



PERSONAL DATA POLICY

Version I

Table of Contents

- I. Definitions..... 3
- II. Purpose..... 3
- III. Scope and Changes..... 3
- IV. Principles for processing personal data..... 4
 - a. Processing in compliance with the law and the rules of integrity..... 4
 - b. Restriction proportional to the purpose of processing..... 4
 - c. Transparency and Clarification..... 4
 - d. Personal Data reduction and data economy 4
 - e. Deletion of personal data 4
 - f. Accuracy and up-to-dateness..... 4
 - g. Privacy and data security 4
- V. Reasons for processing personal data..... 5
 - a. Principles regarding the processing of personal data belonging to customers and business partners 5
 - Data processing for contractual relationship..... 5
 - Data processing for advertising purposes..... 5
 - Data transactions made due to our legal obligations or expressly stipulated by law..... 5
 - Principle of legitimate interest in the processing of personal data..... 5
 - Processing of sensitive personal data 5
 - Data processed exclusively through automated systems 5
 - User information and Internet 5
 - b. Principles regarding the processing of personal data of employees 6
 - Data transactions that are expressly stipulated in law and carried out due to legal obligations 6
 - Processing of data in accordance with legitimate interest..... 7
 - Processing of sensitive personal data 7
 - Data processed exclusively through automated systems 7
 - Telecommunications and Internet 7
- VI. Principles of Transferring Personal Data 8
- VII. Data Owner’s Rights 8
- VIII. Privacy..... 9
- IX. Security..... 9
- X. Controls and Audits..... 9
- XI. Data breach management 9
- XII. Obligation for Registration to Data Controllers Registry..... 10

I.Definitions

Explicit Consent	Consent that is related to a specific issue, based on information and expressed with free will.
Anonymizing	To render data in such a way that it can no longer be associated with an identified or identifiable person, even when the personal data is matched with other data
Personal Data	All information related to a real person whose identity is known or could be identified.
Sensitive Personal Data	Biometric and genetic information concerning race; ethnicity; political opinions; philosophical opinions; religion, sect or other beliefs; appearance; subscriptions to associations, foundations or unions; health; sex life; convictions; and data concerning security measures.
Processing of Personal Data	Any kind of transaction performed on the data such as obtaining, saving, storing, protecting, modifying, editing, describing, transferring, receiving, making available, classifying or blocking the use of the personal data in fully or partially automated or non-automated ways, provided that it is part of any data recording system.
Council	Personal Data Protection Council
Policy	MİDAS PAZARLAMA VE DIŞ TİCARET ANONİM ŞİRKETİ Personal Data Protection and Processing Policy
Data Processor	A natural and legal person who processes personal data on behalf of the data controller based on his/her authorization
Data Controller	The person who defines the purpose and the means of processing personal data and who is responsible for the management of the data recording system where data is kept systematically.

II.Purpose

As we, MİDAS PAZARLAMA VE DIŞ VE TİCARET ANONİM ŞİRKETİ having its registered address at Molla Fenari Mahallesi, Şerefefendi Sokak, No: 36, Fatih/İstanbul and being registered under the MERSIS No. 0387004540500017 ("FİGARO"), are the data controller as per Law No. 6698 on the Protection of Personal Data ("KVKK") promulgated in Official Gazette No. 29677 dated 7 April 2016, the purpose of this policy is to regulate the methods and principles to be adopted in ensuring compliance with the liabilities imposed on data controllers under the relevant law.

III.Scope and Changes

This Policy, which is prepared in accordance with KVKK, applies to all personal data of our current and potential customers and employees, as well as employees, shareholders, and officials of the institutions with which we cooperate, and third parties, processed through automated means or

non-automated means provided that they are part of any data registry system. FİGARO reserves the right to make changes in the Policy in line with the amendments to be made in the KVKK and related regulations.

IV.Principles for Processing Personal Data

FİGARO has adopted the following principles in collecting, processing, and analyzing personal data.

a. Processing in Compliance with the Law and the Rules of Integrity

FİGARO will collect and process personal data lawfully and fairly in order to protect the rights of data owners. The principles of proportionality and necessity will be considered in the execution of these activities.

b. Restriction Proportional to the Purpose of Processing

Personal data can only be processed for the specified purposes before data is collected. Additional changes to the purpose are only possible to a limited extent and with justification.

c. Transparency and Clarification

Data owners should be informed in detail before their personal data is collected and processed. Prior to data collection, beneficiaries should be informed of the following:

- The identity of the data controller and its representative, if any
- Purpose of processing personal data
- Parties that personal data provided to and purpose of transfer
- Method and legal grounds for the collection of personal data,
- The rights of the person, whose personal data is processed, in accordance with Article 11 of KVKK.

d. Data Economy

Prior to the processing of personal data, it is necessary to determine whether and to what extent it is necessary to achieve the purpose. Anonymous or statistical data can be used if the purpose is acceptable and proportional.

e. Deletion of Personal data

After the expiry of the periods stipulated in the relevant laws for record-keeping obligations and proof-keeping procedures, personal data that is no longer required are deleted or destroyed or made anonymous.

f. Accuracy and Up-to-Dateness

Personal data must be accurate, complete and up-to-date if known. Inaccurate or missing data should be deleted, corrected, completed, or updated.

g. Privacy and Data Security

Personal data should be stored and kept as confidential information. Personal Data should be protected and kept confidential on a personal level by taking the necessary administrative and technical measures to prevent unauthorized access, unlawful transactions, sharing, accidental loss, alteration, or destruction.

V.Reasons for Processing Personal Data

Collection and processing of personal data will be carried out for the purposes set out in the Clarification Text and below.

a. **Customer and Business Partners Data**

- **Data processing for contractual relationship:** Personal data of existing and potential customers and business partners (in case the business partner is a legal entity) can be processed for the establishment, implementation, and termination of a contract without further approval. During the contracting phase prior to the contract, personal data can be processed to prepare an offer, purchase form, or to meet the data owner's requests for the execution of the contract. In the process of contract preparation, data owners can be contacted in the light of the information they provide.
- **Data processing for advertising purposes:** Personal data is processed for advertising or market and public opinion researches, provided that the purpose of collecting this information is compatible with the specified purposes. Data owners are informed that their information will be used for advertising purposes. Data owners may refrain from providing or consenting to the processing of data that is reported to be used for advertising purposes. Explicit consent of the data owner is required for data to be processed for advertising purposes. In this respect, data controller can obtain the explicit consent of the data owner via electronic approval, mail, e-mail, or telephone. The use of personal data for advertising purposes is prohibited without the explicit consent of the data owner.
- **Data transactions made due to our legal obligations or expressly stipulated by law:** Personal data may be processed without further approval if the processing is clearly stated in the applicable legislation or for the fulfillment of a legal obligation stipulated by the legislation. The type and scope of data processing should be required for legally permitted data processing and must comply with the applicable legal provisions.
- **Principle of legitimate interest in the processing of personal data:** Personal data may also be processed without further approval when it is necessary for a legitimate interest of FIGARO. Legitimate interests are generally legal interests.
- **Processing of sensitive personal data:** Sensitive personal data are processed in accordance with the provisions of KVKK provided that adequate measures are taken by the Council. Except for the health and sexual life of the personal data owner, sensitive personal data are processed with the explicit consent, and in the absence of explicit consent, within the scope of the exceptions stipulated in KVKK. Personal data relating to the health and sexual life of individuals is provided by persons who are under the obligation of confidentiality or competent public institutions and organizations for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.
- **Data processed exclusively through automated systems:** The processing of personal data obtained through automated systems shall not justify and legitimate the use of such data in business or transactions that adversely affect the personal data owner. The personal data owner has the right to object to the occurrence of a result against the person himself/herself due to the analysis of the data processed exclusively through automated systems. FIGARO will endeavor to take the necessary measures in accordance with the request of the personal data owner.
- **User information and Internet:** If the personal data are collected, processed, and used on the website or applications, users who are the personal data owners should be informed about the use of the information they have stored on the site, privacy statement,

and cookies. Privacy statement and cookie information are integrated in an easily identifiable, directly accessible, and continuously available way for the related person.

b. Principles regarding the processing of personal data of employees

It is obligatory to collect and process personal data of the employees in the process of the establishment, execution, and termination of the employment contract. Explicit consent of employees may not be obtained for such transactions. Personal data of potential employee candidates are also processed in job applications. In case the candidate's job application is rejected, the personal data obtained during the application is stored during the appropriate data storage duration for a later selection phase and is deleted, destroyed, or anonymized at the end of this period. The following principles should be considered in the processing of personal data of employees.

- **Data transactions that are expressly stipulated in law and carried out due to legal obligations:** Personal data of the employee data can be processed without prior approval if the processing is clearly stated in the relevant legislation or in order to fulfill a legal obligation stipulated by the legislation.
- **Processing of data in accordance with legitimate interest:** Personal data of the employees can be processed without further approval where FIGARO has a legitimate interest. Legitimate interests are generally legal or economic interests. In personal cases where it is necessary to protect the interests of the employees, personal data may not be processed for legitimate interests. Before data is processed, it must be determined whether there are interests that require protection. If the data of the employees are processed based on the legitimate interest of FIGARO, it should be examined whether this processing is proportional and whether the legitimate interest does not violate the right of the employee to be protected.
- **Processing of sensitive personal data:** Sensitive personal data are processed only under certain conditions. Such data is defined as follows: biometric and genetic information concerning race; ethnicity; political opinions; religion; philosophical opinions; sect or other beliefs; appearance; subscriptions to associations, foundations or unions; health; sex life; convictions; and data concerning security measures. FIGARO processes these Sensitive Personal Data that are necessary to be processed for the continuation of the business to a limited extent by obtaining the consent of the data owners. Sensitive personal data can only be processed if the employee has provided explicit consent and by taking the necessary administrative and technical measures. The following cases constitute the exception to this provision and in such cases, personal data may be processed even if the employee does not have explicit consent.
 - Sensitive personal data except the health and the sexual life of the employee can be processed in cases stipulated by the law,
 - Sensitive data relating to the health and sexual life of the employee can be processed by persons who are under the obligation of confidentiality or competent public institutions and organizations for the purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment and nursing services, planning and management of health-care services as well as their financing.
- **Data processed exclusively through automated systems:** If personal data belonging to employees are processed exclusively through automated systems as a part of the business relationship, the employee has the right to object to result against the person himself/herself that is produced through a fully automated processing of these personal data.

- **Telecommunications and Internet:** Telephone equipment, e-mail addresses, intranet and internet along with internal social networks are provided by FİGARO primarily for work-related assignments. They are a tool and resource belonging to FİGARO. They should be used within the applicable legal regulations and FİGARO's internal regulations. There is no general monitoring of telephone and e-mail communications or intranet/internet use. To defend against attacks on the IT infrastructure or individual users, protective measures are taken for the connections to the network used by FİGARO that block technically harmful content or analyze the attack patterns. For security reasons, the use of telephone equipment, e-mail addresses, the intranet/internet and/or internal social networks can be blocked for a temporary period. Evaluations of this data from a specific person can be made only if there is a concrete suspicion. The evaluations can be conducted by relevant departments provided that the principle of proportionality is met.
- **Prohibition of Access:** FİGARO makes maximum efforts to process, protect, and maintain personal data, which are collected in accordance with legal obligations and legitimate interests by obtaining the explicit consent of its employees, in accordance with their purpose of collection, and only shares personal data with relevant employees. Regarding the jobs performed by employees within the scope of their job descriptions and any works and transactions they perform regarding data without access permission or need for access in cases where FİGARO does not have explicit written authorization, the relevant employee will be held personally responsible and legal measures will be taken. Therefore, employees should be provided with regular training on the unlawful disclosure and sharing of personal data, and disciplinary process should be established in case the employees do not comply with the security policies and procedures.

VI. Transfer of Personal Data

Transfer of personal data to third parties outside FİGARO will be carried out for the purposes set out in the Clarification Test and below. Accordingly, FİGARO may transfer personal data to the following persons and institutions for certain purposes;

- to FİGARO's business partners limited to ensure the fulfillment of the objectives of establishing a business partnership,
- to the suppliers of products and services that FİGARO provides externally, who provide the products and services necessary to perform its commercial activities,
- to FİGARO subsidiaries limited to ensure the execution of commercial activities that require the participation of FİGARO subsidiaries
- to FİGARO shareholders limited to the design of the strategies regarding the commercial activities of FİGARO in accordance with the provisions of KVKK and the audit purposes,
- to legally authorized public institutions and organizations limited to the purpose requested by the relevant public institutions and organizations within their legal authority,
- to legally authorized private law persons limited to the purpose requested by the relevant private law persons within their legal authority.

The personal data processed by FİGARO can be transferred to foreign countries if the data owner has provided explicit consent, or there are exceptions specified in Articles 5/2 or 6/3 of KVKK, or the country to which data will be transferred is among the safe countries to be announced by the Council, or the data controllers in Turkey and the relevant foreign country undertake in writing that adequate protection will be ensured and the Council has given permission in the absence of adequate protection in the country to which the data transfer will be made.

VII. Data Owner's Rights

Personal Data Owners shall have the right

- to learn whether their personal data are processed or not,
- to request information if his/her personal data is processed,
- to learn the purpose of his/her data processing and whether this data is used for intended purposes,
- to know the third parties to whom his/her personal data is transferred at home or abroad,
- to request the rectification of the incomplete or inaccurate data, if any, and to request reporting of the operations carried out pursuant to subparagraphs (d) and (e) to third parties to whom his/her personal data have been transferred,
- to request the deletion or destruction of personal data, despite being processed in compliance with the provisions of this Law and other relevant laws, in the event that the reasons for the processing no longer exist and to request reporting of the operations carried out in this regard to third parties to whom his/her personal data have been transferred,
- to object to the occurrence of a result against the person himself/herself due to the analysis of the data processed exclusively through automated systems, and
- to request compensation for the damage arising from the unlawful processing of his/her personal data.

If FIGARO receives such a request, it must be answered within the specified time period. For this reason, FIGARO will provide the necessary information to the data owners about the exercise of the rights mentioned above and the assessment method of the requests.

The exceptions to the above rights granted to personal data owners in the KVKK are listed below. In such cases, FIGARO has no obligation to answer requests coming from data owners:

- Personal data is processed for the purpose of official statistics and for research, planning and statistical purposes after having been anonymized,
- Personal data is processed with artistic, historical, literary or scientific purposes, or within the scope of freedom of expression provided that national defense, national security, public security, public order, economic security, right to privacy or personal rights are not violated or they are processed so as not to constitute a crime,
- Personal data is processed within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations duly authorized and assigned to maintain national defense, national security, public security, public order or economic security, and
- Personal data is processed by judicial authorities or execution authorities with regard to investigation, prosecution, criminal proceedings, or execution proceedings.

Pursuant to the KVKK, the persons concerned cannot claim their other rights, except for the right to claim the damages, in the following cases:

- Personal data processing is required for the prevention of a crime or crime investigation.
- Personal data processing is carried out on the data which is made public by the data subject himself/herself.
- Personal data processing is required for inspection or regulatory duties and disciplinary investigation and prosecution to be carried out by the public institutions and organizations and by professional associations having the status of public institution, assigned and authorized for such actions, in accordance with the power conferred on them by the law.
- Personal data processing is required for the protection of the State's economic and financial interests with regard to budgetary, tax-related, and financial issues.

Personal data owners can send their requests regarding the rights mentioned above, by filling in and signing the Personal Data Application Form available at our website (www.figaro.com.tr) and posting the original version to FİGARO (Molla Fenari Mahallesi, Şerefefendi Sokak, No:36, Fatih/İstanbul) by hand or by registered letter with photocopies of their identity cards. For applications made by the personal data owner on behalf of a person other than himself/herself, he/she must have a power of attorney duly issued by the right holder. FİGARO may request additional information from the relevant person in order to determine whether the applicant is personal data owner, and may ask questions of the personal data owner regarding their application to clarify issues in their application.

FİGARO will conclude the request free of charge as soon as possible and within thirty (30) days at the latest, depending on the nature of the request.

VIII. Privacy

Personal data is subject to data secrecy. Any unauthorized collection, processing, or use of such data by employees is prohibited. Unauthorized use is unauthorized data processing that employees perform outside their legitimate duties. The “need to know” principle applies. Employees may have access to personal data only if it is appropriate for the type and scope of the task in question.

Employees are prohibited to use personal data for private or commercial purposes, to disclose it to unauthorized persons, or to make it available in any other way. Supervisors must inform their employees about the obligation to protect data secrecy at the start of the employment relationship. This obligation shall remain in force even after employment has ended.

IX. Processing Security

FİGARO takes the necessary measures and controls to ensure the appropriate level of security to prevent personal data from being processed and accessed illegally and to ensure the protection of the data, and carries out the necessary audits or has them being carried out. This applies regardless of whether data is processed electronically or in paper form. Before the introduction of new methods of data processing, particularly new IT systems, technical and organizational measures to protect personal data must be defined and implemented. These measures are based on the state of the art, the risks of processing, and the need to protect the data which is determined by the process for information classification. The technical and organizational measures for protecting personal data are part of company's information security management and are adjusted continuously to the technical developments and organizational changes.

X. Controls and Audits

Compliance with the Personal Data Protection and Processing Policy and KVKK is checked regularly with data protection audits and other controls.

XI. Data Breach Management

FİGARO shall immediately implement the security measures necessary for the protection of personal data seized in contradiction with the provisions of this Policy and KVKK and shall notify the relevant person and the Council as soon as possible. For this purpose, FİGARO is responsible for establishing systems and application methods that enable personal data owners to communicate their requests and complaints regarding their personal data in the most effective way and within the shortest time possible. If deemed necessary by the Council, this may be announced on the Council's website or by any other means.

XII. Obligation for Registration to Data Controllers Registry

As per Article 16 of KVKK, FİGARO was registered to the Data Controllers Registry. Accordingly, the information and documents submitted to the Council for registration are as follows:

- identity and address of FİGARO and of its representative, if any,
- purposes for which the personal data will be processed,
- explanations about group(s) of personal data owners as well as about the data categories belonging to these people,
- recipients or groups of recipients to whom the personal data may be transferred,
- personal data which is envisaged to be transferred abroad,
- measures taken for the security of personal data, and
- maximum period of time required for the purpose of the processing of personal data.