Privacy policy

Data Processing by the Association of German Banks

1. Introduction

1.1 Definitions and legal bases

1.2 Data processing within the Association of German Banks

1.3. Aim of our privacy policy

1.4. Who is responsible and whom can I apply to?

2. Publicly accessible web offerings

2.1. Provision of websites and creation of log files

2.2. Use of external services

2.2.1. Cookies

2.2.2. Google Analytics

2.2.3. Shariff/use of social media plugins

2.2.4. Facebook Custom Audience

2.2.5. LinkedIn Conversion-Tracking

2.2.6. Embedding of third-party services

2.2.6.1. SlideShare

2.2.6.2. Twitter

2.2.6.3. YouTube

2.2.6.4. Flickr

2.2.6.5. Yumpu

2.2.6.6. SoundCloud

2.3. Finanzchat

2.4. Email contact, including contact forms on the websites

2.5. Enquiries about protection ceiling

2.6. Orders

2.7. Student competitions

2.8. Mailjet delivery service

3. Contact databases of the Association of German Banks

3.1. What sources and data do we use?

3.2. Why do we process your data and on what legal basis?

3.3. Who will obtain my data?

3.4. Will data be transferred to a third country?

3.5. How long will my data be stored?

3.6. Automated individual decision-making? Will profiling take place?

4. Ombudsman Scheme of the German private banks

4.1. What sources and data do we use?

4.2. Why do we process your data and on what legal basis?

4.3. Who will obtain my data?

4.4. Will data be transferred to a third country?

4.5. How long will my data be stored?

4.6. Do you have an obligation to make your data available?

4.7. Automated individual decision-making? Will profiling take place?

5. What rights to data protection do I have?

6. Changes to privacy policy

1. Introduction

1.1 Definitions and legal bases

The present privacy policy is based on the definitions used by European lawmakers when issuing the General Data Protection Regulation (GDPR). Our privacy policy is intended to be easy to read and understand. To ensure this, we should like to briefly explain the definitions and legal bases used (Article 4 of the GDPR).

'data subject' means any identified or identifiable natural person whose personal data are processed by the controller (i.e. the party responsible for processing – in this case, the Association of German Banks).

'personal data' means any information relating to a data subject; an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

'processing' means any operation or set of operations which is performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration,

retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The processing of personal data is lawful only if and to the extent that at least one of the following applies:

- Article 6(1)(a) of the GDPR serves as the legal basis for processing operations where we obtain consent for a specific purpose of processing.
- If the processing of personal data is necessary for the performance of a contract to which the data subject is party – as is, for example, the case with processing operations that are necessary for the delivery of goods or the provision of any other service or consideration – processing is based on Article 6(1)(b) of the GDPR. The same goes for processing operations that are necessary to take steps prior to entering into a contract, e.g. in the case of enquiries about our products or services.
- Where our association is subject to a legal obligation requiring the processing of personal data, e.g. to comply with tax provisions, processing is based on Article 6(1)(c) of the GDPR.
- In rare cases, the processing of personal data may be necessary to protect vital interests of the data subject or another natural person. This would, for example, be the case if a visitor to our association were injured and their name, age or other vital data had to be subsequently passed on to a doctor, hospital or other third parties. Processing would then be based on Article 6(1)(d) of the GDPR.
- Finally, processing operations may be based on Article 6(1)(f) of the GDPR. This is the legal basis for processing operations that are not covered by any of the aforementioned legal bases if processing is necessary to pursue a legitimate interest of our association or a third party, except where such interest is overridden by the interests or fundamental rights and freedoms of the data subject.

If the legal basis ceases to exist over the course of time, e.g. where consent is withdrawn or a legitimate interest no longer applies, the personal data must be erased or excluded from processing, taking due account of statutory storage periods.

1.2 Data processing within the Association of German Banks

As a leading trade association, we represent the interests of our member banks. To perform the tasks set out in our articles, we also process information about natural persons. We process personal data solely within the limits of the statutory provisions

of the German Federal Data Protection Act (BDSG), the European General Data Protection Regulation and the country-specific data protection provisions applying to our association and, in particular, **solely for our own purposes**.

We generally don't store data relating to customers of our member banks centrally or share such data with member banks in an intermediary capacity. We only process and pass on your data if, as a bank customer, you make use of either of the following services:

- Our Ombudsman Scheme for the resolution of disputes: data relating to customers (applicants) that these have made available to us in compliance with the rules of procedure for out-of-court dispute resolution are transferred to member banks (respondents).
- Our Account Search Scheme: enquiries from heirs and other authorised persons which are addressed to us direct or have been received by our member associations and sent on to us are forwarded to our member banks.

We **don't** operate as a **data processing service provider** (processor) within the meaning of Article 28 of the GDPR **for our member banks**.

When we transfer **personal data to third parties** (usually service providers handling orders) in cases other than those mentioned above, we do so in accordance with the provisions of the German Federal Data Protection Act and the European General Data Protection Regulation. When we do so, we limit the amount of data we transfer to a strict minimum.

We generally erase personal data or exclude it from processing as soon as the purpose of processing no longer applies. We only continue to store such data where this is stipulated by national or European lawmakers in Union regulations, laws or other provisions to which the controller is subject. The individual time limits for erasure of data are set out in our erasure guidelines, compliance with which is mandatory, taking due account of the respective storage periods. On expiry of the periods, the relevant data are routinely erased.

We have implemented numerous technical and organisational measures in all processing operations to ensure that the personal data we process are protected as fully as possible. Nevertheless, web-based transfers of data in particular may display security gaps, so that absolute protection cannot be guaranteed.

1.3 Aim of our privacy policy

This privacy policy is designed to inform the **general public** about the type, amount and purpose of personal data we process in connection with use of our **web offerings** (**section 2**). **Special processing operations accessible to the general public,** such as those concerning contact forms, newsletter subscriptions or enquiries about deposit protection ceilings, are also addressed.

Besides informing the general public, this privacy policy serves to inform our

- **contacts** in the political, administrative, business, etc., sectors,
- **service providers** and
- **committee and other working body members**

whose personal data are processed in our contact databases (**section 3**).

Since we process and transfer bank customer data in the course of our **dispute resolution proceedings**, this privacy policy (**section 4**) informs the data subjects (usually applicants in the proceedings) separately about the processing of their personal data.

In addition, this privacy policy **(section 5)** informs all data subjects about their **rights**.

This privacy policy is thus a tool we use to perform our obligations resulting from Articles 13, 14 and 21 of the GDPR.

1.4 Who is responsible and whom can I apply to?

The party responsible for the purposes of the GDPR, other data protection legislation in force in the member states of the European Union and other provisions of a data protection nature is:

Bundesverband deutscher Banken e. V. (Association of German Banks)
Burgstraße 28
10178 Berlin
Germany
Tel.: +49 30 1663-0
bankenverband@bdb.de

Vereinsregister (Register of Associations) Amtsgericht Charlottenburg (Charlottenburg District Court) Registernummer (Register No.) 19142Nz

Our Data Protection Officer can be contacted by email at **datenschutzbeauftragter@bdb.de** or by post at the above address. Any data subject can address enquiries and concerns relating to data protection directly to our Data Protection Officer at any time.

Those responsible for our regional associations' websites and for the Entschädigungseinrichtung deutscher Banken (Compensation Scheme of German Private Banks) are indicated in the respective site notice:

Baden-Württemberg: **https://bw.bankenverband.de/impressum/**
Bayern: **https://by.bankenverband.de/impressum/**
Bremen: **https://hb.bankenverband.de/impressum/**
Hamburg: **https://hh.bankenverband.de/impressum/**
Hessen: **https://he.bankenverband.de/impressum/**
Niedersachsen: **https://ni.bankenverband.de/impressum/**
Nordrhein-Westfalen: **https://nw.bankenverband.de/impressum/**
Rheinland-Pfalz: **https://rp.bankenverband.de/impressum/**
Saarland: **https://sl.bankenverband.de/impressum/**
Schleswig-Holstein: **https://sl.bankenverband.de/impressum/**
Entschädigungseinrichtung deutscher Banken: **https://www.edb-banken.de/impressum/**

2. Publicly accessible web offerings

We generally process personal data of persons making use of our web offerings only if and to the extent that this is necessary to make available a functioning website as well as our web content and services. Where a data subject wishes to make use of special services via one of our websites, processing of personal data may thus be necessary.

If processing of personal data is necessary in our view and there is no legal basis for such processing other than consent, we generally obtain such consent from the data subject, except in cases where consent cannot be obtained beforehand for practical reasons and processing of data is permitted by law.

This policy applies to the following websites and associated subdomains: **https://bankenverband.de/**, **https://bankenombudsmann.de/**, https://www.edb-

banken.de/, **http://einlagensicherung.de/**, **https://einlagensicherungs-fonds.de/**, **http://schulbanker.de/**, **https://bw.bankenverband.de/,** **https://by.bankenverband.de/,** **https://hb.bankenverband.de/,** **https://hh.bankenverband.de/,** **https://he.bankenverband.de/,** **https://ni.bankenverband.de/,** **https://nw.bankenverband.de/,** **https://rp.bankenverband.de/,** **https://sl.bankenverband.de/,** **http://www.jugendundwirtschaft.de/** and **https://sh.bankenverband.de/.**

This privacy policy thus covers the Finanzchat (finance chat) service offered on our website, newsletter subscriptions, etc. and processing operations following contact made with us via our online contact forms or through email enquiries, such as those concerning deposit protection ceilings or applications for the SchulBank project.

2.1 Provision of websites and creation of log files

You may use our websites for information purposes only, i.e. if you don't register or otherwise send us information, without disclosing any personal data. Nevertheless, whenever you view our web pages, our system automatically records data on every server access concerning our offerings (so-called 'server log files'). The access data include the name of the web page you requested, file, request date/time, volume of data transferred, 'successful request' report, type of browser plus version, your operating system, referrer URL (the page previously visited), IP address and the requesting provider. We use the log file data, without matching it to your person or any other profile, solely for statistical analysis for the purpose of operating, securing and optimising our websites. At the same time, we reserve the right to subsequently check the log file data if we have legitimate grounds for suspecting unlawful use.

Temporary system storage of your IP address is necessary to enable delivery of the website to your computer. For this purpose, your IP address has to remain stored for the duration of the session. The legal basis for temporary storage of data and log files is Article 6(1)(f) of the GDPR.

The data are erased as soon as they are no longer necessary for achieving the purpose of their collection. Where the data are recorded for the purpose of making available our web offerings, this is the case when the respective session ends. Where the data are stored in log files, this is the case after 14 days at the latest. The data may also be stored for longer. In this case, your IP address will be erased or scrambled so that it can no longer be attributed to you.

Recording data for the purpose of making available our web offerings and storing data in log files are essential for operating our websites. You consequently have no right of objection thereto.

2.2 Use of external services

2.2.1 Cookies

We use cookies on our websites. Cookies are small text files that are stored on your computer via your browser. A cookie contains a unique sequence of characters that identify your browser when you visit a website again. The use of cookies improves the user-friendliness and security of our websites.

We also use cookies on our websites that allow us to analyse your surfing behaviour. The data we collect from you in this way are pseudonymised through appropriate technical arrangements. They can therefore no longer be attributed to you. The data are not stored together with other personal data. When you view our web pages, a banner informs you that we use cookies for analysis purposes and refers you to this privacy policy. At the same time, it informs you how you can block storage of cookies in your browser settings.

Cookies are stored on your computer and transmitted to us from there. This means that you, as a user, have full control over the use of cookies. You can deactivate cookies in your browser settings. You can also view our web pages without any cookies. You can delete cookies that have already been stored in your browser settings. However, blocking cookies may result in reduced website functionality. Please note that when you delete all browser cookies you also delete previously set opt-out cookies and need to reset these.

The purpose of using technically necessary cookies is to make using our websites easier for you. We cannot provide some of our website functions without using cookies. These functions need to be able to recognise your browser after you move from one web page to another. We don't use the data we collect from users via technically necessary cookies to create user profiles. We use analysis cookies to enhance the quality of our websites and their content. Through analysis cookies, we learn how our websites are used and can thus continuously optimise our offerings.

The legal basis for processing personal data using cookies is Article 6(1)(f) of the GDPR. The legal basis for processing personal data using cookies for analytical purposes is your consent to this in accordance with Article 6(1)(a) of the GDPR. Please note: many online company ad cookies can be managed via the US website **http://www.aboutads.info/choices**/ or the EU website **http://www.youronlinechoices.com/uk/your-ad-choices**.

2.2.2 Google Analytics

Our websites use Google Analytics, a web analytics service provided by Google Inc. (1600 Amphitheatre Parkway Mountain View, CA 94043, USA) ('Google'). Google Analytics uses cookies, text files that are stored on your computer and allow us to analyse how you use our websites. The information generated by cookies – socio-demographic data, if any, and data on your use of a website (including your IP address, though this is abbreviated, i.e. anonymised, by using the 'anonymizeIp' function so that it can no longer be matched to a particular connection) – is transferred to a Google server in the US and stored there. Where IP anonymisation is activated on our websites, however, Google abbreviates your IP address beforehand in European Union member states or in other countries signatory to the Agreement on the European Economic Area. Only in exceptional cases is the full IP address transferred to a Google server in the US and abbreviated there. Google uses this information to analyse your website usage and compile reports on website activities for website operators and to provide further services associated with web and website usage to website operators. Google may also transfer such data to third parties provided this is stipulated by law or provided third parties process such data on Google's behalf. Google will never combine your IP address with other Google data. You can block installation of cookies in your browser settings.

You may object to collection of your data by Google Analytics and processing of these data by Google in the future by installing a deactivation add-on for your browser (**http://tools.google.com/dlpage/gaoptout?hl=en-GB**).

We use Google Analytics to analyse and continuously improve our websites. The statistics we obtain enable us to improve our web offerings and make them more attractive for you. In the exceptional cases in which personal data are transferred to the US, Google recognises the EU-US Privacy Shield: https://www.privacyshield.gov/EU-US-Framework. The legal basis for using Google Analytics is Article 6(1)(f) of the GDPR.

The data we transmit are automatically erased after 14 months. Data whose storage period has expired are automatically erased once a month.

Third-party provider information: Google Dublin, Google Ireland Ltd., Gordon House, Barrow Street, Dublin 4, Ireland, fax: +353 (1) 436 1001. User terms and conditions: http://www.google.com/analytics/terms/de.html, privacy overview: **http://www.google.com/intl/de/analytics/learn/privacy.html** and privacy policy: **http://www.google.de/intl/de/policies/privacy**.

2.2.3 Shariff/use of social media plugins

We are pleased whenever our readers recommend and discuss content of our websites on Twitter, Facebook and LinkedIn. For this purpose, we use social media buttons (also social media plugins), namely the buttons developed by the c't 'Shariff' project.

Shariff ensures that social networks can only request data from users once these click on the appropriate button. Shariff replaces social networks' customary 'Share' buttons and protects your surfing behaviour from prying eyes. A single click on the button is enough to share information with others. You don't have to do anything else – the webmaster has already taken care of everything. Customary social media buttons transfer your data every time you visit a web page and give the social networks full details of your surfing behaviour (user tracking). For this, you don't have be logged in or a network member. A Shariff button, on the other hand, only establishes direct contact between a social network and a visitor when the latter actively clicks on the share button.

Only when you click on the button is the respective social network provider informed that you have visited one of our websites. In addition, data such as IP address, request date/time and request content are transferred. Where Facebook is involved, the provider says that in Germany the IP address is anonymised immediately after being collected. Activating the plugin therefore means that your personal data are transferred to the provider and stored there (where US providers are involved, in the US). As the provider collects data via cookies in particular, we recommend that before clicking on the button you delete all cookies via your browser's security settings.

We have no influence on the data collected or data processing operations nor do we know the full extent of data collection, the purposes of processing or the storage

periods. Likewise, we have no information on erasure of the data collected by the respective social network provider.

The provider stores the data about you in the form of a user profile and uses it for advertising, market research and/or customised website design purposes. It does so in particular (also for non-logged-in users) to deliver personalised ads and to inform other social network users about your activity on our websites. You have the right to object to the creation of such a user profile; to exercise this right, you must contact the respective provider. Through plugins, we give you the opportunity to interact with social networks and other users so that we can improve our web services and make them more attractive for you. The legal basis for using plugins is Article 6(1)(f) of the GDPR.

Data are transferred irrespective of whether you have an account with the provider and are logged in there. If you are logged in with the plugin provider, the data that we collect from you are matched directly to your account with the provider. If you use the activated button and, for example, link a web page, the provider stores this information as well in your user account and publicly discloses it to your contacts. We recommend that after using a social network you always log out, particularly before activating the button, as you can in this way avoid data being matched to your profile with the plugin provider.

For further information on the purpose and scope of data collection and processing of data by the plugin provider, please see the privacy policies of the providers listed below. These also contain further details of your rights and settings to protect your privacy.

Addresses and URLs of social network providers together with privacy policies:

Facebook Inc., 1601 S California Ave, Palo Alto, California 94304, USA; http://www.facebook.com/policy.php; further information on data collection: **http://www.facebook.com/help/186325668085084** and https://facebook.com/about/privacy/. Facebook recognises the EU-US Privacy-Shield: https://www.privacyshield.gov/EU-US-Framework.

Twitter, Inc., 1355 Market St, Suite 900, San Francisco, California 94103, USA; https://twitter.com/privacy. Twitter recognises the EU-US Privacy Shield: https://www.privacyshield.gov/EU-US-Framework.

LinkedIn Corporation, 2029 Stierlin Court, Mountain View, California 94043, USA; http://www.linkedin.com/legal/privacy-policy. LinkedIn recognises the EU-US Privacy Shield: https://www.privacyshield.gov/EU-US-Framework.

For further information on Shariff, please go to **heise.de**.

2.2.4 Facebook Custom Audiences

Our websites contain remarketing tags provided by Facebook (1601 South California Avenue, Palo Alto, CA 94304, USA). When visiting Facebook or other websites also using such tags, website users can in this way enjoy personalised ads (Facebook ads). Our aim is to show you ads that are of interest to you so as to make our websites more attractive for you. The legal basis for processing your data is Article 6(1)(f) of the GDPR.

When you visit our websites, your browser and the Facebook server are automatically directly connected via the remarketing tags. Please note that, as the website provider, we have no influence on the amount of data collected by Facebook through the use of such tags or on how Facebook uses such data and can only inform you to the best of our knowledge as follows: through Custom Audiences integration, Facebook is informed that you have visited one of our web pages or clicked on one of our ads. If you are registered with a Facebook service, Facebook can match this visit to your account. Even if you are not registered with or logged in to Facebook, the provider may obtain and store your IP address and other identifiers. For more information, please see Facebook's privacy policy (**www.facebook.com/about/privacy**). If you don't want your data to be collected via a Custom Audience, you can get more Information about Custom Audiences here: **https://www.facebook.com/legal/terms/customaudience?ref=fbb-blog_new-requirements-for-custom-audiences.**

According to Facebook, the data we transmit fall into five categories: so-called Http headers, pixel-specific data, button click data, form field names and optional data.

These are explained at **https://www.facebook.com/business/gdpr**. According to Facebook, the data are automatically erased or anonymised after 90 days. Please see **https://www.facebook.com/help/206635839404055?ref=dp**.

Data whose storage period has expired are automatically erased once a month.

For further information on data processing by Facebook, please go to **http://www.facebook.com/about/privacy**.

2.2.5 LinkedIn conversion tracking

We use the LinkedIn conversion tracking retargeting tool provided by LinkedIn Ireland (Wilton Plaza, Wilton Place, Dublin 2, Ireland) (»LinkedIn«). For this purpose, we have integrated the LinkedIn insight tag that allows LinkedIn to gather statistical, pseudonymised data on your visits to and use of our websites and to provide us with aggregated statistics based on these. In addition, such data enable us to make you interesting personalised offers and recommendations. The legal basis for processing data is Article 6(1)(f) of the GDPR.

The relevant data are stored in a cookie. You can block storage of cookies via a browser setting. Alternatively, you can object to this type of data processing by using the following link (**https://www.linkedin.com/help/linkedin/answer/62931?lang=en#user-profile**) to install an opt-out cookie that remains on your device until you delete the cookies. This option is open to both LinkedIn members and non-members.

The data we transmit comprise the IP address, time stamp, so-called 'page events' (according to LinkedIn, these include, for example, page views) and – if you are a LinkedIn member – other personal data. According to LinkedIn, the aforementioned personal data are automatically erased after 90 days, unless they have been edited or are used in LinkedIn campaigns. For further details, please go to **https://www.linkedin.com/help/linkedin/answer/87150/linkedin-marketinglosungen-und-die-datenschutz-grundverordnung-dsgvo-?lang=en**.

Data whose storage period has expired are automatically erased once a month.

For more information on LinkedIn conversion tracking, please see LinkedIn's privacy policy.

2.2.6 Embedding of third-party services

Our online content includes services of third parties – YouTube, Vimeo, Twitter, SlideShare, Yumpu, Flickr and Soundcloud. This content can be viewed directly on our website. When you visit the website, these providers will be informed that you have viewed the corresponding sub-page of our website. Further data will also be transmitted irrespective of whether you have a user account which you are logged into or whether you have no user account. If you don't want data to be matched to your profile, you need to log out before activating the relevant button. You have the right to object to the creation of these user profiles, but to exercise this right, you need to contact the relevant provider. We embed these services to show you content which

will be of interest to you in order to make our website more attractive for you. The legal basis for processing your data is Article 6(1)(f) of the GDPR.

2.2.6.1. SlideShare

The SlideShare platform of SlideShare Inc. (1 Montgomery St., Suite 1300, San Francisco, CA 94104, USA) is used on the websites operated by the Association of German Banks to publish our own presentations, among other things. For more information, see the privacy policy of SlideShare at **https://www.linkedin.com/legal/privacy-policy**. We don't use SlideShare plugins on our websites.

2.2.6.2. Twitter

Our websites use content produced on Twitter. This service is offered by Twitter Inc. (795 Folsom St., Suite 600, San Francisco, CA 94107, USA). The content is made visible by embedding it on our website. For further information, see Twitter's privacy policy at **http://twitter.com/privacy**.

2.2.6.3. YouTube

We have included YouTube videos in our online content. These are stored on **http://www.YouTube.com** and can be played directly on our website. They are all embedded using the 'privacy-enhanced mode', meaning that no data about you will be transmitted to YouTube if you don't play the videos. Only if you play the videos will data be transmitted. We have no influence over this transmission of data. Further information on the purpose and extent of the collection and processing of data by YouTube is available in its privacy policy at https://www.google.com/intl/en/policies/privacy. Google will also process your personal data in the US and recognises the EU-US Privacy Shield: **https://www.privacyshield.gov/EU-US-Framework**.

2.2.6.4. Flickr

We use the platform Flickr (Oath (EMEA) Limited, 5-7 Point Square, North Wall Quay, Dublin 1) to publish photographs, among other things. For further information, see Flickr's privacy policy at **https://policies.oath.com/ie/en/oath/privacy/index.html**. We don't use Flickr plugins on our websites.

2.2.6.5. Yumpu

Yumpu is a service of i-Magazine AG (Gewerbestrasse 3, 9444 Diepoldsau, Switzerland), which makes a digital platform available for the publication of magazines, brochures and catalogues. Our websites use Yumpu embeds to display publications. Further information about the tool can be found in the Terms of Service and privacy policy of Yumpu and i-Magazine AG.

2.2.6.6. SoundCloud

Plugins of the social network SoundCloud (SoundCloud Limited, 33 St James Square, London SW1Y 4JS, UK) may be embedded in our web pages. Further information can be found in the privacy policy of SoundCloud at **https://soundcloud.com/pages/privacy/05-2018**.

2.3 Finanzchat

You can use our Finanzchat (finance chat) service to ask a question. For technical reasons, you need to enter a name to do so. The Association of German Banks doesn't require you to provide your real name or your email address. If you don't want information to be matched to your identity, select a user name which will make this impossible, e.g. by entering a pseudonym. The user data entered in the input mask are transmitted to us and stored (time stamp and pseudonym). No data are forwarded to third parties. The data are used only to conduct the chat.

We only process the personal data entered into the input mask for the purpose of replying to the question.

The data are erased as soon as they are no longer needed to achieve the purpose for which they were collected. For personal data entered into the input mask, this is the case when the conversation with the user has ended, i.e. when it can be inferred that the matter in question has been clarified.

2.4 Email contact, including contact forms on the websites

You can contact us at the email addresses made available on our websites. Emails to us are also generated by the contact forms provided. The personal data of users transmitted with these emails are stored in our email archive. No data are passed on to third parties. The data are used only for the purpose of conducting our conversation.

The legal basis for processing data transmitted in an email is Article 6(1)(f) of the GDPR. When we are contacted by email, we have a legitimate interest in processing the personal data therein in order to deal with the reason for the contact. Article 6(1)(b) of the GDPR provides a further basis for processing the data. Processing is necessary for the purpose of handling an enquiry which constitutes a quasi-contractual relationship. The consent criterion in accordance with Article 6(1)(a) of the GDPR also provides justification for storing these data while the task is being handled.

The Association of German Banks generally treats emails as business correspondence and has determined that they will be retained in its email archive for a period of eleven years. At the end of this period, they are automatically deleted. This does not apply to emails sent to our mailbox for job applications, bewerbungen@bdb.de. In this case, applicants' data are erased six months after the purpose of processing the data no longer applies – or, in other words, after a decision on the application has been made. The common mailboxes for the Ombudsman dispute resolution scheme (e.g. **Ombudsmann@bdb.de**) are also excluded from the general rules governing emails (for further information, see section 4).

2.5 Enquiries about protection ceiling

Bank customers can contact the Association of German Banks over the internet to enquire about the protection ceiling of a member bank affiliated to the Deposit Protection Fund (cf. no. 20 (1), sentence 5 of the General Business Conditions of the private banks). Enquirers use the input mask on the web page https://einlagensicherungsfonds.de/abfrage-der-sicherungsgrenze/ for this purpose. The enquiry is sent to the association in the form of an email and stored there until a response is sent. The association replies by email, with the personal data of the enquirer automatically included in the reply. For the purpose of preserving evidence, the reply email from the association with the personal data of the enquirer is stored for a long period of time.

This is because, if a compensation event occurs, the enquirer could claim that the association had provided inaccurate information about the member bank's protection ceiling at the time of the enquiry. By storing the reply email, the association will be able to demonstrate the content of the information actually supplied to the enquirer. The storage of email enquiries sent to the Deposit Protection Fund therefore serves the purpose of preserving evidence and thus of protecting the legitimate interests of the Association of German Banks (Article 6(1)(f) of the GDPR). The data are not used for any other purpose; in particular, the information is not released to member banks or third parties. The emails are stored on a separate server at the association's data centre for 30 years and are not available for processing other than for the above purpose of preserving evidence. Interests of the data subjects which would override the association's legitimate interests are not discernible. Data subjects are explicitly informed about the storage of their email enquiries and about the purpose of this storage.

2.6 Orders

Brochures and other publications can be ordered on our websites and electronic newsletters, etc. can be subscribed to. A newsletter is subscribed to by means of a declaration of consent (double opt-in method) and by providing an email address (optional: name, first name and company). To receive brochures and other publications by post, orderers are asked to provide their name, first name, address and email (optional: company and telephone details).

The legal basis for processing the data is Article 6(1)(b) of the GDPR. Processing serves the purpose of performing a task in a quasi-contractual relationship. With respect to the newsletter, in particular, processing during the period of dealing with the task is also legitimised by the existence of consent in accordance with Article 6(1)(a) of the GDPR.

The personal data are only processed during the period in which the task is dealt with and are subsequently erased without delay. The only exception to this standard procedure is if an order is placed by email. In this case, the email is automatically

deleted from the email archive of the Association of German Banks after eleven years.

2.7. Student competitions

On the websites **http://schulbanker.de**, **http://www.jugendundwirtschaft.de** and **http://europeanmoneyquiz.de**, interested users can find information about the student competitions we organise and email us questions. They can also register or apply to take part in the competitions. For the European Money Quiz, the procedure described in section 2.4 applies except that the names and contact details of the winners in Germany are forwarded to the European Banking Federation (EBF), which organises the European final in Brussels. The contact details contained in any registrations and applications for the other two competitions are forwarded direct to the service providers we commission to conduct them. For the Schul|banker bank management game, this is ILTIS GmbH (**http://www.iltis.de**). On the Jugend und Wirtschaft (Youth and the Economy) project, our association works together with the IZOP Institute **(http://www.izop.de).**

The legal basis for processing the data is Article 6(1)(b) of the GDPR. The data are processed for the purpose of performing a task in a quasi-contractual relationship. In the course of the competition, there may be further processing of personal data. In this case, separate declarations of consent will – if necessary – be obtained from data subjects (consent criterion in accordance with Article 6(1)(a) of the GDPR). This applies, for example, if images or film of those taking part are going to be published. The personal data of those taking part in a competition will be stored for six years after the competition has ended and will then be erased. The data of persons who do not take part will be erased immediately by the service providers. This general rule does not apply if the Association of German Banks is contacted direct by email. These emails will be automatically deleted from our email archive after eleven years.

2.8. Mailjet delivery service

On our website we offer users the opportunity to receive news by email (newsletters/ alerts). Anyone wishing to make use of this service must provide a valid email address and confirm that the owner of the email address provided agrees to receive the newsletter. No further data are collected. This information is only used to send the newsletter.
Newsletters are sent by Mailjet (SAS Mailjet, 13-13bis, rue de l'Aubrac – 75012 Paris, FRANCE). Mailjet's privacy policy can be found at **https://www.mailjet.com/privacy-policy/**.

The email addresses and other above data of the recipients of our newsletters are stored on Mailjet's servers. Mailjet uses this information to send and evaluate newsletters on our behalf. Mailjet will not use the data of our newsletter recipients to write to them itself and will not pass on data to third parties.

3. Contact databases of the Association of German Banks

Data subjects in this category are representatives of member banks, member associations and other member organisations of the Association of German Banks who work on our committees and other working bodies. Also affected are contacts in the political, administrative, business, press, broadcasting, religious, academic and cultural communities who simply make use of the broad range of information services and events we offer. In addition, we process personal data of service providers in the context of an agreed exchange of services and the maintenance of contacts.

Users of our restricted-access portals (committee members, etc.) will be informed separately about the processing of their data in addition to this general privacy policy.

3.1 What sources and data do we use?

We process personal data which we receive from you in the course of performing the tasks set out in our Articles of Association or which we obtain from publicly accessible sources.

We process the following data of our members and other persons attending our committee and working group meetings: name, title, position/function, membership of committees or working groups, business address and telecommunications details, and – if provided by the person in question or publicly available – private address and telecommunications details and date of birth.

With respect to our contacts in the political and administrative communities, etc. we only process data which are publicly accessible (e.g. in public registers, in publicly accessible sources of organisations in which the contacts work) and/or which our contacts have made available to us for contact maintenance purposes (e.g. in the form of a business card, by letter or email or when registering for an event). Only the contact details of these persons are stored, i.e. name, title, position/function and possibly date of birth and address and telecommunications details.

With respect to service providers, we process the name, title, position/function, address and telecommunications details.

3.2. Why do we process your data and on what legal basis?

a. To fulfil contractual/quasi-contractual obligations (Article 6(1)(b) of the GDPR)

We process personal data of committee members and other persons active in working bodies of the Association of German Banks in order to fulfil the objectives of our association as set out in our articles (available at **www.bankenverband.de**). The internal opinion-forming process of the association takes place in the association's official committees, which are made up of staff of member banks and/or regional associations. These committees may set up other working bodies, made up of staff or other representatives appointed by member banks. To carry out the association's committee work, it is necessary to process personal data of the persons appointed by member banks. Owing to the legal framework governing the association, there is at least a quasi-contractual arrangement in place. Specifically, the purpose of processing the data is

- to maintain lists of the representatives appointed by member banks to the committees and other bodies of the association,
- to organise association events (e.g. conferences, committee meetings),
- to operate a web-based membership portal permitting users to manage access to information electronically disseminated on web applications such as committee documents, other information, working papers, and invitations to committee and working group meetings, and also to event organisation managed with the help of a web application,
- to contact persons by telephone and
- correspond with them by post and email.

The processing of personal data of service providers is also covered by Article 6(1)(b) of the GDPR.

b. After weighing legitimate interests (Article 6(1)(f) and Article 9(2)(e) of the GDPR)

Personal data may also be processed after weighing the legitimate interests of those involved if the processing serves the purpose of fulfilling the objectives of the

association and interests of the data subjects which would override the association's legitimate interests are not discernible.

- The data for the above access management of web applications for committee and other working body members also serve the legitimate interests of the Association of German Banks in being able to manage and control access to information. A further legal basis in addition to the quasi-contractual arrangement is therefore the legitimate interests of the Association of German Banks.
- Processing the personal data of contacts in political and administrative communities, etc. can also be justified after weighing the interests of those involved. The only data to be processed come from public sources or have been actively made available by the data subjects. Should any information about a contact fall within the scope of the 'special categories of personal data' under Article 9(1) of the GDPR (e.g. information about membership of a political party, a trade union or a religion), we will only process this information if it has been manifestly made public by the data subject (cf. Article 9(2)(e) of the GDPR) or if we can infer the consent of the contact because the information was actively made available to us (see also under point c. below).
- Processing the personal data of service providers can also be justified on the basis of Article 6(1)(f) of the GDPR. This is because the Association of German Banks has a legitimate interest in maintaining its list of contacts and in laying the groundwork for future contractual relationships.

c. On the basis of your consent (Article 6(1)(a) of the GDPR)

If you have given us your consent for the processing of personal data for certain purposes (e.g. the publication of photos taken at one of our events, distribution of a newsletter), this processing is then legitimate on the basis of your consent.

If you provide the association or its staff with your contact details in the form of a business card, a letter or an email, we regard this as consent permitting us to store this information with a view to contacting you again in the course of our association's work. This consent will only cover the processing of 'special categories of personal data' under Article 9(1) of the GDPR (e.g. information about membership of a political party, a trade union or a religion) if you actively make the information available to the association in your specific role as a representative of a political party, a trade union or a religion.

3.3. Who will obtain my data?

At the Association of German Banks, the only people who will have access to your personal data are those who need the data to fulfil our association's objectives. The data will be processed by staff of the association who have been specifically assigned this task and who are committed to treating your data in the strictest confidence. Your interests will therefore be adequately protected. Processors appointed by us (Article 28 of the GDPR) may also obtain data for these purposes and are also committed to confidentiality. These processors are normally companies operating in the fields of IT services and printing. The Association of German Banks will not forward information about you to third parties unless this is required by law or you have consented to your data being passed on.

3.4. Will data be transferred to a third country?

At present, no data are transferred to third countries, nor are there any plans to do so. Data would only be transferred to countries outside the European Union and European Economic Area (so-called third countries) if

- there was a legal requirement to do so (e.g. tax reporting requirements),
- you had given us your consent or
- the transfer was justified in terms of data protection on the grounds of legitimate interests and no overriding interests of the data subject existed which merited protection.

3.5 How long will my data be stored?

We will process and store your personal data as long as this is necessary and legitimate for the purpose of performing the tasks set out in our articles. If the Association of German Banks no longer has a legitimate interest in processing certain data, or if you withdraw your consent to the processing, these data will normally be erased. The only exceptions are if it – temporarily – continues to be necessary to process the data in order to satisfy statutory record retention obligations, such as those concerning business letters under the German Fiscal Code (Abgabenordnung), or in order to preserve evidence in the event of a legal dispute arising within the statute of limitations.

3.6 Automated individual decision-making? Will profiling take place?

We use no automated individual decision-making (including profiling) in accordance with Article 22 of the GDPR.

4. Ombudsman Scheme of the German private banks

Data subjects in this category are those applying for dispute resolution through the Ombudsman Scheme, or those applying on their behalf, or persons who initially only want information about how the scheme works. Applicants will be informed separately and in more detail about the processing of their data in addition to this general privacy policy.

4.1. What sources and data do we use?

We process personal data which we receive from you or your statutory or legal representative in the course of handling dispute resolution. We also process personal data which we have received from the respondent, i.e. the member bank in question, or which we may have received from other dispute resolution entities. In a few cases, we also process personal data which we have legitimately obtained from publicly available sources (e.g. telephone directories) and are permitted to process.

4.2. Why do we process your data and on what legal basis?

Your personal data are processed solely for the purpose of replying to enquiries and thus informing you about the proceedings we offer and for the purpose of conducting the proceedings.

The main legal basis for the Ombudsman Scheme and the associated data processing is our 'Rules of Procedure of the Ombudsman Scheme of the German private banks' and the German Regulation on Financial Dispute Resolution Entities under Section 14 of the German Injunctions Act (Unterlassungsklagengesetz) and on their Proceedings (Verordnung über die Verbraucherschlichtungsstellen im Finanzbereich nach § 14 des

Unterlassungsklagengesetzes und ihr Verfahren [Finanzschlichtungsstellenverordnung]). The processing of personal data is necessary for the purpose of fulfilling our statutory remit and conducting the dispute resolution proceedings. Processing is therefore permissible under Article 6(1)(b) and (c) of the GDPR. In the light of your enquiry or application for dispute resolution, moreover, the processing of your data is not only in your own interest but also in our legitimate interests (Article 6(1)(f) of the GDPR) in handling your enquiry or application for dispute resolution swiftly and efficiently.

4.3. Who will obtain my data?

At the Association of German Banks, only staff of the Ombudsman Scheme Office within the meaning of the Rules of Procedure will have access to your data.

In accordance with the Rules of Procedure, your data will be transmitted only to those directly involved in your case. These persons are, first, your statutory or legal representative who is representing you in the case and to whom you have issued a power of attorney. They also comprise the specialist departments at the respondent bank which will process your application, and the ombudspersons who will finally decide on your case. The protection of your personal data is additionally ensured by the fact that, under the Rules of Procedure, all staff of the Ombudsman Scheme Office and the ombudspersons themselves are obligated to treat the proceedings as strictly confidential.

It may also happen that – if your application does not fall within our jurisdiction – we will need to forward it to the responsible dispute resolution entity. In this case, the staff of the responsible dispute resolution entity, the staff of the respondent bank and the ombudspersons of the responsible dispute resolution entity will also obtain your data. We will always inform you separately about the transfer in such a case, however.

Service providers used by us (processors within the meaning of Article 28 of the GDPR) may have access to your data for a short period of time for the purpose of maintaining and monitoring our data processing equipment. These will normally be companies responsible for servicing and maintaining the IT applications needed to conduct the dispute resolution, but may also be service providers in the fields of telecommunications, printing services or logistics. They are naturally also subject to the requirements of the European General Data Protection Regulation and the German Data Protection Act and thus also required to maintain strict confidentiality.

4.4. Will data be transferred to a third country?

No personal data are transferred to countries outside the European Economic Area (EEA) or to an international organisation. When standard IT components are serviced remotely, the possibility cannot be excluded that, to correct an error, an IT service provider in a third country (e.g. the US) may in rare cases have limited and managed access to personal data.

Should we transfer personal data to service providers outside the EEA, the transfer will only take place if the European Commission has confirmed that the third country has an adequate level of data protection or if other adequate data protection guarantees are in place (e.g. in the form of a company's binding internal data protection rules or EU standard agreement clauses). We will inform you of details separately if this is legally required.

4.5 How long will my data be stored?

When storing case files and data, we apply the retention periods for documents specified by the German Commercial Code (Handelsgesetzbuch). The Code requires documents to be retained for six years, with the retention period always starting at the end of the calendar in which the case was terminated. At the end of this retention period, the files are destroyed and the data are erased.

4.6. Do you have an obligation to make your data available?

You only have to provide us with the personal data needed to handle your enquiry or to conduct the dispute resolution proceedings. If you do not provide us with the information needed to conduct the proceedings, your case may be rejected.

4.7. Automated individual decision-making? Will profiling take place?

We use no automated individual decision-making (including profiling) in accordance with Article 22 of the GDPR.

5. What rights to data protection do I have?

Every data subject has the right to information under Article 15 of the GDPR, the right to rectification under Article 16 of the GDPR, the right 'to be forgotten' under Article 17 of the GDPR, the right to restrict processing under Article 18 of the GDPR, the right to object to the processing of personal data under Article 21 of the GDPR and the right to data portability under Article 20 of the GDPR. The right to information and the right to be forgotten are subject to the restrictions set out in sections 34 and 35 of the German Data Protection Act. You can enforce these rights vis-à-vis the Association of German Banks. You also have the right to lodge a complaint with the responsible data protection authority (Article 77 of the GDPR in conjunction with section 19 of the German Data Protection Act). The authority with jurisdiction over us is:

Berliner Beauftragte für Datenschutz und Informationsfreiheit
Friedrichstr. 219
10969 Berlin
Germany
Email: **mailbox@datenschutz-berlin.de**

At any time, you can withdraw your consent permitting us to process your data. This also applies to the withdrawal of consent given to us before the GDPR took effect, i.e. before 25 May 2018. Please note that the withdrawal of consent covers only future processing of personal data. Processing which took place before the withdrawal will not be affected.

Information about your right to object under Article 21 of the GDPR

Individual right to object

You have the right to object at any time, on grounds relating to your particular situation, to the processing of your personal data based on Article 6(1)(f) of the GDPR (data processing on the basis of striking a balance between legitimate interests). This also applies to profiling based on this provision within the meaning of Article 4(4) of the GDPR. If you object, we will no longer process your personal data unless we can demonstrate compelling legitimate grounds for the processing

which override your interests, rights and freedoms or if the processing serves the purpose of establishing, exercising or defending legal claims.

How to object

There is no special form to fill in. Just send your objection to the following address, quoting 'objection' as the subject, and include your name, address and date of birth:

Association of German Banks
Attn. Managing Director of Internal Affairs
Burgstr. 28
10178 Berlin
Germany

6. Changes to privacy policy

We reserve the right to modify the privacy policy to adjust it to changes in the legal basis or in the event of changes to our services or to how we process data. Changes to the privacy policy will have no effect on the validity of other contracts or agreements.

Privacy policy as at 15 January 2019