Addiko Bank

Addiko Group

Data Protection and Information Security Guidelines

Data protection

Data protection is an increasingly important topic, particularly since the General Data Protection Regulation (GDPR) entered into force on 25 May 2018. GDPR strengthened the rights of data subjects, imposed new requirements on data controllers and data processors when managing and handling personal data, and increased expectations of clients, employees, other stakeholders and regulators.

As Addiko Group's banking business involves processing of personal data, protecting such data remains of the utmost importance and a key priority.

Processes and systems

Each Addiko entity appointed a Data Protection Officer (DPO) as a specialized, independent function, who reports directly to the respective local Management Board. The group DPO coordinates data protection tasks across the CSEE subsidiaries and the Holding in Austria. This ensures dedicated direct and indirect reporting lines, as well as a regular exchange on data protection topics and developments.

Addiko established a data protection compliance management framework, inter alia setting forth policies, processes as well as technical and organizational measures. This established group-wide data protection compliance framework also applies to our entities in non-EU countries, who have to comply with GDPR standards unless mandatory local data protection and privacy laws require otherwise.

All Addiko entities run individual data processing inventories and standard processes for the handling of requests enabling the exercising of data subjects' rights (e.g. access, rectification, erasure). In addition, data protection impact assessments are carried out for critical systems.

New products or changes to existing products are subject to a structured product implementation process including the application of an extensive risk assessment as well as data protection and information security risks.

Data protection training & education

The data protection framework is established via an extensive Group Data Protection policy and applies to all employees.

The Data Protection Officers (DPOs) in each subsidiary consequently raise awareness by communicating to employees the importance of the responsible treatment of personal data of both, customers and employees, in line with the applicable data protection laws.

Education and training on data protection requirements are a key factor in ensuring effective data protection in Addiko. Our employees are regularly trained on the application of data protection compliance via an online tool (e-learning program).

Third parties and Binding Corporate Rules

Disclosure of personal data to third parties is subject to the execution of data processing and non-disclosure agreements.

Addiko Group uses multi-party data protection agreements, in line with the requirements set out in Art 28 GDPR, when a service or a third party is providing a service to at least two entities within Addiko Group. Therefore, compliance with data protection requirements is ensured and respective oversight enabled.

Addiko Bank AG has applied for the approval of Binding Corporate Rules (BCRs) to facilitate intra-group transfers from its subsidiaries within the EU to those subsidiaries outside the EU.

Data subjects' rights

Right to access to data

Addiko Group informs all customers and employees about the collection, use, sharing and retention of personal data.

The data subjects (customers, employees) have the right to obtain information whether or not their personal data is processed, which data is processed and certain additional information. Access to data is granted free of charge, unless the request is manifestly unfounded or excessive. Each request is documented in our data management system.

Right to rectification of data

The data subjects have the right to obtain without undue delay the rectification of inaccurate personal data, including the right to complete incomplete data.

Right to restriction and erasure of data

The data subjects have the right to request the restriction of the processing of personal data, e.g. when the accuracy of data is objected, and to request the erasure of their personal data without undue delay if there is an issue with the underlying legality of the data processing. Correspondingly, Addiko Group is committed to comply with all reasonable requests.

Data breaches

Within Addiko we implemented various reporting and escalation processes to ensure that any (potential) data breaches can be assessed and handled in a timely and effective manner.

The Group Data Breach Management policy enables all Addiko entities to comply promptly with legal requirements that apply to them as owner, processor and/or custodian of personal data, and to reduce the risk of a potential data breach that may cause serious financial or reputational damage to Addiko.

Data breaches are reported to the responsible Data Protection Authority and affected data subjects are notified in a timely manner in case of any data breach in accordance with the applicable data protection laws.

Information security

Addiko has established a state-of-the-art information security framework with information security policies, standards and manuals that adequately protects information assets and associated technologies, applications, systems, and processes in our digital ecosystem.

Given that Addiko – as any other institution – relies on its IT systems for a variety of functions it has developed and implemented a comprehensive information security management framework in accordance with international industry standards. Employees are being trained regularly on a mandatory basis. Addiko performs vulnerability scans on a monthly basis and regular penetration tests.