Personal Data Policy and Implementation Procedures

İnterkap Ambalaj San. ve Tic. A.Ş.	**Personal Data Policy and Implementation Procedures**	Rev. V2
Document No:		Date: 19.01.2021
Related Units	İnterkap Ambalaj San. ve Tic. A.Ş Human Resources Department İnterkap Ambalaj San. ve Tic. A.Ş Finance Department	
Revisions	First Publishing	Date: 16.03.2020

With the Personal Data Policy and Implementation Procedures ("**Policy"**), **İnterkap Ambalaj San. ve Tic. A.Ş** ("**Company**") sets forth the procedures that shall be implemented to the; processing, protection, storage and annihilation of the personal data.

Company shall create the necessary structure, procedures and processes for compliance with the legislations and shall actualize the necessary mechanism to create awareness with the employees and business partners.

From Company website, it is reachable to the Privacy Policy, Terms and Conditions, Personal Data Processing and Protection Enlightenment Text, Application Request Form and this Policy text.

1. Purpose

This Policy is prepared in order to determine the procedures and principles regarding the data collection, protection, storage and destruction of personal data carried out by the Company.

The Company aims to process, store, annihilate, share the data belonging to the Company employees, employee nominees, service providers, suppliers, visitors and other third party entities, and ensure that the relevant persons exercise their rights effectively in accordance with the relating legislations especially in accordance with the Law on Protection of Personal Data, numbered 6698 ("**Law**").

The work and transactions regarding the collection, storage and annihilation of personal data are carried out in a limited and measured scope, in accordance with the Policy prepared by the Company in this direction, the implementation principles and decisions of the Personal Data Protection Board and the Law.

2. Scope

Personal Data of the Company employees, employee nominees, service providers, suppliers, visitors and any other third entity falls under the scope of this Policy and this Policy shall be applied in all recording media where personal data owned or managed by the Company are processed and in activities related to personal data processing.

3. Definitions

The defined terms in the policy are used in the meanings they are defined below.

Recipient Group: The real or legal entity that the personal data is being transferred to.

Related User: Except for the person or unit responsible for the technical storage, protection and backup of the data, the persons who process personal data within the organization of the data controller or in accordance with the authorization and instruction received from the data controller.

Annihilation: The deleting, abolishing or anonymization of the personal data.

Law: Law on the Protection of the Personal Data numbered 6698.

Recording Media: Any media that is either completely or partially automatic, or all kinds of media containing personal data processed by non-automatic means provided that it is part of any data storage system.

Personal Data: Any information relating an identified or at least identifiable real person.

Personal Data Owner: Real person whose personal data is processed.

Processing of Personal Data: Any transaction on the personal data completed by any ways, such as; the obtaining personal data by fully or partially automated or non-automatic means provided that they are part of any data recording system, recording, storing, preserving, changing, re-arranging, declaring, taking over, making obtainable, classifying and preventing the usage.

Personal Data Processing Inventory: Personal data processing activities carried out by data controllers depending on the business processes; The inventory, which they have created by associating with the personal data processing purposes, the data category, the recipient group and the data subject group, and elaborated by explaining the maximum period required for the purposes for which the personal data is processed, the personal data foreseen to be transferred to foreign countries and the measures taken regarding data security.

Board: Personal Data Protection Board.

Authority: Personal Data Protection Authority

Sensitive Personal Data: Any information regarding a person’s race, ethnical origins, political opinions, philosophical beliefs, religion, sect or any other belief, clothes, membership to any association, foundation or union, health, sexual life, conviction and security measures and any biometric and genetical data

Periodic Annihilation: The deletion, abolishment or anonymization process to be carried out ex officio at recurring intervals specified in the personal data storage and destruction policy in the event that all the conditions for processing personal data included in the law are eliminated**.**

Policy: It refers to this Policy, on which data controllers make the basis for the process of determining the maximum time required for the purpose for which personal data are processed, and for deletion, abolishment and anonymization.

Registry: The Data Controller Registry kept by Personal Data Protection Authority Chairmanship.

Data Processor: Real or legal entity processing personal data on behalf of the Data Holder, with the authorization of Data Holder.

Data Recording System: The recording system into which the personal data is processed after being restructured according to certain criteria.

For any term not defined at the Policy, the legal definitions shall be applicable.

4. Protecting the Rights of the Data Owner

The Company carries out the necessary internal channels, internal operations, administrative and technical arrangements in order to evaluate the rights of personal data owners and keep the personal data owners updated in accordance with Law.

In the event that personal data owners submit their requests regarding their rights in writing to the Company in accordance with Article 11 of the Law, the Company shall conclude the request as soon as possible and free of charge within 30 days at the latest, depending on the nature of the request. In case the transaction needs an extra fee, the fee determined by the Board shall be taken by the Company. While exercising their rights, the personal data owners shall convey their demands in writing or by means which are set forth by the Law. Since the Board has not determined any other method yet, at this stage, data owners are required to submit their requests in writing.

5. Responsibility and Work Distribution

All units and employees of the Company shall support actively the responsible units in the proper application, monitoring and constant audit of the administrative and technical measures taken under the scope of this Procedure, and in the creation of the proper technical measures primarily to ensure the safety of all data processing mediums in order to prevent the unlawful processing of the personal data, unlawful obtaining of the personal data and also the lawful processing, storing, annihilation, sharing of the personal data. Bell Group companies and the Company has created the data inventory regarding the personal data processing, with the participation of their related units and employees.

6. Information on Storage and Disposal

The personal data relating the employees, employee nominees, visitors, suppliers, service providers and any other engaging third parties, the employees of the institutions and organizations are kept and annihilated in accordance with the Law by the Company. Within this scope, please find the detailed information on storage and annihilation below in order.

Accordingly, within the framework of the Company's activities, personal data are stored for the period stipulated in the relevant legislation or in accordance with our processing purposes and in any case within the scope specified in the VERBIS records in the personal data inventory.

7. Legal Reasons for Storage

Personal data processed within the framework of the company's activities are stored in accordance with the relevant legislation, in personal data inventory, within the scope specified in VERBIS records or for the period specified in this Policy to the extent applicable.

As such, the personal data are stored in accordance with the laws applicable on the Company and its activities and other secondary regulations in force pursuant to these laws, if there are mandatory retention and proof periods, taking these periods into consideration. The notable and primary legislations are listed below.

- Law No. 6698 on Protection of Personal Data,
- Turkish Code of Obligations No. 6098,
- Social Insurance and General Health Insurance Law No. 5510,
- Occupational Health and Safety Law No. 6331,
- Labor Law No. 4857,
- Regulation on Health and Safety Measures to be Taken in Workplace Building and Extensions,
- Regulation on Archive Services,

Tax Procedure Law No. 213

The retention periods for the processes determined in line with the personal data inventory are also regulated in Article 18 of this Policy.

8. Processing Purposes Requiring Storage

The company stores the personal data processed within the framework of its activities for the following purposes:

- To carry out human resources processes,
- To provide corporate communication,
- Ensuring company security,
- To ensure occupational health and safety,
- To be able to do statistical studies,

- To be able to carry out works and transactions as a result of contracts and protocols signed,
- To ensure the fulfillment of legal obligations as required or required by legal regulations,
- To establish contact with real / legal persons who have business relations with the company,
- To be able to provide documents that qualify as evidence to the relevant institutions, organizations, courts and enforcement offices within the scope of the obligation to prove as evidence in future legal disputes,
- To provide selection and placement services and to create the necessary documentation for these services.

9. Reasons for Annihilation

Personal data is deleted, destroyed by the Company at the request of the person concerned or ex officio deleted, destroyed or anonymized by the Company in following cases:

- The amendment or abolition of the relevant legislation provisions that form the basis for processing
- The disappearance of the purpose requiring processing or storage,
- In cases where the processing of personal data takes place only on the condition of explicit consent, the person concerned withdraws their explicit consent,
- Acceptance of the application made by the Company for the deletion and annihilation of personal data within the framework of the rights of the person concerned in accordance with Article 11 of the Law,
- In the event that the Company rejects the application made by the person concerned with the request for deletion, annihilation or anonymization of the personal data, finds the answer inadequate or does not receive a response within the period stipulated in the Law; the person concerned filing a complaint to the Board and this request is approved by the Board,
- In the event that the maximum period requiring the storage of personal data has passed and there are no conditions to justify the storage of personal data for a longer period.

10. Technical and Administrative Measures

In order to store the personal data safely, prevent the unlawful processing and accessing, and ensure the lawful annihilation of the personal data, in accordance with the related articles of the Law, the measures listed below in 11th, 12th, 13th and 14th clause of this policy are taken.

11. Technical Measures

The technical measures taken by the company in relation to the personal data it processes are listed below:

- As a result of real-time analysis with information security event management, risks and threats that may affect the continuity of information systems are continuously monitored.

- Access to information systems and authorization of users; It is done through the enterprise active directory and security policies through the enterprise and authorization matrix.
- The necessary measures for the Company's information systems, software and physical safety of the data are being taken.
- Risks to prevent unlawful processing of personal data are determined, technical measures are taken in accordance with these risks and technical controls are carried out for the measures taken.
- Accesses to storage mediums where personal data are stored are recorded and inappropriate access or access attempts are kept under control.
- The Authority takes the necessary measures to ensure that the deleted personal data are inaccessible and unavailable for the relevant users.
- In case personal data is illegally obtained by others, a suitable system and infrastructure has been established by the Authority to notify the relevant person and the Board.
- Security deficits are tracked and updated with the suitable security patches the information systems are kept up to date.
- Secure record keeping (logging) systems are used in electronic environments where personal data are processed.
- To ensure the safe storage, data backup programs are used.
- Access to the Company website is encrypted with SHA 256 Bit RSA algorithm using secure protocol (HTTPS).
- Sensitive personal data security trainings have been provided for employees involved in sensitive personal data processing processes, confidentiality agreements have been made, and the authorities of users with access to data have been defined.
- Electronic environments where sensitive personal data are processed, stored and/or accessed are preserved using cryptographic methods, cryptographic keys are kept in secure environments, all transaction records are logged, security updates of the environments are constantly monitored, necessary security tests are carried out regularly, test results are recorded.
- Adequate security measures are taken in physical environments where sensitive personal data are processed, stored and/or accessed, and unauthorized entry and exit are prevented by ensuring physical security.

12. Administrative Measures

Administrative measures relating the personal data they process, taken by the Company are listed below:

- In order to improve the quality of employees, training is provided on the prevention of unlawful processing of personal data, prevention of illegal access to personal data, protection of personal data, communication techniques, technical knowledge skills, Law and other relevant legislation.
- The training regarding these areas are annually updated.
- Legal Consultancy Service is being taken to ensure the compliance with the Law and legislation regarding protection of the personal data.
- Employees sign confidentiality agreement relating the operations carried out by the Company.

- A disciplinary procedure is set forth for the employees who do not comply with the security policy and procedures.
- Before starting to process personal data, the Company fulfills the obligation to enlighten the relevant persons.
- Personal Data Processing Inventory has been prepared.
- Work flow processes were defined for each service and transferred to employees; and they have been added to the common archive area so that everyone can access it whenever they want.
- The administrative measure arrangements are included in the contracts and at the transactions between the Company and clients,
- The administrative measure arrangements are included in the contracts and at the transactions between the Company and suppliers

13. Annihilation Techniques

At the end of the period foreseen in the relevant legislation or the storage period required for the purpose for which they are processed, personal data are destroyed by the Company either ex officio or upon the application of the relevant person, again in accordance techniques with the provisions of the relevant legislation.

14. Anonymization of the Personal Data

Anonymization of the personal data is the process of rendering of personal data that cannot be associated with an identified or identifiable natural person under any circumstances, even if they are matched with other data.

In order for personal data to be anonymized; Personal data must be rendered in such way that they must be made unrelated to a specific or identifiable natural person unrelated to an identified or identifiable natural person, even through the use of appropriate techniques in terms of the recording medium and the relevant field of activity, such as the return of personal data by the data controller or third parties and/ or matching the data with other data.

15. Periodic Annihilation

In accordance with the 11th article of the Regulation on Deleting, Annihilation or Anonymization of the Personal Data, the Company has set the periodic annihilation period as 6 months.

16. Transfer of the Personal Data

The Company may transfer the data owner's personal data to third parties by taking the necessary security measures in line with the personal data processing purposes in accordance with the legislation and by obtaining explicit consent in cases where explicit consent is required. The Company acts in accordance with the regulations set forth at the 8th article of the Law. According to the 8th article, the personal data shall not be transferred to the third parties without the explicit consent of the data owner. However, when the circumstances specified in the second paragraph of Article 5 of

the Law exist, personal data may be transferred to third parties in the country without the explicit consent of the data owner.

17. Transfer Abroad

As a rule, personal data cannot be transferred abroad without the explicit consent of the data owner in accordance with Article 9 of the Law. However, the personal data may be transferred abroad without explicit consent, in the presence of one of the reasons stated in article 5 of the law and if the foreign country has the below-mentioned mechanisms:

- Adequate protection shall be available
- In the absence of adequate protection, the data holders both in Turkey and foreign countries shall guarantee an adequate protection in writing, and if the Board approves.

The Company may transfer the personal data to an abroad country in which the data holder who has an adequate protection or at least guaranteeing an adequate protection resides, in line with the lawful personal data processing reasons, if the explicit consent of the data owner present or the explicit consent is not present but one of the below-mentioned reasons is present:

- In the event that an explicit regulation in legislation for transfer of the personal data,
- If it is necessary for the protection of the life or body integrity of the personal data owner or someone else, and if the personal data owner is unable to disclose her consent due to the actual impossibility or their consent is not legally valid;
- If it is necessary to transfer personal data of the parties to the contract, provided that it is directly related to the establishment or performance of a contract,
- In the event that the data transferring is necessary in order for Company to fulfill their legal responsibilities,
- In the event that personal data are made public by the personal data owner,
- In the event that the transfer of personal data is mandatory for the establishment, exercise or protection of a right,
- In the event that the personal data transfer is mandatory for the legitimate interests of the Company, provided that it does not harm the fundamental rights and freedoms of the personal data owner.

As the main principle, the Company embarked on the limitation and proportionality principles and the explicit consent by any means if applicable, at the necessary transfers abroad. The informative text on the website of the company ensures the explicit consent to be obtained with a separate document after the necessary information provided in the legislation.

18. Sensitive Personal Data

The Company processes the sensitive personal data in the light of the principles of limitation and proportionality as stipulated by the legislation. In this direction, all administrative and technical measures have been taken.

If the Media where sensitive data are processed, stored, and/or accessed are electronic:
a) The storage of the data with cryptographic methods,
b) Keeping the cryptographic keys in different and safe medias,
c) Secure logging of transaction records of all transactions performed on the data,
d) Continuous monitoring of the security updates of the environment where the data is located, regularly performing/having the necessary security tests, recording the test results,
e) In the event that the data is accessible through a software, completing the authorization of users, regularly performing/having the necessary security tests, recording the test results,
f) Providing at least two-step authentication system if remote access to data is required,

If the sensitive data are processed, stored, and/or accessed in physical environment:
a) Ensuring the adequate security measures for the environment in which the sensitive personal data is kept (e.g. for electrical leakage, fires, floods, burglary, etc.)
b) Ensuring the physical security of these environments and preventing unauthorized entries and exits,

In the event of a transfer of sensitive personal data:
a) If data need to be transferred via e-mail, the Company transfers them in encrypted form using a corporate e-mail address or a Registered Electronic Mail (REP) account,
b) If data need to be transferred via medias such as memory stick, CD, DVD, etc., the Company encrypts them using cryptographic methods and keeps the cryptographic keys in different environments,
c) If transfer is made between servers in different physical environments, the Company transfers data between servers by setting up a VPN or using sFTP method,
d) If the data needs to be transferred via paper media, the necessary measures have been taken against risks such as theft, loss or being seen by unauthorized persons by the Company.

19. Transferred Third Parties

In accordance with Articles 8 and 9 of the Law, the Company may transfer the personal data of data owners to third parties categorically listed below:

- Companies in countries where personal data is legally protected, especially Bell Group companies,
- Business partners,
- Banks and insurance companies,
- Legally authorized state institutions and organizations.

20. Updating Period

The Policy is reevaluated when needed and it is updated to the extent where necessary.

21. Enforcement

The policy is deemed to have entered into force after its publication on the Company website.