Data Protection and Information Security Policy

Contents

As Bosch Rexroth Otomasyon Sanayi ve Ticaret A.Ş. (“Bosch” or “Company”), we attach great importance to the privacy and safety of your personal data. In this context, we would like to inform you on how we process the personal data belonging to our customers, suppliers, business partners, their employees and authorities, and all other third parties, as well as for what purposes we use this information, and how we protect it.

All concepts and expressions used in this statement shall have the meaning attributed to them in Law No. 6698 on the Protection of Personal Data ("**KVKK**") and relevant regulations. The term "you" in this statement refers to your party. The term "personal data" has been used in this document to also include personal data of special nature. Please see Appendix - Abbreviations for a full list of meanings expressed by the terms and abbreviations used in the Policy.

We would like to remind you that if you do not accept the terms of this policy, you should not convey any personal data to us. If you prefer not to convey any personal data to us, it may not be possible for us at times to provide you with services and respond to your requests, or we may not guarantee the full functionality of the services we offer to you.

We would like to remind you that it is your responsibility to ensure that the personal data you provide to our Company is accurate, complete, and up to date. Beyond that, if you share the personal data of other persons with us, it shall also be incumbent upon you to gather this information in accordance with all legal obligations in your locality. This shall mean that you have obtained the consent of the third parties in question as regards us gathering, processing, using and disclosing their personal data, and our Company shall not be held liable in this respect.

ABOUT BOSCH

Bosch Group is one of the leading technology and service suppliers of the world. Bosch has approximately 394.500 employees worldwide (as of 31 December 2020). The company has 71,6 billion Euros sales in 2020. Bosch’s activities are divided in four sectors: Mobility Solutions, Industry Technologies, Consumer Goods, Energy and Structure Technologies. As one of the leading IoT companies in the world Bosch presents innovative solutions for smart homes, Industry 4.0 and connected mobility. Bosch follows its sustainable, safe and exciting mobility vision. By using its experience in sensor technology, software and service and its own IoT cloud; the Company provides

The Bosch Group is a leading global supplier of technology and services. It employs roughly 394,500 associates worldwide (as of December 31, 2020). According to preliminary figures, the company generated sales of 71.6 billion euros in 2020. Its operations are divided into four business sectors: Mobility Solutions, Industrial Technology, Consumer Goods, and Energy and Building Technology. As a leading IoT provider, Bosch offers innovative solutions for smart homes, Industry 4.0, and connected mobility. Bosch is pursuing a vision of mobility that is sustainable, safe, and exciting. It uses its expertise in sensor technology, software, and services, as well as its own IoT cloud, to offer its customers connected, cross-domain solutions from a single source. The Bosch Group’s strategic objective is to facilitate connected living with products and solutions that either contain artificial intelligence (AI) or have been developed or manufactured with its help. Bosch improves quality of life worldwide with products and services that are innovative and spark enthusiasm. In short, Bosch creates technology that is “Invented for

life.". The Bosch Group comprises Robert Bosch GmbH and its roughly 440 subsidiaries and regional companies in 60 countries. Including sales and service partners, Bosch's global manufacturing, engineering, and sales network covers nearly every country in the world. The basis for the company's future growth is its innovative strength. At 126 locations across the globe, Bosch employs some 73,000 associates in research and development, as well as roughly 30,000 software engineers.

The company was set up in Stuttgart in 1886 by Robert Bosch (1861-1942) as "Workshop for Precision Mechanics and Electrical Engineering." The special ownership structure of Robert Bosch GmbH guarantees the entrepreneurial freedom of the Bosch Group, making it possible for the company to plan over the long term and to undertake significant up-front investments in the safeguarding of its future. Ninety-two percent of the share capital of Robert Bosch GmbH is held by Robert Bosch Stiftung GmbH, a charitable foundation. The majority of voting rights are held by Robert Bosch Industrietreuhand KG, an industrial trust.

The words "we", "Company" or "Bosch" mentioned in this Policy refer to Bosch Rexroth Otomasyon Sanayi ve Ticaret A.Ş. registered in Bursa Trade Registry with trade registry no 75190 , resident in Işıktepe OSB Mahallesi Siyah Cadde No:29 Nilüfer/Bursa - which controls your Personal Data.

DATA PROTECTION AND INFORMATION SECURITY POLICY

We as Bosch ensure that the confidentiality, integrity and availability of our assets are protected, the risks related to business processes are reduced to an acceptable level and compliance with the Personal Data Protection Law no. 6698 with our "Data Protection and Information Security Policy".

By Bosch executive management:

- To protect the reliability and institutional reputation of our company,
- To keep our company's activities without interruption,
- To ensure compliance with all legal regulations and contracts related to information security,
- To create information security awareness for parties involved in internal and external issues and to convey the relevant obligations,
- To train technical and behavioral perfections to increase information security awareness,
- To ensure compliance with the Law on Protection of Personal Data Law no. 6698

Bosch is committed to implementing applications for "Data Protection and Information Security", systematically managing it, ensuring continuous improvement of the system, and allocating the resources needed by the system with senior management approval of "Data Protection and Information Security Policy".

Respectfully submitted to your information.

OUR PRINCIPLES FOR PROCESSING PERSONAL DATA

All personal data processed by our Company are processed in accordance with KVKK and relevant regulations. As per Article 4 of KVKK, the following are the fundamental principles we uphold when processing your personal data:

- **Lawfulness and Conformity with Rules of Bona Fides**: Our Company complies with legal obligations and general rules of honesty and reliability when processing personal data. In that regard, our Company takes into account the principle of proportionality in processing personal data, and does not use this data for purposes other than what is required.
- **Ensuring That Personal Data is Accurate and Up to Date**: Our Company ensures that the personal data that it processes in consideration of the fundamental rights of the data subjects and its own legitimate interests is accurate and up to date.
- **Processing Data for Specific, Explicit, and Legitimate Purposes**: Our Company explicitly determines its goal of legitimate and lawful processing of personal data. Our Company processes personal data to the extent necessary to provide its products and services.
- **Relevant, Limited, and Proportionate to the Purposes for Which Data is Processed**: Our Company processes personal data in a manner that allows the specified set of goals to be achieved, and avoids processing personal data unnecessarily or not in keeping with achieving the stated goals.
- **Retaining Data for the Period of Time Stipulated by Relevant Legislation or the Purpose for Which Data is Processed**: Our Company stores personal data to the extent that it's stipulated in regulations and for the purposes for which data is processed. In that regard, our Company first determines whether relevant regulations specify a time period for the storage of personal data, and if there is indeed a period of time in the law, observes this period, and if there is no period of time specified, stores personal data only as long as it is necessary. When this period ends or the reasons for processing data no longer exist, the data is erased, destroyed, or anonymized by our Company.

DATA SUBJECT CATEGORIES

The following are the categories of data subjects, except for the employees whose data is processed by our Company (including interns and employees of subcontractors). We have a separate, internal policy for processing the personal data of our employees. Those who fall outside the scope of the categories listed below can also send us requests as per KVKK; their requests shall also be evaluated.

RELEVANT PERSON CATEGORY	EXPLANATION
Customer	Natural or legal persons who purchase our products
Potential Customer	Real or legal persons that have shown interest in purchasing our products, or are considered, in conformity with rules of bona fides, to have such an interest
Visitor	Real persons who entered the physical premises (offices etc.) of our Company on the occasion of an event or for other purposes, or who visited our website
Third Person	Third-party real persons who are associated with the abovementioned real persons for the purposes of ensuring the commercial transactional safety between our Company and the abovementioned persons, protecting their rights, and achieving their

	interests (e.g. sureties, companions, family members and relatives) or all real persons whose personal data our Company has to process even though it is not explicitly stated in the Policy (e.g. former employees)
Employee and Intern Candidates	Real persons who applied for a position at our Company or dropped their CVs or related information for our review
Employees, Shareholders, Officials of the Institutions with Which We Cooperate	Real persons, including shareholders and officials, that work at organizations with which our Company has a business relationship (including, but not limited to, business partners and suppliers)

WHEN DO WE COLLECT YOUR PERSONAL DATA?

We collect your personal data typically in the following situations:

- When you purchase and use our products,
- When you sell us goods or offer us a service,
- When you subscribe to our newsletter or opt in to our marketing messages,
- When you contact us via email or phone to file complaints or give feedback,
- When you apply for a position at our Company,
- When you attend our events, seminars, conferences, and other organizations,
- When you contact us for any purpose as a potential customer/supplier/business partner/subcontractor.

We shall process the personal data we collect in the abovementioned situations only in accordance with this Policy.

WHICH TYPES OF PERSONAL DATA DO WE PROCESS ABOUT YOU?

The personal data we process about you varies depending on the nature of the business relationship between you and us (e.g. customer, supplier, business partner etc.) and on the means of communication you choose to contact us (e.g. phone, email, written document etc.).

Basically, our personal data processing methods involve situations in which you participate in our business activities or surveys, or otherwise interact with us by phone or email. In this context, the personal data we process about you can be broken down into these categories:

Data categories	**Examples**
ID information	Information found of ID documents such as name, surname, title, date of birth etc.
Contact information	Email, phone number, address

Data categories	Examples
Pictures and/or videos that can identify you	Pictures, videos and audio that is processed when you visit our Company or when you attend an event organized by our Company, for reasons of security
Financial data	Bank account data, billing information
Any other information you voluntarily decide to share with Bosch	Personal data you share with us of your own accord, feedback, opinion, requests, complaints, assessments, and comments that you share with us, and our evaluations regarding the same, as well as uploaded files, fields of interest, and information shared with us for our detailed review before we establish a business relationship with you
Electronic data collected automatically	We may also collect electronic data that is sent to us by your computer, smartphone, or another device when you visit or use our website or applications, subscribe to our newsletter, or interact with us through other electronic channels (e.g. device hardware model, IP address, operating system version and settings, your date and duration of using our digital channels or products, your actual location when you activate location-based products or features, the links you click, movement sensor data etc.)
Information on legal transaction and compliance	Your personal data, as well as audit and inspection data arising from our legal obligations, payment of our debt, identification of our legal receivables and rights, and need for compliance with our Company policies
Corporate Client/Supplier Data	Information obtained regarding data subject customers/suppliers or employees and signatories working for any customer/supplier as a result of the operations conducted by our business units,
Incident management and security information	Information and assessments regarding events that have the potential to impact the employees, executives, or shareholders of our company, including license plates and vehicle information, travel and transport information
Personal data collected from other sources	We may also collect your personal data from public databases, and using the methods and platforms with which our business partners collect data on our behalf, to the extent that is lawful as per existing laws and regulations. For instance, before we establish a business relationship with you, we may do research about you using public records in order to ensure the technical, administrative, and legal security of our commercial activities and transactions.

Data categories	Examples
	In addition, it is also possible that the personal data of third parties might be conveyed to us through you (e.g. the personal data of any of your guests, sureties, companions, family members etc.). In order for us to manage our technical and administrative risks, we may process your personal data via methods that are used in accordance with generally accepted legal and commercial conventions and the principle of bona fides.

PROCESSING THE PERSONAL DATA OF EMPLOYEE CANDIDATES

We process the personal data of Employee Candidates such as the schools they graduated from, prior business experiences etc. so that we can better understand their qualifications and evaluate their fitness for the vacant position, and in order to verify the accuracy of the information they have provided to us, do research about the candidate by contacting third parties, comply with the relevant regulations, and implement the recruitment rules and human resources policies of our Company.

The personal data of employee candidates is processed via the job application form found online; the electronic job application form of our Company; the applications submitted to our Company or through recruitment or consultancy firms; interviews conducted face-to-face or online, checks carried out about the employee candidate by our Company; and recruitment tests conducted by human resources experts in order to verify the fitness of the employee candidate for the vacant position.

When applying for a position, employee candidates are informed via a detailed privacy notice - as per KVKK - before they share their personal data with us, and their explicit consent is sought if necessary for the processing of their personal data.

PROCESSING THE PERSONAL DATA OF VISITORS AT OUR OFFICES

Our Company processes the personal data of visitors to our premises during their check-in and check-out processes, for the purposes of ensuring the physical safety of our Company, employees, and visitors, and monitoring compliance with workplace rules. In that regard, in order to monitor the visitor check-in/check-out activity, the name and surname of visitors are verified through their ID cards and their name-surname and the last 6 digits of Turkish identification numbers are recorded in a special software allocated to visitor management. However, the identity of the visitor is not kept during the time they are at the company premises, and the identity card is returned to the visitor after the abovementioned digital registration is complete.

The visitor is informed with a privacy notice located at the security checkpoint before their personal data is collected and processed. However, since our company has a legitimate interest in this case, we do not seek the explicit consent of the visit as per Article 5/2/f of KVKK. This data is only available within our systems and as hard copy documents and not transferred to another environment unless the Company's security is under threat. However, this information can be utilized to prevent crime or ensure the security of the Company. Each location disposes of these documents in accordance with their retention periods.

PROCESSING PERSONAL DATA VIA CLOSED CIRCUIT CAMERA RECORDING

Security cameras are used to ensure the safety of our Company and premises, which involves processing personal data. Our Company has the following purposes for its security camera monitoring: enhance the quality of the services on offer, ensure the physical and material safety of the individuals at our offices and the premises within which our offices are located, prevent misconduct, and protect the legitimate interests of data subjects.

The personal data processing activity conducted by our Company via security cameras, is being carried out in accordance with the Constitution, KVKK, Law No. 5188 on Special Security Services, and relevant regulations.

Our Company processes personal data in keeping with the purposes for which they are collected as per Article 4 of KVKK, and in a limited and measured manner. Individuals are never monitored in a way that pursue security goals at the expense of infringing upon their privacy. In that regard, warning signs are placed in common halls where CCTV recording is conducted, and thereby informing data subjects. However, their explicit consent is not sought as the Company has a legitimate interest in preserving CCTV records. In addition, as per Article 12 of KVKK, we take all necessary technical and administrative measures to ensure the security of personal data obtained as a result of the CCTV monitoring activity.

In addition, a procedure has been prepared and implemented by our Company governing the locations where CCTV cameras are installed, the angles that the cameras monitor, and the time periods for which records are kept. This procedure is taken into account before CCTV cameras are installed. Installing cameras in a way that transcends the purpose of security and infringes upon the privacy of individuals is not allowed. Only select Company personnel can access CCTV recordings, and their authorizations are regularly reviewed. The personnel who can access these records sign a letter of undertaking, committing that they shall protect the personal data in a lawful manner.

Our Company conducts camera recordings in the entrances, external walls, archive rooms, system rooms, etc. in order to ensure the protection of the building. The recording process is monitored by the security unit.

FOR WHICH PURPOSES DO WE USE YOUR PERSONAL DATA?

Our purposes for using your personal data vary depending on the nature of the business relationship between you and us (e.g. customer, supplier, business partner etc.). The main

purposes for which we process your personal data are listed below. Personal data processing activities regarding Employee Candidates are explained in the section above titled "The Processing of Personal Data Belonging to Employee Candidates".

Our Purposes for Processing Personal Data	**Examples**
Evaluating potential suppliers/business partners	Managing our assessments and conflict-of-interest evaluations as per our risk rules, periodic inspection of suppliers
Establishing and managing relationships with customers, and managing and closing out our contracts with our suppliers/business partners	Conducting the sales processes of our company's products, presenting offers for our products, conducting necessary tests for our customer who would like to try our product before sales, supplying goods, invoicing (including e-invoice and return invoice processes), following invoices from e-archive system for our customers and suppliers outside the scope of e-invoice, creating purchase forms for suppliers, reviewing and revising subcontracts/protocols within the frame of contracts concluded with suppliers, drawing up and performing contracts, ensuring legal transaction safety after conclusion of contracts, conducting after sales product tests and troubleshooting the existing problems if necessary, developing our services, evaluating new technologies and applications, determining and implementing our Company’s business and commercial strategies, managing operations (requests, proposals, evaluations, orders, budgeting, contracts), organizing product logistics and obtaining vehicle/driver information, conducting financial operations and conducting agreements with suppliers and customers in this regard, managing financial affairs, conducting check, bond and lien processes, presenting alternatives to natural and legal persons within the frame of commercial relations, visiting current customers and vendors, archiving contracts, when necessitated by our commercial relations conducting translation processes, making damage calculations within the frame of insurance processes, notifying famages to the insurance companies and receiving payments by conducting expert investigations, controlling the suppliers’ compliance to quality standards and conducting necessary inspections in this regard, conducting documentation operations within the frame of quality standards, granting work permits within the factory, conducting accounting processes during the period from

Our Purposes for Processing Personal Data	Examples
	order to payment, opening of current financial year records, conducting collection, payment and credit operations
Managing direct marketing processes	Sending marketing messages via email, SMS and phone regarding our services, conducting satisfaction surveys or evaluating your opinions, complaints and comments you post on social media, online platforms, or other venues, giving you feedback, informing our customers of what's new about our Company, carrying out marketing activities with event participants, sharing photographs taken at fairs within the frame of social media activities, conducting e-mailing activities after fair participations, obtaining potential customer information in order to expand customer portfolio.
Communication and support (upon your request)	Responding to your queries for information about our services, providing support as regards requests coming through our channels of communication, and updating our records and database (in relation to the new customer and new vendor card creation processes), communicating with customers and suppliers in the fairs our Company participates in, exchanging business cards, finding solutions to the complaint reports of sales or quality control departments and reporting the actions taken
Compliance with legal obligations	Managing taxation and insurance processes; fulfilling our legal obligations arising from Law No. 5651 and relevant regulations, Law No. 6563 on Regulation of Electronic Commerce and relevant regulations, Turkish Penal Code No. 5237, Law No. 6698 on Protection of Personal Data; managing processes at public institutions; managing relevant processes within the context of compliance with the laws and regulations we are subject to regarding obligations to store records and to notify, compliance and audit, audits and inspections by authorities, following and concluding lawsuits, and disclosing data at the request of legal authorities; managing the necessary processes for the protection of copyright and intellectual property rights as per the requirements specified in order to fulfill our legal obligations in accordance with the KVKK, in our dealings with regulatory institutions or as stipulated by

Our Purposes for Processing Personal Data	Examples
	existing regulations, requesting necessary documents from onboarding subcontracted employees as per occupational health and safety legislation
Protecting the Company’s interests and security	Conducting the necessary auditing activities to protect the company's interests, checking against conflicts of interest, ensuring the legal and commercial safety of the persons in a business relationship with our company, keeping CCTV records to protect company devices and assets, taking the necessary technical and administrative measures, conducting efforts to enhance the services we offer, enforcing and auditing the implementation of workplace rules, planning and executing social responsibility activities, protecting the commercial reputation and trust built by Bosch group companies, reporting and intervening in - as well as taking measures for - all incidents, accidents, complaints and loss-theft situations taking place in the premises, communicating the rules that must be complied with in case of hazardous situations that might arise during maintenance-repair work and measuring the professional competence of subcontractors, ensuring consistency in employee clock-in/clock-out times, obtaining necessary information for security, carrying out quality-focused and standard audits, and fulfilling our reporting and other responsibilities specified by law, as well as assessing the fitness of suppliers to be on the field, collecting customer information for emergency situations
Planning and executing the company's commercial activities	Within the frame of determining, planning, and implementing the short-term, medium-term, and long-term commercial policies of the Company, determining and implementing the Company's commercial and business strategies; conducting activities as regards communications, market research, social responsibility, purchasing
Reporting and auditing	Ensuring communication with companies belonging to Bosch group companies, conducting the internal auditing and reporting processes related to necessary business activities

Our Purposes for Processing Personal Data	Examples
Protecting rights and interests	Mounting legal defense against legal rights claims such as lawsuits, investigations etc. filed against our Company, performing the judgments of mediations, civil and public lawsuits, conducting lawsuit, arbitration and other legal procedures in order to protect our Company's rights and interests

HOW DO WE USE YOUR PERSONAL DATA FOR MARKETING PURPOSES?

Since marketing activities are not considered among the exceptions regulated in Article 5/2 of KVKK, we seek your consent as a rule for processing your personal data for marketing purposes. Our Company may send you regular promotional messages regarding our products, services, events, and promotions. Such promotional communications may be sent to you via email, newsletter, phone, SMS, mail, or social network belonging to third parties.

In order to provide you with the most effective and custom-made experience, these communications may be tailored to your preferences (for instance, when you indicate these to us, in accordance with the conclusions drawn from your website visits or links on our emails you have clicked, based on your cookie preferences).

Based on your consent, we are able to conduct marketing activities including internet and social media advertising, targeting, re-targeting, cross-selling, campaigns, sales, offering personalized product/service opportunities, using cookies for this purpose, giving you commercial offers based on your preferences and most recent purchases, additionally monitoring your usage habits based on your previous visits Bosch websites and applications and delivering customized products; processing your data to create personalized ads, campaigns, advantages, and other benefits and managing various marketing and CRM efforts, creating new product and service models, sending you commercial electronic messages (campaigns, newsletters, customer satisfaction surveys, product and service advertisements etc.); sending you gifts and promotions; organizing corporate communications and arranging events and invitations, and issuing notifications related to them.

When stipulated by existing regulations, we shall seek your consent before launching any such activity. In addition, you shall reserve the right to revoke (suspend) your consent any time you see fit. You may opt out of email, e-newslaetter and SMS messages and therefore stop all marketing communications by following the "opt-out" instructions within each message.

You may contact us any time to ask us to stop sending you any marketing messages (you can find contact details in the section titled "What are Your Rights Regarding Your Personal Data?").

Commented [MT(1]: Eğer Bosch uygulamaları aracılığıyla söz konusu faaliyetler yürütülmüyorsa bu kısım çıkarılmalıdır.

Commented [AM(2]: Bu linklerin değişebileceği göz önünde bulundurduğumuzda daha genel bir cümle yazılabilir mi?

Commented [MT(3R2]: Bosch internet siteleri ve uygulamaları şeklinde daha genel bir ibare yazılmasının sakıncası olacağını düşünmüyoruz.

FOR WHICH LEGAL REASONS DO WE PROCESS YOUR PERSONAL DATA?

We process your personal data in accordance with the legal reasons specified below, as per the Turkish Commercial Code No. 6102, Turkish Code of Obligations No. 6098, Tax Procedure Law No. 213, Article 5 of KVKK and relevant electronic commerce regulations:

Legal Reason	**Examples**
We process your personal data by seeking your consent in cases where it is necessary as per KVKK and relevant regulations (We would like to remind you that you may always revoke your consent)	We seek your consent to conduct marketing activities.
Whenever existing regulations permit	Naming the relevant person on the invoice as per Article 230 of Tax Procedure Law
When it is necessary to protect the critical interests of a person	Transferring the medical data of a board member that faints at a board meeting
When we are obliged to enter into a contract with you, execute the contract, and fulfill our obligations arising from the contract	Obtaining the bank account information of a customer due to our contractual relationship with suppliers
Fulfilling our legal obligations	Fulfilling our tax obligations, and submitting to court information that is requested by a court order
When your personal data is made public by you	You sending us email for us to contact you, using publicly information that you made public on social media and similar platforms
Our obligation to process data for establishing or protecting a right, using our legal rights, and mounting a defense against legal claims made against us	Storing and using when necessary documents that are in the form of proof/evidence
When our legitimate interests necessitate it so long as fundamental rights and freedoms are not violated	Ensuring the security of our company's communications and information, managing the Company's activities, identifying dubious transactions and researching them in compliance with our risk rules, benefiting from storage, maintenance, and support services in order to receive IT services, leveraging cloud

Legal Reason	Examples
	technology in order to ensure the effectiveness of Company activities and benefit from technological developments

WHEN DO WE SHARE YOUR PERSONAL DATA?

Domestic Transfer of Personal Data

Our Company is under the obligation of acting in accordance with the regulations, including KVKK, and decisions made by the Board. As a principle, the personal data and personal data of special nature belonging to data subjects cannot be shared by our Company with other real or legal persons without the explicit consent of these data subjects.

On the other hand, it is possible to share this data without explicit consent in situations specified in Article 5-6 of KVKK. Our Company may share personal data with third parties and companies under the umbrella of the Bosch group companies based in Türkiye unless otherwise stipulated in the law or relevant regulations (or in a contract entered into with the data subject), so long as it complies with all the conditions specified in KVKK and other regulations and takes the necessary security measures outlined in regulations.

International Transfer of Personal Data

Just as our Company may transfer personal data to third parties in Türkiye, it may also transfer personal data outside Türkiye, after processing it in Türkiye or processing and storing it abroad, in accordance with the Law and relevant regulations and taking the necessary security precautions specified in the law. We transfer your personal data using cloud technology taking all necessary technical and administrative measures in the process. We do this to manage our Company's activities in the most effective manner possible and to leverage existing technology. Other than that, we'd like you to note that we do not transfer your personal data overseas.

Domestic and International Parties to Which Personal Data is Transferred

We do not share your personal data except in the special circumstances described here. Access to your personal data within Bosch shall be limited only to those who need to know the information for the purposes defined in this Policy. In order to achieve the purposes for which your data is collected (for detailed information about these purposes, see "For what purposes do we use your personal data?"), we transfer your personal data to the following persons and institutions:

1. *Bosch group companies:* Since we operate under Bosch Group Companies, your data may be shared or made available to the Bosch group companies with which we operate in Türkiye or abroad. This sharing will only be made with authorized employees of the relevant Bosch group companies. However in general, our data sharing processes with

Bosch group companies is carried out through financial reports that focus on company profitability and efficacy and does not contain any personal data. In some special cases we may share personal data with Bosch group companies, rather than sharing anonymized data

In a similar manner, we share your personal data with Bosch group companies with which we operate under. In this regard, we transfer personal data to relevant Bosch group companies in accordance with KVKK Art. 5/2 (f) for the purposes of conducting management operations (legal, technical, marketing, finance, operation etc.), managing lawsuits and legal processes, conducting customer invoicing processes, sharing the necessary information for the organization of structural work, managing day to day financial matters, conducting board of directors decision processes, conducting personnel processes, evaluating supplier firms, conducting contract processes with supplier and subcontractor firms, conducting brand management processes.

2. *Service Providers:* They represent the parties that our Company has established business cooperation with for activities such as sales, promotion, marketing and after sales support. Similar to many businesses we too work with reliable third parties such as IT technology providers, consultancy firms providing e-system services, consultancy service providers, shipping companies, travel agencies in order to manage our business activities in the most effective manner possible, equipped with the most recent technologies, and in that regard, we may share data to continue these activities. This act of sharing data is limited to establishing and conducting business cooperation. We use cloud technology to manage our Company's activities in the most efficient manner possible and reap the maximum benefit from technological developments, and in that regard, we process your personal data with cloud technology service providers domestically and internationally. In this regard, personal data sharing is conducted in compliance with KVKK Articles 8 and 9 regulating data transfers.

3. *Public Agencies and Institutions:* Where stipulated by law or in cases where we need to protect our rights, we may share your personal data with public, legal, and administrative authorities (e.g. Police Department, Tax Offices, law enforcement agencies, courts and enforcement agencies).

4. *Private Entities:* As per relevant regulations, we may share personal data on a limited basis and for a specific purpose if a private entity that has the right to receive information or documents from our Company issues a request (e.g. Occupational Safety and Security Firms, Audit Firms).

5. *Professional Advisors, and Others:* For providing you with the salary and side benefits you have earned, managing company credit card transactions and defining/allocating a company credit card on your name, we share your your personal data with the persons and entities specified below including professional consultants:

- Banks
- Insurance companies

- Auditors
- Lawyers
- Accountants
- Logistics firms, warehouses
- Shipping companies
- Shuttle service firms
- Other external professional consultants

6. *Other parties in connection with corporate transactions:* In addition, we also share your personal data with parties such as firms from which we receive services or consultancy at home or abroad, as well as customers, sub-contractors, suppliers and business partners, for the purposes of managing the contracts entered into for carrying out company business activities and managing the resulting contractual and commercial relationships, ensuring the efficiency and security of company processes, during the sale of a company, or the sale of part of a company to another company, or when names, assets or shares belonging to Bosch are subject to any restructuring, merger, joint venture or other types of sales or disposal (including those in connection with the declaration of bankruptcy or similar transactions).

FOR HOW LONG DO WE STORE YOUR PERSONAL DATA?

We store your personal data solely for the purposes for which we collected them and for a period of time necessary to fulfill the said purposes. We determine these periods separately for each business process, and we destroy your personal data in accordance with KVKK if there are no other reasons for which we should keep them at the end of the process.

We take into account the following criteria when determining when do destroy your personal data:

- The period of time generally accepted in the sector in which the data controller operates, with respect to the purposes for which data in the relevant category is processed,
- The period for which the legal relationship with relevant persons that requires the processing of personal data continues,
- The period for which the legitimate benefit that the data controller shall gain as a result of processing data will continue in accordance with laws and the principle of bona fides,
- The period for which the risk, costs, and obligations associated with storing data in accordance with its processing purpose shall continue in legal terms,
- Whether the maximum period to be determined is conducive to keeping the data in the relevant category accurate and up to date if necessary,
- The period for which the data controller is legally obligated to store the personal data in the relevant category,
- The expiry date during which the data controller may claim a right associated with the personal data in the relevant category.

HOW DO WE DESTROY YOUR PERSONAL DATA?

As per Article 138 of the Turkish Penal Code and Article 7 of KVKK, despite being processed under legal provisions and other related laws, personal data shall be erased, destructed or anonymized by the controller, ex officio or upon demand by the data subject, upon disappearance of reasons which require the process.

In that regard, we have prepared a Policy on Storing and Destroying Personal Data. Our Company reserves the right to not fulfil the requests of the data subject in cases where we have a legal right and/or obligation to store personal data. When personal data is processed automatically - provided that it is part of a data recording system - we implement the procedure of physically destroying the data in a manner that ensures it can never be used again. When our Company cooperates with another person or entity to process personal data on its behalf, the personal data in question shall be deleted by this person or entity irrevocably. As per law, our Company may anonymize personal data when the reasons for which they were processed no longer apply.

METHODS OF DESTROYING PERSONAL DATA

Deleting Personal Data

Despite being processed in accordance with the law, personal data shall be erased by our Company ex officio or upon demand by the data subject, upon disappearance of reasons which require the process. Deleting personal data refers to process by which personal data can never be accessed or used again. Our Company takes all necessary technical and administrative measures to ensure that deleted personal data becomes inaccessible to users and cannot be used again for any purpose.

The Process of Deleting Personal Data

The process that must be followed while deleting personal data is as follows:

- Identifying the personal data subject to erasure.
- Identifying the users of each fragment of personal data, using an authorization or control matrix or a similar system.
- Identifying the powers of the relevant users, including accessing, recovering, and re-using data.
- Deactivating and destroying the abovementioned powers of accessing, recovering, and re-using data.

Methods of Deleting Personal Data

Data Recording Medium	Explanation
Personal Data Found in Servers	For personal data found in servers whose period of storage has ended, the system administrator deactivates the right to access the data, and then deletes the data itself.

Personal Data Found in Electronic Environments	Personal data found in electronic media whose period of storage has ended is rendered inaccessible and unusable to all employees (relevant users) other than the database administrator.
Personal Data Found in Physical Media	Personal data found in physical media whose period of storage has ended is rendered inaccessible and unusable to all employees other than the document archive administrator. In addition, documents are crossed out/painted/deleted line by line to ensure they are completely unintelligible.
Personal Data Found in Portable Media	Personal data kept in flash storage whose period of storage has ended is encrypted by the system administrator and stored in a secure environment, with only the system administrator authorized to access it using encryption keys.

Since personal data can be stored in various recording media, they must be deleted using methods fit for the type of medium they are found in. The following examples illustrate this point:

Application-as-a-Service Cloud Solutions (Office 365, Salesforce, Dropbox etc.): In cloud systems, data should be deleted using the delete command. While carrying out this procedure, it must be ensured that the user does not have the ability to retrieve any deleted data.

Personal Data in Written Form: Personal data in written form should be obscured. Obscuring is done by shredding the paper if possible, and if not, painting the paper in indelible ink and thereby making it irrevocably unintelligible.

Office Files Found in a Central Server: The file should be deleted with the delete command in the operating system, or it should be rendered in accessible by removing the users' access to the index where the file or folder in question is located. While carrying out this procedure, it must be ensured that the user is not the system administrator.

Personal Data Found on Portable Media: Personal data found on portable media should be stored with encryption and deleted using software fit for use on this media.

Databases: The lines where personal data are found must be deleted with database commands (DELETE etc.). While carrying out this procedure, it must be ensured that the user is not the database administrator.

Destroying Personal Data

Despite being processed in accordance with the law, personal data shall be erased by our Company ex officio or upon demand by the data subject, upon disappearance of reasons which require the process. Destroying personal data refers to process by which personal data can never be accessed or used again. The data controller is obligated to take all technical and administrative measures with regard to destroying personal data.

Data Recording Medium	Explanation
Personal Data Found in Physical Media	Personal data in written form whose period of storage has ended is irrevocably destroyed using shredders.
Personal Data Found in Optical/Magnetic Media	Personal data on optical or magnetic media whose period of storage has ended is destroyed by melting, burning, or grinding the media. In addition, magnetic media are put through a special device that exposes the media to extreme magnetic force, rendering any information that is on it inaccessible.

Destroying Physically: Personal data can be processed automatically, provided that it is part of any data recording system. When personal data is processed automatically, we implement the procedure of physically destroying the data in a manner that ensures it can never be used again.

Deleting safely from software: While deleting and/or destroying personal data processed automatically or semi-automatically and stored in digital environments, we use methods that ensure personal data is irrevocably deleted from any relevant software.

Secure Data Deletion by Expert: In some cases, our company can cooperate with an expert for deleting personal data. In such cases, personal data are deleted/destroyed by the expert in a manner that renders the data irrevocable.

Obscuring: This refers to rendering personal data physically unintelligible.

Methods of Destroying Personal Data

In order to destroy personal data, it is necessary to find all copies of the said data and destroy them using one or more of the methods listed below, depending on the system 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-magnetization: this is the process of making corrupting data and making it unreadable by passing magnetic media through a special device and exposing it to a very high-value magnetic field. ii) physical destruction: it is the process whereby optical media and magnetic media are destroyed physically through methods such as melting, burning or pulverizing. Personal data is rendered inaccessible by melting, burning, or grinding optical or magnetic media. With respect to solid hard disks, if the method of overwriting or magnetization does not work, this media must also be physically destroyed. iii) Overwriting: Refers to the process of writing random binary data (0s and 1s) at least for seven times on magnetic or rewritable optical media, thereby rendering old data irretrievable. This process is carried out using proprietary software.

Peripheral Systems: The methods of destruction that can be used depending on the type of medium/environment are found below: i) Network devices (switch, router etc.): The storage media found in these devices are fixed. Such products typically have a delete command but lack

a destroy command. Personal data must be destroyed using one or more of the methods listed in (a). ii) Flash-based media: Personal data found on flash-based hard disks with interfaces such as ATA (SATA, PATA etc.) and SCSI (SCSI Express etc.) must be destroyed using the <block erase> command if it is supported, and if not, one or more of the methods mentioned in (a), or the method of destroying data recommended by the manufacturer must be used. iii) Magnetic tape: This refers to media that carry data with micro magnets found on flexible tape. Personal data must be deleted using de-magnetization by exposing the media to highly magnetic environments, or by way of physically burning or melting the media. iv) Units such as magnetic disks: This refers to media that carries data using micro magnets found on flexible (plate) or fixed media. Personal data must be deleted using de-magnetization by exposing the media to highly magnetic environments, or by way of physically burning or melting the media. v) Mobile phones (SIM cards or fixed storage areas): There is a delete command in smartphones; however, there is no command to destroy. Personal data must be destroyed using one or more of the methods listed in (a). vi) Optical disks: this refers to data storage media such as CDs and DVDs. Personal data must be destroyed by physically burning, grinding, or melting the media. vii) Peripheral units such as printers, fingerprint-activated access gates whose data recording media are modular: Confirming that all data storage media are taken out of the relevant devices, personal data must be destroyed by using one or more of the methods listed in (a). viii) Peripheral units such as printers and fingerprint-activated access gates whose data storage media are fixed: There is a command to delete data in most such devices, but there isn't a command to destroy data. Personal data must be destroyed using one or more of the methods mentioned in (a).

Paper and microfiche: Personal data on the said media must be destroyed by permanently destroying the media. While carrying out this procedure, the media must be shredded to pieces so small that they cannot be put back together by putting the media in a paper shredder, both horizontally and vertically, if possible. Personal data transferred to an electronic environment by scanning a paper document must be destroyed using one of more of the methods listed in (a).

Cloud Environment: Personal data must be encrypted in cloud systems, and encryption keys must be separate for each cloud solution procured for storing personal data. When the business relationship with a cloud provider ends, all copies of the encryption keys must be destroyed to render personal data in accessible. In addition to the abovementioned environments, the destruction of personal data on devices that need repair or have been sent for maintenance is carried out as follows: i) destroying personal data found on a device using one or more of the methods mentioned in (a) before the said device is sent to third-party firms such as manufacturers, vendors, or service providers; ii) In cases where it is not possible or appropriate to destroy data, removing and storing the data storage media, and sending other parts to third-party firms such as manufacturers, vendors, and service providers, iii) taking the necessary measures to ensure that the technicians who come in to do maintenance work or repairs on the equipment are not able to copy personal data and transfer it outside the company.

Anonymizing Personal Data

Anonymizing personal data refers to the process by which personal data can never be associated with an identified or identifiable person, even by cross-referencing it with other sources of data. As per law, our Company may anonymize personal data when the reasons for which they were processed no long apply. To verify that data is anonymized, it is necessary to

ensure that data cannot be associated with an identified or identifiable person using any data storage methods, including the retrieval of the data by the data controller or recipient groups, and/or comparing the data with other data sources. Our company takes all technical and administrative measures with regard to anonymizing personal data.

As per Article 28 of KVKK, anonymized personal data can be processed for purposes such as research, planning, and statistics. Such processing is outside the scope of KVKK; therefore, the explicit consent of the data subject shall not be sought.

Methods of Anonymizing Personal Data

Anonymizing personal data refers to the process by which personal data can never be associated with an identified or identifiable person, even by cross-referencing it with other sources of data.

To verify that data is anonymized, it is necessary to ensure that data cannot be associated with an identified or identifiable person using any data storage methods, including the retrieval of the data by the data controller or recipient groups, and/or comparing the data with other data sources.

Anonymizing personal data refers to a process by which all direct and/or indirect identifiers in a dataset are taken out, thereby preventing the relevant person to be identified or to be singled out in a group or crowd. Data that does not point to a specific person as a result of the abovementioned procedure is considered anonymized. In other words, anonymized data is data that has lost its ability to identify a person, and its connection with the person has been severed. The purpose of anonymizing data is severing the connection between the data and the person that the data identifies. The methods to severe this connection, such as grouping, masking, deriving, generalizing, and randomizing - which are applied to the records kept in the data recording system housing the personal data in question - are called anonymization methods. The data that is processed with anonymization methods must have lost its ability to identify a person.

The following are examples to methods of anonymization:

Anonymization Techniques that Do Not Create Value Irregularity: When methods that do not introduce value irregularity are used for anonymization purposes, the values that the data in the cluster have are not subjected to any change, addition, or omission; instead, changes are introduced to entire rows and columns in the cluster. Therefore, while the data set at large is modified, the values located in the fields preserve their original state.

Removing Variables

This is an anonymization technique whereby one or more of the variables in a table are removed. This means removing all columns in the table. This method can be used on the grounds that the variable is a highly effective identifier, an alternative solution cannot be found, the variable is too sensitive to be made public, or it doesn't serve analytical purposes.

Removing Records

This method involves removing a row that is unique in the dataset, which strengthens anonymization and reduces the possibility of generating extrapolations based on the dataset. In

general, the records that are taken out are records that do not have common values with other records and that can easily be guessed by individuals familiar with the dataset. For instance, let's say that only one person was included to represent an entire sector in a dataset that contains survey results. In this case, it might be preferable to remove the record referring to the individual, rather than removing the entire "sector" variable.

Local Suppression

The purpose of local suppression is to make the dataset more secure and reduce the risk of predictability. If the combination of values belonging to a record create a rare situation, and this causes the likelihood of that person being singled out to rise, then the value that causes the rare situation is changed to "unknown".

Generalization

This refers to the process whereby a special value in the personal data is converted into a more generic value. This is the most frequently used technique when creating cumulative reports and in operations conducted over aggregate numbers. The new values shows the aggregate values or statistics referring to a group that makes it impossible to identify a single person. For example, let's say that a person with a Turkish identification number of 12345678901 purchased diapers from an e-commerce platform, and then purchased wet wipes. Using the generalization method, we can achieve a result that says xx% of the people who purchase diapers from the e-commerce platform also buy wet wipes.

Top and Bottom Limit Coding

The method of top and bottom limit coding is implemented by defining a category for a certain variable and combining the values that remain in the grouping created by this category. Generally, the lowest and highest values of a variable are brought together, and a new definition is made for these values.

Global Coding

Global coding is a grouping method used for datasets to which bottom and top coding cannot be applied or which don’t include numeric values or have values that cannot be listed numerically. Generally, it is used where certain values are grouped to facilitate making predictions and assumptions. A common and new group is formed for the selected values and all the records in the dataset are replaced with this new definition.

Sampling

In the sampling method, instead of the whole dataset, a subset taken from the dataset is disclosed and shared. In this way, as it is not known whether a person, who is known to be within the whole dataset, is found in the disclosed or shared sample subset, the risk of making accurate predictions on the persons is reduced. Simple statistical methods are used in the determination of the subset to be used for sampling. For example, if a dataset concerning the demographics, professions and health conditions of women living in Istanbul is disclosed or shared after anonymization, it may be meaningful to scan and make predictions from the dataset concerning a woman who is known to be living in Istanbul. However, if the data is disclosed or shared after anonymization by leaving only the records of the women whose

registered province is Istanbul and removing the records of those who are registered in other provinces, since an intruder who has accessed the data cannot predict whether a woman, who is known to live in Istanbul, is registered in Istanbul or not, he/she will not be able to make accurate predictions about whether the information of the woman he/she knows is included in this body of data.

Anonymization Methods That Create Value Irregularity: In contravention to the abovementioned methods, in methods that create value irregularity, the current values are altered, and the values of the dataset are distorted. In this case, as the values of the records are changing, it is necessary to precisely calculate the benefit is expected to be obtained from the dataset. Although the values in the data set are indeed changing, it may still be possible to benefit from this body of data by protecting the overall statistics from being distorted.

Micro-aggregation

In this method, all the records in the dataset are first arranged in a meaningful order, and then the whole set is divided into a certain number of subsets. Afterward, the average value for the specified variable in each subset is calculated, and the value in the subset for that variable is replaced with the average value. Therefore, the average value of that variable valid for the whole dataset will not change.

Data Swapping

Data swapping refers to record alterations obtained by swapping the values of a subset of variables between selected pairs of records. This method is typically used for variables that can be categorized, and the main idea is to transform the database by swapping the values of the variables between the records of the individuals.

Adding Noise

In this method, additions and omissions are applied to ensure a determined level of distortion in a selected variable. This method is employed mostly for datasets that contain numerical values. Distortion is applied equally to each value.

Statistical Methods That Strengthen Anonymization

As a result of bringing some values of anonymized datasets together in unique scenarios, the possibility may emerge of being able to determine the identities of the people in the records or making assumptions concerning their personal data.

For this reason, the anonymization procedure may be strengthened by minimizing the uniqueness of the records within the dataset by applying various statistical methods to the anonymized datasets. The main objective of these techniques is to minimize the risk of disrupting anonymization while preserving, to a certain degree, the benefit to be obtained from the data set.

K-Anonymity

Being able to identify persons or predict information belonging to a certain person in the anonymized data sets when indirect identifiers fall together in the right combinations has called into question the reliability of anonymization processes. Therefore, the necessity arose of

making the datasets anonymized by means of various statistical methods more reliable. K-anonymity has been developed to enable the definition of more than one person using certain fields in a dataset so as to prevent people who demonstrate individual characteristics in certain combinations from being exposed. In the event that there are more records than one regarding the combinations formed by gathering some of the variables in a dataset, the probability of identifying the persons that correspond to this combination is reduced.

L-Diversity

L-Diversity method, developed on the basis of the studies carried out on the deficiencies of K-anonymity, takes into account the diversity formed by the sensitive variables corresponding to the same variable combinations.

T-Closeness

Although the L-diversity method provides diversity in personal data, as the method does not care about the content and sensitivity levels of the personal data, there may be circumstances where it cannot provide sufficient protection. The anonymization of personal data in such a way by calculating the closeness levels of the values among them and dividing them into subclasses according to these closeness levels is called the method of T-closeness.

Choosing the Anonymization Method

Our Company decides on which of the abovementioned methods and techniques to use depending on the nature of the data on hand, and the following features and properties of the dataset that we own:

Nature of the data,
Data size,
Type of physical media used to store data,
Data diversity,
The benefit expected from the data / the purpose of processing the data,
The frequency of processing the data,
The reliability of the party to which data will be transferred,
Whether the effort to anonymize the data will be meaningful,
The scope of the impact that might occur if the anonymized nature of the data is harmed,
Distribution of the data,
Controlling the access of the users to the data, and
The probability that an individual may make a meaningful effort to prepare and launch an attack that will distort the anonymity of the data.

When anonymizing a body of data, our Company checks, through the agreements it strikes and the risk analyses it conducts, whether the anonymized data would regain its ability to identify a person when combined with information that is public or that is known to be at other companies that the company shares the data with.

Reliability of Anonymization

When making the decision to anonymize a set of personal data rather than deleting or destroying it, our Company takes into account the following points: Whether it would be possible

that the anonymization of the data would be compromised when it is combined with another dataset, or it achieves a meaningful whole if multiple sources of data create a unique case, or whether values come together to enable assumptions to be made and conclusions to be drawn. Our Company conducts regular checks as the aspects mentioned in this provision change, and ensures that anonymity is preserved.

Risks Pertaining to the Distortion of the Anonymity of Anonymized Data in a Reverse Procedure

Since the procedure of anonymization is applied to personal data and seeks to remove the identifying qualities of a dataset, there is the risk of reversing this procedure with various interventions, recovering the dataset's ability to identify real persons. This is referred to as distortion of anonymity. Anonymization can be made manually, automatically, or featuring a mix between the two. However, what is important is that necessary measures must have been taken so that the users of the anonymized data that has been shared and disclosed are not able to harm the anonymity of the data in any shape or form. Intentional efforts to distort anonymity are called "attacks aimed at distorting anonymity". In that regard, our Company does research on whether there is the risk of reversing the anonymity of a dataset and recovering its ability to identify a real person and takes action in accordance with the results of this research.

HOW DO WE PROTECT YOUR PERSONAL DATA?

As per the Personal Data Security Guide published by the KVK Institution in a bid to protect your personal data and prevent it from being accessed unlawfully, our Company takes all the necessary administrative and technical measures, carries out procedures internally, prepares disclosure statements and explicit consent forms, conducts or outsources the necessary audits to ensure compliance with KVKK provisions as per Article 12/3 of KVKK. The results of such audits are evaluated as part of the Company's internal mechanisms, and necessary action is taken to improve the quality of the measures taken.

Your personal data shall be transferred to the physical archives and IT systems of our Company and/or our suppliers, and preserved in both digital and physical environments. The measures taken to ensure the safety of personal data are explained in great detail under two separate headings.

Technical Measures

In order to protect personal data, we use generally accepted technology standards and business safety methods, including the technology called Secure Socket Layer (SSL). However, information can be accessed by unauthorized persons over the Internet, without the necessary precautions in place. Depending on the state of the art in technology, associated costs, and the nature of the data to be protected, we take the necessary measures to prevent your personal data from being impacted by destruction, loss, tampering, unauthorized disclosure, or unauthorized access. In that respect, we enter into contracts with the service providers we work with regarding data safety.

1) Ensuring Cyber Security: In order to ensure data safety, we use cyber security products, but the technical measures we have in place are not limited to these. Measures such as firewalls and network tunnels comprise the first line of defense against internet-borne attacks. With that said, nearly all software and hardware go through some installation and structuring efforts. Taking into account that old versions of some commonly used software might have documented security loopholes, unused software and services are removed from devices. For that reason, we prefer to delete unused software and services for ease of use, rather than keeping them updated. Using patches and software updates, we regularly check whether the security measures we have in place for the proper functioning of the software and hardware are sufficient.

2) Access Restrictions: Access to systems that include personal data is restricted and is reviewed on a regular basis. In that regard, employees are given access that is proportionate to their job description, and they are given access to the relevant systems with user ID - password combinations. It is ensured that when determining the passwords, complex combinations that include uppercase and lowercase letters, numbers, and symbols, rather than easily predictable sequences of letters and numbers that are associated to personal information. An authorization and control matrix is thereby created.

3) Encryption: Aside from using strong passwords, access restrictions are preserved by limiting password login attempts to protect against common attacks such as the use of brute force algorithms (BFA), requiring regular password changes, using the administrator account only when necessary, and swiftly deleting the accounts of (or blocking the access of) employees whose relationship with the data controller has been terminated.

4) Anti-virus Software: In order to protect our systems from malicious software, we also use anti-virus and anti-spam products that scan the system network on a regular basis and detect threats, and we keep this software updated. If personal data is to be obtained from various websites and/or mobile applications, then it is ensured that the connections are based on SSL or a more secure protocol.

5) Monitoring the Safety of Personal Data: We check which software and services are operated in IT networks, detect any penetration attempts or unusual movements, keep regular logs of the actions of all users, and report security issues as soon as possible. Again, a formal reporting procedure is being established for employees to report security weaknesses in systems and services or threats that exploit them. Evidence is collected and stored securely in undesirable events such as information system crashes, malicious software, decommissioning attacks, incomplete or incorrect data entries, violations that disrupt privacy and integrity, and information system exploitations.

6) Securing the Environments That Include Personal Data: If personal data is stored in devices or in the paper format at the data controller's premises, physical security measures are taken against threats such as theft or loss of data. The physical environments where personal data is stored is protected against external risks (fire, flooding etc.) in appropriate ways and entries to and exits from these environments are controlled.

If personal data is in an electronic environment, access may be restricted between network units, or they may be separated, in order to prevent security breaches. For instance, if personal data is processed in an area of the network demarcated for the purpose of processing data, then existing resources may be concentrated on securing this area, rather than the entirety of the network.

The same measures are taken for paper media, electronic media and devices that are located outside the company's premises and that contain personal data belonging to the company. As a matter of fact, although personal data security breaches are often caused by the theft or loss of devices containing personal data (laptop, mobile phone, flash disk, etc.), personal data to be transferred by e-mail or mail is also handled with care and by taking adequate measures. If employees access the information system network with their personal electronic devices, adequate security measures are also taken for them.

Access control authorization and/or encryption methods are used against the loss or theft of devices containing personal data. In this context, the password key is stored in an environment accessible only to authorized persons, and unauthorized access is prevented.

The physical paper documents that include personal data are stored in environments where they can be accessed only by the authorized personnel, thereby preventing unauthorized access.

If the personal data processed in compliance with article 12 of the Law is obtained by third persons through unlawful means, our company runs a system that ensures notification of such issue to the data subject and Data Protection Board as soon as possible. If it is deemed necessary by the Data Protection Board, this issue may be announced on the web site of the Data Protection Board or via any other means.

7) Storage of Personal Data in the Cloud: In the case of storage of personal data in the cloud, the company must also evaluate whether the security measures taken by the cloud storage service provider are adequate and appropriate. A two-stage authentication control is applied to have a detailed knowledge of the personal data stored in the cloud, to create backups of it, synchronize it, and access it remotely where necessary. Personal data are encrypted in cloud systems and transferred to cloud environments in an encrypted format, and separate encryption keys are created for each cloud solution procured for storing personal data. When the business relationship with a cloud provider ends, all copies of the encryption keys are destroyed to render personal data inaccessible. Access to data storage areas where personal data is stored is logged and inappropriate access or access attempts are instantly communicated to relevant parties.

8) Procurement, Development, and Maintenance of IT Systems: Security requirements are taken into account when determining any needs with regard to the procurement and development of new systems, or the improvement of existing systems by the Company.

9) Creating Back-Ups of Personal Data: In the event that personal data is harmed, destroyed, stolen, or lost for any reason, the Company uses back-ups to get operations back on track

as soon as possible. The back-ups of personal data can only be accessed by the system manager, and dataset back-ups are kept outside the network.

Administrative Measures

- All activities carried out by our Company have been analyzed in detail at each business unit, and as a result of this analysis, we have prepared a process-oriented personal data processing inventory. Necessary legal and technical measures are taken by determining the risky areas in this inventory. (e.g. The documents required by KVKK were prepared in consideration of the risks in this inventory.)
- The personal data processing activities carried out by our Company are monitored by IT security systems, technical systems, and legal methods. Policies and procedures are determined with relation to personal data safety, and regular checks are conducted in this regard.
- Our Company may at times procure services from external service providers in order to meet its IT technology needs. In such cases, we proceed when we are certain that the Data Processing service providers are able to provide, at a minimum, the security provided by our Company. To achieve this, we enter into an agreement with the Data Processor, and the agreement contains the following issues:
    - The Data Processor shall act only in accordance with the instructions of the Data Controller for the data processing purposes specified in the agreement, and in keeping with KVKK and relevant regulations,
    - It shall act in compliance with the Personal Data Storage and Destruction Policy,
    - The Data Processor shall be obligated to keep secrets indefinitely concerning the personal data it processes,
    - The Data Processor shall be obligated to notify the Data Controller in case of a data breach,
    - Our Company shall conduct or delegate necessary audits on the Data Processor's systems that contain personal data, and shall review the reports prepared as a result of the audits, or visit service provider on-site,
    - It shall take all necessary technical and administrative measures for the security of personal data.
    - In addition, the categories and types of personal data transmitted to the Data Processor are also specified in a separate article, to the extent that is permitted by the nature of the relationship between the Data Processor and our Company.

- In keeping with the data minimization principle stressed by the Company's guides and publications, personal data are reduced to a bare minimum and unnecessary, out-of-date, and useless data is not gathered, and if it was gathered before KVKK, then it is destroyed in accordance with the Personal Data Storage and Destruction Policy.
- Experts are recruited for technical issues.
- Our Job Contracts, which are to be signed during recruitment processes, feature provisions on confidentiality and data safety, and our Company requests that employees abide by these provisions. Employees are informed and trained on a regular basis in terms of the legal aspect of protecting personal data and taking necessary measures to achieve that

purpose. The roles and responsibilities of the employees have hereby been reviewed and the job descriptions have been revised.

- Technical measures too are taken with respect to technological developments, and these measures are periodically checked, updated, and renewed.
- Access authorization is restricted, and is reviewed on a regular basis.
- The technical measures that are taken are reported to the relevant supervisors on a regular basis; risk factors are reviewed and technological solutions are actively pursued.
- Software and hardware that include virus protection systems and firewalls are installed.
- Back-up software is used in order to safely store personal data.
- Security systems are used for storage areas; the technical measures that are taken are periodically reported as per internal control principles, and the issues that constitute risk factors are reviewed and necessary technological solutions are pursued. The files/print-outs stored in physical environments are located at the premises of suppliers, and are destroyed in accordance with the specified procedures.
- The executive management also shows ownership towards the issue of Protecting Personal Data; a special Committee has been set up and has launched (KVK Committee). A management policy governing the working principles of the KVK Committee has entered into force, explaining the committee's mission in great detail.

HOW DO WE PROTECT YOUR PERSONAL DATA OF A SPECIAL NATURE?

A separate policy has been prepared and has entered into force regarding the processing and protection of personal data of special nature.

As per Article 6 of KVKK, personal data relating to the race, ethnic origin, political opinion, philosophical belief, religion, sect or other belief, clothing, membership to associations, foundations or trade-unions, health, sexual life, convictions and security measures, and the biometric and genetic data are deemed to be personal data of special nature, as their unlawful processing can lead to grave injustices or discrimination. Therefore, the law stipulates a higher standard of protection for personal data of this type.

As per Article 10 of KVKK, our Company notifies Relevant Persons when collecting personal data of special nature. We process personal data of special nature by taking appropriate precautions as per KVKK and conducting or commissioning necessary audits. Another categorical condition for processing personal data of special nature is the explicit consent of the data subject. Our Company allows data subjects to express their explicit consent regarding a specific topic, on the basis of being notified, and of their own free will.

Our Company seeks the written consent of Relevant Persons when processing personal data of special nature. However, as per Article 6/3 of KVKK, explicit consent is not sought if one of the conditions specified in Article 5/2 of KVKK is present. In addition, Article 6/3 of KVKK stipulates that personal data relating to health and sexual life may only be processed without obtaining the explicit consent of the data subject for purposes of protection of public health, operation of preventive medicine, medical diagnosis, treatment, and care services, planning and management of health services and financing by persons under the obligation of secrecy or authorized institutions and organizations. Whatever the pretense, general data processing

principles are taken into account in all relevant processes, and compliance with such principles is sought.

Our Company takes special measures to ensure the protection of personal data of special nature. As per the principle of data minimization, personal data of special nature is not collected unless necessary for the relevant business process, and such data is only processed where necessary. When personal data of special nature is processed, our Company takes all necessary technical and administrative precautions to comply with provisions specified by the Data Protection Board and other legal obligations.

WHAT ARE YOUR RIGHTS WITH RESPECT TO YOUR PERSONAL DATA?

As per Article 11 of KVKK, you as the data subject have the following rights with respect to your personal data:

- Learn whether your personal data is processed or not,
- Request information if your personal data is processed,
- Learn the purpose of your data processing and whether this data is used for intended purposes,
- Know the third parties to whom your personal data is transferred at home or abroad,
- Request the rectification of the incomplete or inaccurate data, if any, and request the notification of third parties to which your personal data has been transferred,
- In the case where, although it has been processed pursuant to the legislative provisions, the reasons requiring it to be processed cease to exist, to request that the personal data is deleted or destroyed, and the third parties to whom personal data is transferred are also notified,
- Object to the processing, exclusively by automatic means, of your personal data, which leads to an unfavorable consequence for the data subject,
- Request compensation for the damage arising from the unlawful processing of your personal data.

You can convey your requests to our Company using one of the methods explained below, as per the Application Communique:

1) After filling out the application form and signing it, please deliver it in person to the following address: Işıktepe OSB Mahallesi Siyah Cadde No:29 Nilüfer Bursa / Türkiye or Kocaeli - Taysad Organize Sanayi Bölgesi - TOSB, 1. Cadde 14. Sokak No:10 Çayırova Kocaeli / Türkiye (we would like to remind you that you'll be asked to verify your identity), or

2) After filling out the application form and signing it, please deliver it via notary public to the following address: Işıktepe OSB Mahallesi Siyah Cadde No:29 Nilüfer Bursa / Türkiye or Kocaeli - Taysad Organize Sanayi Bölgesi - TOSB, 1. Cadde 14. Sokak No:10 Çayırova Kocaeli / Türkiye, or

3) Fill in the application form and sign it with a "secure electronic signature" defined in the Electronic Signature Law No. 5070, and send the electronically signed form to bosch.rexroth@hs01.kep.tr via email.

The application is required to have the following:

If the name, surname and application are written down, the signature is for citizens of the Republic of Türkiye. Name, surname, signature if the application is in written form, Turkish identification number for Turkish citizens, ethnicity, passport number and ID number (if possible) for foreigners, residency or business address, email address, phone and fax number if any, and the subject of application. The information and documents relevant to the application are also attached.

It is not possible for third persons to make applications on behalf of data subjects. In order for the data subject to make a personal data request with regard to another individual, the data subject must produce a power of attorney letter prepared for the concerned individual, notarized and carrying a wet signature. With regard to the application that you make in order to exercise your abovementioned rights as data subject, it is essential that you clearly explain your request, that your request concerns yourself or if you're acting on behalf of another person, you are specially authorized to act on their behalf and you have documents to support your authorized status, that your application includes ID and address information, and that your application is supplemented with documents verifying your identity.

Your applications made according to this guide shall be finalized as soon as possible, and at most within 30 days. Such applications are made free of charge. However, in the event that this effort leads to an expense, you shall be charged according to the fees determined by the Data Protection Board.

Provided that you as data subject file a request with our Company with regard to your rights in line with the style and means of communication stipulated in the Law, your request shall be processed immediately and executed free of charge within thirty days, depending on the nature of the request. However, in the event that this effort leads to an expense, you shall be charged according to the fees determined by the Data Protection Board. Our Company might request information from the data subject in order to verify whether the applicant is indeed the data subject in question. Our Company might also pose questions to the data subject so as to clarify any points mentioned in the application.

As per Article 14 of KVKK, if the application is declined, the response is found unsatisfactory or the response is not given in due time, the data subject may file a complaint with the Data Protection Board within thirty days as of learning about the response of the controller, or within sixty days as of the application date, in any case.

WHAT ARE THE CASES IN WHICH DATA SUBJECTS CANNOT EXERCISE THEIR RIGHTS?

As the following cases are exempted from the scope of the law pursuant to Article 28 of KVKK, data subjects are not entitled to exercise their rights:

- Processing of personal data for the purposes such as research, planning, and statistics through anonymization by official statistics.
- Processing of personal data for the purposes of art, history, literature or science, or within the scope of freedom of expression, provided that national defense, national security, public safety, public order, economic safety, privacy of personal life or personal rights are not violated or it does not constitute a crime.
- Processing of personal data within the scope of preventive, protective and intelligence-related activities by public institutions and organizations who are assigned and authorized for providing national defense, national security, public safety, public order or economic safety.
- Processing of personal data by judicial authorities and execution agencies with regard to investigation, prosecution, adjudication or execution procedures.

Pursuant to Article 28/2 of KVKK, data subjects are not entitled to exercise their rights in the following cases, except for the right to request compensation:

- Processing of personal data is necessary for prevention of crime or investigation of a crime.
- The data processed is made public by the data subject herself/himself.
- Processing of personal data is necessary for the performance of supervisory or regulatory duties, or disciplinary investigation or prosecution by assigned and authorized public institutions and organizations and professional organizations with a public institution status.
- Processing of personal data is necessary for the protection of economic and financial interests of the state related to budget, tax, and financial matters.

OTHER ISSUES

As explained in great detail above, your personal data shall be stored and preserved, classified with regard to market research, financial and operational processes, and marketing activities, updated in various periods, transferred to third persons and/or suppliers and/or service providers and/or our foreign shareholders to the extent possible as per relevant regulations and in accordance with the principle of confidentiality, as well as transmitted, stored, processed through reporting, and documented electronically and physically in accordance with the policies we are bound by and for reasons specified by other authorities.

Where there is a conflict between KVKK/other regulations and this Policy, the provisions of KVKK and other regulations shall take precedence.

This Policy prepared by our Company has entered into force pursuant to the decision made by the Bosch Board of Directors.

We would like to remind you that we may update this Policy in the future to reflect changes in regulations and company policies. We shall publish the up-to-date version of the Policy on our website.

User/Users have irrevocably agreed, acknowledged, and declared that they have read this Policy on the Protection of Personal Data before entering the website, that they shall comply with all the provisions of the Policy, and that the entirety of the contents of our website, as well as all electronic and computer records belonging to our Company are considered conclusive evidence as per Article 193 of the Code of Civil Procedure.

Data Protection and Information Security Department

Last update: **17.04.2024**

Version: **v1.3**

APPENDIX - ABBREVIATIONS

ABBREVIATIONS	
Law No. 5651	The Law on the Regulation of Publications on the Internet and Combating Crimes Committed by Means of Such Publication, which entered into force after being published on the Official Gazette No. 26530 on May 23, 2007
Constitution	the Republic of Türkiye Constitution No. 2709 dated November 7, 1982, published on the Official Gazette No. 17863 on November 9, 1982
Application Communique	Communique on the Principles of Application to the Data Controller, which entered into force after being published on the Official Gazette No. 30356 on March 10, 2018
Relevant Person/Relevant Persons or Data Subject	Refers to the Bosch's and/or Bosch group companies' customers, corporate customers in a business relationship, business partners, shareholders, officials, employee candidates, interns, visitors, suppliers, employees of the companies in a business relationship, third persons, and any real person whose personal data is processed.
The Regulation on the Deletion, Destruction, and Anonymization of Personal Data	The Regulation on the Deletion, Destruction, and Anonymization of Personal Data that entered into force on January 1, 2018, after being published on the Official Gazette No. 30224 on October 28, 2017
KVKK	The Law on the Protection of Personal Data that entered into force after being published on the Official Gazette No. 29677 on April 7, 2016
Data Protection Board	Personal Data Protection Board
KVK Institution	Personal Data Protection Institution
E.g.	Example
Policy	Bosch Policy on the Protection of Personal Data and Privacy
Company/Bosch	Bosch Rexroth Otomasyon Sanayi ve Ticaret A.Ş.
Turkish Penal Code	Turkish Penal Code No. 5237 dated September 26, 2004, which was published on the Official Gazette No. 25611 on October 12, 2004