DATA PROTECTION AND COOKIES

Information data pursuant to Articles 13 and 14 of the General Data Protection Regulation (GDPR) on the processing of personal data

We take the protection of your personal data very seriously. We treat your personal data confidentially and in accordance with the statutory provisions. In this privacy policy we inform you about the data processing of your personal data.

As a rule, it is possible to use our website without providing your personal data independently. Insofar as personal data (for example, name, address or e-mail address) is collected on our pages, this is always done to enable the use of the website or on a voluntary basis.

(Status 15.09.2024)

1 WHO IS RESPONSIBLE FOR DATA PROCESSING AND WHOM CAN I CONTACT?

Responsible for data processing

Kathrein Privatbank Aktiengesellschaft
Wipplingerstraße 25, 1010 Wien
Tel: +43 1 53151-0
E- Mail: datenschutz@kathrein.at

Contact data of the Data Protection Officer of the Bank

Mag. Daniela Bollmann, LL.M
Telephone +43 1 71707-8603
E- Mail: datenschutzbeauftragter@rbinternational.com

2 WHAT DATA DO WE PROCESS AND FROM WHAT SOURCES?

We process the personal data that we receive from you as part of our business relationship. In addition, we process data that we have legitimately received from credit bureaus (CRIF GmbH), debtor directories (Kreditschutzverband von 1870) and from publicly available sources (e.g., business register, association register, land register or media) or that are provided legitimately by other companies affiliated with the bank.

Personal data comprise your personally identifiable data and contact data (e.g. name, address, date and place of birth, nationality etc.) or data relating to identity papers and travel documents (e.g. specimen signature, identification card data). It can also include payment transaction and clearing data (e.g. payment instructions, turnover data in payment transactions), creditworthiness information (e.g. type and amount of income, recurring payment obligations for schooling and education of children, loan payments, rent payments), data relating to marketing and sales, loan transactions, video and/or audio recordings (e.g. video or phone recordings), electronic protocol and identification data (apps, cookies, IP addresses etc.), financial identification data (data relating to credit or debit cards) or AML (Anti Money Laundering) and compliance data, as well as other data similar in nature to the categories listed above.

3 WHAT IS THE PURPOSE AND THE LEGAL BASIS FOR DATA PROCESSING?

We process your personal data in accordance with the provisions of the European Union General Data Protection Regulation (GDPR) and the Data Protection Act 2018.

3.1 To fulfill contractual obligations (Art. 6 (1) (b) GDPR)

Processing of personal data (Art. 4 (2) GDPR) occurs to provide and arrange for bank transactions and financial services including but not limited to performance under our agreements with you and execution of your orders as well as performance of pre-contractual measures.

The purposes of processing data is determined first and foremost by the specific product (e.g. account, loan, securities, deposits, credit- and debit cards) and may, among other things, include needs assessments, consultation, asset management and administration and execution of transactions.

Such data processing occurs for example in connection with debit cards (also called ATM cards) provided to you by Kathrein and which you can use to execute payment transactions with retailers at POS terminals and online (e-commerce payments in online shops), to withdraw cash from respective ATM or cash machines and to facilitate transactions between debit cards ("ZOIN" – as far as available).

For those transactions, the financial institution of the card holder and of the recipient of the payment must be identifiable in order for those institutions to settle the transactions with each other. For that purpose, nearly all financial institutions operating within Austria have signed an agreement with PSA Payment Services Austria GmbH (PSA) (the PSA agreement).

The agreement aims to regulate the mutual rights and obligations of the financial institutions and the PSA. The agreement stipulates the terms financial institutions have agreed upon regarding transactions (e.g., withdrawal of funds) executed by non-customers of the bank at bank-owned cash machines or payment transactions through POS terminals. PSA is responsible for the technical aspects of the transaction with eligible cards among those institutions. In addition, PSA operates its own ATMs or cash machines. To facilitate the transaction and settle payments between the financial institutions, the institutions must process the data of their own customers.

The legal basis for processing data are a variety of Acts, e.g. the Austrian Banking Act (Bankwesengesetz), the Austrian Payment Services Act (Zahlungsdienstgesetz, ZaDiG), the Financial Markets Anti-Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG), etc., with which the parties to the PSA agreement must comply, and the agreement between the financial institution and its customer (e.g. checking account agreement, credit or debit card agreement). To exercise your rights in connection with the data processing measures listed above, please contact Kathrein.

For credit cards, the exchange of personal data, especially with the creditcard-issuer or merchants and account-holding banks is necessary for the execution of the credit card transaction.

For specific details regarding data processing activities referenced above, please read the respective agreements and relevant terms and conditions.

3.2 To fulfill legal obligations (Art. 6 (1) (c) GDPR)

Processing of personal data might be necessary to fulfill a range of legal requirements (arising from the Banking Act, the Financial Markets Anti-Money Laundering Act, the Securities Supervision Act, the Stock Exchange Act etc.) as well as due to regulatory requirements (e.g. those established by the European Central Bank, the European Financial Authority, the Austrian Financial Market Authority etc.), which the bank is subject to as an Austrian financial institution.

Examples of such cases are:

- Filing of suspicious activity reports with the Financial Intelligence Unit (Geldwäschemeldestelle) (Section 16 FM-GwG)
- Providing information to the FMA in accordance with the Securities Supervision Act (WAG) and the Stock Exchange Act (BörseG) in order to monitor compliance with the provisions governing the misuse of insider information in the market
- Providing information to the financial penalty authorities in response to financial penalty proceedings for deliberate financial crimes
- Providing information to federal tax authorities in accordance with Section 8 of the Austrian Accounts Register and inspection of Accounts Act (Kontenregister- und Konteneinschaugesetz)
- Assess and manage risks
- Credit assessment for lending (creditworthiness)

3.3 As part of your consent (Art. 6 (1) (a) GDPR

If you have given consent to processing of your personal data for specific- purposes (e.g. transfer of data to the recipients named in the consent, notifications via e-banking, the data will only be processed for the purposes and to the extent stated in the consent form. Consent can be withdrawn at any time and will become effective for future processing of data.

Examples of such cases are:

- The evaluation of your data such as master data (e.g. company name, contact data), commercial data (e.g. balance sheet, profit and loss statement), account/product and service data (e.g. payment history, transactions, custody account data), other documents and agreements, as well as data from ongoing meetings, - data on/from devices and communication channels (e.g. customer interactions via websites), user-generated content (including audio and video content), - data on third-party products/accounts/services (e.g. funds), - data from business relationships with other banks if you have made use of the option to include these accounts in your electronic banking (e.g. in accordance with PSD 2)
- and the query of external creditworthiness databases (Kreditschutzverband von 1870, CRIF GmbH) in order to assess your creditworthiness in advance for credit offers made to you by Kathrein on its own behalf.
- to evaluate data on your business relationships with other banks (accounts, loans, investments) and on your payment behavior derivable therefrom, which the bank can access because you have made use of the option to include these business relationships in your electronic banking with the bank.
- to provide you with high quality customer service,
- to provide you with tailored and appropriate information and offers, including from companies whose products and services are marketed by the aforementioned RBI Group companies,
- to develop services and products tailored to the interests of your business in order to further improve the user-friendliness of our service facilities and products;

3.4 To safeguard legitimate interests (Art. 6 (1) (f) GDPR in general

If necessary, data processing may be conducted to protect legitimate interests of the Bank or third parties. In the following cases, data processing takes place to safeguard legitimate interests.

Examples of such cases are:

- Consultation and exchange of data with credit bureaus (for example Österreichischer Kreditschutzverband 1870, CRIF) for the determination of creditworthiness or default risks
- General info mails and newsletters on service, products and related market information
- Video surveillance to collect evidence in case of crime or to prove transactions and deposits (such as at the cash desk) - especially to protect customers and employees
- Certain telephone records (for quality assurance or in the case of complaints), and if stated by law (e.g. Austrian securities act)

- Measures for business management and further development of services and products
- Measures to protect customers and employees as well as to secure the property of Kathrein and to prevent, contain and investigate criminally relevant conduct.
- Measures in Fraud Transaction Monitoring, against anti-money laundering, terrorist financing and offending crime. At the same time, data evaluations (among others in payment transactions) are carried out. These measures also serve for your protection.
- Data processing for law enforcement purposes
- Asserting legal claims and defense in legal disputes
- Ensuring the IT security and IT operations of the Bank
- Prevention and investigation of criminal acts

3.5 To safeguard legitimate interests (Article 6 (1) (f) GDPR) in the marketing of our services

The evaluation of your data processed by Kathrein for the purpose of

- providing you with individual information and offers from Kathrein and the companies listed below under “Product and service data”, whose products Kathrein arranges or provides:
- developing services and products that are tailored to your interests and life situation, and
- further improving the usability of our service facilities such as e-banking, apps, self-service devices and others

is based on our legitimate interest for the marketing of our services. The evaluation of the data for this purpose takes place only as long as you have not objected to this.

The following data, which either Kathrein itself has collected itself or which you have transmitted to Kathrein, will be evaluated:

Personal data / master data
Gender, professional title, name, date of birth, country of birth, nationality, marital status, tax status, level of education, profession, employer, authentication information such as driver's license data, income data, address and other contact data such as telephone number or email address, geographic location data, securities risk category in accordance with your investor profile, housing situation such as renter or owner and apartment or house, family relations (without collecting the personal data of those individuals), number of persons in the household, data provided during consultation sessions such as hobbies and interests or planned purchases and automobile, household expenses, internal ratings such as evaluation of income and expenses and assets and liabilities by Kathrein.

Product and service data of Kathrein
Data on the service of Kathrein which you use, including

- means of payment used by you, such as debit and credit cards,
- debits and credits and arrears on accounts and loans
- interest rates and charges or charges charged in connection with these services, - payment behavior, including the options you can use to place your order (for example e-banking),
- payment transactions incoming and outgoing, recipients and senders, payment orders transmitting intermediaries, amount, purpose and payment references, payer references,
- the frequency and type of transfers, in cashless payments, the data of the traders or service providers receiving the payments and information on transactions concluded with them,
- Data from e-banking (these are usage and content data from e-banking and the e-banking mailbox)
- Savings and securities transactions and custody accounts, including details of securities held

Data from services, website and communications
Data relating to the use of electronic services and websites, functions of the websites and apps as well as e-mail messages between you and Kathrein, information about viewed websites or content and links accessed, including external websites, content response time or download errors, and the usage period of websites and information on the use and subscriptions of newsletters of Kathrein.

This information is collected by way of using automated technologies, such as cookies or web beacons (counting pixels used to register e-mails or websites), or web-tracking (recording and analysis of surfing behavior) on the website or e-banking and using external service providers or software (for example Google Analytics).

Online queried account and custody account data
Data on information about accounts and depots requested online via service providers, data of these service providers, content and purpose and frequency of queries and content of the given information.

Technical data of the mobile devices used for data access
Information about devices and systems used for accessing websites or portals and apps or other means of communication, such as internet protocol addresses or types and versions of operating systems and web browsers, and additional device identifications and advertising identifications or location information and other comparable data on devices and systems.

Data on user-generated content
Information uploaded on websites or apps of Kathrein such as comments or personal messages and photos or videos and similar content.

Data regarding products and services procured from other companies
Data of products and services provided to you by Kathrein, which are from companies affiliated with Kathrein, esp. Kathrein Capital Management GmbH, Raiffeisen Bank International AG, Raiffeisen Kapitalanlage-Gesellschaft mbH, Raiffeisen-Leasing GmbH (the members of the RBI Group can be found on the website under "Use of your data"): Raiffeisen Bausparkasse Gesellschaft mbH, UNIQA Österreich Versicherung AG, Raiffeisen Kapitalanlage-Gesellschaft mbH, Raiffeisen-Leasing GmbH, Raiffeisen Immobilien Vermittlung GmbH , Raiffeisen Analytik Ges.m.b.H., Raiffeisen Beratung Direkt Ges.m.b.H, as well as Card Complete Service Bank AG.

Data of products and services provided to you by Kathrein, which are not from companies affiliated with Kathrein.
These data include the personal data and the detailed data of the products, such as the item of transactions including securities transactions, terms, interest, charges, debits, credits and arrears. If the products brokered are payment instruments, the analyzed data also includes: payment behavior, incoming and outgoing payment transactions, recipients and senders, payment service providers, amounts, purpose, payment references, originator references, frequencies and types of money movements, cashless payments, data of the dealers or service providers and information about these closed deals.

4 WHO RECEIVES MY DATA?

Within Kathrein, your data will be disclosed to those departments, employees and subsidiaries that need it to fulfill contractual, legal and/or supervisory obligations and legitimate interests or for which you have given us your consent.

In addition, contractually bound processors (in particular IT and back-office service providers) receive your data as far as they require the data to fulfill their respective service. All processors are contractually obligated to treat your data confidentially and to process it only in the context of providing the service.

If there is a legal or regulatory obligation, public authorities and institutions (European Banking Authority, European Central Bank, Austrian National Bank, Austrian Financial Market Supervisory Authority, tax authorities, etc.) as well as our Bank and auditors may be the recipients of your personal data.

With regard to a data transfer to other third parties, we would like to point out that Kathrein as an Austrian bank is obliged to observe banking secrecy in accordance with § 38 BWG and therefore is obliged to keep confidentiality regarding to all customer-related information and facts that have been entrusted to us or made available due to the business relationship. Kathrein may only disclose such personal information, if you have exempted us in writing and expressly from banking secrecy, or if the Bank is legally obliged by law to such a disclosure.

The recipients of personal data in this context may be other credit and financial institutions or similar entities. We disclose to such recipients only those data as we need in order to conduct the business relationship with you. Depending on the respective contract, these recipients may be e.g., correspondent banks, stock exchanges, custodian banks, credit bureaus or other companies affiliated with the Bank (due to regulatory or legal obligation).

Data from the video surveillance of Kathrein can be used on a case by case basis by competent authorities or the court (for evidence in criminal matters), security services (for security purposes), courts (to secure evidence in civil cases), employees, witnesses, victims (under the enforcement of their claims), insurance (exclusively for the settlement of insurance claims), lawyers and other bodies for the purpose of law enforcement.

5 IS THERE A DATA TRANSFER TO A THIRD COUNTRY OR TO AN INTERNATIONAL ORGANIZATION?

A transfer of data to third countries (outside the European Economic Area - EEA) will only take place if this will be necessary for the execution of your orders (e.g. payment and securities orders), or if so required by law or if you have given us your explicit consent.

In addition, data may be transferred to Kathrein´s and RBI's subsidiaries or processors in third countries or subcontractors of Kathrein´s and RBI's processors in third countries. These are obliged to comply with European data protection and security standards. Information about this can be obtained from us.

Payments and cash withdrawals with debit and credit cards can lead to the necessary involvement of international card organizations and thus possibly to data processing by these card organizations in third countries. For example, the data protection measures taken by MasterCard ("Binding Corporate Rules") are available here.

If so required by law, we will separately provide you with further details.

6 HOW LONG WILL MY DATA BE STORED?

We process your personal data, as far as necessary, for the whole duration of the entire business relationship (beginning with the conclusion of a contract, its execution and ending with its termination) as well as in accordance with the mandatory storage and documentation obligation as required by law, in particular pursuant to the following Austrian legal provisions: the Companies Code (Unternehmensgesetzbuch, UGB), the Federal Fiscal Code (Bundesabgabenordnung, BAO), the Banking Act (Bankwesengesetz BWG), the Financial Market Money Laundering Act (Finanzmarkt-Geldwäschegesetz, FM-GwG) and the Securities Supervision Act (Wertpapieraufsichtsgesetz, WAG).

Moreover, the data storage is also subject to the statutory limitation periods, e.g. under the Austrian General Civil Code (Allgemeines Bürgerliches Gesetzbuch, ABGB) and may in certain cases last up to 30 years.

Data from the video-surveillance of the Bank will be deleted in principle latest after 90 days if no longer required for the purposes of video surveillance.

7 WHICH DATA PROTECTION RIGHTS DO I HAVE?

You have the right to information, correction, deletion or restriction of the processing of your stored data, a right to object to the processing and a right to data portability in accordance with the requirements of data protection law.

If you wish to exercise your rights, please contact datenschutz@kathrein.at or the data protection officer. If, in your view, the response to your rights is not carried out in accordance with the GDPR, you are welcome to contact us again or file a complaint with the Austrian Data Protection Authority, Barichgasse 40-42, 1030 Vienna, Austria, www.dsb.gv.at.

8 AM I OBLIGED TO PROVIDE DATA?

As part of the business relationship, you must provide us with all personal information that is necessary to enter into and to maintain the business relationship with you, and also those data that we are required by law to collect. If you do not provide us with these data, we will generally decline either to conclude or to complete the contract, or we will be unable to execute an existing contract or we would be forced to terminate such contract. However, you are not obliged to give your consent to the processing of data if such data is not necessary for the performance of a contract or is not required by law or regulation.

9 IS THERE AUTOMATED DECISION-MAKING?

For the establishment and implementation of the business relationship, we generally do not use fully automated decision-making in accordance with Article 22 DSGVO. In connection with products to be concluded online, an automated rejection of the online conclusion may occur if your information does not meet the requirements defined for the product. In these cases, please contact a customer service representative. If we use these procedures in other individual cases, we will inform you of this separately, insofar as this is provided for by law.

10 CONTACT FORM

If you contact us by form on the website or by e-mail, the data you provide and transmit will be stored by us for a maximum of twelve months for the purpose of processing the inquiry and in case of follow-up questions. In this way, we pursue our legitimate interest in being able to offer you the best possible service and to open up ways for you to exchange information with us. If you do not wish your data to be shared and/or stored in this way, please send your objection to datenschutz@kathrein.at.

11 ONLINE SOCIAL MEDIA PRESENCE

Our online presences in social networks or on platforms serve the communication and information of interested parties or customers.

As a rule, user data is processed for market research and advertising purposes, e.g., to create usage profiles. These usage profiles can be used, among other things, to place advertisements that correspond to the user's interests. Cookies are stored on the user's computer for this purpose, with the help of which the user's usage behavior and interests are stored. In addition, user data can also be stored in the usage profiles across devices (this primarily concerns users who are logged in to the relevant platform). It is possible for us to place target group-oriented advertising and to perform an anonymized analysis of the use of our online presence.

The processing of users' personal data is based on your consent (a declaration of consent, e.g., by activating a checkbox or confirming a button).

Below you will find details and information on possible data transfers to third countries (countries outside the European Union - EU or the European Economic Area - EEA) based on the provider information on processing and objection options.

- Facebook, Meta Platforms Ireland Ltd., 4 Grand Canal Square, Grand Canal Harbour, Dublin 2, Irland
  Privacy policy https://facebook.com/about/privacy/
  Opt-Out www.facebook.com/settings?tab=ads and www.youronlinechoices.com
  Joint data processing agreement: https://de-de.facebook.com/legal/terms/page_controller_addendum
- Twitter, Twitter International Company, One Cumberland Place, Fenian Street, Dublin 2, D02 AX07 Irland
  Privacy policy https://twitter.com/de/privacy
  Opt-Out https://twitter.com/personalization

- LinkedIn, LinkedIn Ireland Unlimited Company, Gardner House, 2 Wilton Place, Dublin 2, Irland
  Privacy policy https://de.linkedin.com/legal/privacy-policy
  Opt-Out https://linkedin.com/psettings/guest-controls/retargeting-opt-out
- Xing, XING AG, Dammtorstraße 29-32, 20354 Hamburg, Deutschland
  Privacy policy and Opt-Out privacy.xing.com/de/datenschutzerklaerung

12 JAVA SKRIPT AND TRACKING PIXEL

On our website, technically necessary cookies and other standard web control elements are used in particular to control and improve our Internet presence (JavaScript and tracking pixels). All data is collected anonymously. This allows us to collect information in order to check for which screen sizes, browsers and operating systems our website should be optimized. JavaScript is a programming language used to evaluate user interactions and to change, reload or generate content.

13 COOKIEBOT CONSENT

Cookieboot Consent is a Consent Management Platform (CMP) from Usercentrics A/S, Denmark.

The domain scans and finds all cookies and trackers, blocking all of them until the end users have given their active and explicit consent. All user consents are then securely stored for legal documentation purposes.

You can view the data protection provisions at the following link: https://www.cookiebot.com/de/privacy-policy/

14 ANONYMOUS STATISTICAL EVALUATION

For anonymous statistical evaluation and extended security precautions during visits to our website, we use services of the company JENTIS GmbH, Schönbrunner Straße 231, 1120 Vienna ("JENTIS"). For this purpose, data is transmitted to JENTIS, which JENTIS evaluates on our behalf in anonymized form. This means that JENTIS GmbH only processes data that cannot be traced back to an identifiable person. In addition, we use JENTIS to anonymize your personal data before transferring it to a third country, thus protecting your data.

You can view the data protection provisions at the following link: https://www.jentis.com/privacy-policy/"

15 GOOGLE ANALYTICS

Our website uses Google Analytics, a web analytics service provided by Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland ("Google"), if you have consented to this. Google Analytics uses cookies that are stored on your computer. The information generated by the cookie about your use of this website (including your anonymized IP address and IDs and the URLs of websites visited) will be transmitted to and stored by Google on servers in Europe. This website uses the IP anonymization option offered by Google Analytics. Your IP address will be shortened by Google within the member states of the European Union or in other contracting states of the Agreement on the European Economic Area.

By using the company JENTIS GmbH, your personal data is anonymized before a potential transfer to a third country. Google thus only receives information that does not allow any conclusions to be drawn about you.

On our behalf, Google will use this information for the purpose of evaluating your use of the website, compiling reports on website activity and providing us with other services relating to website activity and internet usage.

You can prevent Google from collecting your data in connection with Google Analytics by downloading and installing the browser plugin available at tools.google.com/dlpage/gaoptout.

In connection with Google Analytics, the Google Tag Manager is also used. Google Tag Manager is also a solution from Google that allows companies to manage website tags via an interface. The Google Tag Manager is a domain without cookies that does not collect any personal data. The Google Tag Manager triggers other tags, which in turn may collect data. We hereby point this out separately. The Google Tag Manager does not access this data. If a deactivation has been made by the user at domain or cookie level, this remains in place for all tracking tags that are implemented with Google Tag Manager.

At https://policies.google.com/terms/de, https://policies.google.com/technologies/partner-sites and https://policies.google.com/privacy/, you will find more detailed information on Google's terms of use and Google's privacy policy.

16 GOOGLE MAPS

If you use the corresponding function and have given your consent, we use the Google Maps API service on our pages. This service is a service of Google, Inc., 1600 Amphitheatre Parkway, Mountain View, CA 94043, USA. By integrating the service on our website, at least the following data are transmitted to Google, Inc.: IP address, time of visit of the website, screen resolution of the visitor, URL of the website (referrer), the identification of the browser (user agent) and search terms.

The data transfer is independent of whether you have a Google account that you are logged in or whether you do not have a Google user account. If you are logged in, the data will be assigned with your account. If you do not wish assignment to your profile, you must log out before activating the button. Google, Inc. stores this data as usage profiles and uses them for the purposes of advertising, market research and/or demand-oriented design of its website. You have the right to object to the creation of these user profiles, whereby you must contact Google Inc. to exercise this right. For more information about the purpose and scope of data collection and processing by Google, Inc., please contact www.google.at/intl/de/policies/privacy/. We do not process the affected data.

17 YOUTUBE-VIDEOS

We have embedded YouTube videos on our website, which are stored on "www.youtube.com" and can be played directly from our website. These are all embedded in the so-called "extended data protection mode", which means that no data about you as a user is transmitted to YouTube if you do not play the videos. Only when you play the videos are YouTube cookies stored on your terminal device and data transmitted to Google Ireland Limited, Gordon House, Barrow Street, Dublin 4, Ireland, as YouTube operator. When playing videos stored on YouTube, at least the following data is transmitted to Google Ireland Limited: IP address and cookie ID, the specific address of the page called up from us, the language setting of the browser, the system date and time of the call-up and the identifier of your browser.

The data transfer takes place regardless of whether you have a user account with Google, via which you are logged in, or whether there is no user account for you. If you are logged in, this data is directly assigned to your account. If you do not want the assignment to your profile, you must log out before activating the button. YouTube or Google Ireland Limited stores this data as usage profiles and uses it for purposes of advertising, market research and/or demand-oriented design of its website. Such an evaluation is carried out in particular (also for users who are not logged in) for the provision of needs-based advertising and to inform other users about your activities on our website. You have the right to object to the creation of these user profiles, and to exercise this right you must contact Google Ireland Limited as the operator of YouTube.

For more information on the purpose and scope of data collection and its processing by Google Ireland Limited, please visit www.google.at/intl/de/policies/privacy. We do not process the data concerned.

18 RECORD ON THE WEB SERVER

Every time a user accesses our website and every time a file is retrieved or attempted to be retrieved from the server, data about this process is stored in a log file on the server. It is not directly traceable for us which user has retrieved which data. We also do not attempt to collect this information. This would only be possible in legally regulated cases and with the help of third parties (e.g. Internet service providers). In detail, the following data record is stored on the server about each retrieval: The IP address, the name of the retrieved file, the date and time of the retrieval, the amount of data transferred, the message whether the retrieval was successful, as well as the message why a retrieval may have failed, the name of your Internet service provider, if applicable, the operating system, the browser software of your computer and the website from which you visit us.

The legal basis for any processing of this personal data is our legitimate interest (Art. 6 para. 1 lit. f DSGVO). This is to be able to detect, prevent and investigate attacks on our website.

In addition, we process your personal data in special cases due to the legitimate interests of us or legal third parties in legal prosecution (Art. 6 para. 1 lit. f DSGVO) or by order of legally authorized authorities or courts (Art. 6 para. 1 lit. c DSGVO).

We generally store data for a period of three months to ensure the security of our website. Longer storage only takes place insofar as this is necessary to investigate detected attacks on our website or to pursue legal claims.

19 COOKIE BLOCKER INFORMATION

Cookies can be blocked, disabled or deleted. There are a variety of tools available to you to do this (including browser controls and settings). Information on this can be found in the help section of the web browser you are using. If you deactivate all cookies used by us, the display of the website may be restricted, for example.