KYOCERA Bilgitaş Turkey Doküman Çözümleri A.Ş.

SENSITIVE PERSONAL DATA PROTECTION AND PROCESSING POLICY

Information on Document	
Name of Document	Policy on Protection and Processing of Sensitive Personal Data of "Kyocera Bilgitaş Turkey Doküman Çözümleri A.Ş."
Target Group	All real persons whose sensitive personal data is processed by "Kyocera Bilgitaş Turkey Doküman Çözümleri A.Ş."
Reference / Reason	Law of 6698 Protection of Personal Data, the decision with number 2018/10 and date 31/01/2018 of the Council of the Protection of Personal Data and other relevant secondary regulations and the resolutions of the Council of Protection of Personal Data

If there is a discrepancy between this Policy on Protection and Processing of Sensitive Personal Data in Turkish and the translation of this document, the text in Turkish shall be valid.

This document cannot be copied or distributed without written permit of Kyocera Bilgitaş Turkey Doküman Çözümleri A.Ş.

1. PURPOSE OF THE POLICY AND CONFIDENTIALITY COMMITMENT

1.1. The primary value and purpose of Kyocera Bilgitaş Turkey Doküman Çözümleri A.Ş. (hereinafter referred to as the "**Company**" briefly) is to protect your fundamental rights and freedoms and your privacy in processing of your sensitive personal data and to secure your sensitive personal data, especially privacy of your personal life. Within this scope, the basic principles adopted for the conformity of the principles for personal data processing transactions carried out by our Company within the framework of the Policy on Protection and Processing of Sensitive Personal Data ("**Policy**") and the personal data processing transactions of our company are defined in accordance with the Law of 6698 Protection of Personal Data and the relevant secondary regulations and implementations and thus, our company provides the necessary transparency by giving information to you, as the data subjects.

1.2. Our company undertakes to process and protect your personal data in accordance with the relevant legislation, this Policy and the procedures that may be applied according to this Policy with the full sense of responsibility.

2. SCOPE OF POLICY

2.1. This Policy is applied to all sensitive personal data of all real persons whose personal data is processed automatically or nonautomatically on condition of being a part of any data recording system. In this context, this Policy applies primarily to employees, job applicants, customers, suppliers, visitors, and all other categories of natural persons whose special categories of personal data may be processed by the Company.

2.2. This Policy covers and applies to all data processing activities directed towards the sensitive personal data that the Company is processing. In this context, the Policy covers all physical and electronic processing environments, including electronic systems, physical archives, cloud computing environments (if used), third-party systems, and systems operated by outsourced service providers where special categories of personal data are processed or stored.

2.3. This Policy does not apply to the data which are not defined as sensitive personal data.

2.4. This Policy may be amended by the approval of the Board of Management from time to time as deemed necessary by the Company or by the relevant legislation.

2.5. If there is a discrepancy between the relevant legislation regulations and this Policy, the relevant legislation regulations shall prevail.

3. ROLES AND RESPONSIBILITIES

3.1. The roles, authorities, and responsibilities of all departments and employees involved in data processing activities are set forth below in order to ensure that special categories of personal data are processed within the Company in a lawful, secure, and accountable manner. Each stakeholder is obliged to act in accordance with the provisions

of this Policy and the applicable Data Protection Regulations within the scope of their respective duties.

3.2. Board of Directors

- Approving and implementing this Policy;
- Ensuring that the necessary organizational structure is established for the implementation of the Policy;
- Overseeing the effective execution of KVKK compliance activities.

3.3. Personal Data Protection Committee

- Ensuring the preparation and updating of the Policy and relevant procedures;
- Monitoring the compliance of special categories of personal data processing activities with applicable legislation;
- Coordinating data breach processes;
- Planning training and awareness activities.

3.4. Information Technology Department

- Implementing technical security measures relating to special categories of personal data;
- Carrying out authorization, access control, logging, backup, and other information security controls;
- Taking the necessary actions to remediate technical security vulnerabilities.

3.5. Human Resources Department

- Ensuring that employees' special categories of personal data are processed in accordance with applicable legislation;
- Acting in accordance with the provisions of the Policy in recruitment, personnel records, and occupational health and safety processes.

3.6. All Employees

- Complying with the provisions of this Policy;
- Maintaining the confidentiality of special categories of personal data they process within the scope of their authority;
- Reporting, without undue delay, any incidents that may affect data security to the relevant departments;
- Not using the access rights assigned to them for purposes other than those for which they were granted.

4. DEFINITIONS

The definitions in this Policy have the meanings mentioned below:

"Personal Data"	All information related to a real person whose identity is known or identifiable,
"Committee"	Committee of Protection of Personal Data of the Company,
"Council"	Council of Protection of Personal Data,

"Authority"	Personal Data Protection Authority,
"KVKKVKK"	Law of 6698 on Protection of Personal Data,
"KVK Regulations"	all regulations and amendments for the protection of Personal data which may be applied in the future and all legislation regulations related to the protection of Personal Data in force, especially KVKK, Council decisions, Authority guides and public announcements, decisions/instructions of other regulative and supervisory authorities, courts and other official bodies,
"KVK Policies"	Policies issued on Protection of Personal Data by the Company,
"KVK Procedures"	procedures defining the obligations to be followed by the Company, the Company employees and the Committee in accordance with the KVK Policies,
"Sensitive Personal Data"	data on race, ethnic origin, political opinion, philosophical beliefs, religion, denomination or other beliefs, appearance, association, foundation and union membership, health, sexual life, criminal conviction and security measure of the people and biometric and genetic data,
"Processing of Sensitive Personal Data"	all kinds of transactions carried out on the data such as obtaining wholly or partly by automatically or nonautomatically on condition of being a part of any data recording system, recording, storing, keeping, changing, reissuing, disclosing, transferring, taking over, making accessible, classifying or preventing using of Personal Data,
"Personal Data Processing Inventory"	An inventory detailing the processing of Personal Data carried out in accordance with business processes, which is compiled by linking such processing activities to the purposes of processing, the category of data, the group of recipients to whom the data is transferred, and the group of data subjects; and which sets out the maximum period necessary for the purposes for which the Personal Data is processed, the Personal Data intended for transfer to foreign countries, and the measures taken regarding data security, as disclosed and detailed by the Company,

5. BASIC PRINCIPLES OF PROCESSING OF PERSONAL DATA

Processing of Sensitive Personal Data in accordance with the law and good faith

The company processes the Sensitive Personal Data in accordance with the law and good faith based on principle of proportionality. Within this scope, the Company processes the Sensitive Personal Data to the extent required by the Company's business activities and limited to such activities.

Ensuring Sensitive Personal Data is Accurate and Up-to-Date Where Necessary

The company takes all kinds of measures required to provide truthful and updated during the time that the sensitive personal data is processed. Within this scope, the Company

establishes the required mechanisms related to providing truthful and updated Sensitive Personal Data and updates the relevant sensitive Personal Data pursuant to the request of the Relevant Person (Data subject) for amendment requests of the Sensitive Personal Data within scope of KVKK Regulations.

Processing of Sensitive Personal Data for Specific, Explicit and Legitimate Purposes

Before the Sensitive Personal Data is processed, the purpose for which the Sensitive Personal Data shall be processed is determined by the Company. Within this scope, the Company explicitly presents the purpose of processing the Sensitive Personal Data and processes the Sensitive Personal Data according to the business activities and for purposes related to such activities. In this context, the relevant persons (data subjects) are informed in accordance with the KVK Regulations and the Explicit Consent of the said persons are obtained when necessary.

Sensitive Personal Data Being Relevant, Limited, and Proportionate to the Purposes for Which They are Processed

The company only collects the Sensitive Personal Data to the extent and in manner required by the business activities and processes them limited to the purposes determined. In this context, the Company avoids from processing the Sensitive Personal Data which are not related to the achieving the purposes determined or not required

Retention of Sensitive Personal Data for the Period Anticipated in the Relevant Legislation or Necessary for the Purpose for Which They are Processed

The company retains the Sensitive Personal Data for the period minimum anticipated in the relevant legislation and necessary for the purpose which they are processed. The Company determines whether a period is anticipated to store the Sensitive Personal Data in the relevant legislation and if a period is determined, it conforms to such period. If there is no legal period, the Sensitive Personal Data is stored for a period required for the purpose which they are processed.

The Sensitive Personal Data is disposed by the Disposal Methods (deletion and/or destruction and/or anonymization) determined and in accordance with the periodical disposal periods at the end of the storing period determined or the application of the Relevant Person (Data Subject). At this stage, it is ensured that the third parties to whom the Sensitive Personal Data is transferred shall delete, destroy or anonymized the Sensitive Personal Data.

The Committee is responsible for managing disposal process. The required procedure is determined by the Committee.

6. PROCESSING OF SENSITIVE PERSONAL DATA

The Sensitive Personal Data is processed in accordance with the rules and principles mentioned in this Policy and by taking all kinds of administrative and technical measures required including the methods determined by the Council and in case that the conditions below are existed:

- Explicit consent of the relevant person (data subject),
- Being explicitly anticipated by laws,
- Being compulsory in order to protect the integrity or the life or body or the person or another person who cannot provide consent due to actual impossibility or whose consent is not lawfully valid,

- If it is related to the personal data of the relevant person (data subject) who has made it public and conformed to the rule of making public,
- Being compulsory to process in order to establish or protect a right,
- Where necessary for the protection of public health, the provision of preventive healthcare, medical diagnosis, treatment and care services, and the planning, management and financing of healthcare services, by persons or authorised bodies and organisations subject to a duty of confidentiality,
- Being compulsory in order to comply with legal obligations in the areas of employment, occupational health and safety, social security, social services and social assistance,
- Foundations, associations and other non-profit organisations or bodies established for political, philosophical, religious or trade union purposes may, provided that they comply with the legislation to which they are subject and their stated objectives, that their activities are limited to their specific fields of operation, and that no information is disclosed to third parties, direct their activities towards their current or former members and affiliates, or towards persons who are in regular contact with such organisations or bodies

7. SENSITIVE PERSONAL DATA PROCESSED BY THE COMPANY AND REASON FOR PROCESSING

The Sensitive Personal Data is processed according to the general principles determined in KVKKVKK, especially the principles defined in the article 4 of KVKKVKK related to the Sensitive Personal Data Processing based on and limited to at least one of the principles of the Sensitive Personal Data Processing determined in the article 5 of KVKKVKK in accordance with the purposes of Personal Data processing of the Company by giving information to the Relevant persons (data subjects) according to the KVK Regulations in the Company. The Processed personal data categories and the detailed information related to the purposes of the personal data processing within the framework of the purposes and principles defined in this Policy are determined in ANNEX 1 (*ANNEX 1 – Sensitive Personal Data Categories and Processing Purposes of Sensitive Personal Data*) of this Policy.

8. RETENTION PERIOD AND DISPOSAL OF PERSONAL DATA

7.1. The Company retains the Sensitive Personal Data for a period required and anticipated in the relevant legal legislation for the purpose of processing. The company primarily determines if there is a period anticipated to retain the Sensitive Personal Data in the relevant legislation and if a period is anticipated, it conforms to such period. If there is no legal period, the Sensitive Personal Data is retained for a period required to process them. The Sensitive Personal Data is not retained by the Company by considering to use it in the future.

7.2. The Company establishes a Personal Data Retention and Disposal Policy in accordance with the Sensitive Personal Data processing inventory and performs its activities related to the Disposal (deletion and/or destruction and/or anonymization) in accordance with the KVK Regulations and the relevant Sensitive Personal Data Retention and Disposal Policy. The Disposal process is managed by the Committee. The Committee establishes the necessary procedure within this scope.

9. TRANSFER OF SENSITIVE PERSONAL DATA

8.1. The Sensitive Personal Data may be transferred by the Company in accordance with the principles set out in this Policy, provided that all necessary administrative and technical measures—including those determined by the Board—are taken and the following conditions are met:

- The personal data may be transferred abroad by data controllers and data processors provided that one of the conditions set out in Articles 5 and 6 of the Act is met and there is an adequacy decision in place regarding the country to which the data is to be transferred, sectors within that country, or international organisations.

- The personal data may be transferred abroad by data controllers and data processors provided that, in the absence of a decision on adequacy, one of the conditions set out in Articles 5 and 6 is met, and provided that the data subject has the opportunity to exercise their rights and have access to effective legal remedies in the country to which the data is to be transferred, and provided that the parties provide one of the appropriate safeguards set out below:

  a) If there is an agreement—not constituting an international treaty—between public institutions and organisations abroad or international organisations and public institutions and organisations in Turkey, or professional bodies with the status of public institutions and the Board's authorisation of the transfer.
  b) If the binding corporate rules, approved by the Board, containing provisions on the protection of personal data, to which companies within a group of undertakings engaged in joint economic activities are required to comply is existed.
  c) If there is a standard contract containing matters such as the categories of data, the purposes of the data transfer, the recipients and categories of recipients, the technical and organisational measures to be taken by the data recipient, and the additional safeguards adopted for special categories of personal data, as announced by the Council.
  ç) If there is a written undertaking containing provisions that ensure adequate protection and the Board's authorisation of the transfer.

- Data controllers and data processors may transfer personal data abroad only on an ad hoc basis and solely where one of the following conditions is met, provided that no adequacy decision exists and none of the appropriate safeguards provided for in the fourth paragraph can be provided:
  a) The relevant persons (data subjects) explicit consent to the transfer, provided that they have been informed of the potential risks.
  b) The transfer is necessary for the performance of a contract between the data subject and the data controller, or for the implementation of pre-contractual measures taken at the relevant person's (data subject's) request.
  c) The transfer is necessary for the conclusion or performance of a contract to be entered into between the data controller and another real or legal person for the benefit of the data subject.
  ç) The transfer is necessary for an outstanding public interest.
  d) The transfer of personal data is necessary for the establishment, exercise or defence of a legal claim.

e) The transfer of personal data is necessary to protect the life or physical integrity of the relevant person or another person, where the relevant person (data subject) is unable to give consent due to actual impossibility or where their consent is not legally valid.
f) The transfer of personal data from a register open to the public or to persons with a legitimate interest, provided that the conditions required by the relevant legislation for access to the register are met and the person with a legitimate interest makes a request.

10. THE COMPANY'S OBLIGATION TO INFORM

9.1. The company informs the relevant persons (data subjects) before processing the Sensitive Personal Data in accordance with the provisions of the Communique on Rules and Principles to be followed to fulfil the Obligation to Inform and the article 10 of KVKK. In the context, the Company notifies the Relevant Person (Data Subject) about by whom the Sensitive Personal Data is processed in accordance with the KVK Regulations as the Data Controller, for which purposes it is used, with whom they are shared, by which methods are used to collect and the lawful reason for processing and the rights of the Relevant persons (data subjects) within scope of processing the Sensitive Personal Data.

9.2. The necessary KVK Procedures are established in order to report all new Personal Data processing procedures to the Committee.

9.3. If the Sensitive Personal Data is transferred to a third party except the Company, the third party undertakes to act in accordance with the obligations mentioned above in written by a contract before processing the Personal Data. In case a Personal Data is transferred to the Company by a third party, each employee is obliged to conform to the process in this Policy and KVK Procedures.

11. RIGHTS OF THE RELEVANT PERSONS (DATA SUBJECTS)

10.1. The relevant persons (data subjects) have the rights mentioned below:

- To know whether the Sensitive Personal Data is processed or not,
- To request information if the Sensitive Personal Data is processed,
- To request information about the purpose of processing and whether the Sensitive Personal Data is used in accord with the purpose,
- To know the third parties to whom the Sensitive Personal Data is transferred at home and abroad,
- To request correction in case the Sensitive Personal Data is processed incompletely or incorrectly and to request information about the transaction performed within this scope and to request the third persons to whom the Sensitive Personal Data is transferred about the transaction performed,
- Even though the Sensitive Personal Data is processed in accordance with the KVKK and other related law provisions, in case the reasons requiring the process such data are no longer existing; to request deletion or destruction of the Sensitive Personal Data and to request the third persons to whom the Sensitive Personal Data is transferred about the transaction performed,
- to raise an objection to a result against the person himself/herself by analysing the processed data executively by the automatic systems and

- to request compensation for the damage arisen due to processing of the Sensitive Personal Data unlawfully.

10.2. The relevant persons (data subjects) can transmit their requests related to their rights mentioned in 10.1 of this Policy by the methods determined by the Council to the Company. They can use "Kyocera Bilgitaş Turkey Doküman Çözümleri A.Ş." Relevant Person (Data Subject) Application Form from the address of https://www.kyoceradocumentsolutions.com.tr/tr.html. However, the updated application methods and the application content should be checked in accordance with the relevant legislation before application and the applications should be made in accordance with the said rules and principles.

10.3. If the relevant persons (data subjects) send their request related to the rights mentioned above in written to the Company, the Company concludes the request according to the qualification of the request in accordance with the KVK Regulation within 30 (thirty) days at the latest without any payment. If a cost is raised related to the conclusion of the requests by the Data Controller, the fees in the tariff determined by the Council may be requested by the Data Controller.

12. SAFETY OF THE SENSITIVE PERSONAL DATA

11.1. The Company has established this Policy and the associated Data Protection Procedures, which are systematic, clearly defined, manageable and sustainable, to ensure the security of Sensitive Personal Data

11.2. The Company, or specialist trainers engaged by the Company to provide support in this area, provide the following for employees involved in the processing of Sensitive Personal Data:

- Regular training is provided on the security of Sensitive Personal Data in accordance with the Data Protection Regulations,
- Confidentiality agreements are entered into,
- The scope and duration of access rights for users authorised to access Sensitive Personal Data are clearly defined,
- The access rights of employees who change roles or leave the company are immediately revoked. In this context, the Personal Data Processing Inventory allocated to the employee by the Company is retrieved.

11.3. If Sensitive Personal Data is processed, stored and/or accessed in electronic environments:

- The electronic media which sensitive personal data is processed, stored and/or accessed is secured by using cryptographic methods,
- the cryptographic keys are kept in secured places,
- Transaction logs of all operations performed on Sensitive Personal Data are securely logged,
- the security updates of the media are followed at all times, the necessary security tests are periodically performed and the test results are recorded,
- If access to Sensitive Personal Data is via software, user authorisations for such software are implemented; security tests for these software applications are carried out regularly by the Company or commissioned, and test results are recorded,
- If remote access to data is required, a two-factor authentication system is provided.

11.4. If Sensitive Personal Data is processed, stored and/or accessed in a physical environment:

- The necessary security measures of the physical media which sensitive personal data is processed, stored and/or accessed are taken and the physical security is provided and the unauthorized access is prevented,
- The necessary security measures of the physical media which sensitive personal data is processed, stored and/or accessed are taken and the physical security is provided and the unauthorized access is prevented.

11.5. If Sensitive Personal Data is to be transferred to third parties:

- If the sensitive personal data needs to be transferred via e-mail, the data is transferred encrypted to the official e-mail address or by using KEP account,
- If it needs to be transferred via media such as flash memory, CD, DVD etc., the data is encrypted by using cryptographic methods and the cryptographic key is kept in another place,
- If the transfer is performed between the servers in different physical environments, the data transfer is performed by installing VPN between the servers or sFTP method,
- If the data needs to be transferred on paper, the measures are taken against risks such as stealing, losing or seeing by unauthorized persons and the paper is sent in "confidential" form.

13. AUDIT

The company has right to audit all company employees and Data Controllers act in complying with KVK Regulations, this Policy and KVK Procedures periodically and ex officio without prior notification and in this context, it performs all necessary audits. The committee establishes KVK Procedures related to such audits and make sure that such procedures are implemented.

14. RESPONSIBILITIES

The committee that is responsible for preparing, revising and implementing this Policy is assigned with the Board decision by the Board of Directors of the Company and in this context, the amendments are applied by such method.

15. AMENDMENTS TO BE MADE IN THE POLICY

This Policy must be reviewed at least once a year with the approval of the Company's Board of Directors. However, it may be reviewed again as needed (e.g., due to legislative changes).
The Company makes the updated Policy version accessible to the relevant persons (data subjects) at the web address below.

The said Website Address:
https://www.kyoceradocumentsolutions.com.tr/tr.html

16. EFFECTIVE DATE OF THE POLICY

This version of the Policy has entered into force in October 2026.

17.SECURITY MEASURES TAKEN BY THE COMPANY

17.1. The Company assesses the existing risks and threats associated with the processing of special categories of personal data by taking into consideration the nature of the data processed, the scope of the data processing activity, the purpose of processing, potential threats to data security, and the potential impacts on Data Subjects. Based on these assessments, appropriate technical and administrative measures are planned, implemented, and, where necessary, reviewed. The security measures taken by the Company with respect to the Processing of Special Categories of Personal Data are as follows:

17.1.1. The Company has established this Policy and the associated Data Protection Procedures, which are systematic, clearly defined, manageable and sustainable, to ensure the security of Sensitive Personal Data.

17.1.2. For employees involved in the processing of Sensitive Personal Data, either by the Company or by specialist trainers from whom the Company receives support on this matter:

a) Regular training sessions are held on the provisions of the Personal Data Protection Law and the security of sensitive personal data,
b) Confidentiality agreements are signed,
c) The scope and duration of access rights for users authorised to access Sensitive Personal Data are clearly defined,
d) The access rights of employees who change roles or leave the company are immediately revoked. In this context, the Personal Data Processing Inventory allocated to them by the Company is retrieved.

17.1.3. If the Sensitive Personal Data are processed, stored and/or accessed in an electronic environment:

a) The personal data is stored by using cryptographic methods,
b) the cryptographic keys are kept in secured places,
c) all transaction records of personal data are logged,
d) the security updates of the media are followed at all times, the necessary security tests are periodically performed and the test results are recorded,
e) If access to Sensitive Personal Data are via software, user authorisations for such software are implemented; security tests for these software applications are carried out regularly by the Company or commissioned, and test results are recorded,
f) If remote access to data is required, a two-factor authentication system is provided.

17.1.4. If Sensitive Personal Data are processed, stored and/or accessed in a physical environment:

a) The sufficient security measures (for example electrical leakage, fire, flood, burglary etc.) are taken according to the environment of the Sensitive Personal Data,
b) The physical security of such environment is provided and the unauthorized access is prevented.

17.1.5. If Sensitive Personal Data are to be transferred to third parties:

a) If the sensitive personal data needs to be transferred via e-mail, the data is transferred encrypted to the official e-mail address or by using KEP account,
b) If it needs to be transferred via media such as flash memory, CD, DVD etc., the data is encrypted by using cryptographic methods and the cryptographic key is kept in another place,
c) If the transfer is performed between the servers in different physical environments, the data transfer is performed by installing VPN between the servers or sFTP method,
d) If the data needs to be transferred on paper media, the measures are taken against risks such as stealing, losing or seeing by unauthorized persons and the paper is sent in "confidential" form.

ANNEX 1 - PERSONAL DATA CATEGORIES AND PROCESSING PURPOSES OF THE PERSONAL DATA

Data Category	Processing Purposes of Personal Data	Legal Basis
16 - Philosophical belief, religion, denomination and other beliefs	Other- Performing and Managing of Recruitment / Personal File Creation Processes	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
16 - Philosophical belief, religion, denomination and other beliefs	Performing of Retention and Archive Activities	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
16 - Philosophical belief, religion, denomination and other beliefs	Providing Information to Authorized Persons, Institutions, and Organizations	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
21-Health Information	Other- Performing and Managing of Occupational Accident Process	LAW NO. 6698, ART. 6/3(f) (MANDATORY DUE TO A LEGAL OBLIGATION)
21-Health Information	Other- Performing and Managing of Recruitment / Personal File Creation Processes	LAW NO. 6698, ART. 6/3(f) (MANDATORY DUE TO A LEGAL OBLIGATION); LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA) (BLOOD TYPE)
21-Health Information	Performing of Retention and Archive Activities	LAW NO. 6698, ART. 6/3(f) (MANDATORY DUE TO A LEGAL OBLIGATION); LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF

		PERSONAL DATA) (BLOOD TYPE)
21-Health Information	Providing Information to Authorized Persons, Institutions, and Organizations	LAW NO. 6698, ART. 6/3(f) (MANDATORY DUE TO A LEGAL OBLIGATION); LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA) (BLOOD TYPE); ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
21-Health Information	Performing of Occupational Health / Safety Activity Process	LAW NO. 6698, ART. 6/3(f) (MANDATORY DUE TO A LEGAL OBLIGATION)
23-Criminal Conviction and Security Measures	Other- Performing and Managing of Recruitment / Personal File Creation Processes	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
23-Criminal Conviction and Security Measures	Performing of Retention and Archive Activities	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
23-Criminal Conviction and Security Measures	Providing Information to Authorized Persons, Institutions, and Organizations	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)
23-Criminal Conviction and Security Measures	Performing of Occupational Health / Safety Activity Process	LAW NO. 6698, ART. 6/3(a) (EXPLICIT CONSENT) (SPECIAL CATEGORIES OF PERSONAL DATA)