**Protection of Personal Data and Privacy Statement**

Contents

[**ABOUT AKKİM** 2](#_Toc8057055)

[**OUR PRINCIPLES FOR PROCESSING PERSONAL DATA** 2](#_Toc8057056)

[**DATA OWNER CATEGORIES** 3](#_Toc8057057)

[**WHEN DO WE GATHER PERSONAL DATA ABOUT YOU?** 4](#_Toc8057058)

[**WHICH PERSONAL DATA DO WE PROCESS ABOUT YOU?** 4](#_Toc8057059)

[**PROCESSING PERSONAL DATA OF EMPLOYEE CANDIDATES** 6](#_Toc8057060)

[**OUR POLICY ON COOKIES** 6](#_Toc8057061)

[**PROCESSING THE PERSONAL DATA OF OUR VISITORS AT OUR OFFICES AND FACTORIES** 7](#_Toc8057062)

[**PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING** 7](#_Toc8057063)

[**FOR WHAT PURPOSES WE USE YOUR PERSONAL DATA?** 8](#_Toc8057064)

[**HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING PURPOSES?** 10](#_Toc8057065)

[**FOR WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?** 10](#_Toc8057066)

[**WHEN DO WE SHARE YOUR PERSONAL DATA?** 12](#_Toc8057067)

[**SOCIAL PLUGINS** 14](#_Toc8057068)

[**HOW LONG DO WE KEEP YOUR PERSONAL DATA?** 15](#_Toc8057069)

[**HOW DO WE DESTROY YOUR PERSONAL DATA?** 1](#_Toc8057070)6

[**HOW DO WE PROTECT YOUR PERSONAL DATA?** 24](#_Toc8057071)

[**HOW DO WE PROTECT YOUR SENSITIVE PERSONAL DATA?** 27](#_Toc8057072)

[**WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?** 28](#_Toc8057073)

[**WHAT ARE THE SITUATIONS WHERE DATA OWNERS CANNOT CLAIM THEIR RIGHTS?** 29](#_Toc8057074)

[**OTHER ISSUES** 30](#_Toc8057075)

[**ANNEX – ABBREVIATIONS** 32](#_Toc8057076)

As Akkim, we attach importance to the privacy and security of your personal data. In this context, while conducting our business relations, we would like to inform you about how we process personal data belonging to our customers, suppliers, business partners, their employees and officials and all other third parties, for what purposes we use them and how we protect this information.

All concepts and expressions used in this notification shall express the meaning attributed to them in the Personal Data Protection Law No.6698 ("**PDPL**") and other legislation. The term "you" in this Notification refers to your person. The term personal data is used to include sensitive personal data. The meanings expressed by the terms and abbreviations in the policy is included in the Annex - Abbreviations.

We would like to remind you that if you do not accept the notification, you should not transmit your personal data to us. If you choose not to transmit your personal data to us, in some cases, it will not be possible for us to offer our services to you or to answer your requests or we will not be able to provide the full functionality of our services.

We would like to remind you that it is your responsibility to ensure that the personal data you transmit to our company are accurate, complete and up to date as far as you know. Beyond that, if you share other people's data with us, it will be your responsibility to collect such data in accordance with local legal requirements. In this case, it will mean that you have obtained all necessary permissions from that third party for us to collect, process, use and disclose their information and our Company will not be held responsible in this context.

# **ABOUT AKKİM**

Ak-Kim, Turkey's leading chemicals manufacturer, was established in Yalova in 1977 and has expanded its production activities in many different areas in the past 40 years. is a chemical company serving its customers in six continents with a wide range of products including chlor-alkali and derivatives, peroxides, methylamines, persulfates, bisulfites, textile auxiliaries, paper and water treatment chemicals and concrete additives.

The expressions "we" or "Company" or "Akkim" in the notification relates to personal data processing activities carried out by Ak-kim Kimya Sanayi ve Ticaret A.Ş (“**Akkim**”), operating in Miralay Şefik Bey Sok. Akhan No:15 34437 Gümüşsuyu – İstanbul, registered to the Istanbul Trade Registry with the number 149773, as a Data Controller.

# **OUR PRINCIPLES FOR PROCESSING PERSONAL DATA**

All personal data processed by our company are processed in accordance with PDPL and relevant legislation. The basic principles we pay attention to while processing your personal data in accordance with Article 4 of PDPL are explained below:

* **Processing in Compliance with Law and Good Faith**: Our company; acts in accordance with the principles introduced by legal regulations and the trust and good faith in the processing of personal data. In this context, our Company takes into account the proportionality requirements in the processing of personal data, and does not use personal data other than what is required by the purpose.
* **Ensuring that Personal Data is Accurate and Up To Date When Required**: Our company; ensures that the personal data it processed are accurate and up to date, taking into account the fundamental rights of personal data owners and their own legitimate interests.
* **Processing for Specific, Clear and Legitimate Purposes**: Our company clearly and precisely determines the purpose of processing personal data that is legitimate and legal. Our company processes personal data in connection with the products and services it offers and as much as necessary for them.
* **Being Related, Limited and Measured for the Purpose of Processing**: Our company processes personal data in a way that is convenient for the realization of the specified purposes and avoids the processing of personal data that are not related or needed to achieve the purpose.
* **Keeping for the Period Stipulated in the Relevant Legislation or Required for the Purpose for which they are processed**: Our company keeps personal data only for the period specified in the relevant legislation or required for the purpose for which they are processed. In this context, our company first determines whether a period is stipulated in the relevant legislation for the storage of personal data, if a period of time has been determined, it acts in accordance with this period, if a period is not determined, it keeps the personal data for the period required for the purpose for which they are processed. Personal data are deleted, destroyed or anonymized by our Company in the event that the time is expired or the reasons requiring processing disappear.

# **DATA OWNER CATEGORIES**

The categories of data owners, except for employees whose personal data are processed by our company (including interns and sub-employer employees), are shown in the table below. A separate policy regarding the processing of personal data of our employees has been created and implemented within the company. People who fall outside of the following categories may also direct their requests to our Company within the scope of PDPL; the requests of these people will also be evaluated within the scope of the Policy.

|  |  |
| --- | --- |
| RELATED PERSON CATEGORY | EXPLANATION |
| Customer | Real or legal persons purchasing our products and services |
| Potential Customer | Real or legal person, who requested or had an interest in purchasing our products and/or using our services or who is evaluated in accordance with the rules of ethics and good faith that he/she may have this interest |
| Visitor | Real persons who enter the physical facilities (offices, factories, etc.), owned or carried out an organization by our company for various purposes or visit our websites |
| Third Person | In order to ensure the security of commercial transactions between our company and the parties mentioned above or to protect the rights of the aforementioned persons and to afford advantages, third party real persons associated with these persons (e.g. guarantor, companion, family members and relatives) or although not explicitly stated in the policy, all real persons (eg former employees) with whom our company has to process their personal data for a specific purpose |
| Employee Candidate / Trainee Candidate | Real persons who have applied for a job to our company in any way or who have opened their curriculum vitae and related information to our Company for inspection |
| Group Company Employee | Employees and representatives of Akkök Holding corporate group in Turkey, of which our company is a member  |
| Employees, Shareholders and Officials of Institutions We Are In Cooperation With | Real persons, including the shareholders and officials of these institutions, working in the institutions with which our company has all kinds of business relations (including but not limited to business partners, suppliers, etc.  |

# **WHEN DO WE GATHER PERSONAL DATA ABOUT YOU?**

We collect your personal data mainly in the following situations:

* When you purchase or use our products and/or services,
* When you sell goods or provide services to us,
* When you subscribe to our newsletters, choose to receive our marketing messages,
* When you contact us via our website, e-mail, social media platforms, other online channels or by phone,
* When you apply for a job with our company,
* When you participate to the events and organizations of our company,
* Indirectly, for example by using "cookies", When customizing the software used to tailor the website to your particular preferences, or while watching your use of certain pages of the site (for example your IP address) or by other technical means that enable us to monitor your use of the site,
* When you contact us for any purpose as a potential customer/supplier/business partner/sub-employer.

We will only process the personal data we obtain in the above cases in accordance with this Notification.

# **WHICH PERSONAL DATA DO WE PROCESS ABOUT YOU?**

The personal data we process about you vary according to the type of business relationship between us (eg customer, supplier, business partner, etc.) and the method of communicating with us (eg telephone, e-mail, website, printed documents, etc.).

Basically, our personal data processing methods are situations where you participate in our business activities or interact with us in any other way, via our website, by phone or e-mail, through electronic applications specific to our customers. In this context, the personal data we process about you can be explained under the following categories:

|  |  |
| --- | --- |
| **Data categories** | **Examples** |
| ID information | Information on identity documents such as name, surname, title, date of birth |
| Contact information | Email, phone number, address |
| Account login information | Login ID |
| Images and/or videos that can identify you | Photo and video images and audio data processed when you visit our company for security reasons or when you participate in events organized by our company, visual data processed with CCTV records when you visit our company facilities |
| Financial data | Credit card data, bank account data, billing information |
| **Data categories** | **Examples** |
| Any other information you decide to voluntarily share with Akkim | Personal data you share with your own initiative, feedback, opinions, requests and complaints, evaluations, comments and our evaluations regarding them, uploaded files, interests, information provided for our detailed review process before establishing a business relationship with you you transmitted to us through social media, online platforms or other channels |
| Electronic data collected automatically | When you visit or use our website or apps, when you subscribe to our newsletters, when you interact with us through other electronic channels, we may also collect electronic data sent to us by your computer, mobile phone or other access device as well as the information you transmit directly to us (E.g. device hardware model, IP address, operating system version and settings, the hour and time of using our digital channel or product, your actual location, which may be collected when you enable location-based products or features, links you click, motion sensor data, etc.) |
| Legal action and compliance information | Your personal data, audit and inspection data processed within the scope of determination, follow-up of our legal receivables and rights and the performance of our debts and our legal obligations, compliance with our Company's policies |
| Corporate customer/Supplier data | Information obtained and produced about data owner customer/supplier or data owners such as employees, authorised signatories within the customer/supplier as a result of the operations carried out by our business units within the framework of our services, |
| Incident management and security information | Information and evaluations collected about events that have the potential to affect our company's employees, directors or shareholders, license plate and vehicle information, transportation and travel information |
| Personal data collected from other sources | To the extent permitted by applicable laws and regulations, we may also collect your personal data through public databases, social media platforms, and methods and platforms where our business partners collect personal data on our behalf. For example, before establishing a business relationship with you, we may conduct research on you from public sources to ensure the technical, administrative and legal security of our commercial activities and transactions. In addition, it may be possible for you to transmit some personal data belonging to third parties to us (For example, personal data of guarantor, companion, family members, etc..). To be able to manage our technical and administrative risks, we may process your personal data through the methods used in accordance with the generally accepted legal, commercial custom and good faith in these areas.  |

# **PROCESSING PERSONAL DATA OF EMPLOYEE CANDIDATES**

# In addition to the above personal data categories, we gather personal data of employee candidates such as the school he/she graduated from, his/her previous work experience, disability status, etc. in order to understand the experience and qualifications of the candidate and to evaluate the suitability for the open position, to check the accuracy of the information transmitted if necessary and to conduct research about the candidate by contacting third parties whose contact information is given by the candidate, to get in contact with the candidate regarding the job application process, to recruite in accordance with the open position, to ensure compliance with legal legislation and to implement our company's recruitment rules and human resources policies.

# Personal data of employee candidates are processed through job application form available in written and electronic media, electronic job application platform of our Company, applications sent to our company physically or by e-mail, face-to-face or electronic interviews conducted by employment and consultancy companies, controls made by our company about the employee candidate, recruitment tests conducted by human resources experts to assess the candidate's suitability during the recruitment process.

# Employee candidates are informed in detail with a separate document in accordance with PDPL before submitting their personal data while applying for a job and their explicit consent is obtained for the necessary personal data processing activities.

# **OUR POLICY ON COOKIES**

Please read our Cookie Policy at [www.akkim.com.tr](http://www.akkim.com.tr) for more information about how we use cookies and other follow-up technologies. Generally, "cookie" is the name given to the information sent by an Internet service server to the user's computer and stored on this computer. The information contained in the ‘Cookies’ can be used when the user returns to that website. ‘Cookies' may contain various information, including how many times the user entered that website. By using individual session ‘cookies’ for each user, we can monitor how you use the site during a single session. Thanks to ‘cookies’, we can offer you some special services by determining which browser you are using.

By using the "help" function available in most browsers, you can learn how to prevent your computer from receiving ‘cookies' and find out if a ‘cookie' has been sent and disable them completely. However, we would like to remind you that if you disable cookies, you may not be able to use this site fully.

This site uses ‘cookies’ for a variety of purposes, including followings:

* Access certain information for the purpose of providing personalized content to you after entering the site;
* Track your preferences you specify while using this site, such as your preferred date and number formats. We value the privacy of your information. We apply the following rules to protect the privacy and security of your confidential information to the highest possible level:
* This site does not always keep ‘cookies’ on your disk drive. ‘Cookies’ are removed when you close your browser or leave the site.
* Information in all ‘cookies’ sent to your computer from this site is sent encrypted.

# **PROCESSING THE PERSONAL DATA OF OUR VISITORS AT OUR OFFICES AND FACTORIES**

Our company processes personal data of visitors coming to our buildings and factories during the entrance and exit procedures for the purposes of ensuring the physical safety of our company, our employees and visitors, and controlling workplace rules. In this context, for the purpose of tracking visitor entrance and exit, the name-surname and TR ID numbers of our visitors are confirmed with their ID cards and recorded in the visitor’s book. However, the visitor's identity card is not kept during his/her stay in the company's offices and factories, and the id card is returned to the visitor after the mentioned record is made in the visitor book. The visitor is informed about the processing of personal data with a clarification text at the security entrance before his/her information are received. However, as our company has a legitimate interest in this context, the visitor's explicit consent is not received in accordance with Article 5/2/f of the PDPL. These data are only physically kept in the visitor register book and are not transferred to another media unless there is a suspicious situation that threatens the security of the Company. However, this information may be used in cases such as crime prevention and ensuring Company security.

In addition, for the purposes specified in the Policy and providing security by our Company; internet access is available to our visitors who request during his/her stay in our company's offices and factories. In this case, the log records regarding your internet access are recorded in accordance with the Law No. 5651 and the mandatory provisions of the legislation regulated by this law; these records are only processed when requested by the authorized public institutions and organizations or to fulfill our legal obligation in the audit processes to be carried out within the Company.

Only a limited number of Akkim employees may access the log records obtained within this framework. Company employees who have access to the aforementioned records access these records only to be used in the request from the authorized public institution and organization or in the audit processes and share with legally authorized persons.

# **PROCESSING PERSONAL DATA THROUGH CLOSED CIRCUIT CAMERA RECORDING**

Security cameras are used to ensure the security of our company and facilities and personal data is processed in this way. Within the scope of monitoring activities with security cameras; our company has purposes such as increasing the quality of the service provided, ensuring the safety of life and property of the physical premises of the company and the people in the company, preventing abuses and protecting the legitimate interests of data owners.

Personal data processing activities performed by our company with security cameras are carried out in accordance with the Constitution, PDPL, Law No. 5188 on Private Security Services and the relevant legislation.

In accordance with Article 4 of the PDPL, our company processes personal data in a related, limited and measured manner with the purpose for which they are processed. The secrecy of the person should not be subjected to monitoring in a way that could result in intervention that exceeds security objectives. In this context, warning signs are placed in common areas where CCTV recording is made and data owners are informed. However, since our Company has a legitimate interest in keeping CCTV records, their explicit consent is not received. In addition, in accordance with Article 12 of the PDPL, necessary technical and administrative measures are taken to ensure the security of personal data acquired as a result of CCTV monitoring.

In addition, a procedure has been prepared regarding the areas with CCTV cameras, the monitoring areas of the cameras, and the retention periods of the recording, and it has been implemented in our Company. This procedure is taken into consideration before the CCTV camera is installed and the camera is then positioned. It is not allowed to position cameras to an extent that exceeds the purpose of security and exceeds the secrecy of persons. Only a certain number of Company personnel access CCTV camera images and these authorizations are regularly reviewed. Personnel with access to these records signs a commitment to protect personal data in accordance with the law.

Image recording is made through the security camera located in the entrance doors in our company offices and factories, building exterior, vehicle passageways, vehicle loading areas, production areas, dining hall, social facility surroundings, visitor waiting area, car park, security cabin and service area of the floor corridors and in order to ensure building security and recording process is audited by the Information Technologies Directorate.

# **FOR WHAT PURPOSES WE USE YOUR PERSONAL DATA?**

Our purposes for using your personal data vary depending on the type of business relationship between us (eg customer, supplier, business partner, etc.). Basically, our purposes for processing your personal data are as follows. Personal data processing activities related to Employee Candidates are explained under the section "Processing Personal Data of Employee Candidates" above.

| **Our Purposes for Processing Personal Data** | **Examples** |
| --- | --- |
| Evaluating potential customers/suppliers/ business partners | Conducting our review and conflict of interest process according to our risk rules  |
| Establishing and managing relationships with our customers / suppliers / business partners | Performing sales transactions of the products and services sold by our company, submitting offers for our products, supply of goods and services, invoicing, the drawing up and executing a contract, ensuring post-contract legal transaction security, ensuring shipment of goods and samples, managing logistics processes, developing products and services, evaluating new technologies and applications, determinating and implementing our company's commercial and business strategies, managing operations (request, offer, evaluation, order, budgeting, contract), product/project/manufacturing/investment quality processes and operations, intraco system and application management operations, financial operations, managing financial affairs |
| Conducting direct marketing processes | Conducting satisfaction surveys or evaluating your opinions, complaints and comments on social media, online platforms or other media, and returning, informing our customers about company innovations, campaigns and promotions, conducting periodic campaign studies, conducting advertisement, promotion and marketing activities, participation in fairs and establishing relationships in fairs, determining and implementing our company's commercial and business strategies, taking photos and videos in organizations, managing marketing activities |
| Contact and support (on your request) | Responding to information requests about our services, providing support for requests received through our communication channels, updating our records and database, providing communication with Akkök Holding group companies located in Turkey, conducting the necessary activities and reporting activities arising from being a group company |
| Compliance with legal obligations | Performing tax and insurance processes, fulfilling our legal obligations arising from the relevant legislation, particularly Law No.5651 and other legislation, Turkish Penal Code No.5237 and Law on Personal Data Protection No.6698, carrying out the processes before official institutions, obligations on record keeping and information, compliance and supervision, audits and inspections of official authorities, following and concluding our legal rights and lawsuits, carrying out the necessary processes within the scope of compliance with the laws and regulations we are subject to such as data disclosure upon the request of official authorities, carrying out activities within the scope of the requirements and obligations determined to ensure the fulfillment of the legal obligations specified in the PDPL as required or nesessitated by regulatory and supervisory institutions and legal regulations, Managing the processes before public institutions and organizations such as the Social Security Institution, Land Registry Directorate, etc. |
| Protection of company interests and ensuring their security | Carrying out necessary audit activities to protect the interests and benefits of the company, controlling conflict of interest, keeping CCTV records in order to ensure the legal and commercial security of the people in business relations with our company and to protect the company equipment and assets, taking technical and administrative security measures, implementation and supervision of workplace rules, managing quality processes, planning and executing social responsibility activities, protecting the commercial reputation and trust built up Akkök Holding group companies, reporting all incidents, accidents, complaints, losses, stolen, etc. occurring in the factory and the building and taking necessary action and taking precautions, transferring the rules to be followed for dangerous situations that may occur during maintenance and repair, and measuring the professional competencies of subcontractors, ensuring the order of entry and exit of company employees and obtaining the information necessary for security, performing our required quality and standard inspections or fulfilling our reporting and other obligations determined by laws and regulations, following up and preventing abuse and unauthorized transactions, defense against legal claims such as lawsuits, investigations etc. against our company |

#

# **HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING PURPOSES?**

Since marketing activities are not evaluated within the scope of the exceptions regulated in article 5/2 and article 6/3 of PDPL, we always obtain your consent to process your personal data within the scope of marketing activities as a rule. Our company may send you regular promotional communications about its products, services, events and promotions. Such promotional communications may be sent to you through different channels such as email, phone, SMS text messages, and mail.

Sometimes these communications may be adapted to your preferences to provide you with the best personalized experience (for example, as you express us these, according to the results of your website visits or based on the links you clicked in our emails).

Based on your consent, we may carry out marketing activities to process for providing you special opportunities for products and services such as internet advertising, targeting, re-targeting, cross-selling, campaign, opportunity and product/service advertisements, to use Cookies for this purpose, to make commercial offers and provide products special for you considering your preferences and recent purchases; to provide advertisements, campaigns, advantages and other benefits special for you for sales and marketing activities and to carry out other marketing and CRM studies, to process for the creation of new product and service models, to send electronic commercial messages (such as campaigns, newsletters, customer satisfaction surveys, product and service advertisements); to send gifts and promotions; to organize corporate communication and other events and invitations in this context and to provide information about them.

When required by the applicable legislation, we will ask for your consent before starting the above activities. You will also be given the opportunity to withdraw (stop) your consent whenever you want. In particular, you can always stop marketing-related notifications from being sent to you by following the unsubscribe instructions included in each email and SMS message.

If you log into an Akkim account, you may be given the option to change your communication preferences under the relevant section of our website or app. You can always contact us to stop sending marketing communications to you (You can find contact details in the section "What Are Your Rights Regarding Your Personal Data?" below).

# **FOR WHAT LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?**

We process your personal data within the framework of the following legal reasons regulated in Article 5 of PDPL, especially the Turkish Commercial Code No. 6102, Turkish Code of Obligations No. 6098, Tax Procedure Law No. 213:

| **Legal Reason** | **Examples** |
| --- | --- |
| In cases where we need to gain your explicit consent in accordance with PDPL and other legislation, we process based on your consent (In this case, we would like to remind you that you can withdraw your consent whenever you want) | We get your consent to carry out our marketing activities.  |
| In any situation permitted by applicable legislation | Including the name of the relevant person on the invoice within the scope of Article 230 of the Tax Procedure Law |
| When there is an obligation to protect vital interests of any person | Giving the health information of the board member who fainted in the board of directors to the doctor  |
| In case of establishing a contract with you, performance of the contract and where we need to fulfill our obligations under a contract | Obtaining the customer's bank account information within the scope of the contractual relationship with the customer |
| Fulfilling our legal obligations, | Fulfillment of our tax obligations, submission of information requested by court decision to the court |
| If your personal data has been made public by you | If you send us an e-mail to contact you, In case the employee candidate writes the contact information on the website where the job application is collected, use of personal data that you have made public by means such as social media channelsfor the purpose of publicization |
| Being mandatory to process data for the establishment or protection of a right, exercising our legal rights and defensing against legal requests opened against us  | Keeping documents that are proof/evidence and using them when necessary |
| In cases required by our legitimate interests, provided that it does not harm your fundamental rights and freedoms | Conducting research in order to ensure the security of our company communication networks and information, to conduct our company activities, to detect suspicious transactions and to comply with our risk rules, benefitting from storage, hosting, maintenance and support services in order to provide IT services in terms of technical and security, making use of cloud technology in order to ensure the efficiency of our company activities and to benefit from the opportunities of technology |

In cases where your Personal Data is processed with explicit consent, if you withdraw your explicit consent, we would like to emphasize that you will be removed from the commercial membership program where processing based on such explicit consent is required and that you will not be able to benefit from the advantages you have benefited thanks to the mentioned processings as of the relevant date.

# **WHEN DO WE SHARE YOUR PERSONAL DATA?**

**Transfer of Personal Data Domestically**

Our company is under the responsibility to act in accordance with the decision and relevant regulations stipulated in the PDPL, especially the article 8 of the PDPL and taken by the Board regarding the transfer of personal data. As a rule, personal data and sensitive personal data belonging to data owners cannot be transferred by our Company to other natural persons or legal entities without the explicit consent of the relevant person.

In addition, in cases stipulated in articles 5 and 6 of the PDPL, transfer is possible without the consent of the relevant person. In accordance with the conditions stipulated in the PDPL and other relevant legislation and by taking the security measures specified in the legislation; (if there is an existing contract signed with the data subject, in the contract in question) our company can be transferred personal data to third parties in Turkey and the company under the Akkök Holding unless otherwise regulated by law or other relevant legislation.

**Transfer of Personal Data Abroad**

Our company also transfers personal data abroad as well as may be transferred to third parties in Turkey, including outsourcing, as stated above, in accordance with the conditions stipulated in the Law and other relevant legislation, by taking the security measures specified in the legislation by processing in Turkey or to be processed and kept outside of Turkey. We transfer your personal data abroad by taking necessary technical and administrative measures through cloud computing technology in order to carry out our company activities in the most efficient way and to benefit from the opportunities of technology.

In accordance with Article 9 of the PDPL, as a rule, we seek the explicit consent of the data owners for the transfer of personal data abroad. However, in accordance with Article 9 of the PDPL, existence of one of the conditions regulated in Article 5/2 or Article 6/3 of PDPL, in the foreign country where personal data will be transferred, provided that

a) Adequate protection is available,

b) Data controllers in the relevant foreign country and Turkey commit to adequate protection in writing or there is the permission of the board in the absence of adequate protection,

without the explicit consent of the data owner, transfer abroad may be made.

Accordingly, in exceptional cases where explicit consent is not sought for the transfer of personal data mentioned above, our Company seeks the condition of having sufficient protection in the country where the data will be transferred in accordance with the PDPL in addition to the conditions of processing and transfer without consent. The Personal Data Protection Board will determine whether sufficient protection is provided; in the absence of adequate protection, it is required that data controllers both in the relevant foreign country and in Turkey should commit to adequate protection in writing or the permission of the board should be available.

**Shared Parties**

We share your personal data only if necessary for the following purposes. Except for these situations, we take special care not to share your personal data. The parties with whom we share personal data are listed below:

* **Akkök Holding group companies**: As we operate under the Akkök Holding corporate group, Your data may be shared with Akkök Holding Inc. established in Turkey or may be made accessible to Akkök Holding Inc. This sharing will only be done with authorized employees in Akkök Holding Inc. However, we would like to state that, in general, data sharing with Akkök Holding group companies is carried out in a way that does not contain personal data within the scope of financial reporting on company activities such as company profitability and efficiency. In some special cases, it may be possible to share personal data with Akkök Holding group companies instead of sharing anonymous information (such as sharing damage information to open an insurance damage file). Akkök Holding Data Sharing Agreement has been signed regarding the transfer of your personal data to Akkök Holding group companies and the necessary measures have been taken.
* **Service providers and business partners:** It defines the parties with which our company establishes business partnerships for purposes such as the sale, promotion and marketing of our Company's products and services, after-sales support, while conducting its commercial activities. Like many enterprise, we may also work with reliable third parties such as information and communication technology providers, consultancy service providers, courier companies, travel agents for functions and services to be carried out in the most efficient way and in accordance with current technologies within the scope of some data processing activities and in this context, we may share data to carry out our activities. This sharing is limited in order to ensure the fulfillment of the establishment and performance purposes of the business partnership. Our company uses cloud computing technologies to carry out its activities in the most efficient way and to benefit from the possibilities of technology at the maximum level and in this context, we may process your personal data domestically and abroad through companies that offer cloud computing services. The marketing services support firm we share with may be established abroad and in this context, data sharing is carried out with abroad in accordance with the provisions on data sharing to abroad pursuant to Article 8 and Article 9 of the PDPL.
* **Official authorities**: In cases required by law or when we need to protect our rights, we may share your personal data with relevant official, judicial and administrative authorities (eg tax offices, law enforcement agencies, courts and enforcement offices, police departments, law enforcement agencies, General Directorate of Population, etc.).
* **Private law persons:** According to the relevant legislation provisions, personal data can be shared within the legal authority of private law persons authorized to receive information and documents from our company limited to the purpose he/she requests (e.g. Occupational Health and Safety Company).
* **Professional consultants**: We may share your personal data with professional consultants such as banks, insurance companies, auditors, lawyers, financial advisors and other consultants.
* **Other persons associated with corporate transactions**: From time to time, we may share your personal data in order to carry out corporate transactions such as the sale, reorganization, merger, joint venture, or other disposition of our business, assets or shares of a business owned by our company (including those in connection with any bankruptcy or similar process).

#

# **SOCIAL PLUGINS**

Our web pages use "social plugins" from social networks, these include particularly the “Share” button of the “Facebook” verifier on the facebook.com page, operated by Facebook Inc., 1601 S. California Ave, Palo Alto, CA 94304, USA. Plugins usually have the Facebook logo. In addition to Facebook, we use plugins of “Google+” (verifier: Google Inc., Amphitheatre Parkway, Mountain View, CA 94043, USA), “YouTube” (verifier: YouTube LLC, 01 Cherry Avenue, San Bruno, CA 94066, USA), “Twitter” (verifier: Twitter, Inc., 1355 Market St, Suite 900, San Francisco, CA 94103, USA), “Pinterest” (verifier: Pinterest Inc., 808 Brannan Street, San Francisco, CA 94103, USA), “LinkedIn” (verifier of customers outside the USA: LinkedIn Ireland Unlimited Company, Wilton Place, Dublin 2, Ireland).

We have consciously made the decision not to use plugins directly from social networks on our website for privacy reasons. Instead, we use an alternative technical solution that allows you to determine whether and when information is provided to operators and such social networks. When you visit our web pages, no information is automatically sent to social networks such as Facebook, Google+, Twitter or Pinterest. Only when you actively click the relevant button, your Internet browser connects to the servers of the specified social network. This means clicking on that elements and then on the symbol of the social network, in this way, you consent to your Internet browser communicating with the servers of the social network and sending the user data of this network to the operator. We do not have any influence on the type and scope of data collected by social networks. For the purpose and scope of data collection and for your rights and options regarding the security of your privacy regarding the processing of data and its use by relevant social network, please refer to the relevant privacy policies of these social networks.

Facebook's privacy policies can be found at <http://www.facebook.com/about/privacy/> and <http://www.facebook.com/help/?faq=186325668085084> .

More information about data usage can be found at <https://policies.google.com/privacy?hl=tr&gl=de> or <http://twitter.com/privacy> pags for “Google+,” “Youtube” or “Twitter”, at <https://policy.pinterest.com/tr/privacy-policy> for Pinterest, at <https://www.linkedin.com/legal/privacy-policy> for LinkedIn.

**Google Maps**

To make your travel easier, we recommend you to use Google Maps in order to show maps and create directions. Google Maps is operated by Google Inc., 1600 Amphitheater Parkway, Mountain View, CA 94043, USA. These pages are tagged as related.

When you use this service, you consent to Google to collect, process and use the information entered by you. The conditions regarding the use of Google Maps can be found at <http://www.google.com/intl/de_de/help/terms_maps.html>.

**Web analysis with Google Analytics**

This web page uses Google Analytics, a web analysis service provided by Google Inc. (”Google”). Google Analytics uses "cookies", which are text files that are stored on your computer and analyze your use of the web page. The information generated by the cookie about your use of this web page (including the shortened IP address) is transferred to a Google server in the United States and stored there. Google will use this information to analyze your use of the web page, to collect reports on web page activity for web page operators and to provide more services related to web page and Internet usage. Google will also pass it on to third parties where appropriate, when this information is legally required or when these parties process this information on behalf of Google. Google will not associate your IP address with your IP address in any way.

You can prevent your information from being used by Google Analytics by installing a plug-in on your browser. You can click on the link below which will take you to the Google page: <http://tools.google.com/dlpage/gaoptout?hl=de>.

**Login**

Registration information is created and processed for statistical purposes every time you log in the website, which ensures that the user remains anonymous:

* The reference (whose link you use to access this web page)
* Search expressions (if the reference is a search engine)
* IP analysis is performed to determine the country of access and verifier
* Browser, operating system, installed plug-ins and screen resolution
* Time to stay on pages
* The specified data are processed by us for legal purposes based on PDPL:
* Providing a trouble-free connection with the web page,
* Ensuring comfortable use of the web page,
* Evaluation of system security and stability and other administrative purposes.

If we become aware of certain signs of illegal use, we reserve the right to check this information retroactively. Within this purpose, if no longer required, the data will be deleted immediately and in any case after six months at the latest.

# **HOW LONG DO WE KEEP YOUR PERSONAL DATA?**

We only keep your personal data for as long as necessary to fulfill the purpose for which it was collected. We keep your personal data only for as long as necessary to fulfill the purpose for which they were collected. We determine these periods separately for each business process and if there is no other reason to keep your personal data at the end of the relevant periods, we destroy your personal data in accordance with PDPL.

While determining the destruction periods of your personal data, we take into account the following criteria:

* The period accepted as per general practice in the sector in which the data controller operates within the scope of the processing of the relevant data category,
* The period that requires the processing of personal data in the relevant data category and the period that legal relationship established with the relevant person continues,
* The period during which the legitimate interest to be obtained by the data controller will be valid in accordance with the law and good faith depending on the purpose of processing the relevant data category,
* The period during which the risks, costs and responsibilities of storing the relevant data category depending on the purpose of processing will continue legally,
* Whether the maximum period to be determined is suitable for keeping the relevant data category accurate and up-to-date when necessary,
* The period during which the data controller is obliged to keep personal data in the relevant data category in accordance with his legal obligation,
* The time-out period determined by the data controller to assert a right based on personal data in the relevant data category.

# **HOW DO WE DESTROY YOUR PERSONAL DATA?**

In line with the regulation of article 138 of the Turkish Penal Code and article 7 of the PDPL, personal data are deleted, destroyed or anonymized based on our company's own decision or if the personal data owner has such a request in case the reasons requiring the processing disappear although they were processed in accordance with the relevant law provisions.

In this context, Personal Data Storage and Disposal Policy has been prepared. In cases where there is a right and/or obligation to save personal data in accordance with the provisions of the relevant legislation, our company reserves the right not to fulfill the data subject's request. When personal data are processed by non-automatic means provided that it is a part of any data recording system, system of physical destruction of personal data in a way that cannot be used later is applied while data is being deleted/destroyed. When our company agrees with a person or organization to process personal data on its behalf, the personal data is securely deleted by these persons or organizations in a way that cannot be recovered. Our company can anonymize personal data when the reasons requiring the processing of personal data that are legally processed disappear.

**DESTRUCTION METHODS OF PERSONAL DATA**

**Deletion of Personal Data**

Our company can delete personal data based on its own decision or upon the request of the personal data owner in case the reasons requiring the processing disappear although they were processed in accordance with the provisions of the relevant law. Deletion of personal data is the process of making personal data inaccessible and unavailable in any way for the relevant users. Our company takes all technical and administrative measures necessary for the deleted personal data to be inaccessible and reusable for the relevant users.

Personal Data Deletion Process

The process to be followed in the process of deleting personal data is as follows:

* Determination of personal data that will constitute the subject of deletion.
* Determining levant users for each personal data using an access authorization and control matrix or a similar system.
* Determining the authorizations and methods of the relevant users such as access, retrieval and reuse.
* Closing and eliminating the access, retrieval and reuse authorization and methods of the relevant users within the scope of personal data.

Methods of Deleting Personal Data

|  |  |
| --- | --- |
| Data Recording Media | Explanation |
| **Personal Data** **on Servers** | For those, whose period that requires the storage of personal data which keep on servers has expired, the system administrator removes the access authority of the relevant users and deletes them. |
| **Personal Data** **on Electronic Media** | Those, whose period that requires the storage of personal data on electonic media has expired, are made inaccessible and reusable in any way for other employees (relevant users) except for the database administrator. |
| **Personal Data** **on the Physical Media** | Those, whose period that requires the storage of personal data on physical media has expired, are made inaccessible ans reusable in any way for other employees, except for the department manager responsible for the document archive. In addition, the blackout process is also applied by scratching/painting/wiping in an unreadable way. |
| **Personal Data** **on Portable Media** | Those, whose period that requires the storage of personal data which keep in flash-based storage media has expired, are stored in secure environments with encryption keys by encrypting by the system administrator and the access authority is given only to the system administrator. |

Since personal data can be stored in various recording media, they should be deleted by appropriate methods. Examples are given below:

Application Type Cloud Solutions as a Service (such as Office 365 Salesforce, Dropbox): In the cloud system, data should be deleted by giving a delete command. It should be noted that the relevant user is not authorized to retrieve deleted data on the cloud system while performing the said transaction.

Personal Data on Paper: Personal data on paper should be deleted using the blackout method. The blackout process is done by cutting the personal data on the relevant documents whenever possible, or in cases where it is not possible, making them invisible to the relevant users by using fixed ink in a way that is irreversible and cannot be read with technological solutions.

Office Files on the Central Server: The file should be deleted with the delete command in the operating system or the access rights of the relevant user on the file or on the index where the file is located should be removed. It should be noted that the relevant user is not the system administrator at the same time while performing the said operation.

Personal Data on Portable Media: Personal data in flash-based storage media should be stored encrypted and deleted using software suitable for these media.

Databases: Relevant lines containing personal data should be deleted with database commands (DELETE vb.). It should be noted that the relevant user is not also a database administrator while performing the said transaction.

**Destruction of Personal Data**

Our company may destroy the personal data upon its own decision or upon the request of the personal data owner in case the reasons requiring its processing disappear although they were processed in accordance with the provisions of the relevant law. The destruction of personal data is the process of making personal data inaccessible, retrievable and reusable in any way. The data controller is obliged to take all necessary technical and administrative measures regarding the destruction of personal data.

|  |  |
| --- | --- |
| Data Recording Media | Explanation |
| **Personal Data on the Physical Media** | Those, whose period that requires the storage of personal data on physical media has expired, is irreversibly destroyed in paper shredders. |
| **Personal Data on Optical / Magnetic Media** | For those, whose period that requires the storage of personal data on optical media and magnetic media has expired, physical destruction process is applied such as melting, burning or pulverizing etc. In addition, magnetic media is passed through a special device and exposed to a high value magnetic field, which is made the data on it unreadable. |

Physical Destruction: Personal data can also be processed in non-automatic ways, provided that it is a part of any data recording system. A system of physical destruction of personal data in a way that cannot be used later is applied while data is being deleted/destroyed.

Securely Deletion from Software: While the data processed in fully or partially automatic ways and stored in digital media is deleted/destroyed; methods are used to delete data from the relevant software in a way that cannot be recovered again.

Securely Deletion by an Expert: In some cases, it may be agreed with an expert to delete personal data on its behalf. In this case, the personal data are securely deleted/destroyed by the expert on this subject so that they cannot be recovered again.

Blackout: Making personal data physically unreadable.

Methods of Destruction of Personal Data

In order to destroy personal data, it is necessary to detect all copies of the data and to destroy them one by one using one or more of the following methods, depending on the type of systems in which the data is located:

Local Systems: One or more of the following methods can be used to destroy data on these systems. i) De-magnetizing: It is the process of deformation of data on it unreadably by exposing the magnetic media to a very high magnetic field by passing through a special device. ii) Physical Destruction: It is the physical destruction of optical media and magnetic media such as melting, burning or pulverizing. It is ensured that data are made inaccessible by processes such as melting, burning, pulverizing or passing the optical or magnetic media through a metal grinder. If overwriting or de-magnetizing is not successful in terms of solid state discs, this media should also be physically destroyed. iii) Overwriting: It is the process of preventing the recovery of old data by writing random data consisting of 0 and 1 at least seven times on magnetic media and rewritable optical media. This process is done using special software.

Environmental Systems: Destruction methods that can be used depending on the media type are as follows: i) Network devices (switch, router etc.): The storage media inside that devices are fixed. Products often have a delete command but no destruction feature. It should be destroyed by using one or more of the appropriate methods specified in (a). ii) Flash-based media: Flash-based hard disks with ATA (SATA, PATA etc.), SCSI (SCSI Express etc.) interfaces should be destroyed by using the <block erase> command if supported, using the manufacturer's recommended method of destruction if not supported or by using one or more of the appropriate methods specified in (a). iii) Magnetic tape: It is a medium that stores data with the help of micro magnet pieces on the flexible tape. It should be exposed to very strong magnetic medium and destroyed by de-magnetizing or physical destruction methods such as burning or melting. iv) Units such as magnetic disk: They are medias that store data with the help of micro magnet pieces on flexible (plate) or fixed media. It should be exposed to very strong magnetic medium and destroyed by de-magnetizing or physical destruction methods such as burning or melting. v) Mobile phones (Sim card and fixed memory areas): There are delete commands in fixed memory areas on portable smartphones, but most do not have a destroy command. It should be destroyed by using one or more of the appropriate methods specified in (a). vi) Optical discs: These are data storage media such as CDs and DVDs. It should be destroyed by physical destruction methods such as burning, breaking into small pieces, melting. vii) Peripherals such as printer, whose data recording medium is removable, fingerprint door access system: It is necessary to verify that all data recording media have been removed and be destroyed by using one or more of the appropriate methods specified in (a) according to their specifications. viii) Peripherals such as printer eith fixed data recording medium, fingerprint door access system: Most of the systems in question have a delete command but not have a destroy command. It should be destroyed by using one or more of the appropriate methods specified in (a).

Paper and Microfiche Media: Since the personal data in these media is permanently and physically written on the media, the main media should be destroyed. While doing this, it is necessary to divide the media into small pieces that are incogitable size by paper shredders, horizontally and vertically if possible, so that they cannot be put back together. Personal data transferred from the original paper format to the electronic media by scanning should be destroyed by using one or more of the appropriate methods specified in (a), depending on their electronic media.

Cloud Media: During the storage and use of personal data in these systems, they should be encrypted with cryptographic methods and, where possible, separate encryption keys should be used for personal data particularly for each cloud solution that is served. When the cloud information service relationship ends; all copies of encryption keys required to make personal data usable should be destroyed. In addition to the above environments, the processes for the destruction of personal data in devices that are malfunctioning or sent for maintenance are performed as follows: i) The personal data contained in it should be destroyed by using one or more of the appropriate methods specified in (a) before transferring the relevant devices to third institutions such as manufacturer, seller, service for maintenance and repair, ii) Where dedormation is not possible or appropriate, data storage media should be disassembled and stored, other defective parts should be sent to third parties such as manufacturer, seller service, iii) Necessary measures should be taken to prevent personnel coming from outside for maintenance and repair purposes from copying personal data and taking out of the institution.

**Making Personal Data Anonymous**

Anonymization of personal data means making it unrelated to an identified or identifiable real person in any way even by matching personal data with other data. Our company may anonymize personal data when the reasons requiring the processing of personal data, processed in accordance with the law diseppear. In order for personal data to be anonymized; they should be made unrelated to an identified or identifiable real person even through the use of techniques appropriate for the recording medium and the relevant field of activity such as the return of personal data by the data controller or recipient groups and/or matching the data with other data. Our company takes all kinds of technical and administrative measures required to anonymize personal data.

In accordance with Article 28 of the PDP Law; Anonymized personal data can be processed for purposes such as research, planning and statistics. Such processing is outside the scope of the PDP Law and the explicit consent of the personal data owner will not be sought.

Anonymization Methods of Personal Data

Anonymization of personal data means making it unrelated to an identified or identifiable real person in any way even by matching personal data with other data.

In order for personal data to be anonymized; it should be made unrelated to an identified or identifiable real person even through the use of techniques appropriate for the recording medium and the relevant field of activity such as the return of personal data by the data controller or recipient groups and/or matching the data with other data.

Anonymization is preventing the identification of the relevant person or losing its distinctiveness within a group or a crowd in a way that cannot be associated with a real person by removing or changing all direct and/or indirect identifiers in a data set. Data that do not refer to a specific person as a result of blocking or losing these features are considered anonymized data. In other words, while the anonymized data is information that identifies a real person before this transaction is taken, after this process it has become unrelated to the relevant person and was disconnected from the person. The purpose of anonymization is to break the link between the data and the person identified by this data. All link break operations, conducted by methods such as automatic or non-automatic grouping, masking, deriving, generalizing, making random applied to the records in the data recording system where personal data are kept, are called anonymization methods. The data obtained as a result of the application of these methods should not be able to identify a specific person.

Exemplary anonymization methods are explained below:

**Anonymization Methods That Do Not Provide Value Irregularity**: In methods that do not provide value irregularity, no change or addition or removal is applied to the values of the data in the set, instead, changes are made to the entire row or column in the set. Thus, while the overall data changes, the values in the fields maintain their original status.

a.Removing Veriables

It is a method of anonymization provided by removing one or more of the variables from the table completely. In such a case, the entire column in the table will be removed completely. This method can be used for reasons such as the variable being a high-grade identifier, the lack of a more appropriate solution, the variable being too sensitive data to be disclosed to the public, or not serving analytical purposes.

b.Removing Records

In this method, anonymity is strengthened by removing a line containing singularity in the data set and the possibility of generating assumptions about the data set is reduced. Generally, the removed records are records that do not carry a common value with other records and that people who have an idea about the data set can easily guess. For example, in a dataset containing survey results, only one person from any industry is included in the survey. In such a case, instead of removing the "sector" variable from all survey results, it may be preferable to remove only the record of this person.

c.Regional Hiding

The purpose of the regional hiding method is to make the data set more secure and to reduce the risk of predictability. If the combination of values ​​belonging to a particular record creates little visible situation or and it is likely to cause that person to become distinguishable in the relevant community, the value that creates the exception is changed to "unknown".

ç. Generalization

It is the process of converting the relevant personal data from a special value to a more general value. It is the most used method when generating cumulative reports and in operations conducted over total numbers. The new values obtained as a result show the total values or statistics of a group that makes it impossible to reach a real person. For example, after one person with TR ID Number 12345678901 purchased diapers from the e-commerce platform, he/she also bought wet wipes. In the anonymization process, by using the generalization method, it can be concluded that xx% of the people who buy diapers from the e-commerce platform also buy wet wipes.

d. Lower and Upper Limit Coding

The lower and upper limit coding method is obtained by defining a category for a certain variable and combining the remaining values in the grouping created by this category. Generally, the low or high values of a certain variable are added together and a new definition is made to these values.

e. Global Coding

Global coding method is a grouping method used in data sets where lower and upper limit coding is not possible, does not contain numerical values, or has values that cannot be numerically sorted. It is generally used where certain values make it easier to make estimates and assumptions by clustering. By creating a common and new group for the selected values, all records in the data set are replaced with this new definition.

f. Sampling

In the sampling method, instead of the whole data set, a subset from the set is disclosed or shared. Thus, since it is not known whether a person known to be included in the entire data set is included in the disclosed or shared sample subset, the risk of producing accurate predictions about people is reduced. Simple statistical methods are used to determine the subset to be sampled. For example; in the event that a data set about demographic information, profession and health status of a women living in Istanbul is disclosed or shared by anonymizing, it may be meaningful to make scans and make predictions in the relevant data set about a woman known to live in Istanbul. However, in the relevant data set, only the records of women whose province is Istanbul is left and anonymization is applied by removing those whose register is in other provinces from the data set, and if the data is disclosed or shared, malicious person accessing the data will not be able to make a reliable estimate as to whether the information of this person he/she knows is included in that data since he/she cannot predict whether the register of a woman, whom he/she knows that she is living in Istanbul, is in Istanbul or not.

**Anonymization Methods Providing Value Irregularity:** Unlike the methods mentioned above; with methods that provide value irregularity, distortion is created in the values of the data set by changing the existing values. In this case, since the values of the records are changing, the benefit planned to be obtained from the data set must be calculated correctly. Even if the values in the data set are changing, it is still possible to benefit from the data by ensuring that the total statistics are not distorted.

Micro Joining

With this method, all records in the data set are first arranged in a meaningful order and then the whole set is divided into a certain number of subsets. Then, by taking the average of the value of each subset of the specified variable, the value of that variable of the subset is replaced with the average value. Thus, the average value of that variable for the entire data set will not change.

Data Exchange

The data exchange method is the record changes obtained by exchanging the values of a variable subset between the pairs selected from the records. This method is mainly used for variables that can be categorized and the main idea is to transform the database by changing the values of the variables between the records of individuals.

Adding Noise

With this method, additions and removals are made to provide a determined degree of distortion in a selected variable. This method is mostly applied to data sets containing numerical values. Distortion applies equally to each value.

**Statistical Methods For Strengthening Anonymization**

As a result of combining some values in records with single scenarios in anonymized data sets, the possibility of identifying the persons in the records or deriving assumptions about their personal data may arise.

For this reason, anonymity can be strengthened by minimizing the singularity of the records in the data set by using various statistical methods in the anonymized data sets. The main purpose of these methods is to minimize the risk of disruption of anonymity while keeping the benefit from the data set at a certain level.

K- Anonymity

In anonymized data sets, if indirect identifiers come together with the right combinations, the fact that identities of the persons in the records can be identified or the fact that information about a particular person can be easily predicted has undermined the confidence in anonymization processes. Accordingly, data sets that were anonymized by various statistical methods had to be made more reliable. K-anonymity has been developed to prevent disclosure of information specific to individuals that show singular characteristics in certain combinations by enabling the identification of more than one person with certain fields in a data set. If there is more than one record belonging to combinations created by combining some of the variables in a data set, the possibility of identifying persons corresponding to this combination is reduced.

L-Diversity

The L-diversity method, created by studies conducted on the shortcomings of K-anonymity, takes into account the diversity created by sensitive variables corresponding to the same variable combinations.

T-Proximity

Although the L-diversity method provides diversity in personal data, there are situations where it cannot provide sufficient protection because the method does not deal with the content and sensitivity of personal data. As such, the process of calculating the degree of proximity of the values among themselves and making the data set anonymized by dividing it into subclasses according to these degrees of proximity is called the T-proximity method.

**Choosing the Anonymization Method**

Our company decides which of the above methods will be applied by looking at the data in its possession and considering the following features regarding the owned data set;

The nature of the data,

The size of the data,

The nature of the data in physical medium,

The diversity of data,

The desired benefit from the data / processing purpose,

Data processing frequency,

The reliability of the party to whom the data will be transferred,

Being meaningful of the effort to be made to anonymize the data,

The magnitude, ingluence area of the damage that may occur in case of disruption of the anonymity of the data,

The distribution/centralization rate of the data,

Users' authorization control to access relevant data and

The probability of being meaningful of the effort construct and implement an attack that will disrupt anonymity.

When a data is made anonymous, our company checks whether the data in question is capable of defining a person again through contracts and risk analysis by using information that is known to be within the body of other institutions and organizations to which personal data is transferred or that is open to the public.

**Anonymity Assurance**

While our company is deciding to make a personal data anonym instead of deletion or destruction, attention is paid to the points that anonymity is not disrupted by combining the anonymized data set with another data set, that one or more values ​​do not form a meaningful whole that could make a record singular and that the values ​​in the anonymized data set do not combine to produce an assumption or result, as the features listed in this article change over the data sets that are anonymized by our company, controls are made and it is ensured that anonymity is preserved.

**Risks of Disrupting Anonymization by Reverse Processing of Anonymized Data**

Since anonymization process is the process that applied to the personal data and for destroying the distinguishing and identifying features of the data set, there is a risk that these transactions will be reversed by various interventions and the anonymized data will become identifying and distinguishing real persons. This situation is expressed as anonymity disruption. Anonymization can only be achieved by manual processes or automatically enhanced processes, or by hybrid processes consisting of combination of both transaction types. However, what is important is that after the anonymized data is shared or disclosed, measures have been taken to prevent anonymity from being disrupted by new users who can access or own the data. The actions carried out consciously regarding the disruption of anonymity are called “attacks against anonymity”. In this context, it is investigated whether there is a risk of reversing personal data that has been anonymized by our Company with various interventions and that the anonymized data will become re-identifying and diftinguishing real persons and the process is established accordingly.

# **HOW DO WE PROTECT YOUR PERSONAL DATA?**

In order to protect your personal data and to prevent unlawful access, necessary administrative and technical measures are taken by our Company in line with the Personal Data Security Guide published by the PDP Authority, procedures are organized within the company, clarification and explicit consent texts are prepared and necessary inspections are carried out or had been made by outsource service to ensure the implementation of PDPL provisions in accordance with article 12/3 of PDPL. These audit results are evaluated within the scope of the internal functioning of the Company and necessary actions are taken to improve the measures taken.

Your personal data mentioned above can be transferred to the physical archives and information systems of our Company and/or our suppliers, and they can be kept in both digital and physical media. The technical and administrative measures taken to ensure the security of personal data are explained in detail below under two titles.

**Technical Measures**

We use generally accepted standard technologies and business security methods, including standard technology called Secure Socket Layer (SSL), for the protection of personal information gathered. However, due to the nature of the Internet, information can be accessed by unauthorized persons over networks without the necessary security measures. We take technical and administrative measures to protect your data from risks such as destruction, loss, tampering, unauthorized disclosure or unauthorized access depending on the current state of the technology, the cost of the technological application and the nature of the data to be protected. In this context, we conclude agreements with the service providers we work with regarding data security.

1. Ensuring Cyber ​​Security: We use cyber security products to ensure personal data security, but the technical measures we take are not limited to this. The first line of defense is established against attacks from environments such as the Internet with measures such as firewall and gateway. However, almost all software and hardware are subjected to some installation and configuration processes. Considering that some commonly used software, especially older versions, may have documented security vulnerabilities, unused software and services are removed from the devices. For this reason, deletion of unused software and services is preferred primarily because of its ease, rather than keeping it up-to-date. With patch management and software updates, it is ensured proper functioning of software and hardware and regular control whether the security measures taken for the systems are sufficient.
2. Access Limitations: Access authorizations to systems containing personal data are limited and regularly reviewed. In this context, employees are granted access authorization to the extent necessary for their job and duties and their powers and responsibilities and access to related systems is provided by using a user name and password. While creating these passwords and codes, it is ensured that combinations of uppercase and lowercase letters, numbers and symbols are preferred instead of numbers or letter sequences that are associated with personal information and are easy to guess. Accordingly, access authorization and control matrix is created.
3. Encryption: In addition to the use of strong passwords and code, in order to protect against common attacks such as the use of brute force algorithm (BFA), access is restricted by methods such as limiting the number of password entry attempts, ensuring that passwords and codes are changed regularly, opening the administrator account and admin authority for use only when needed and deleting the account or closing the entries without losing time for employees who have been dismissed from the data controller.
4. Anti Virus Software: In order to protect against malicious software, products such as antivirus and antispam are used that regularly scan the information system network and detect threats, and they are kept up-to-date and necessary files are regularly scanned. If personal data is to be obtained from different websites and/or mobile application channels, it is ensured that the connections are made with SSL or a more secure way.
5. Monitoring of Personal Data Security: Checking which software and services are running in information networks, determining whether there is an infiltration or a movement that should not occur in information networks, Keeping regular records of all users' transaction activities (such as log records), Reporting of security problems as quickly as possible are carried out. Again, a formal reporting procedure is established for employees to report security weaknesses in systems and services or threats that use them. Evidence is collected in case of undesirable events such as information system crash, malicious software, attack for discard, incomplete or incorrect data entry, violations that disrupt privacy and integrity, abuse of the information system and stored securely.
6. Ensuring the Security of Media Containing Personal Data: If personal data are stored on the devices located in the data controllers' premises or in paper medium, physical security measures are taken against threats such as theft or loss of these devices and papers. Physical medias containing personal data are protected against external risks (fire, flood, etc.) with appropriate methods and entry / exit to these medias is controlled.

If personal data is in electronic media, access can be restricted between network components or the components are separated in order to prevent personal data security breach. For example, if personal data is processed in this area by restricting it to a certain part of the network that is used only for this purpose, Available resources can only be allocated to secure this limited area, not for the entire network.

Measures at the same level are also taken for paper media, electronic media and devices located outside the Company premises and containing personal data belonging to the Company. As a matter of fact, although personal data security breaches often occur due to the theft and loss of devices containing personal data (laptop, mobile phone, flash disk, etc.), personal data to be transferred by e-mail or mail are also sent carefully and by taking adequate precautions. In case the employees access the information system network with their personal electronic devices, sufficient security measures are also taken for them.

The method of using access control authorization and / or encryption methods is applied against cases such as the loss or theft of devices containing personal data. In this context, the password key is stored in an environment that only authorized persons can access and unauthorized access is prevented.

Documents in paper media containing personal data are also stored in a locked way and in environments that can only be accessed by authorized persons, and unauthorized access to such documents is prevented.

In accordance with article 12 of PDPL, if personal data is obtained by others illegally, our Company notifies this situation to the PDP Board and data owners as soon as possible. The PDP Board, if it deems necessary, may announce this on the website or by any other method.

1. Storing Personal Data in the Cloud: In the case of storing personal data in the cloud, the company should evaluate whether the security measures taken by the cloud storage service provider are sufficient and appropriate. In this context, two-stage authentication control is applied for knowing in detail what the personal data stored in the cloud is, backing up, ensuring synchronization and remote access to these personal data if required. During the storage and use of personal data in these systems, it is ensured that they should be encrypted with cryptographic methods, sent to the cloud media by encrypting and, where possible, separate encryption keys should be used for personal data particularly for each cloud solution that is served. When the cloud information service relationship ends; all copies of encryption keys that could be used to make personal data usable are destroyed. By logging access to data storage areas where personal data are, improper access or access attempts are instantly communicated to those concerned.
2. Procurement, Development and Maintenance of Information Technology Systems: Security requirements are taken into consideration while determining the needs for the procurement, development or improvement of existing systems by the company.
3. Backup of Personal Data: In cases where personal data is damaged, destroyed, stolen or lost for any reason, the Company ensures that it is activated as soon as possible by using the backed up data. Backed up personal data can only be accessed by the system administrator, and data set backups are kept off the network.

**Administrative Measures**

* All activities carried out by our company have been analyzed in detail for all business units, and as a result of this analysis, a process-based personal data processing inventory has been prepared. Risky areas in this inventory are identified and necessary legal and technical measures are taken continuously (For example, the documents to be prepared within the scope of PDPL have been prepared by considering the risks in this inventory)
* Personal data processing activities carried out by our company are audited by information security systems, technical systems and legal methods. Policies and procedures regarding personal data security are determined and regular controls are carried out within this scope.
* From time to time, our company may obtain services from external service providers in order to meet its information technology needs. In this case, the process is carried out by making sure that the said Data Processing external service providers are met at least the security measures provided by our Company. In this case, a written contract is signed with the Data Processor and this contract includes at least the following points:
	+ The Data Processor should act in accordance with the data processing purpose and scope specified in the contract only in line with the instructions of the Data Controller and in accordance with the PDPL and other legislation,
	+ The Data Processor should act in accordance with the Personal Data Storage and Destruction Policy,
	+ The Data Processor is subject to the indefinite confidentiality obligation regarding the personal data processed by it,
	+ In case of any data breach, the Data Processor is obliged to immediately notify the Data Controller of this situation,
	+ Our Company will make or have the necessary audits made on the systems of the Data Processor containing personal data, and may examine the reports resulting from the audit and the service provider company on site,
	+ It should take necessary technical and administrative measures for the security of personal data; and
	+ Also, as long as the nature of the relationship between the Data Processor and us allows, the categories and types of personal data transferred to the Data Processor are also specified in a separate article.
* As the Institution emphasizes in its guides and publications, personal data are reduced as much as possible within the framework of the data minimization principle and personal data that are not necessary, outdated and not serving a purpose are not collected and if it was collected in the period before the PDPL, it is destroyed in accordance with the Personal Data Storage and Destruction Policy.
* Expert staff on technical issues are employed.
* Our company has determined provisions regarding confidentiality and data security in the Employment Agreements to be signed during the recruitment process of its employees and asks employees to comply with these provisions. Employees are regularly informed and trained on the law on protection of personal data and taking necessary measures in accordance with this law. The roles and responsibilities of the employees were reviewed within this scope and their job descriptions were revised.
* Technical measures are taken in line with technological developments, the measures taken are periodically checked, updated and renewed.
* Access authorizations are limited and the authorities are regularly reviewed.
* The technical measures taken are regularly reported to the officer, and the risk factors are reviewed and efforts are made to create the necessary technological solutions.
* Software and hardware including virus protection systems and firewalls are installed.
* Backup programs are used to ensure the safe storage of personal data.
* Security systems are used for storage areas, the technical measures taken are periodically reported to the relevant person as required by internal audits, the necessary technological solutions are created by re-evaluating the risk factors. Files/outputs stored in physical media are stored through the supplier companies worked with and then destroyed in accordance with the determined procedures.
* The issue of Personal Data Protection is also adapted by the senior management, a special Committee (PDP Committee) was established on this subject and started to work. A management policy regulating the working rules of the Company's PDP Committee has been put into effect within the Company and the duties of the PDP Committee have been explained in detail.

# **HOW DO WE PROTECT YOUR SENSITIVE PERSONAL DATA?**

A separate policy regarding the processing and protection of sensitive personal data has been prepared and put into effect.

Since data on race, ethnicity, political thought, philosophical belief, religion, sect or other beliefs, appearance, membership of association, foundation or union, health, sexual life, criminal conviction and security measures as well as biometric and genetic data carry the risk of causing victimization or discrimination when they are processed unlawfully, Article 6 of the PDPL has organized these data as sensitive personal data and subjected the processing of these data to a more sensitive protection.

Our company clears the Relevant Persons during the acquisition of sensitive personal data in accordance with Article 10 of the PDPL. Sensitive personal data are processed by taking measures in accordance with the PDPL and by carrying out/having the necessary inspections carried out. As a rule, one of the conditions for processing sensitive personal data is the explicit consent of the data owner. Our company offers data owners the opportunity to express their explicit consent on a specific subject, based on keeping informed and with free will.

As a rule, our company obtains the explicit consent of the Related Persons in writing for the processing of sensitive personal data. However, in accordance with article 6/3 of the PDPL, in the presence of any of the conditions specified in article 5/2 of the PDPL, the explicit consent of the Related Persons is not sought. In addition, Article 6/3 of PDPL regulates that personal data related to health and sexual life can be processed by persons under the confidentiality obligation or authorized institutions and organizations without seeking the explicit consent of the relevant person for the protection of public health, performing preventive medicine, medical diagnosis, treatment and care services, planning and management of health services and financing. Regardless of the reason, general data processing principles are always considered in processing processes and compliance with these principles is ensured.

Our company takes special measures to ensure the security of sensitive personal data. In accordance with the principle of data minimization, sensitive personal data are not gathered unless required for the relevant business process and are processed only when necessary. In case of processing sensitive personal data, necessary technical and administrative measures are taken to comply with legal obligations and to comply with the measures determined by the PDP Committe.

# **WHAT ARE YOUR RIGHTS REGARDING YOUR PERSONAL DATA?**

As data owners, you have the following rights regarding your personal data in accordance with Article 11 of the PDPL:

* To learn whether your personal data is being processed by our Company,
* If your personal data has been processed, to request information regarding this,
* To learn the purpose of processing your personal data and whether they are used in accordance with their purpose,
* To know the third parties to whom your personal data was transferred domestically or abroad,
* To request correction of your personal data in case of incomplete or incorrect processing and to request notification of the transaction made within this scope to third parties to whom your personal data was transferred,
* Although it was processed in accordance with the provisions of PDPL and other relevant laws, to request the deletion or destruction of your personal data in case the reasons requiring the processing are eliminated and to request notification of the transaction made within this scope to third parties to whom your personal data has been transferred,
* To object to the occurrence of a result against you by analyzing the processed data exclusively through automated systems,
* To request the compensation of your damage in case you suffer damage due to unlawful processing of your personal data.

You can send your requests to our Company free of charge in accordance with the Application Communiqué by the method stated below:

1. After filled out the form on [**www.akkim.com.tr**](http://www.akkim.com.tr) and signed with wet signature, submission personally to Ak-kim Kimya Sanayi ve Ticaret A.Ş. Miralay Şefik Bey Sok. Akhan No:15 34437 Gümüşsuyu – İstanbul address (We would like to remind you that you will need to submit your ID card).
2. After filled out the form on [**www.akkim.com.tr**](http://www.akkim.com.tr) and signed with wet signature, sending to Ak-kim Kimya Sanayi ve Ticaret A.Ş. Miralay Şefik Bey Sok. Akhan No:15 34437 Gümüşsuyu – İstanbul address through a notary public.
3. After filled out the form on [**www.akkim.com.tr**](http://www.akkim.com.tr) and signed with your “secure electronic signature” within the scope of Electronic Signature Law No. 5070, sending secure electronic signed form to akkim@hs02.kep.tr address by registered e-mail.
4. Submission in writing using your e-mail address previously notified to our company and registered in our Company's system.

In the application;

Name, surname and signature if the application is in writing, T.R. Identification number for Turkish citizens, nationality, passport number or identification number for foreigners, residential or workplace address for notification, e-mail address, telephone and fax number for notification, if any, the subject of the request should be. Information and documents on the subject are also attached to the application.

It is not possible to make requests by third parties on behalf of personal data owners. In order for a person other than the personal data owner to make a request, there must be a wet signed and notarized copy of the special power of attorney issued by the personal data owner regarding the issue on behalf of the applicant. In the application that you will make to exercise your rights you have and above mentioned as personal data owner and include your explanations about the right you request to exercise; the matter you request must be clear and understandable, the subject you request must be related to you own or if you are acting on behalf of someone else, you must be specially authorized in this regard and document your authority, the application must contain identity and address information and documents certifying your identity must be attached to the application.

Applications made within this scope will be finalized in the shortest possible time frame and within 30 days at the most. These applications are free of charge. However, if the transaction requires an additional cost, the fee in the tariff determined by the PDP Committee may be applied.

In case the personal data owner submits his/her request to our Company in accordance with the prescribed procedure, our company will conclude the relevant request free of charge as soon as possible and within thirty days at the latest depending on the nature of the request. However, if the transaction requires an additional cost, the fee in the tariff determined by the PDP Committee will be collected from the applicant by our Company. Our company may request information from the relevant person in order to determine whether the applicant is the owner of personal data. In order to clarify the matters included in the application of the personal data owner, our company may ask a question to the personal data owner about his/her application.

In case your application is rejected by our Company in accordance with Article 14 of PDPL, you find our answer insufficient or we do not respond to the application in time; you can make a complaint to the PDP Committee within thirty days from the date you learn the response of our company, and in any case within sixty days from the date of application.

# **WHAT ARE THE SITUATIONS WHERE DATA OWNERS CANNOT CLAIM THEIR RIGHTS?**

Personal data owners cannot claim the above-mentioned rights of personal data owners in these matters, since the following cases are excluded from the scope of PDPL in accordance with Article 28 of the PDPL:

* Processing of personal data for purposes such as research, planning and statistics by making them anonymous with official statistics.
* Processing of personal data for artistic, historical, literary or scientific purposes or within the scope of freedom of expression providing that they do not violate national defense, national security, public security, public order, economic security, privacy of private life or personal rights or constitute a crime.
* Processing of personal data within the scope of preventive, protective and intelligence activities carried out by public institutions and organizations authorized by law to ensure national defense, national security, public security, public order or economic security.
* Processing of personal data by judicial or execution authorities in relation to investigation, prosecution, trial or execution proceedings.

In accordance with the article 28/2 of the PDPL; In the cases listed below, personal data owners cannot claim their other rights, except the right to demand compensation:

* Processing of personal data is necessary for the prevention of crime or for a criminal investigation.
* Processing personal data made public by the personal data owner himself.
* Processing of personal data is necessary for the performance of supervisory or regulatory duties and for disciplinary investigation or prosecution by attendant and authorized public institutions and organizations and professional organizations that are public institutions on the basis of authority given by law.
* Processing of personal data is necessary for the protection of the economic and financial interests of the State regarding budget, tax and financial issues

# **OTHER ISSUES**

As explained in detail above, Your personal data can be stored and kept, can be classified as per market research, financial and operational processes and marketing activities, can be updated in different periods and, to the extent permitted by the legislation, within the framework of the laws and confidentiality principles, can be transferred to third parties and/or suppliers and/or service providers and/or our foreign shareholders as required by the service, information can be transferred and stored in accordance with the policies we adhere to and for reasons stipulated by other authorities, can be processed by reporting, records and documents can be arranged in electronic or paper media as the basis for processing.

In case of inconsistency between the provisions of PDPL and other relevant legislation and this Policy, PDPL and other relevant legislation provisions will be applied first.

This document prepared by our company entered into force in accordance with the decision taken by the Board of Directors of Ak-Kim.

We would like to remind you that we may make updates to this statement due to the legislative provisions that may change over time and the changes that may occur in our company policies. We will published the most current version of the Notice on our website.

Before entering the website, user/users accepted, declared and committed irrevocably that they have read this Personal Data Protection Policy, they will comply with all the matters stated here, the contents of the website and all electronic media and computer records belonging to our Company will be considered as definitive evidence in accordance with Article 193 of the Civil Procedure Law.

## **ANNEX – ABBREVIATIONS**

|  |
| --- |
| ABREVIATIONS |
| Law No. 5651 | [Law on Regulation of Publications on the Internet and Suppression of Crimes Committed By Means of Such Publications](https://tureng.com/tr/turkce-ingilizce/law%20on%20regulation%20of%20publications%20on%20the%20internet%20and%20suppression%20of%20crimes%20committed%20by%20means%20of%20such%20publications), entered into force by being published in the Official Gazette dated May 23, 2007 and numbered 26530  |
| Constitution | The Constitution of the Republic of Turkey numbered 2709, dated November 7, 1982, published in the Official Gazette dated November 9, 1982 and numbered 17863 |
| Application Notice | Communiqué on Application Procedures and Principles to the Data Controller, entered into force by being published in the Official Gazette numbered 30356 dated March 10, 2018 |
| Relevant Person/Relevant Persons or Data Owner | It refers to the real person whose personal data is processed, such as customers, corporate customers with whom it has commercial relations, business partners, shareholders, officials, candidate employees, interns, visitors, suppliers of Akkim and/or Akkök Holding group companies, employees of the institutions it works with, third parties and other persons, including but not limited to those listed herein. |
| Regulation on Deletion, Destruction or Anonymization of Personal Data | Regulation on Deletion, Destruction or Anonymization of Personal Data, published in the Official Gazette dated October 28, 2017 and numbered 30224 and entered into force as of January 1, 2018 |
| PDPL | The Law on Protection of Personal Data published in the Official Gazette dated April 7, 2016 and numbered 29677 |
| PDP Committee | Personal Data Protection Committee |
| PDP Institution | Personal Data Protection Institution |
| a. | Article |
| Ex. | Example |
| Policy | This Akkim Personal Data Protection and Privacy Policy |
| Company/Akkim | Ak-kim Kimya Sanayi ve Ticaret A.Ş |
| Turkish Penal Code | Turkish Penal Code numbered 5237 and dated 26 September 2004; published in the Official Gazette dated October 12, 2004 and numbered 25611 |