CATEGORIES OF DATA SUBJECTS	EXPLANATIONS
Customer	Natural or legal persons who purchase our products or render our services

Potential Customer	Natural or legal persons who have requested or are interested in purchasing our products and/or rendering our services or that may have interest in our products and/or services which have been assessed in accordance with the rules of custom and good faith
Visitor	Natural persons who have entered the workplaces (offices, hotel, etc.) owned or managed by Bilgili Holding Group for various purposes or who have visited our websites
Third Parties	Third party natural persons (e.g. guarantor, companion, family members and relatives) associated with Bilgili Holding Group whose personal data are processed in order to ensure the security of commercial transactions with the aforementioned parties, or to protect the rights and interests of the aforementioned persons as well as natural persons (e.g. former employees) in which our Company has to process their personal data for a specific purpose.
Employees	Natural persons who work under Bilgili Holding Group with an employment contract
Prospective Employees / Interns	Natural persons who have applied to Bilgili Holding Group in any way or who have submitted their resumes and relevant information to be reviewed by our Company
Employees, Shareholders, Authorities of Companies We Work With	Natural persons that are employed by the companies that Bilgili Holding Group work with, including its shareholders and authorities (including but not limited to business partners, suppliers, etc.)

2.3. CONDITIONS OF PROCESSING PERSONAL DATA

Processing of Personal Data has been defined in Article 3 of the Law. Accordingly, processing of personal data has been accepted as any operation which is performed upon personal data such as collection, recording, storage, preservation, alteration, adaptation, disclosure, transfer, retrieval, making available for collection, categorization or blocking its use by wholly or partly automatic means or otherwise than by automatic means which form part of a filing system.

The conditions for the processing of personal data are listed in Article 5 of the Law and it is possible to process personal data if at least one of the following conditions exists:

i. Explicit Consent of the Data Subject

One of conditions of processing personal data is obtaining the explicit consent of the data subject. The data subject must give his/her explicit consent for specific, explicit and legitimate purposes.

In the performance of data processing by While the data controller executes its data processing, it should first take into consideration whether it can base such processing on one of the other data processing conditions. If it cannot base its processing upon any of the aforementioned conditions, the explicit consent of the person concerned should be sought.

IN THE EVENT THAT THERE ARE ANY OF THE PERSONAL DATA PROCESSING CONDITIONS STATED HEREINBELOW, THE DATA SUBJECT'S PERSONAL DATA MAY BE PROCESSED WITHOUT HIS/HER EXPLICIT CONSENT.

ii. Personal Data Processing is Explicitly Permitted by the Laws

If it is explicitly stated in the law that (in other words, if there are clear provisions in the relevant law that) the data controller may process the data subject's personal data, this means that there is the personal data processing condition. E.g. the data controller providing information on the salary of its employees upon the Social Security Institution's request.

iii. The Data Subject is Physically Incapable of Giving Consent and it is Mandatory to Process Personal Data

In the event that it is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent, the relevant data subject's personal data may be processed. Legally, in the event of an impossibility, the data subject's personal data must be processed in order to protect the life or body integrity. E.g. to determine the location of a person whose freedom is restricted or the suspect by means of a telephone, computer, credit card, debit card or other technical instrument.

iv. The Personal Data Processing is Directly Related to the Fulfillment or the Execution of a Contract

The data subject's personal data may be processed if this is necessary to do so for the fulfillment or the execution of the contract between the parties (i.e. data controller and the relevant data subject), provided that such processing is limited with such purposes. For example, in order to pay the money according to a contract, the creditor's bank account number is obtained or another example is when the bank obtains the data subject's salary slip, title deed records, document of non-execution debt during the credit agreement with the data subject. Another example is when the seller can process the address of the buyer in order to fulfill the obligation to deliver goods or when the employer has processed the bank information of the employees in order to pay their salary.

v. The Personal Data Processing is Necessary for the Data Controller to Fulfill its Legal Obligations

Our Company may process the personal data in order to fulfill its legal obligations. For example, the company may obtain and process its employee's personal data such as their bank account number, their social security number, their marital status, their dependents, whether their spouses work in order to pay their salaries.

vi. The Data Subject Discloses His/Her Personal Data to the Public

In the event where the data subject discloses his/her personal data to the public, such personal data may be processed limited to such purpose. For example, the data subject may publicly announce his/her contact information for communication purposes. On corporate websites (i.e. intranet), it is also possible if employees' telephone numbers and corporate e-mail addresses are shared with other people who use the intranet. However, in order for personal data to be considered as being disclosed to the public, it is necessary that the data subject wishes that such data to be known to be public. In order to disclose such data to the public, there must be the data subject's consent for such disclosure. Otherwise, having a data subject's personal data in a public place does not mean that such data is overt. In addition, in such case, the relevant personal data should not be misused.

vii. The Personal Data Processing is Necessary for the Establishment, Usage or Protection of a Right:

The data subject's personal data may be processed if it is necessary for the establishment, usage or protection of a right.

It is possible to process the data subject's personal data if it is necessary for the establishment, usage or protection of a right. For example, a company uses some of its former employee's personal data as evidence in the lawsuit. In addition, after the expiry/termination of the contract, documents such as invoices, contracts and sureties are kept until the end of the statute of limitations for the purpose of possible legal proceedings.

viii. The Personal Data Processing is Necessary for the Legitimate Interests of the Data Controller, provided that the Fundamental Rights and Freedoms of the Data Subject are not Harmed

The data subject's personal data may be processed if it is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

In order to process such data due to such condition, the data controller must have a legitimate interest and it must not harm the data subject's fundamental rights and freedoms. The data controller's legitimate interest is related to the its interest in and benefit of the processing of personal data. The benefit of the data controller may gain must be in a similar level to a legitimate, relevant, sufficiently effective, specific, and already existing interest of the data subject with regards to his/her fundamental rights and freedoms. The data controller must have a transaction that is related to its current activities which is executed for its benefit in the near future.

The application of such provision requires a two-stage evaluation. In the first evaluation, the existence of the data controller's legitimate interest is determined and in the second evaluation, it is determined that such interest does not harm the data subject's fundamental rights and freedoms. When conducting such assessment, is important not to confuse the legitimate interest of the Company with its purpose of processing personal data. The purpose of processing personal data is specifically related to the processing of the personal data. However, the data controller's legitimate interest can be interpreted in a broader sense. The data controller's legitimate interest is related to the benefit that will be obtained as a result of data processing. The benefit of the data controller must be relating to and be in a similar level to a legitimate, specific, and existing interest of the data subject. For

example, a company may process its employee's personal data for their promotion, to increase their salaries or social rights or for restructuring without harming their fundamental rights and freedoms of employees.

2.3. CONDITIONS OF PROCESSING SPECIAL CATEGORIES OF PERSONAL DATA

Special categories of personal data are data that may cause discrimination or victimize the data subject. Therefore, such personal data need to be protected more strictly than other personal data.

Pursuant to Article 6 of the Law, "Data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics are special categories of personal data." Our Company takes all necessary measures to comply with the Board Decision numbered 2018/10 published in the Turkish Official Gazette on 07.03.2018 with the number 30353 namely "Adequate Measures that Must be Taken by Data Controllers when Processing Special Categories of Personal Data."

Special categories of personal data may be processed with the data subject's explicit consent or limited to the conditions stipulated in the Law. The law also makes a distinction within the special categories of personal data. Accordingly, special categories of personal data other than those relating to the data subject's health and sexual life, can be processed without explicit consent.

Our Company may process special categories of personal data (if applicable) in line with the principles determined in this Policy and under the following circumstances, provided that all kinds of administrative and technical measures are taken (including methods that may be determined by the Board):

- i. **Special categories of personal data except those concerning health and sexual life**, may be processed without the data subject's explicit consent, provided that it is clearly stipulated in the laws, in other words, provided that it is expressly determined in the relevant law regarding the relevant activity.
- ii. **Special categories of personal data relating to health and sexual life**, may only be processed without taking the data subject's explicit consent by people bound by confidentiality due to their occupation or by authorized institutions in order to preserve public health, give medicines, diagnosis, treatments, care, health services and financial planning thereof.

In an event where there are other reasons than those explained herein, it is necessary to obtain the data subject's explicit consent in order to process his/her special categories of personal data.

2.4. SPECIAL CASES WHEN PERSONAL DATA IS BEING PROCESSED

2.4.1. Building Entries and Personal Data Processing Activities in the Building, Website and its Visitors

In order to ensure that the users of our websites make their visits to the sites in accordance with the purposes of the visit, to display customized content to them and to perform online advertising activities (such as cookies), the internet transactions are recorded in the website.

Personal data of the users who visit the Website such as their IP address, the times and type of service used and the data transferred amount are processed by our Company in accordance with the Law.

2.4.2. Building Entrance and Camera Monitoring Activities

In order to ensure security in the buildings, the Company carries out surveillance activities in accordance with the Law on Private Security Services and the relevant legislation. Furthermore, in order to ensure security in our company's buildings and facilities, security camera monitoring activities are carried out for the purposes specified in the applicable legislation and in accordance with the personal data processing conditions specified in the Law. In accordance with Article 10 of the Law, the Company informs the data subject regarding camera surveillance. Additionally, in accordance with Article 4 of the Law, our Company processes personal data in a relevant, limited and measured manner in connection with the purpose for which it was processed. The purpose of our Company's video camera monitoring activities is limited to the purposes set out in this Policy. In this context, the monitoring areas as well as the number and recording term of surveillance cameras are sufficient and limited to reach this security objective. There is no camera monitoring process in areas that may result in an intervention of privacy or that exceeds the security objectives. Only authorized employees have access to these recordings that are recorded and stored digitally. A limited number of people who have access to the records have declared that they will protect the confidentiality of such personal data data they access through a confidentiality undertaking.

2.4.3. Monitoring Entrances and Exits of Guests Entering into the Buildings and Other Facilities

The Company carries out personal data processing activities in order to ensure security and to monitor the guest entrances and exits in the premises and facilities of our Company for the purposes specified in this Policy. While the names and surnames of guests who enter our Company's premises' are taken, the data subjects are informed

in this context by means of the clarification texts presented thereto. The data obtained for the purpose of monitoring the guest entrances and exits are processed only for this purpose and the such personal data are recorded as hard copies.

2.5. PURPOSES OF PROCESSING PERSONAL DATA

In general, our purposes for processing personal data are as follows:

- Negotiating, executing and fulfilling contracts
- Providing products and services
- Customizing the products and services offered in accordance with demands; updating and developing these products and services due to customer needs, legal and technical developments
- Using user identification systems in relation to the products and services offered
- Announcing new or existing products, services and campaigns, conducting sales and marketing activities
- Carrying out marketing researches
- Creating statistics and analyzing usages
- Paying and collecting payments relating to products and services, choosing the payment method
- Providing contact/communication
- Conducting business relations with cooperating companies, suppliers, resellers and service providers
- Carrying out reporting activities within the framework of cooperation
- Evaluating the application process of lessees and carrying out lease relations
- Developing and planning the business strategics of Bilgili Holding Group
- Communicating with customers of Bilgili Holding Group for surveys to measure their satisfaction level
- Managing judicial/administrative processes, responding to requests from public istitutions and establishments, fulfilling legal obligations in accordance with legislations, resolving legal disputes
- Conducting investment relations
- Conducting job interviews, evaluating job applications
- Establishing, executing and terminating contracts and business relationships
- Giving Bilgili Holding Group’s employees their rights and benefits arising from their contracts, evaluating the employee’s performances and works
- Opening up user accounts, giving in-house IDS and lunch vouchers to employees
- Tracking the Company’s vehicles
- Registering of participants in an event where the Company participates in an organization
- Executing participants lists and giving certificates in an event where the employees are given trainings
- Creating and following up visitor records
- Ensuring the internal and enviromental security of the Company and the security of the Website and Applications
- Creating the personal data inventories
- Evaluating and responding to written, verbal or electronically submitted questions, requests, suggestions, complaints and applications, including those relating to personal data

In accordance with Article 10 of the Law and its relevant legislation, the Company informs the data subjects and processes their personal data in line with the general principles set forth in the Law and the principles set forth in Article 4 of the Law limited and based on at least one of the personal data processing conditions set forth in Article 5 and 6 of the Law.

In this respect, our Main and Sub-Objectives regarding Personal Data Processing are detailed hereinbelow:

MAIN OBJECTIVES	SUB-OBJECTIVES
To plan and/or execute of our Company's human resources policies and processes	To manage all employee recruitment processes

<p>To carry out the necessary work by the relevant business units for the execution of our commercial and operational activities carried out by our Company and to conduct the related business processes</p>	<ul style="list-style-type: none"> • To monitor finance and accounting works • To plan and execute internal and external reporting activities of the Company • To plan and execute processes relating to supply services • To plan and execute procurement processes • Establishing and managing the Information Technologies infrastructure • To conduct Information Security activities • To conduct corporate communication activities in order to plan and/or execute organizations such as events, invites and/or meetings • To plan and manage Corporate Governance activities • To plan and monitor social responsibility and sponsorship activities • To conduct investment relations • To negotiate and monitor contracts • To announce new or existing products, services and campaigns and to conduct sales and marketing activities • To execute personal data inventories
<p>To plan and execute our Company's business strategies</p>	<ul style="list-style-type: none"> • To manage relations with business partners and suppliers • To execute strategic planning activities • To plan and execute advertising and promotional activities relating to our Company • To plan risk assessment activities and feasibility studies to select potential suppliers

3. MATTERS REGARDING PERSONAL DATA PROTECTION

3.1. ENSURING PERSONAL DATA PROTECTION

Pursuant to Article 12 of the Law, the Company takes the necessary measures according to the nature of the personal data to be protected in order to prevent unlawful disclosure, access, transfer or otherwise security of personal data. In this context, in accordance with the guidelines published by the Board, the Company ensures and makes others ensure to have the necessary level of security and take the administrative measures and audits.

All administrative and technical measures taken by the Bilgili Holding Group within the framework of the principles of Article 12 of the PDPL in order to safely store the data subject's personal data, to prevent illegal processing and accessing and destroying are listed below:

3.1.1. TECHNICAL MEASURES

- Internally monitoring the systems installed
- Using penetration test to identify system weaknesses and taking necessary measures, including monitoring to eliminate weaknesses
- Using strong passwords in electronic environments where personal data are being processed
- Regularly monitoring the user authorizations and accesses to personal data and ensuring compliance with data security principles
- Limiting access to personal data stored electronically as per logical access principles and limiting access to personal data stored in other ways as per the necessary and sufficient access principles
- Taking adequate security measures in environments where special categories of personal data are being processed, stored and/or accessed and preventing unauthorized access in these environments
- Ensuring destruction of personal data in a way that it cannot be re-obtained and that there is no trail thereof
- Pursuant to Article 12 of the Law, protecting digital mediums where personal data is stored with encrypted or cryptographic methods in order to meet information security requirements.

3.1.2. ADMINISTRATIVE MEASURES

- Bilgili Holding Group fulfills its obligation to enlighten the data subjects before starting to process their personal data.
- Bilgili Holding Group employees sign documents containing confidentiality obligations and commitments relating to activities carried out by the Company.
- “Personal Data Processing Inventories” are prepared in accordance with the principles described in the Law.
- The Company restricts access to the stored personal data for only limited personnel in order for them access as per their job description while taking into consideration its importance and whether the personal data is special categories of personal data or not.
- The Company conducts the necessary audits in order to ensure the implementation of the provisions of the Law in its own legal entity and, where necessary, eliminates the confidentiality and security weaknesses resulting from the audits.
- Concerning transfer of personal data, the Company signs a framework agreement regarding the protection and data security of all personal and legal persons with those who it transfers personal data to or ensures data security by adding provisions regarding this to existing contracts.
- The Company employs experienced and knowledgeable personnel in the processing of personal data and provides necessary training to its personnel regarding the scope of data protection legislation and data security,
- In the event that the processed personal data is unlawfully obtained by others, the Company informs the data subject and the Board as soon as possible.
- In the event that storage services are obtained from other companies, the Company ensures that that company's storage and annihilation services shall be in compliance the regulations stated in this Policy and the provisions of the relevant legislation, by determining that such services shall be regularly reported and that provisions regarding these are in the relevant contracts.

3.2. PROTECTION OF SPECIAL CATEGORIES OF PERSONAL DATA

The Law attributes importance on the risk of causing personal injury or discrimination when certain personal data is processed unlawfully. These type of data which are called special categories of personal data are data relating to race, ethnic origin, political opinions, philosophical beliefs, religion, sect or other beliefs, appearance and dressing, membership of association, foundation or trade-union, health, sexual life, criminal conviction and security measures, and biometrics and genetics.

Bilgili Holding Group protects “special categories of personal data” determined by the Law very sensitively and processes them in accordance with the Law. In this context, technical and administrative measures taken by Bilgili Holding Group for the protection of personal data are carefully implemented in terms of special categories of personal data and thus, Bilgili Holding Group executes the necessary audits regarding these data.

3.3. AWARENESS ACTIVITIES AND AUDITS WITHIN THE COMPANY

Bilgili Holding Group gives the necessary training to business units in order to raise awareness for the prevention of unlawful processing of personal data, unlawful access to personal data and for the protection of personal data.

Necessary systems are established to raise awareness of the Company's employees regarding the protection of personal data, and works with consultants if necessary. In this respect, our Company evaluates the attendance to related trainings, seminars and information sessions and updates its trainings in parallel with the revisions in the relevant legislation. These training activities are renewed periodically every year within the scope of in-house training activities, and training activities are executed during the orientation process for every new employee.

4. RIGHTS OF THE DATA SUBJECT AND USING THESE RIGHTS

4.1. RIGHTS OF THE DATA SUBJECT AND CONDUCTING THE APPLICATION PROCESS

Data subjects have the rights determined hereinbelow:

- (1) Find out whether or not personal data has been processed,
- (2) Request information about the processing of personal data if it has occurred,
- (3) Find out the purpose of processing the personal data and whether or not it was processed for this purpose,
- (4) Know third parties to whom personal data was transferred either domestically or abroad,
- (5) Request that personal data processed incorrectly or incompletely be corrected and request that third parties to whom the transaction in correction was made are informed,
- (6) Request that personal data be erased or destroyed if the reasons that required processing no longer apply in spite of the fact that it was processed in accordance with the provisions of the PPD or other applicable legislation, and request that third parties to whom personal data was transferred as part of this process be informed,

- (7) Object to any unfavourable consequences arising from the analysis of processed data via exclusively automatic systems,
- (8) Request remedy of damages if they incur losses due to the unlawful processing of personal data.

Exercise of the Rights of the Data Subject: Data subjects shall be able to communicate their claims regarding their rights listed in section 3.1 (“Rights of the Data Subject”) to our Company as per the methods determined by the Board.

Accordingly, data subjects shall be fill in the Bilgili Holding Group Data Subject Application Form found at <http://www.bilgiholding.com/i/files/BilgiliHoldingGroup-ApplicationForm.pdf>

An example of the form may be found as Annex-1 herein.

Our Company Responding to the Applications: Our Company takes the necessary administrative and technical measures to respond to applications to be made by the data subject in accordance with the Law and its relevant legislation. In the event where the data subjects duly submit their requests to the Company regarding their rights determined in section 3.1. under the title (“Rights of the Data Subject”), their requests shall be answered by our Company within 30 days at the latest following its receipt. However, if a charge is specified by the Board, the cost on the fee schedule specified may be collected.

4.2. INFORMING THE DATA SUBJECT

Pursuant to Article 10 of the PDPL, our Company informs data subjects in accordance with the relevant legislation related to the procedures and principles to be followed for the obligation to inform that needs to be fulfilled by the data controller or by those who are authorized by the data controller.

In this context, our Company informs the persons concerned as to who the personal data is processed by, for what purposes it is processed for and who these data are being transferred to, for which purposes and which methods they are collected, the legal reason of processing and rights of the data subjects have with regards to their personal data.

The following circumstances are considered as exemptions from the obligation to inform:

Article 10 of the Law stipulates the data controller or those who are authorized by the data controller needs inform the data subjects during the processing of their personal data. Therefore, as a rule, those responsible for processing personal data must fulfill their obligation to inform. However, in the event that personal data processing is within the scope of the activities specified in Article 28 of the Law titled “Exceptions”, it is not obligatory to fulfill the obligation to inform. The following circumstances are considered as exceptions to the obligation to inform:

- i. Processing of personal data by natural persons in the course of a purely personal or household activity, provided that obligations relating to data security are complied with and data are not transferred to third parties.
- ii. Processing of personal data for the purposes of official statistics and, through anonymization, research, planning, statistics and similar purposes.
- iii. Processing of personal data for the purposes of art, history, and literature or science, or within the scope of freedom of expression, provided that national defence, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated.
- iv. Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defence, national security, public safety, public order or economic safety.
- v. Processing of personal data by judicial authorities and execution agencies for investigation, prosecution, adjudication or execution procedures.

In this context, a data controller who processes personal data for purposes of research, planning and statistics in the context of official statistics or by making such data anonymous does not need to provide any clarification provided that such obligation is not made only for these data.

While preparing our clarifications texts, the following steps were followed:

- 1. The Data Controller determined and analyzed in detail the types of personal data it processes.
- 2. In accordance with the principles set forth in Article 4 of the Law, the purposes were determined for each personal data that is processed by the data controller, and their purposes were clearly and comprehensibly included in our clarification texts.
- 3. In cases where there is transfer of personal data, the purpose of domestic and international transfer and the transferees (natural persons and/or legal entities) thereof has been stated in the clarification texts.
- 4. Our data controllers determined that they processed personal data on the basis of the processing conditions set out in Articles 5 and 6 of the Law. Such information is also included in our clarification texts.

5. Additionally, our data controllers have completed the necessary works to ensure that the rights of the data subjects determined in Article 11 of the Law are properly stated in these texts.

Furthermore, “Guidelines for the Fulfillment of the Obligation to Inform” published by the Personal Data Protection Authority was used as a reference for when the data subject will be informed and such information has been given in TABLE-2 hereinbelow:

When Personal Data is Obtained Directly from the Person Concerned	When obtaining personal data from the data subject
When Personal Data is not Obtained Directly from the Person Concerned	Within a reasonable period of time from the receipt of personal data
	If personal data will be used for communication with the person concerned, the first time the data subject is contacted
	If personal data will be transferred, when the personal data is transferred for the first time at the latest

5. TRANSFER OF PERSONAL DATA

Our Company is able to transfer the data subject’s personal data and special categories of personal data to third parties (companies, public and private authorities, natural persons) by taking the necessary security measures in accordance with the lawful personal data processing purposes.

5.1. TRANSFERRING PERSONAL DATA DOMESTICALLY

Pursuant to Article 8 of the Law, it is determined that the personal data obtained for processing in accordance with the general principles set forth in the law may be transferred to third parties with the explicit consent of the data subject.

The Law seeks the same conditions in terms of processing personal data and transferring it within the country. This article also specifies the conditions in which personal data can be transferred to third parties without the express consent of the person concerned. However, domestic processing of personal data does not mean that they can be transferred directly without any other condition. In other words, the conditions in Articles 5 and 6 of the Law should be sought separately for the transfer of personal data. In this respect, our Company acts in accordance with the regulations stipulated in Article 8 of the Law.

5.1.1. Transferring Personal Data Domestically, Excluding Special Categories of Personal Data

The conditions under which personal data may be transferred to third parties by taking the necessary care and taking all necessary security measures by our Company including the methods stipulated by the Board are determined as follows:

- i. It is expressly permitted by any law;
- ii. It is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- iii. It is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract;
- iv. It is necessary for compliance with a legal obligation which the controller is subject to;
- v. The relevant information is revealed to the public by the data subject himself/herself;
- vi. It is necessary for the institution, usage, or protection of a right;
- vii. It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

5.1.2. Transferring Special Categories of Personal Data Domestically

The conditions under which special categories of personal data may be transferred to third parties by taking the necessary care and taking all necessary security measures by our Company including the methods stipulated by the Board are determined as follows:

Our Company may transfer special categories of personal data to third parties in line with the principles determined in this Policy and under the following circumstances, provided that all kinds of administrative and technical measures are taken (including methods that may be determined by the Board):

- i. **Special categories of personal data except those concerning health and sexual life**, may be transferred without the data subject's explicit consent, provided that it is clearly stipulated in the laws. Otherwise, the data subject's explicit consent must be obtained.
- ii. **Special categories of personal data relating to health and sexual life**, may only be processed without taking the data subject's explicit consent by people bound by confidentiality due to their occupation or by authorized institutions in order to preserve public health, give medicines, diagnosis, treatments, care, health services and financial planning thereof. Otherwise, the data subject's explicit consent must be obtained.

Contrary to the fact that personal data may only be data related to natural persons, a "data controller" or a "data processor" may be a natural person and a legal person. Any natural or legal person that carries out transactions on personal data is either the data controller or the data processor, according to the purposes and methods of data processing. In this context, our Company acts in accordance with the provisions of Article 8 of the Law for all kinds of data transfer between these two persons.

5.2. TRANSFER OF PERSONAL DATA INTERNATIONALLY

The conditions necessary in order to transfer of personal data abroad according to Article 9 of the Law:

- i. Explicit consent of the data subject
- ii. If the foreign country to whom personal data will be transferred has an adequate level of protection (countries that are considered safe by the Board), the existence of the conditions determined in the Law (the conditions stated in Article 5/2 and 6/3 of the Law)
- iii. In case there is not an adequate level of protection in the foreign country subject to transfer and there are the conditions determined in the Law the conditions stated in Article 5/2 and 6/3 of the Law), the data controllers must undertake in writing to provide an adequate level of protection and obtaining the Board's permission.

The Law seeks the same conditions for processing of personal data and the transfer of such data abroad. Additionally, the Law has determined that additional measures should be taken for the transfer of personal data abroad.

If the person has given explicit consent, it is possible to transfer their personal data abroad. For conditions other than obtaining explicit consent, the Law introduces different provisions for the transfer of personal data abroad, depending on whether there is adequate protection in the country it will be transferred to.

5.1.2. Having Adequate Protection

5.1.2.1. Transfer of Personal Data Other Than Special Categories of Personal Data When There Is Adequate Protection

With due diligence executed by the Company and all necessary security measures taken by the Company, including the methods stipulated by the Board, the conditions under which personal data can be transmitted to third parties in countries that are considered safe by the Board are determined as follows:

- i. The conditions under which the personal data can be transferred to third parties by taking the necessary care and taking all necessary security measures by our Company including the methods stipulated by the Board are determined as follows:
- ii. It is expressly permitted by any law;
- iii. It is necessary in order to protect the life or physical integrity of the data subject or another person where the data subject is physically or legally incapable of giving consent;
- iv. It is necessary to process the personal data of parties of a contract, provided that the processing is directly related to the execution or performance of the contract;
- v. It is necessary for compliance with a legal obligation which the controller is subject to;
- vi. The relevant information is revealed to the public by the data subject himself/herself;
- vii. It is necessary for the institution, usage, or protection of a right;
- viii. It is necessary for the legitimate interests of the data controller, provided that the fundamental rights and freedoms of the data subject are not harmed.

5.1.2.2. Transfer of Special Categories of Personal Data When There Is Adequate Protection

In accordance with the principles determined in this Policy and with the Company taking all necessary security measures, including the methods stipulated by the Board, the conditions under which personal data can be transmitted to third parties in countries that are considered safe by the Board are determined as follows:

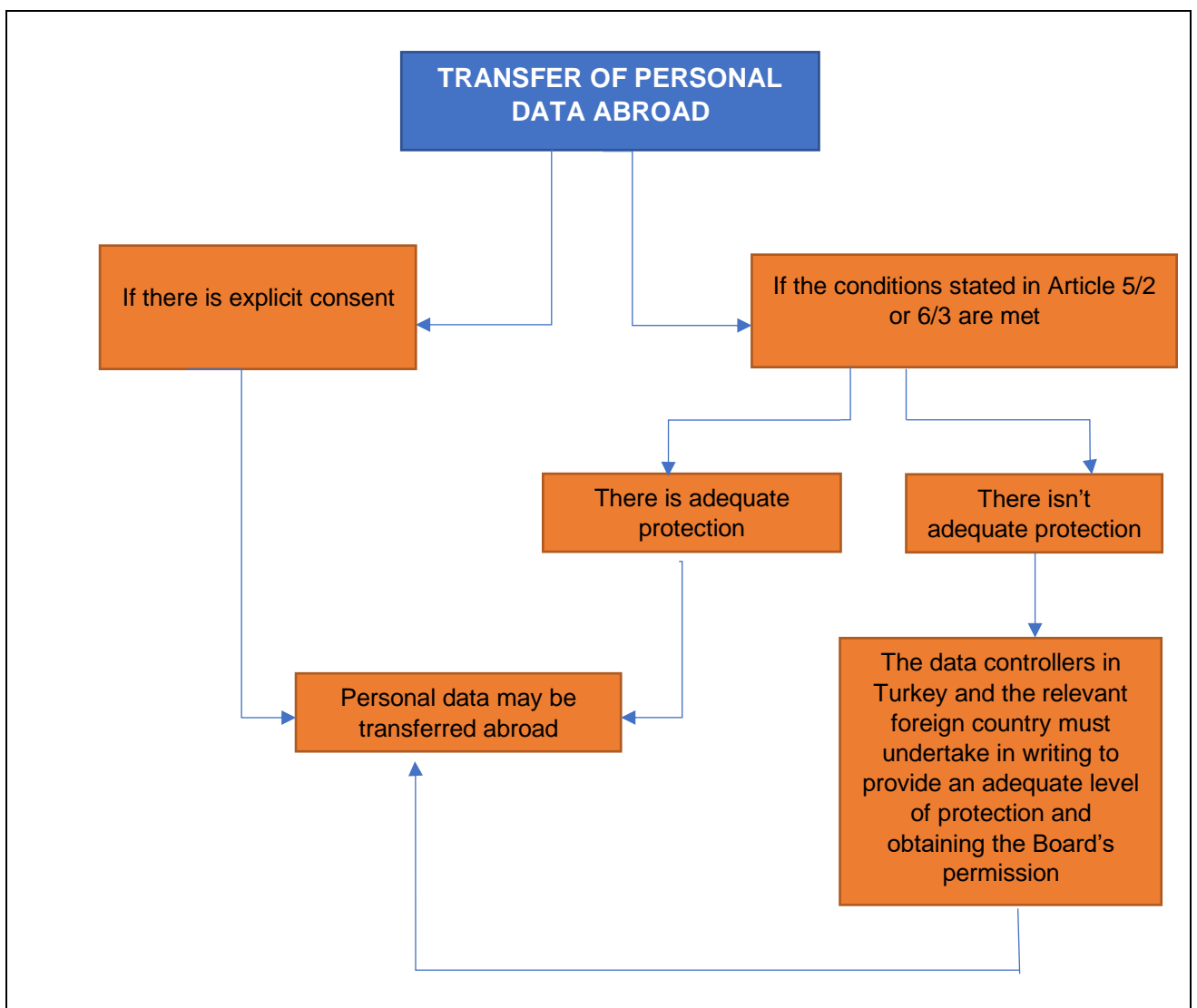
- i. **Special categories of personal data except those concerning health and sexual life**, may be transferred without the data subject's explicit consent, provided that it is clearly stipulated in the laws. Otherwise, the data subject's explicit consent must be obtained.
- ii. **Special categories of personal data relating to health and sexual life**, may only be processed without taking the data subject's explicit consent by people bound by confidentiality due to their occupation or by authorized institutions in order to preserve public health, give medicines, diagnosis, treatments, care, health services and financial planning thereof. Otherwise, the data subject's explicit consent must be obtained.

5.1.3. Personal Data Transfer To Countries That Do Not Have Adequate Protection

The conditions are as follows:

- At least one of the conditions determined in Article 5 or 6 of the Law must be fulfilled.
- The data controllers in Turkey and the relevant foreign country must undertake in writing to provide an adequate level of protection.
- The Board must give permission to do so.

In summary, when transferring personal data to countries abroad, the data controller must act in line with the following table found in the guide published by the Personal Data Protection Authority on its website:



In addition, without prejudice to the provisions of international conventions, if Turkey's or the relevant person's interests will seriously suffer, personal data may transferred abroad with the permission of the Board if the opinion of the relevant public institutions or organization is obtained.

5.2. THIRD PARTIES THAT PERSONAL DATA MAY BE TRANSFERRED TO

Bilgili Holding Group may transfer Personal Data domestically or internationally to the following third parties, who may be natural or legal persons, in accordance with Articles 8 and 9 of the Law, in order to achieve the purposes set out in Article 2.6 of this Policy:

- Consultants
- Audit firms
- Companies who provide services
- Companies it cooperates with
- Customers
- Shareholders
- Suppliers
- Banks and financial institutions
- Judicial and public authorities

In particular, with respect to the hotel business and other businesses that are in contact with customers, the personal data that customers have given explicit consent for them to be shared, may be collected, stored, processed, saved and used by Bilgili Holding Group, in order to communicate with customers and send messages, for the purposes of providing them various advantages, providing them with personal advertisements, promotions, sales, marketing, notifications, membership transactions, customer satisfaction surveys and researches and for fulfilling its legal obligations. Bilgili Holding Group may transfer these personal data to foreign licencees, franchisees and other institutions and organisations it obtains services from, except for the third parties mentioned above for the same purposes, provided that the international regulations and agreements and the local regulations of the relevant countries allow them to do so, and further provided that it is not in contradiction with the Turkish legislation and the provisions of this Policy.

6. STORING AND ANNIHILATING PERSONAL DATA

6.1. RECORDING MEDIUMS OF PERSONAL DATA

Personal data of data subjects are stored safely electronically or physically by Bilgili Holding Group as determined in the table below in accordance with the limits specified in KVKK and other relevant legislation for the purposes determined above and especially in order to (i) carry out its business activities, (ii) fulfill its legal obligations, (iii) determine and fulfill its obligations relating to its employee's rights and benefits, and (iv) manage its relationships with its customers.

STORAGE ENVIRONMENT OF PERSONAL DATA

ELECTRONIC MEANS	NON-ELECTRONIC MEANS
Personal computers (Desktop and laptop)	Manual data records (Surveys, guest books)
Mobile devices	Written, printed, visual, presentation documents
Optical discs	Documents stored in the archive physically
Servers (Web, e-mail, back-up, database, file sharing, exchange)	
Softwares (Office softwares, portals, VERBIS, other software relating to accounting, human resources and accommodation)	
Information security devices (Firewall, intrusion detection and blocking, log files, anti virus, etc.)	
Equipments such as printers, scanners, photocopy machines etc.	

6.2. REASONS TO STORE PERSONAL DATA

Article 3 of the Law defines the processing of personal law, Article 4 of the Law determines that the personal data processing should be executed for specific, explicit and legitimate purposes and Article 5 and 6 of the Law lists the conditions of personal data processing. It is necessary to comply with the general principles of Article 4 of the

Law, the technical and administrative measures to be taken within the scope of Article 12 of the Law, provisions of relevant legislation, Board decisions and personal data storage and annihilation policy when erasing, destructing and anonymising personal data.

Accordingly, within the framework of our Company's activities, personal data is stored for a reasonable period as required by the relevant legislation or in accordance with our processing purposes.

In this context, our Company first determines whether a period is stipulated in the related legislation for the storage of personal data, and if a period is determined, it acts in accordance with this period. If there is no legal term that is determined, personal data is stored for as long as it is necessary for the purpose for which it was processed. Personal data is annihilated at the end of the designated storage periods with the specified annihilation methods (erasure, destruction and/or anonymization) in accordance with the periodic annihilation periods or due to the application of the data subject.

All transactions relating to the erasure, destruction and anonymization of personal data are recorded and these records are kept for at least three years, excluding terms arising from other legal obligations.

The reasons that require storage are as follows:

- i. Storing personal data as they are directly related to the fulfillment or the execution of a contract
- ii. Storing personal data as they are necessary for the establishment, usage or protection of a right
- iii. Storing the personal data is necessary for the legitimate interests of Bilgili Holding Group, provided that the fundamental rights and freedoms of the data subject are not harmed
- iv. Storing personal data in order for Bilgili Holding Group fulfill their legal obligations
- v. Storing personal data is expressly determined in the relevant legislation
- vi. Having explicit consent of data subjects for storing of personal data requiring explicit consent of data subjects

6.3. REASONS TO ANNIHILATE PERSONAL DATA

Pursuant to the Regulation, personal data of data subjects are erased, destructed or anonymized by Bilgili Holding Group ex officio or due to their request in the following cases:

- i. Amendment or abolition of the provisions of the relevant legislation which constitute the basis for processing or storing personal data
- ii. The purpose of processing or storing personal data no longer exists
- iii. In the event that the conditions determined in Article 5 and 6 of the Law that require the processing of personal data in Articles 5 and 6 of the Law no longer exist and it is annihilated at the request of the relevant person or ex officio by the Company
- iv. If the processing of personal data occurs only in accordance with the explicit consent, when the relevant person revoke his/her consent,
- v. In accordance with Article 11 of the Law, within the framework of the rights of the relevant person, its application relating to the request for erasure, destruction or anonymization of his/her personal data is accepted by the data controller
- vi. In the event that the data controller rejects, finds inadequate or does not respond in time to the application made by the data subject relating to the request for erasure, destruction or anonymization of his/her personal data and such data subject complaints to the Board and the Board accepts such application
- vii. Although the maximum period determined for storage of personal data has elapsed, there is no longer a reason to justify storing personal data for a longer period of time

6.4. STORAGE AND ANNIHILATION TERMS RELATING TO PERSONAL DATA

The following criteria are used in order to determine the storage and annihilation periods of personal data obtained by Bilgili Holding Group in accordance with the PDPL and other relevant legislation:

- 1. If the legislation stipulates a period for storing the personal data, this period shall be abided by. Following the expiry of the said period, personal data shall be processed within the scope of the following second paragraph.
- 2. In the event that the period foreseen in the legislation for the storage of personal data expires or if there is no provision for the storage of the said data in the relevant legislation;
 - i. Personal data are classified into two main categories: personal data and special categories of personal data (as per its definition stated in Article 6 of the PDPL). All personal data that are special categories of personal data are annihilated. The method to be used for the annihilation of such data is determined according to the importance of the data and its storage by Bilgili Holding Group.

- ii. The compliance of the personal data storage with the principles specified in Article 4 of the PDPL is examined such as whether the Bilgili Holding Group has a legitimate aim in storing data. Personal data stored which is found to be in contradiction with the principles stated in Article 4 of the PDPL are erased, destroyed or made anonymous.
- iii. It is determined which of the exceptions stipulated in Articles 5 and 6 of the PDPL are within the scope of the personal data storage. Within the framework of the exceptions identified, reasonable periods of time are determined for the personal. If such periods expire, personal data are erased, destroyed or made anonymous.

Personal data whose storage period has expired shall be annihilated in accordance with the procedures set forth in this Policy within 6 month terms within the framework of the “Storage and Annihilation Periods” annexed to this Policy (ANNEX-2). If separate annihilation periods are required for Bilgili Holding Group companies, these periods shall be announced on the website of that Bilgili Holding Group company or at the headquarters of the same Bilgili Holding Group company.

All transactions concerning the deletion, destruction and anonymization of personal data are recorded and the records are kept for at least three years, excluding those kept for other legal obligations.

6.5. ANNIHILATION PROCEDURES RELATING TO PERSONA DATA

In the event that the personal data processing purposes listed in the Law and Regulation no longer exist, personal data, obtained by Bilgili Holding Group in accordance with the PDPL and other relevant legislation, are deleted ex officio or with the application relating to the request of the Relevant Person by Bilgili Holding in compliance with the Law and the relevant legislation with the following techniques determined hereinbelw.

6.5.1. ERASURE AND DESTRUCTION TECHNIQUES RELATING TO PERSONAL DATA

The procedures and principles regarding the erasure and destruction of personal data by Bilgili Holding Group are as follows:

ERASING PERSONAL DATA:

Secure Erasure from Softwares: When erasing personal data processed in fully or partially automated ways and stored in digital mediums, methods for deleting data from the respective software are rendered in such a way that they are inaccessible and no longer available to the respective users.

The following acts will be considered as erasure: deleting relevant personal data found the cloud system by giving a “delete” command, removing the user's access rights on the relevant file or directory on the central server, deleting the relevant roles in databases by using database commands, deleting the data in portable medias (i.e. flash media) by using appropriate software.

However, provided that the deletion of personal data will result in inaccessibility of other data in the system and inability to use such data, archived personal data shall also be deemed deleted if the personal data cannot be traced back to the relevant person (i.e. anonymized) provided that the following conditions are met:

- Personal is not accessible to any other institution, organization or person,
- All necessary technical and administrative measures are taken to ensure access to personal data only by authorized persons.

Secure Erasure by an Expert: In some cases, the Company may agree with an expert to erase personal data on its own behalf. In this case, personal data are securely deleted by the person skilled in this profession in such a way that they are inaccessible and no longer available to the respective users.

Removing Personal Data Found Physically (On Paper): It is a method of physically cutting out or removing or crossing-out the relevant personal data from the document so it is unreadable, even with technological solutions, to prevent them from being used for these data to not be used other than their purpose or for erasure due to the request of the data subject.

DESTRUCTING PERSONAL DATA:

De-magnetization: It is a method of corruption data on magnetic media by passing them through special devices that will be exposed to high magnetic fields for the data to be unreadable. It should be noted that if the destruction by this method is not successful, the data can only be destructed physically.

Physical Destruction: Personal data can also be processed in non-automated ways, provided that it is part of any data recording system. When destroying such personal data, a system of physical destruction of personal data is implemented in such a way that it cannot be used after the destruction process. Destruction of data on found paper and microfiche media should also be done in this way since they cannot be destroyed in any other way.

Overwriting: Overwriting is a method of destroying data that makes it impossible to read or recover old data by writing random data of 0 and 1 at least seven times over magnetic media and rewritable optical media via special software.

During these aforementioned matter, Bilgili Holding Group fully complies with the provisions of the and the PDPL, the Regulation and other relevant legislation in order to ensure data security and takes all necessary administrative and technical measures.

6.5.2. ANONYMIZING TECHNIQUES RELATING TO PERSONAL DATA:

The procedures and principles regarding the anonymization of personal data by Bilgili Holding Group are as follows:

Anonymous Valuation Methods that provide Value Irregularity: The methods of anonymization that provide value irregularities are made without any change, addition, subtraction of the stored personal data. These are the methods of anonymization by generalizing, replacing, or removing a particular group of data or sub-data from any group of personal data.

Variable Subtraction: After the descriptive personal data is extracted, those that have a “high-grade descriptor” are removed from the variables formed by the data gathered and the current data set is made anonymous.

Removing Records: In the recording method, the data containing singularity are removed from the records and the stored data is made anonymous. For example, if there is only one senior manager in a company, the data belonging to that person can be made anonymous by removing data that employees at the same level might have such as seniority, salary and gender.

Partial Secretion: In the partial secretion method, hiding the relevant personal data provides anonymisation if a single data has a defining characteristic as a combination is made for the data to be less visible. For example, if only one person in a company's football team's reserve list is 65 years old, and such data is stored with personal data relating to gender and health, writing “Unknown” instead of “Age:65” or leaving such section blank will provide anonymization.

Coding Lower and Upper Limits: Coding lower and upper limits method helps to anonymize personal data by combining the values in the data group containing predefined categories by defining a certain criterion.

Generalization: With the data aggregation method, many data are generalized and thus, such personal data cannot be associated with any person.

Global Coding: With the data generating method, a more general content is created for personal data and thus, it ensures that personal data cannot be associated with any person.

ANONYMIZATION METHODS THAT PROVIDE VALUE IRREGULITY:

Unlike those that do not provide value irregularities, in anonymization methods that provide value irregularities create distortions by changing some data in the personal data groups. When using these methods, deviations will need to be applied with caution and in line with the expected benefit. It is possible to continue to provide the expected benefit from the data by ensuring that the total statistics are kept intact.

Adding Noise: This method is made anonymous by adding a certain amount of deviations to the existing data in a determined plus or minus direction, especially in a dataset where numerical data are predominant. For example, in a data group (+/-) with weight values, 3 kg deviation is prevented from displaying actual values and the data is anonymized. Deviation is applied equally to each value.

Micro Merge: In the micro merge method, all data are first divided into groups by ordering them in a meaningful order (such as big to small), and the mean value of the groups will be anonymized by replacing the relevant data in the current group. For example, for salary information; If two groups of less than or equal to 10,000 TL are made, the sum of the salaries of persons receiving salaries of 10,000 TL or less is divided by the number of persons and the value obtained in the salary set of all persons receiving salaries of less than 10,000 TL shall be seen.

Data Exchange: In the data exchange method, the values of a variable are exchanged between each of the pairs selected from the data stored. In this method, which is generally used for data that can be categorized, the aim is to transform the database by exchanging the data of the data owners with each other.

Pursuant to Article 28 of the PDPL, if personal data are processed anonymously with official statistics for research, planning and statistics purposes, this will be outside the scope of the Law and no explicit consent will be required.

6.6. PERIODIC ANNIHILATION TERM REGARDING PERSONAL DATA

In line with Article 11 of the Regulation, our Company has determined the annihilation period as 6 month terms. Accordingly, periodic annihilation is carried out every June and December.

6.7. DISTRIBUTION OF TASKS AND RESPONSIBILITY REGARDING THE STORAGE AND ANNIHILATION OF PERSONAL DATA

All units and employees of the Company are required to implement the technical and administrative measures taken by the responsible persons in the department within the scope of the Policy, increase and monitor the training and awareness of every employee in the relevant department, monitor and control the personal data in accordance with the law, prevent the unlawful access to personal data and prevent the unauthorized access to personal data. Furthermore, the Company actively supports the departments for taking technical and administrative measures to ensure data security in all environments where personal data is processed in order to ensure proper storage. The title, duty and responsibility details of the persons involved in the storage and annihilation of personal data are provided in Annex-3.

7. ENFORCEMENT DATA AND UPDATE OF THE POLICY

This policy contains information in accordance with the Law and other legislation on personal data and will enter into force on the date of its publication on the www.bilgiliholding.com website. The policy may be updated from time to time due to legal amendments, changes to the Bilgili Holding Group's personal data processing purposes or for other reasons.

Updates will be effective as of the date of publication of the new updated Policy on the Website. The Policy (Version 1.0) was executed by Bilgili Holding and had entered into force on April 6, 2018 has been renewed as version 2.0 of the Policy.

This Policy is published on Bilgili Holding's website at www.bilgiliholding.com and made available to the data subjects.

ANNEX-1

BILGILI HOLDING GROUP DATA SUBJECT APPLICATION FORM

1. APPLICATION METHOD

If you have a request concerning your rights as defined in Article 11 of the Personal Data Protection Law numbered 6698 (“Law”), you can fill out this form to submit it to Bilgili Holding Group, as per Article 13 of the Law and Article 5 of the Communiqué on the Procedures and the Principles of Application to Data Controllers.

	APPLICATION METHOD	COMPANY'S ADDRESS	DETAILS TO MARK ON THE FORM
1. Hard Copy Application	Personal application with wet signature, given in person, with registered letter or sent via a notary public	Bilgili Holding Group Sair Nedim Cad. No:20 K:6 Besiktas/Istanbul	The following statement should be written on the envelope/notification: “Request for Information in the Context of Personal Data Protection Law”
2. Application via E-mail	By sending an e-mail	mersis@bilgiliholding.com	The subject line should read: “Request for Information in the Context of Personal Data Protection Law”

2. Your ID and Contact Details

Please fill in the section below to enable us to contact you and to verify your identity:

Name and Surname:	
Turkish Republic Citizenship Number, or for foreign nationals: Passport Number or ID Card Number:	
Residential Address/Work Address:	
Mobile Phone Number:	
Landline Number:	
E-Mail Address:	

3. Your Status in Relation to the Company

Customer

Vistor

Employee

Former Employee

Other (please specify):

4. Request Details

Please explain your request clearly. Any documents related to the matter should be attached to the application.

5. Please Select a Reply-To-Address

Please reply to my residential / workplace address which I have indicated under item 2 above.

Please reply to my e-mail address which I have indicated under item 2 above.

I kindly request that you assess my application as per Article 13 of the Law and that you let me know the outcome.

I hereby acknowledge, declare and undertake that the information and the documents I supplied with this application are true and up-to-date, I understand that the school may ask for additional information to reach a conclusion about my request, and that in the case any extra charges occur, I have been informed that I may have to pay the amount set by the Personal Data Protection Board.

Applicant's (Data Subject's):

Name-Surname:

Application Date:

Signature:

ANNEX-2

TABLE REGARDING STORAGE AND ANNIHILATION TERMS RELATING TO PERSONAL DATA

PROCESS	STORAGE TERM	ANNIHILATION PERIOD
Planning and execution of corporate communication activities	10 years following the termination/expiry of the business relationship	Within 30 days of the data subject's application regarding the request for annihilation
General assembly procedures	10 years	180 days following the expiry of the storage term
Responding to courts and enforcement officer requests regarding information of personnel	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Execution of contracts	10 years	180 days following the expiry of the storage term
Employment	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Payroll	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Organization of personal health and personal accident insurance policies	1 year	180 days following the expiry of the storage term
Allocating vehicles to employees	1 year	180 days following the expiry of the storage term
Occupational health and safety practices	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Log / Recording / Tracking Systems	2 years	180 days following the expiry of the storage term
Master data generation processes	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Information on the Company's shareholders and board members	10 years	180 days following the expiry of the storage term
Payment procedures	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Customer information	10 years	180 days following the expiry of the storage term
Contract process and the maintenance of the contract	10 years following the termination/expiry of the business relationship	180 days following the expiry of the storage term
Reporting accidents	10 years	180 days following the expiry of the storage term
Sharing meeting minutes with participants	10 years	180 days following the expiry of the storage term
Preparing documents	10 years	180 days following the expiry of the storage term
Filing training records	10 years	180 days following the expiry of the storage term
Emergency Preparations	1 year	180 days following the expiry of the storage term
Lease Agreements	10 years	180 days following the expiry of the storage term

ANNEX-3

DISTRIBUTION OF TASKS AND RESPONSIBILITY REGARDING THE STORAGE AND ANNIHILATION OF PERSONAL DATA

TITLE	DUTY	RESPONSIBILITY
Assistant General Manager - Legal Affairs	Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Human Resources Director	Human Resources Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
IT Director	IT Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Financial Director	Finance Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Director of Operations	Operations and Administrative Affairs Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Sales Manager	Sales and Marketing Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Purchasing Manager	Construction Department - Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Hotel's General Manager	Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period
Dorm Manager	Responsible for implementing personal data storage and annihilation policy	Management of the personal data annihilation process in accordance with the periodic annihilation perioda and ensuring compliance of the processes within the task with the storage period