Beko

GLOBAL PROTECTING AND RETAINING INFORMATION POLICY

GLOBAL PROTECTING AND RETAINING INFORMATION POLICY

1. RECORD TYPES

The Policy applies to the information contains in the following records:

- Paper,
- Electronic files including but not limited to databases, word documents, Poweroint presentations, spreadsheets, webpages, and e-mails,
- Photographs, scanned images, CD-ROMs and memory sticks. The Policy aims to cover all types of records created by the company, such as;
- All corporate governance documents such as board and board committee materials, meeting minutes,
- All documents and information to be kept within the legal hold period within the scope of the local laws and regulations, which are applicable in the countries that Company operates ("**Beko**" or "**Company**" refers to all companies directly or indirectly, individually or jointly controlled by **Arçelik A.Ş**. and it's joint ventures),
- Contracts,
- All documents related to research and development /intellectual property and trade secrets,
- Technology software licenses and related agreements,
- Marketing and sales documents,
- Invoices,
- All employee records,
- E-mails.

2. RECORD CLASSIFICATION

Existing business process is necessary to establish the record's value. During this process, all record categories need to be reviewed and evaluated according to its;

• Legal value
• Operational value
• Historical value

Accordingly, records and documents are classified as "public, personal and confidential". The Company's retention schedule is developed and constituted with respect to the records classification by fulfilling legal, administrative, financial and/or historical obligations.

3. CLASSIFICATION LEVELS

a. Public: the document/record which made publicly available by the authorized corporate communications departments. Such information contains public information that can be revealed without affecting Company. It is not incompliance with persons' privacy or knowledge of this information does not subject Company to any kind of financial or reputation loss or does not threaten the security of Company assets.

b. Personal: the document/record is made up of individuals' own (for personal usage not business related) data and/or information including personal e-mails, tables and any other documents belong to individuals.

c. Confidential: All kinds of information, which are not publicly available or are not made publicly available by Company are considered confidential including, but not limited to technical, operational, financial information.

Confidential Information covers all types of information pertaining to the customer or vendor records, actual and former employees, third parties that the Company has business interaction and national security information retained due to the employees' positions.

4. GENERAL PRINCIPLES REGARDING CONFIDENTIAL INFORMATION

Within the concept of its business activities and relationship with third parties, Company may process Confidential Information for the following reasons:

- Regulatory reasons to act in compliance with the obligations,
- Technical reasons to develop and maintain the product quality,
- Contractual reasons to perform or manage business operations or to establish, exercise or defend legal claims,
- Client or vendor interaction pertaining to Company's business operations to respond or make inquiries,
- Transactional reasons such as shipments, deliveries, transportation and support services,
- Financial matters, including but not limited to payment processing, accounting, auditing, monitoring, billing and collecting processes,
- Customer, vendor or due diligence reasons, covering the corporate intelligence, market researches, product benchmarking and questionnaires,
- Security considerations to protect and maintain Company products, services, websites and working locations.

Company employees acknowledge that violating the confidentiality, during and after the employment and disclosing the confidential information without authorization to third parties, can result in serious competitive disadvantage to the company whereas causing immeasurable financial, legal and other types of damages to the Company. The obligation not to circulate or disclose confidential information is applied even though the related information might not be specifically identified or marked as confidential.

Regarding Company's obligations pertaining to the Confidential Information, the following criteria must be taken into consideration at minimum:

- Confidential information cannot be used to knowingly convert a company business opportunity for personal use,
- It is not accepted to trade in the Company's stocks, or the stocks of any other company, based on the confidential information,
- Divulging confidential information to third parties so that they might trade in stocks, is prohibited,
- Seeking out, accepting or using of a confidential information of or from a competitor of Company is illegal.

The circulation and transferring the confidential data is done under the following criteria:

- Regarding Company's aim to be compliant to all rules and regulations of the countries that it has operations, the confidential information can be transferred to law enforcement authorities or regulators, with taking the legal authorizations at all times,
- The confidential information can be shared with Company's contracted service providers where the confidentiality is protected with contract terms or non-disclosure agreements, which only act upon the instructions of Company.

5. MINIMUM RETENTION PERIOD

Using the records value criteria, the Company develops a recommended retention period and schedule procedure for each category of records and documents by comprehensively, fulfilling administrative, financial and/or historical obligations. The recommended minimum retention schedule is determined for each records and documents category by the Company where local and international laws and regulations are identified.

Company retains records and documents regarding the Company's retention schedule and procedure. Unless any specific law and regulation provides for a longer or shorter retention period than the Company's retention schedule, the Company shall follow the instructions of Company retention schedule.

As long as a record and/or a document has not been specified as permanently preserved, the retention period is identified in accordance with the retention schedule. For "permanent preservations" monitoring is defined and scheduled within the retention period procedure.

6. DISPOSITION

Each department is responsible from ensuring the retention schedule.

When the retention period is expired, the record and/or document are reviewed by the relevant Director (or their delegate) in consultation with relevant stakeholders such as, Head of IT, Head of Legal and Compliance and/or other senior managers and a 'disposition action' is agreed upon.

A "disposition action" is either:

- the further retention of the record or document within Company
- the destruction of the record or document.

The record and document reviewing should be performed as soon as possible after the expiration of the retention period. The disposition decision is reached having regard to:

- continuous business accountability needs (including audit)
- current legislation

If the record and document has any long-term historical or research value:

- costs related to sustained storage versus costs of destruction need to be reviewed
- the legal, political and reputational risks associated with keeping, destroying or losing control over the record/documents need to be reviewed.

Disposition records must be kept by the disposing department for future audit purposes.

a. Further Retention of Records and Documents

Irrespective of the Company's Record Retention Policy, if the record and/or document is necessary by any part of the business, and upon receiving notice of a lawsuit, government investigation or other legal action against Company, records and documents are preserved and safeguarded. Otherwise, the Company applies the following disposition actions.

b. Destruction of Paper/Electronic Records and Documents

Destruction should be conducted in a way that keeps the confidentiality of the records/ documents and that correspond with non-disclosure agreements. All copies including backup or preservation copies should be erased at the same time in the same direction.

The Record Retention Policy requires soft copies of paper/electronic records to be erased complying with the IT procedure. Giving the fact that deletion of the soft copy files is not considered to be a sufficient method, this procedure should be complying with IT procedures.

Destruction of any record which are classified as confidential level shall be complied with the local laws and regulations, which are applicable in the countries that Company operates.

7. AUTHORITY AND RESPONSIBILITIES

This Policy is published by Company Legal and Compliance Department, and the Company is responsible for ensuring the compliance with the Policy by all its employees. Any violation of this Policy will result in disciplinary action, up to and including termination of employment.

This Policy will be periodically reviewed by the assigned Legal and Compliance Department to ensure compliance with new or revised laws and regulations.

Version Date: 2.12.2019