Data protection information for business partners

Updated: 21 November 2024

1. Name and contact details of person responsible and their representatives

Erste Abwicklungsanstalt AöR
Friedrichstr. 84
40217 Düsseldorf
Tel.: +49 (0) 211 91345 780
Fax: +49 (0) 211 91345 789
E-mail: info@aa1.de
Register entry: Commercial register, District Court of Düsseldorf, HRA 20869
Represented by:
Christian Doppstadt
Horst Küpker

2. Contact details of the Data Protection Officer

Oliver Walter
Data Protection Officer
Erste Abwicklungsanstalt AöR
Friedrichstr. 65
40217 Düsseldorf
Telephone: + 49 (0) 211 91345 925
Fax: +49 (0) 211 91345 789
E-mail: eaa_datenschutz@aa1.de

3. Role of Erste Abwicklungsanstalt AöR

The Erste Abwicklungsanstalt AöR ("**EAA**") is a winding-up agency within the meaning of section 8a (1) sentence 1 of the Financial Market Stabilisation Fund Act (Finanzmarktstabilisierungsfondsgesetz – FMStFG) and was established by the Financial Market Stabilisation Authority (Bundesanstalt für Finanzmarktstabilisierung – FMSA) on 11 December 2009. The EAA is a structurally and commercially independent public law entity with partial legal capacity operating under the umbrella of the FMSA. As such, it is not classified as a credit institution for the purposes of section 1 of the German Banking Act (Kreditwesengesetz – KWG), nor does it carry out activities requiring a permit for the purposes of EU Directive 2006/48/EC dated 14 June 2006. The EAA has around 60 employees in Düsseldorf. The EAA operates as an asset manager pursuing a clear public mandate: it is winding up the risk exposures and non-strategic business units (transferred assets) transferred from the former WestLB AG (now Portigon AG) and its domestic and foreign subsidiaries in a value-preserving and risk-minimising manner. This serves to stabilise the financial market. To this end, it may undertake all types of bank and financial service transactions as well as other activities.

4. Purpose of the processing of personal data by the EAA

The personal data of business partners are processed in connection with the initiation, execution and termination of business relationships as well as the settlement of the portfolios transferred, in particular those consisting of loans, bonds, derivatives and shareholdings. The EAA's activities include ongoing credit risk monitoring, maintaining credit records and shareholdings, risk evaluations, the preparation of various kinds of portfolio reports, the sale of assets and shareholdings and the refinancing of the portfolio. In line with its mandate, the EAA has in addition established its own money-market and capital-market programmes with regular contact to investors.[1] In the exercise of its activities the EAA also uses various service providers/contract processors.

Personal data are also processed by the EAA in order to:

- fulfil statutory requirements, e.g. KWG, the Money Laundering Act (Geldwäschegesetz – GwG), the Fiscal Code (Abgabenordnung – AO), the Securities Trading Act (Wertpapierhandelsgesetz – WpHG)
- for business partner management
- for supplier and service provider data management

[1] Can be viewed at https://www.aa1.de//investor-relations/treasury/

5. Groups of persons affected, relevant data or categories of data and legal basis in each case

In order to fulfil the purposes mentioned under 4) above, the personal data or categories of data listed below will essentially be collected, processed and used in full or in part on the legal basis mentioned below for the following groups of persons concerned:

Groups of persons	Data and categories of data	Legal basis
Borrowers and providers of collateral (including the beneficial owners, legal representatives and other contact partners)	• Name details • Address and communication details • Transaction and contract details, billing and performance data, account details • Data relating to creditworthiness • Outstanding loan amount, interest amount • Address and functional data of commercial tenants of real estate that serves as loan collateral • Data in the course of visits from contact partners to the EAA (surname, first name, date of visit, company, contact partner at the EAA) • Data in connection with identification in accordance with the Money Laundering Act	Art. 6 (1) b) GDPR[2]; Art. 6 (1) c) GDPR in conjunction with KWG; Art. 6 (1) f) GDPR [building security]; Art. 6 (1) c) GDPR in conjunction with GwG

[2] Available at http://eur-lex.europa.eu.

Suppliers, service providers, banks, counterparties and investors	• Name details of contact partners • Address and communication details • References, qualification and remuneration of consultants used • Transaction and contract details, billing and performance data, account details • Data to settle and check services, deliveries and procurements together with sales of assets and shareholdings • Recording of traders' telephone calls[3] • Chat recordings on trading platforms[4] • Data in the course of visits from contact partners to the EAA (surname, first name, date of visit, company, contact partner at the EAA)	Art. 6 (1) b) GDPR / Art. 6 (1) f) GDPR; Art. 6 (1) c) GDPR in conjunction with MaRisk BTO 2.2.1 and BaFin Circular 5/2017; Art. 6 (1) f) GDPR (building security); Art. 6 (1) c) GDPR in conjunction with GwG

[3] MaRisk BTO 2.2.1 no. 4 obliges the EAA to record the business conversations of traders on a recording medium and to store these records for three months as a minimum. In the light of this obligation, the EAA operates a telephone system for its traders until 30 September 2019. The records of the telephone calls must be hold for six months (longest until end of March 2020). Since 1 October 2019, the EAA has made use of an exemption due to the reduced trading volume and no longer records (see Hannemann, R.; Steinbrecher I.; Weigl T.: Mindestanforderungen an das Risikomanagement (MaRisk) - Kommentar, Schäffer-Pöschel, Stuttgart, 2019, 5th edition, page 1184).

[4] Under BaFin Circular 5/2017 (GW) – Appropriate business-related security systems within the meaning of section 25h (1) sentence 1 KWG – the EAA is obliged to store correspondence (chats, news etc.) on trading platforms for a ten-year period.

	• Data in connection with identification in accordance with the Money Laundering Act	

As the EAA does not have a banking licence, JP Morgan SE, Frankfurt/Main, will be used to manage the EAA's payment transaction accounts (Lorobank) and for the safekeeping of asset securities (custodian bank), and Deutsche Bank AG, Frankfurt, will be used as the issuing and paying agent for liability securities. In this context, personal data may also be passed on. However, both institutions are to be regarded as separate data controllers under data protection law with their own data protection notices to which we refer.

6. Recipients or categories of recipients to whom data may be transferred

The personal data on the groups of persons affected are essentially passed on to the following recipients in order to fulfil the purposes stated under 4):

Groups of persons	Recipients and categories of recipients
Borrowers and providers of collateral (including the beneficial owners, legal representatives and other contact partners)	• Internal bodies involved in the execution of the relevant business processes (in particular, Asset Management, Bookkeeping, Tax department, Legal department, Accounting and IT) • Public agencies that receive data due to legal provisions (e.g. financial authorities, the Federal Financial Supervisory Authority (Bundesanstalt für Finanzdienstleistungsaufsicht – BaFin), the Deutsche Bundesbank, FMSA) • External bodies, such as affiliates and external contractors, where these are involved in credit processing and contract performance (e.g. IT or service providers) or due to fulfilment of legal obligations (e.g. auditors)
Suppliers, service providers, banks, counterparties and investors	• Internal bodies involved in the execution of the relevant business processes (e.g. Bookkeeping, Accounting and IT)

	• Public agencies that receive data due to legal provisions (e.g. financial authorities, the Federal/State Audit Office, FMSA, BaFin, the Deutsche Bundesbank, FMSA) • External bodies such as affiliates and external contractors (e.g. logistics partners or computer centre, auditors)

7. Standard periods for the erasure of data

The legislator has enacted a variety of storage obligations and periods. Once these periods have expired, the corresponding data are routinely erased if they are no longer necessary for the fulfilment of the contract. Thus, the commercial law data or financial data of a completed fiscal year are erased after a further ten years as a matter of principle in accordance with legal provisions, unless longer retention periods are prescribed or necessary for legitimate reasons. If data are not affected by this, they will be erased when the purposes mentioned under 3) no longer apply.

8. Planned data transmissions to third countries

Data transmissions to third countries are only made in the context of fulfilling a contract, of necessary communication and other exceptions explicitly stated in the GDPR. In all other respects, there is generally no transfer to third countries. Where the EAA or its contract processors use service providers in third countries (like USA or India) to fulfil their tasks, corresponding standard EU contracts are signed to ensure adherence to the European data protection level. In the direction of the USA, certifications under the US/EU Data Privacy Framework can also be considered. Any further requirements arising from the ECJ ruling on Privacy Shield dated July 16, 2020 will be coordinated with the service providers.

9. Rights of data subjects

Every data subject has a right of access pursuant to Art. 15 GDPR, the right to rectification pursuant to Art. 16 GDPR, the right to erasure pursuant to Art. 17 GDPR, the right to restriction of processing pursuant to Art. 18 GDPR, the right to object pursuant to Art. 21 GDPR and the right to data portability pursuant to Art. 20 GDPR. With regard to the right of access and the

right to erasure, the restrictions pursuant to section 34 and section 35 of the Federal Data Protection Act (Bundesdatenschutzgesetz – BDSG) apply.[5]

Where the processing of data is based on consent, the data subject has the right to withdraw their consent at any time, the withdrawal of consent not affecting the lawfulness of the processing carried out on the basis of consent until revocation.

10. Right to lodge a complaint with a supervisory authority

Each data subject has the right to lodge a complaint with the competent supervisory authority for data protection (Art. 77 GDPR in conjunction with section 19 BDSG new), i.e. in particular to the supervisory authority in the member state of the data subject's place of residence or to the supervisory authority responsible for the EAA:

The Federal Commissioner for Data Protection and Freedom of Information
Graurheindorfer Str. 153
53117 Bonn
Telephone: +49 (0)228 997799-0
Fax: +49 (0)228 997799-5550
E-Mail: poststelle@bfdi.bund.de

11. Background to the provision of personal data

The provision of personal data may be required by law or contract or may be necessary to enter into a contract. There may also be an obligation to provide personal data. In individual cases, the Data Protection Officer under 2) is available to provide clarification.

12. Automated decision-making including profiling

No automated decision-making including profiling takes place.

13. Further processing of personal data

The EAA does not intend to use the personal data it has collected for any other purpose than that for which they were collected. In the context of migrations to new service providers and systems or their further development, it may well be that personal data is processed for test purposes in individual cases. However, this is done very restrictively, in particular by applying

[5] Available at https://www.bgbl.de

the requirements of necessity and data minimisation and within the framework of a balancing of interests according to Art. 6 (1) f) GDPR. The same protective measures are used in the test environment as in the production environment. Among other things, measures for access protection and deletion requirements after testing are observed.