Privacy notice

Last updated July 2023

How we use your personal information

Your information will be held by Lloyds Bank Corporate Markets Wertpapierhandelsbank GmbH, which is part of Lloyds Banking Group (the "**Group**"). This privacy notice explains how companies within the Group use and look after your personal information. This includes what you tell us about yourself, what we learn by having you as a customer, and your marketing choices. This notice also tells you about your privacy rights and how the law protects you.

This privacy notice addresses our customers. Lloyds Bank Corporate Markets Wertpapierhandelsbank GmbH enters contracts with legal entities (companies). We process the personal data of our customers' representatives, economic beneficiaries and contact persons to pursue the purposes explained in this privacy notice.

This privacy policy relates only to the processing of your data by Lloyds Bank Corporate Markets Wertpapierhandelsbank GmbH., if you would like to see how the Group processes personal information please see the Lloyds Banking Group plc privacy notice here.

Our Privacy Promise

We promise:

- To keep your personal information safe and private.
- Not to sell your personal information.
- To give you ways to manage and review your marketing choices at any time.

Personal information and the law	**The control you have**	**How personal information is used**
This section tells you who we are, what your personal information is, and how we get it. It explains how the law protects you by controlling what is allowed to happen to it.	This section explains your data protection rights and covers how to exercise your rights (e.g. lodge a complaint, withdraw your consent, receive a copy of your personal data).	This tells you who we share personal information with. It explains what it's used for (processing purposes), which data will be used and which legal basis allows us to process your data.
1. Who we are 2. How the law protects you 3. Where we collect personal information from 4. How long we keep your personal information 5. If you choose not to give personal information		1. Who we share your personal information with 2. How we work out what marketing you receive 3. Credit Reference Agencies (CRAs) 4. Fraud prevention agencies 5. Sending data outside of the UK and EEA

Personal information and the law

Text
Who we are This section gives you the legal name of the company that holds your personal information. This is known as the Legal Entity. It also tells you how you can get in touch with us.
Lloyds Banking Group is made up of a mix of companies, set up on different legal entities. The Data Controller for your personal data is: LLOYDS BANK CORPORATE MARKETS WERTPAPIERHANDELSBANK GmbH Thurn-und-Taxis-Platz 6, 60313 Frankfurt am Main. Germany Phone: +49 69 273 90 525 Email: LBCMWDataPrivacy@lloydsbanking.com Managing directors: Chris Strobbe, MD Marktfolge, Eva Porz, MD Markt We'll let you know which Group entity you have a relationship with, at the time you take out another product or service with us. You can find out more about us at www.lloydsbankinggroup.com. **Contacting us about data privacy** Concerning questions about this privacy notice, processing of your data, your rights or other data protection topics, our data protection officer (DPO) would be pleased to help you: Post: Xamit Bewertungsgesellschaft mbH, Monschauer Straße 12, 40549 Düsseldorf Germany Email: info@xamit.de
About personal information The term personal information is a synonym of the term personal data, which is legally defined in Article 4 (I) GDPR as follows:

'personal data' means any information relating to an identified or identifiable natural person ('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;

How the law protects you

This section sets out the legal reasons we rely on, for each of the ways we may use your personal information.

As well as our Privacy Commitment, your privacy is protected by law. This section explains how that works.

Data Protection law says that we are allowed to use personal information only if we have a legal basis for doing so. This includes sharing it outside Lloyds Banking Group. The law says we must have one or more of the following as a legal basis before processing your personal information:

- To enter into or fulfil a contract we have with you (Art. 6 (I) b) GDPR), or
- When it is our legal duty (Art. 6 (I) c) GDPR), or
- When it is in our legitimate interest (Art. 6 (I) f) GDPR), or
- When you consent to it (Art. 6 (I) a) GDPR).

When we have a business or commercial reason of our own to use your information, this is called a 'legitimate interest'. We will tell you what that is, if we are going to rely on it as the reason for using your personal information. Even then, it must not unfairly go against your interests.

Here is a list of all the ways that we may use your personal information, and which of the reasons we rely on to do so. This also tells you which personal information we use.

Purpose	Legal Basis	Description of legitimate interests (if applicable)	Potential Data Used
• Pursuant to MiFID II (Markets in Financial Instruments Directive II) we are obliged to record all communication with customers (e.g. calls, e-mails, text messages, letters).	• Legal Duty (Art. 6 (I) c) GDPR)		Voice recordings of calls
• To communicate with our customers' (legal entities) contact persons and answer their questions and concerns	• Legitimate Interests (Art. 6 (I) f) GDPR)	To be able to meet the following purposes: • To enter into a contract with your business. • To fulfil our obligations as set out in a contract with your business. • To manage how we work with other companies that provide services to us and our customers. • To respond to complaints that may be made about our fulfilment of a contract.	• First and last name, • Role title, • Work telephone number, • Work email address, • Work address, • Transactions, • Concern/issue

		• To exercise our rights set out in agreements or contracts. • To create customer master data • To perform orders/instructions. • To make and manage payments, for means of handling transactions and claims management.	
• To perform statutory checks in accordance with relevant law: • Pursuant to § 11 (I) Money Laundering Act (GwG), we are legally obliged to conduct banking transactions with identified persons only. We are therefore legally obliged to check your identity. • To the extent required when we are submitting reports to national supervisory authorities (e.g. BaFin, German and other national tax authorities) • Compliance with the required examination in accordance with EU Regulations 2580/2001, 881/2002 and 753/2011 to avoid breaches of the regulations in the fulfilment of our contractual obligations. We are legally obliged to report positive hits to the Central Office for Financial Transaction Investigations (§ 43 (I) No. 2 Money Laundering Act). • Implementation of our due diligence required by the Money Laundering Act §§ 6 and 10 (I) No. 4 in particular, with regard to politically exposed persons: determining if representatives and economic beneficiaries of our customers (companies), a family member or a person known to be a close associate are a politically exposed person	• Legal Duty (Art. 6 (I) c) GDPR)		• First and last name, • Role/job title, • Work telephone number, • Work email address, • Work address, • Current and previous personal addresses, • Date of birth, • Place of birth, nationality, • Tax and/or national identifier and passport details, • Company name, • Company registration number, • Address of head office location, • Names of legal representatives, • Beneficial owner (y/n) • Status (= result of pep check: non-pep or category e.g. Diplomatic staff, member of parliament, party executive…)

• To study how our customers use products and services from us and other organisations. • To develop new products and services that may be of interest to our customers. • For that purpose, the processed data will be used for the creation of reports and for evaluation.	• Legitimate Interests (Art. 6 (I) f) GDPR)	• To improve our products and services and develop new ones. • For identification and persecution of financial risks • For concentrating our sales activities • For fulfilment of (contractual) obligations regarding our customers.	• First and last name, • Role/job title, • Work telephone number, • Work email address, • Work address, date of birth, • Place of birth, nationality, • Tax and/or national identifier and passport details, • Company name, • Company registration number, • Address of head office location, • Names of legal representatives, • Beneficial owner • Status (= result of PEP check: non-PEP or category e.g. diplomatic staff, member of parliament, party executive…) • products/services • transactions • concern/issue
• To undertake audits that assess and test business and technical controls in respect of our business processes and systems. • Data testing	• Legitimate Interests (Art. 6 (I) f) GDPR)	• Obtaining quality, security, and other standards certification • Ensure that personal information is processed correctly by systems. • Identify errors in processing and production of reports. • Compliance with legal obligations	
• External auditing of our business to ensure compliance with regulatory and statutory standards. • Internal reporting	• Legitimate Interests (Art. 6 (I) f) GDPR)	• End of year business audits • Audited financial statements. • Tax law assessments and reporting • Management of our company including assessment of business performance • Financial reconciliations	
• Development, testing and migration to, new systems to the extent it is not possible to use test or anonymised data	• Legitimate Interests (Art. 6 (I) f) GDPR)	• Identify data issues and problems with new solutions. • Enhance the operation of our business and • Facilitate the introduction of new products and or services for customers	
• Security	• Legitimate Interests (Art. 6 (I) f) GDPR)	• Test the security of our systems. • Investigate security breaches. • In the development of reports relating to data breaches to be sent to the relevant public authorities and regulators. Your details will not be provided to public authorities unless legally required	
• Legal disputes	• Legitimate Interests (Art. 6 (I) f) GDPR)	• Processing evidence for use in establishing, exercising or defending legal claims	
• Criminal investigations	• Legitimate Interests (Art. 6 (I) f) GDPR)	• Investigation of suspected criminal or illegal activity	

		• Reporting suspected criminal or illegal activity to law enforcement agencies	
• To communicate with you about our products and services • To contact you about taking part in market research about existing and new products and services	• Consent (Art. 6 (I) a) GDPR)		• First and last name, • Role/job title, • work telephone number, • work email address, • work address.

Where we collect personal information from

This section lists all the places where we get personal data that counts as part of your personal information.

We may collect personal information about individuals in your business from other Lloyds Banking Group companies and any of these sources:

Personal information you give to us

This covers data that you give and data provided by people linked with you or your business's product or service, or people working on your behalf.

- When you apply for our products and services.
- When you talk to us in meeting or on the phone including recorded calls and notes we make and as required by law.
- When you use Group websites, mobile device apps or web chat to communicate with us or the Group.
- In emails and letters.
- In financial reviews and interviews.
- In customer surveys.

Personal information from outside organisations

- Other financial services companies (*to fulfil a payment or other service as part of a contract with you, or to help prevent, detect, and prosecute unlawful acts and fraudulent behaviour*)
- Public information sources. *To the extent that they have information which we are allowed to collect by law. For example, names of directors on your company's management board.*
- Government and law enforcement agencies.
- To comply with the legal obligations arising from EU Regulations 2580/2001, 881/2002 and 753/2011, we use databases from external providers with information on persons subject to sanctions.
- To comply with our obligations under the Money Laundering Act, we must determine whether prospects are so-called politically exposed persons (PEP). For this purpose, we use databases of external providers with information on known, politically exposed persons and on persons from their closest environment.

Credit Reference Agencies (CRAs)

This section explains how we work with outside companies to decide whether to provide you with products and services. It explains what we do and why we do it.

We carry out identity checks when you apply for a product or services for you or your business. We may use Credit Reference Agencies to help us with this.

We will share your business information (business name) with CRAs, and they will give us information about you. We'll use this information to:

- Assess whether you or your business are who you say you are.
- Make sure what you've told us is true and correct.
- Help detect and prevent financial crime.

We do not access or seek information about you in terms of your personal financial position or history. Your personal information is only processed in relation to your role within your business.

You can find out more about the CRAs on their websites, in the Credit Reference Agency Information Notice. This includes details about:

- Who they are.
- Their role as fraud prevention agencies.
- The data they hold and how they use it.
- How they share personal information.
- How long they can keep data.
- Your data protection rights.

Here are links to the information notice for the Credit Reference Agency we use:
Schufa Holding AG

How long we keep your personal information.

This section explains how long we may keep your information for and why

We will keep personal information relating to your personnel for as long as you are a receiving products and services from us and up to 10 years after. The reasons we may do this are:

- To respond to a question or complaint, or to show whether we gave you fair treatment.
- To study customer data as part of our own internal research.
- To obey rules that apply to us about keeping records. For example, Commercial Code §§ 238 and 257, Tax Code § 147, Money Laundering Act § 8, etc.

Calls that are recorded to comply with MiFID II will be stored for five years.

We may also keep your personal information for longer than 10 years if we cannot delete it for legal or regulatory reasons. As an example, if a legal hold is placed on it as part of ongoing legal proceedings. For the preservation of evidence, we retain personal information in accordance with the statutory limitation periods according to sections 195ff. of the German Civil Code. The storage duration of your personal information may exceed the duration stated above. The statutory limitation periods can be up to 30 years. The normal limitation period is 3 years.

If you choose not to give personal information

You can choose not to give us personal information. In this section we explain the effects this may have.

We may need to collect personal information by law, or to enter into or fulfil a contract we have with your company, or to meet our legitimate interests.

If you choose not to give us this personal information, it may delay or prevent us from fulfilling our contract with your company or doing what we must do by law. It could mean that we cancel a product or service you have with us.

We sometimes ask for information that is useful, but not required by law or a contract. We will make this clear when we ask for it. You do not have to give us these extra details and it won't affect the products or services you have with us.

The control you have

This section explains your rights under data protection law and gives details of how to contact us to make a complaint about data privacy. It also shows you where you can get in touch with the data protection supervisory authority.

You have the legal right to:

- **Access** to your personal information that we process (Art. 15 GDPR)
- **Rectification and completion** of your personal information (Art. 16 GDPR)
- **Erasure** (Art. 17 GDPR)
- **Restriction of processing** (Art. 18 GDPR)

  Data portability (Art. 20 GDPR)
- **Withdrawal of your consent** (Art. 7 GDPR) with effect for the future. The withdrawal of consent will not affect the lawfulness of processing based on consent before its withdrawal.
- You have the right to express your point of view and contest any automated decision (Art. 22 GDPR).

- You also have the right to **object** to the processing of your personal information which is based on our legitimate interests or the legitimate interests of a third party at any time, on grounds relating to your particular situation (Art. 21 GDPR). This also applies to profiling based on these provisions within the meaning of Art. 4 (4) GDPR.
- **Objection to direct marketing –** You have the right to object to the processing of your personal information for the purpose of direct marketing at any time without giving reasons.

To exercise these any of these rights, you can contact us via:

Post: Xamit Bewertungsgesellschaft mbH,
Monschauer Straße 12,
40549 Düsseldorf
Germany
Email: info@xamit.de

You also have the legal right to complain to the supervisory authority (Art. 77 GDPR).

For Lloyds Bank Corporate Markets Wertpapierhandelsbank GmbH, the relevant regulator is der Hessische Beauftragte für Datenschutz und Informationsfreiheit. Find out on their website (https://datenschutz.hessen.de/)) about how to report a concern.

How personal information is used.

Who we share your personal information with

We may share your personal information with outside organisations such as tax authorities. This is so that we can provide you with products and services, run our business, and obey rules that apply to us. In other cases, we use selected vicarious agents and service providers who work for us as commissioned data processors (in accordance with Art. 28 GDPR) and may obtain access to your personal information in the required scope. Commissioned data processors are subject to numerous contractual obligations and may, in particular, process your personal information only on our instructions and solely for the fulfilment of the orders received from us. Here we list all the types of organisations that we may share your personal information with.

Lloyds Banking Group

We may share your personal information with other companies in Lloyds Banking Group (core functions of our business are outsourced to other Group entities for efficiency purposes). Such companies work as commissioned data processors for us.

Authorities

This means official bodies that include:

- Law enforcement and fraud prevention agencies.
- German and other national tax authorities. *For example the United States Internal Revenue Service if you are a US citizen*

Banking and financial services

Outside companies, we work with such services to provide services to you and to run our business.

- Agents, suppliers, sub-contractors and advisers
  These are types of firm that we use to help us run our business.
- Agents who help us to collect what is owed to us
- Credit reference agencies (such as Schufa Holding AG)
- Someone linked with you or your business's product or service.
  This could mean a joint account holder, trustee, or fellow company director.
- Other financial services companies (other members of a syndicate providing services)
- Companies you ask us to share your personal information with. *For example specific third parties who may be interested in your bonds.*

General business

Outside companies the Group uses to help grow and improve our business, only where we have your consent to do so.

- Market researchers
  These firms may get in touch with you on our behalf to ask you for your opinions and feedback. Sometimes these firms will combine what you tell them with data from other sources to study it. They will use this to produce reports and advice that help us understand our customers' point of view, so that we can improve the way we work as a business.
- Advisers who help us to come up with new ways of doing business.
  This might be a legal firm, IT supplier or consultancy.

Company mergers, takeovers and transfers of products or services
We may also share your personal information if the ownership of products or services or the make-up of Lloyds Banking Group changes in the future:

- We may choose to sell, transfer, or merge parts of our business, or our assets, including products or services. Or we may try to bring other businesses into Lloyds Banking Group. *This is sometimes called Mergers & Acquisitions or 'company takeovers'.*
- During any such process, we may share your personal information with other parties involved. We'll only do this if they agree to keep your personal information safe and private.

Other recipients of personal information
- Auditors
- Banks, payment service providers
- Call centres
- Data Protection Officer
- Service providers for mass file destruction
- Service providers for printing, letter shops
- Service providers for mailing
- Service providers for sanction list screenings (according to EU regulations 2580/2001, 881/2002 and 753/2011)
- Service providers for 'PEP' screenings
- Your e-mail provider (in case of communication via e-mail)
- Courts, lawyers, contractual partners, consultants, business partners, law enforcement authorities, opposing lawyers, state or federal criminal police (for legal disputes or actual suspicious cases)
- IT service providers
- Tax counsellors
- Service providers for telecommunication
- Financial auditors
- Insolvency Court (In the case of ongoing insolvency proceedings against one of our customers, we are obliged to provide the Insolvency Court with information on financial and transaction data as well as assets and debts of this customer upon request in accordance with § 5 Insolvency Regulation)
- Tax authorities, customs authorities (In accordance with § 33 of the Inheritance Tax and Gift Tax Act and § 30a (2) and (3), § 93 and § 208 of the Tax Code, in current legal cases against one of our customers we are obliged to make statements about such customers after submission of a judicial authorization from a tax or customs authority)
- Central Office for Financial Transaction Investigations (Pursuant to Section 43 (1) (2) of the Money Laundering Act, we are obliged to report hits to the Central Office for Financial Transaction Investigations when comparing your data with penalty lists (which we carry out in order to fulfil our statutory obligation under EU Regulations 2580/2001, 881/2002 and 753/2011))

Sharing data that does not say who you are

We may share or sell some data to other companies outside Lloyds Banking Group, but only when it is grouped so that no-one's identity can be known or found out.

We combine data in this way so we can look for general patterns and trends. When we combine data this way, we use all of the information – including historical data – that we hold about you and our other customers.

We do this to learn about the types of customers we have, how they use our products, and services. The law says this is not considered to be personal information after it has been grouped in this way.

Sending personal information outside the UK and EEA (European Economic Area)

This section tells you about the safeguards that keep your personal information safe and private, if it is sent outside the UK and EEA.

Following the decision of the European Commission on 28th June 2021 that the UK has adequate data protection measures in place offering the same level of protection as the EEA, we will store and process your information in the UK as well as in the EEA.

We will only send your personal information outside of the UK and European Economic Area ('EEA') to:

- Follow your instructions.
  For example, where it is necessary as part of a transaction involving an overseas counter party or as part of the fulfilment of a contract.
- Comply with a legal duty.
  For example, we share information about US citizens with the US tax authority.
- Work with our suppliers who help us to run or deliver our services - this includes IT service providers and Group. Core functions of our business are outsourced to Group entities (as commissioned data processors) located in the UK.

If we do transfer your personal information outside the UK and EEA to our suppliers, we will make sure that it is protected to the same extent as in the UK and EEA. We'll use one of these safeguards:

- Transfer it to a non-EEA country with privacy laws that give the same protection as the UK and EEA. Learn more on the European Commission website. The EU Commission determines which non-EU / EEA countries (third countries) have an adequate level of data protection. The following countries have obtained an adequacy decision from the EU Commission (last updated on 7 July 2021): Andorra, Argentina, Canada (restricted to processing under PIPEDA), Faroe Islands, Guernsey, Isle of Man, Israel, Japan, Jersey, New Zealand, Switzerland, United Kingdom, Uruguay.
- Put in place a contract which incorporates the EU Standard Contract Clauses with the recipient that means they must protect it to the same standards as the UK and EEA. Read more about this here on the European Commission Justice website. This means applies to IT service providers outside the EEA and commissioned Group entities in the UK.