DATA PROTECTION GUIDELINES

2023

BAWAG Group

BAWAG Group Data Protection Guidelines

Introduction

The protection of information, data and ICT systems and to safeguard the interests and privacy of our customers, employees, suppliers and other stakeholders is of utmost importance to BAWAG Group.

BAWAG Group adheres to data protection in accordance with the General Data Protection Regulation and banking secrecy in accordance with the Austrian Banking Act.

In accordance with Article 5 GDPR, we only collect, process and use personal data from our customers to the extent that it is: expressly approved by them; legally permissible; and, expedient and necessary to carry out the services offered. Data will not be passed on to third parties unless we are legally entitled or obliged to do so.

Legal Basis	**For any separate usage of data, a designated legal basis according to Article 6 GDPR, similar legal regulations, or a confirmation by the customer is mandatory**
Purpose limitation and data minimization	BAWAG Group collects and processes personal data solely for the stated purposes. The personal data is adequate, relevant and limited to these purposes
Privacy by Design	Adherence to the data protection guidelines is something that must be considered from the initial stages of the development phase when designing any new products or processes
Privacy by Default	Pre-settings for data collection preferences must be configured in a data protection friendly way that ensures adherence to the data minimization principle

Information, right of access, right to rectification, deletion, data portability and objection of individuals' data

BAWAG Group informs all concerned individuals with specific information sheets on privacy.
The information sheets for customers are made available on the group companies' websites.

The information sheets for customers are made available on the group companies' websites or before entering into a contract with the bank. Employees can obtain this information on the internal information platform or upon conclusion of employment contracts. Suppliers also receive an information sheet.

Information regarding Art. 13 and 14 GDPR	BAWAG Group informs all concerned individuals about collection, use, sharing and retention of data (including data transfers to third parties) with information sheets on privacy. The information sheets for customers are made available on the group companies' websites or before entering into a contract with the bank. Employees can obtain this information on the internal information platform or upon conclusion of employment contracts. Suppliers also receive an information sheet. The information contains in particular: • the purpose of the processing • legal basis and/or legitimate interest • information in case of data sharing under legal requirements (e.g. Kontenregister, Einlagensicherung) • if applicable, the recipient and category of transmitted data • storage period • information about the existence of the right to information, rectification, restriction, withdrawal and data erasure; further contact information on where the customer can turn to can be found in the information sheet • if there is an obligation to provide data: consequences of non-provision • profiling and logic involved • data was not disclosed by the customer - source and data categories are to be cited • contact details of the Bank / data protection officer
Right of access	Individuals are entitled to receive information about their stored data. They are informed whether or not personal data is processed and receive information according to Art. 15 GDPR (including a copy of the personal data undergoing processing).

Right to rectification	Individuals have the right to obtain, without undue delay, the rectification of inaccurate personal data concerning them (like updating the borrower's employer). Considering the purposes of the processing, the individual has the right to have incomplete personal data completed (like completing rating data).
Right to erasure	Personal data will be erased without undue delay when • the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed; • individual withdraws consent on which the processing is based and where there is no other legal ground for the processing; • individual objects to the processing and there are no overriding legitimate grounds for the processing; • personal data have been unlawfully processed; or • personal data have to be erased for compliance with a legal obligation in European Union or Member States
Right to data portability	Individuals receive the personal data in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller. Individuals have the right to have their personal data transmitted directly from one controller to another, where technically feasible.
Right to object	Individuals have the right to object to the processing of data and to request deletion. BAWAG Group has to prove legitimate interest in keeping the data stored, such as fulfillment of regulatory requirements and legal obligations. Otherwise, the data is deleted without restrictions.

BAWAG Group Data Protection organization, controls and processes

BAWAG Group has been in the past and continues to be fully committed to the implementation and adherence towards high data protection standards. Our current implementation follows the framework set out by the European General Data Protection Regulation (GDPR) and Austrian Data Protection Act.

Executive body Non Financial Risk and Environmental Social Governance Committee	The Non Financial Risk and Environmental Social Governance Committee is the company's executive body responsible for Privacy. Voting Members of the committee: • All Management Board Members (Chair: Chief Risk Officer; 1st Deputy: Chief Executive Officer; 2nd Deputy: Chief Financial Officer) • Head of Financial Crime Management & Compliance • General Counsel • Head of Strategic Risk Management • ESG Officers Non-Voting Members of the committee also include representatives of the technology division. Other Division Heads or subsidiaries are invited for specific NFR and ESG topics in their entities.
Chief Administrative Officer	The Data Protection Office reports regularly to the CAO. Timely information and exchange on new laws, guidelines and decisions as well as procedures. The implementation is discussed with the CAO, who decides on it.
Data Protection Office Art. 37 (1) GDPR	In accordance with the GDPR, which has been in force since 2018, a data protection office has been established in BAWAG Group. The aim is to prevent the risks that may result from noncompliance with legal regulations and requirements and to contribute to improved control and management.

Data Protection Officer MMag. Barbara Wagner	MMag. Wagner has been responsible for data protection in the BAWAG Group since 2003 and was appointed as data protection officer in 2016. MMag. Barbara Wagner is an expert and has other roles in relation to data protection as well: • Auditor at the "Verein österreichischer betrieblicher und behördlicher Datenschutzbeauftragter privacyofficers.at" • Austrian representative of the banks at the "European Banking Federation" • Advisory council of the magazine "Datenschutz konkret" The Group Data Protection Officer advises the relevant stakeholders within BAWAG Group.

Policies	An extensive Data Protection Policy applies to all employees. The Data Protection Policy governs all relevant business lines and subsidiaries. It is updated annually.
Training All employees & contractors	Training is provided to all employees, including contractors. For training purposes an obligatory e-learning program has been rolled out. Each new employee must complete the e-learning program at the beginning of their employment relationship. The e-learning program is constantly updated on the basis of new case law and current incidents and is rolled out on a regular basis to all employees. Each training ends with a test, in which a minimum grade has to be achieved in order for the training to be recognized. The e-learning must be completed every two years.
Special trainings	In addition to these regular training courses, training courses are also carried out due to special incidents. These ad hoc trainings can be in form of specific training for individual employees, trainings for certain departments or information provided to the entire bank via an article on the company's intranet.
Data Protection Single Point of Contact System	Moreover, Data Protection SPOCs (Single Point of Contacts) within all divisions and subsidiaries help to raise the awareness for a compliant treatment of personal data of our customers and employees. External staff, cooperation partner and contractors are also trained in data protection.

BAWAG Group Data Protection controls and processes

BAWAG Group's commitment to high data protection standards is ensured by several layers of controls, defined processes, and risk evaluation

Layers of Control Annual Audit	As part of the audit of the annual financial statements by external auditors, sub-areas of data protection are also checked.
Internal Audit	Internal Audit holds annual audits in individual divisions. In the course of these audits the topic of data protection is covered.
Complaint Management	BAWAG Group has also created a central complaint management system and an internal control system (IKS).
Customers	With the information sheet on data protection in accordance with Article 13 GDPR, customers are informed what their data is being processed for. The information sheet is checked annually by the data protection office. Furthermore, when a risk assessment is carried out the information sheet is reviewed for whether a revision is necessary.
Employees	Our employees are obliged in writing to comply with data protection and confidentiality in accordance with the Banking Act. They will be kept in the loop with the regulations and requirements of data protection on a regular basis through training courses (see also under "Training") and other suitable measures. The data protection office provides ongoing information on current data protection developments and organizes training courses and lectures for employees.
Jurisdiction	The implementation of the restrictive legal requirements of the Banking Act - to which every financial institution is subject to - also supports us in being compliant with the General Data Protection Regulation.
Protective measures on the subject of ethics	In view of growing market integration and the increasing use of technology, economic crime is on the rise. For this reason, BAWAG Group is stepping up requirements to be met by employees in respect of reporting acts of economic crime in its business operations.
Whistleblowing	Therefore BAWAG Group established a whistleblowing system for the anonymous receipt and processing of information as early as 2013. The BKMS®System is an Internet-based system accepting tip-offs concerning acts of economic crime in German and English. The system is barrier free. In 2023 the system was adapted to the new whistleblower protection laws.

	Entitled to report in Austria and Germany are: • Employees of a BAWAG Group AG company or workers assigned to one of the BAWAG Group AG companies, • Applicants of a BAWAG Group AG company In addition, the following persons are entitled to report in Austria: • Self-employed business partners and their employees, suppliers and subcontractors of a BAWAG Group AG company or • Members of the management board, supervisory board and shareholders of a BAWAG Group AG company Every tip-off is immediately and comprehensively followed in order to be able to sufficiently take legal deadlines into account. Investigations are initiated in all cases with sufficient initial suspicion. Investigations are conducted - in accordance with the need-to-know principle - with the greatest possible confidentiality in the smallest possible group of people. The data protection department is responsible for maintaining this system. BKMS has the following certificates: • ISO27001 by datenschutz cert GmbH • EuroPrise by the EuroPriSe Certifcation Authority (Barrierefreiheitszertifizierung) Accessibility certification by TÜV Austria and • Penetration Test and Retest by Recurity Labs GmbH
Contact with regulators Legal developments	The Austrian Data Protection Authority is responsible for complaints and procedures relating to data protection. The data protection office is in constant contact with the Data Protection Authority and answers their requests as well as consciously monitors legal developments.

BAWAG Group Data Protection processes

Data minimization, data deletion after the statutory retention periods have expired	We are committed to the data minimization principle. Only data that is necessary to achieve the purpose is collected. The statutory retention periods are stored for each process in the records of processing activities (including the legal basis for the storage of data). Customer data is automatically deleted after the statutory retention period (7 years according to UGB and BAO and 10 years according to FM-GwG) has expired. The deletion of data whereby the retention period has expired takes place once a year. BAWAG Group informs all customers and employees about deletion routine with the information on privacy (Art. 13 and 14 GDPR). The information sheet for customers is made available on the group companies' websites and before entering into a contract with the bank. Employees can obtain this information on the internal information platform or upon conclusion of employment contracts.
Third parties	The specifications of the purchasing process are described in BAWAG's purchasing guidelines. During each contract negotiation, the department, which is responsible for concluding contracts, checks whether and which personal data is being processed. When contracts are concluded, the following is agreed with processors: • Data Processing Agreement • Code of Conduct • Outsourcing conditions BAWAG Group only enters into business relationships with suppliers that comply with, and agree in writing to comply with, the principles and requirements for suppliers of goods and services as defined in the Code of Conduct for Supplier. Sample contracts for order processing were drawn up by the data protection office. These contain the regulations of the GDPR and our data protection regulations in accordance with the company's policy. Third parties with whom data is to be shared must comply with, the companies` data processing and non-disclosure agreements. Service providers from outside the European Union may only be consulted if they have an adequate level of data protection. The technical and

	organizational measures (TOM's) of each partner must be attached to the contract. Each contract is recorded in the central contract database and any new recipients are added to the records of processing activities. Outsourcing Assessment/Outsourcing Quality Committee: In the case of outsourcing, an outsourcing assessment must be carried out. There is a separate policy on outsourcing, "Outsourcing Assessment Template", in which outsourcing, risks and measures are described. In the case of insignificant outsourcing, no notification of the supervisory authority is required and a simplified risk assessment takes place. Significant outsourcing, on the other hand, must be reported to the supervisory authority and is subject to an extended risk assessment compared to insignificant outsourcing. The outsourcing of cloud providers is also subject to a procedure specified in the outsourcing policy. The outsourcing assessments must be approved by the Outsourcing Quality Committee. The data protection officer is part of this committee. The assessment takes place not only for new contracts, but also for contract extensions and changes. In the case of significant outsourcing, there is a quarterly review. A data protection assessment is part of it. IT security in the life cycle When the processing of personal data is outsourced, it mostly affects IT applications. The protection of data and IT security must be guaranteed throughout the life cycle of the IT system. The requirements for this are regulated in the Group Policy for Security in the System Life Cycle. It regulates IT and data security in all phases - from development, testing, operation to the decommissioning of the IT application. Security measures are provided with regard to the different system environments (development, test, production). BAWAG's Chief Information Security Officer developed this guideline in consultation with the data protection officer. In addition, we have certificates/audits presented to us. Our Internal Audit department also conducts regular audits.

Data breaches Proactive measures	Every employee receives regular data protection training as part of a mandatory e-learning program. The training ends with a test. An employee passes the test if a certain minimum number of questions have been answered correctly. All data protection requirements that the bank must adhere to are described in a Data Protection Policy that applies to all employees (permanent and temporary).
Reactive measures	There is a clear approach defined in case a data breach is suspected: the data protection department, the head of division of Financial Crime Management & Compliance and the chief information security officer (CISO) are notified. If the incident is confirmed, the Managing Board is also to be informed. According to Data Protection Law Data breaches must be reported to the Data Protection Authority. In the event of a breach, the data protection authority must be informed immediately, at least within 72 hours after becoming aware of the breach This report includes: • Description of the violation ✓ Affected category of persons ✓ Number of affected persons ✓ Affected data ✓ Approximate number of affected records • Contact details of the data protection officer • Description of possible consequences of the data protection breach • Description of the measures taken or planned to remedy the infringement Affected persons are notified in a timely manner in case of a data breach. Employees who were involved in the data breach have to undergo an additional training.

Risk assessment for products, processes and systems Privacy by Design & Privacy by Default Questionnaire	With Privacy by Design and Privacy by Default, BAWAG Group implements data protection by technology design and privacy-friendly default settings. New product ideas or changes to products as well as new process designs need to undergo a product introduction process with an extensive risk assessment, including data protection and ICT risks. Additionally, BAWAG Group has introduced a security-in-the-system-life-cycle concept that is designed to ensure an adequate level of security at any stage, i.e. from conception to implementation and decommissioning of systems. To support this, the data protection office and IT-Security developed a data protection assessment questionnaire. This questionnaire must be filled out in advance. The new product, process or system will only be approved if the data protection impact assessment is positive.
Data Protection Software	The data protection management system, otris, privacy supports the various activities. The records of processing activities in accordance with Article 30 GDPR are also kept in this software as the data protection impact assessment (Articles 35 and 39 GDPR) that may be necessary when new products, processes and systems are introduced. In addition, an annual check of the records of processing activities is also carried out against the active IT systems.
Mechanisms for data subjects to raise concerns about data privacy	Customers can use a form on our website for raising concerns about data privacy. Such customer inquiries are forwarded directly to the data protection department. Furthermore customers can raise concerns in the eBanking. The information sheet (Art. 13 and 14 GDPR) for customers contains on the first page contact details to which customer inquiries can be sent. These are postal and email addresses. The contact options are used by customers. In 2022 we received 632 customer requests on data protection.
Third parties with whom the data is shared	The data protection and IT standards specified by the bank are agreed on in contracts with third parties.

	All data uses on each purpose are listed in the records of processing activities. All IT systems are taken into account. According to the GDPR, the records of processing activities don't have tocontain the legal basis. For greater transparency, the bank has decided to include the legal basis for every data processing. Before obtaining and storing data the legal basis and data protection principles according Art. 5 and 6 GDPR are checked. User data is obtained and processed when the bank adheres to those principles. The information sheet according Art. 13 and 14 GDPR provides information to the data subjects. Where an explicit consent is needed customers are informed in the product applications online and offline. Explicit consent will be obtained where necessary. BAWAG Group does not rent or sell personal data to third parties. The data is only used for purposes laid down in the data protection information sheet. All third parties that receive personal data have to commit to the following: *"The Processor shall only process personal data as contractually agreed or as instructed by the Controller, unless the Processor is legally obliged to carry out a specific type of data processing. Should the Processor be bound by such obligations, the Processor is to inform the Controller thereof prior to processing the data, unless informing him is illegal. Furthermore, the Processor shall not use the data provided for processing for any another purposes, specifically his own."*