Privacy Policy

Last updated: October 2025

Safe Labs GmbH, Unter den Linden 10, 10117 Berlin (hereinafter “**Safe Labs**”, “**we**” or “**us**”) takes the protection of personal data very seriously.

We treat personal data confidentially and always in accordance with Regulation (EU) 2016/679 (hereinafter “**General Data Protection Regulation**” or “**GDPR**”), the German Federal Data Protection Act (hereinafter “**BDSG**”), and in accordance with the provisions of this Privacy Policy.

The aim of this Privacy Policy is to inform you (hereinafter “**Data Subject**” or “**you**”) in accordance with GDPR Art.12 et seq. about how we process your personal data and for what purposes we process your personal data when using our website https://safe.global/ and other websites we own and operate (hereinafter “**Website**” and together “**Websites**”) as well as our mobile applications, services or contacting us.

Unless otherwise stated in this Privacy Policy, the terms used here have the meaning as defined in the GDPR.

Table of Contents

1. Glossary

What do some of the capitalized terms mean in this policy?

1. “**Blockchain**” means a mathematically secured consensus ledger such as the Ethereum Virtual Machine, an Ethereum Virtual Machine compatible validation mechanism, or other decentralized validation mechanisms.
2. “**Transaction**” means a change to the data set through a new entry in the continuous Blockchain.
3. “**Smart Contract**” is a piece of source code deployed as an application on the Blockchain which can be executed, including self-execution of Transactions as well as execution triggered by 3rd parties.
4. “**Token**” is a digital asset transferred in a Transaction, including ETH, ERC20, ERC721 and ERC1155 tokens.
5. “**Wallet**” is a cryptographic storage solution permitting you to store cryptographic assets by correlation of a (i) Public Key and (ii) a Private Key or a Smart Contract to receive, manage and send Tokens.
6. “**Recovery Phrase**” is a series of secret words used to generate one or more Private Keys and derived Public Keys.
7. “**Public Ke**y” is a unique sequence of numbers and letters within the Blockchain to distinguish the network participants from each other.
8. “**Private Key**” is a unique sequence of numbers and/or letters required to initiate a Blockchain Transaction and should only be known by the legal owner of the Wallet.
9. “**Safe Account**” is a modular, self-custodial (i.e. not supervised by us) smart contract-based Wallet. Safe Accounts are **open-source** released under LGPL-3.0.
10. “**Safe Interfaces**” refers to Safe{Wallet} a web-based graphical user interface for Safe Accounts as well as a mobile application on Android and iOS.
11. “**Safe Account Transaction**” is a Transaction of a Safe Account, authorized by a user, typically via their Wallet.
12. “**Profile**” means the Public Key and user provided, human readable label stored locally on the user's device.

2. Your information and the Blockchain

Blockchains, also known as distributed ledger technology (or simply “DLT”), are made up of digitally recorded data in a chain of packages called “blocks”. The manner in which these blocks are linked is chronological, meaning that the data is very difficult to alter once recorded. Since the ledger may be

distributed all over the world (across several “nodes” which usually replicate the ledger) this means there is no single person making decisions or otherwise administering the system (such as an operator of a cloud computing system), and that there is no centralized place where it is located either.

Accordingly, by design, records of a Blockchain cannot be changed or deleted and are said to be “immutable”. This affects your ability to exercise your rights such as your right to erasure (“right to be forgotten”), or your rights to object or restrict processing of your personal data because data on the Blockchain cannot be erased and cannot be changed. Although smart contracts may be used to revoke certain access rights, and some content may be made invisible to others, it is not deleted.

In certain circumstances, in order to comply with our contractual obligations to you (such as delivery of Tokens) it will be necessary to write certain personal data, such as your Wallet address, onto the Blockchain; this is done through a smart contract and requires you to execute such transactions using your Wallet’s Private Key.

In most cases ultimate decisions to (i) transact on the Blockchain using your Wallet, as well as (ii) share the Public Key relating to your Wallet with anyone (including us) rests with you.

IF YOU WANT TO ENSURE YOUR PRIVACY RIGHTS ARE NOT AFFECTED IN ANY WAY, YOU SHOULD NOT TRANSACT ON BLOCKCHAINS AS CERTAIN RIGHTS MAY NOT BE FULLY AVAILABLE OR EXERCISABLE BY YOU OR US DUE TO THE TECHNOLOGICAL INFRASTRUCTURE OF THE BLOCKCHAIN. IN PARTICULAR THE BLOCKCHAIN IS AVAILABLE TO THE PUBLIC AND ANY PERSONAL DATA SHARED ON THE BLOCKCHAIN WILL BECOME PUBLICLY AVAILABLE.

3. How we use personal data

3.1. When visiting our Website and using Safe Interfaces

When visiting our Website or using Safe Interfaces, we will collect and process personal data. Such personal data will be stored in different instances

1. We connect the Wallet to the web Safe{Wallet} app to identify the user via their public Wallet address. For this purpose we process:

    1. public Wallet address, and
    2. WalletConnect connection data.

2. When you create a new Safe Account we process the following personal data to compose a Transaction based on your entered data to be approved by your Wallet:

    1. your public Wallet address,
    2. account balance,
    3. smart contract address of your Safe Account,
    4. addresses of externally owned accounts, and
    5. user activity.

3. When you create a Profile for a new Safe Account we process the following personal data for the purpose of enabling you to view your Safe Account after creation as well as enabling you to view all co-owned Safes Accounts:

    1. your public Wallet address, and
    2. account balance.

4. When you create a Profile for an existing Safe Account for the purpose of allowing you to view and use them in the Safe Interface, we process your

    1. public Wallet address,
    2. Safe Account balance,
    3. smart contract address of the Safe Account, and
    4. Safe Account owner's public Wallet addresses.

5. When you initiate a Safe Account Transaction we process the following personal data to compose the Transaction for you based on your entered personal data:

    1. your public Wallet address, and
    2. smart contract address of Safe Account.

6. When you sign a Safe Account Transaction we process the following personal data to enable you to sign the Transaction using your Wallet:

1. Safe Account balance,
2. smart contract address of Safe Account, and
3. Safe Account owner's public Wallet addresses.

7. To enable you to execute the Transaction on the Blockchain we process:

    1. your public Wallet address,
    2. Safe Account balance,
    3. smart contract address of Safe Account,
    4. Safe Account owner's public Wallet addresses, and
    5. Transactions signed by all Safe Account owners.

8. When we collect relevant personal data from the Blockchain to display context information in the Safe Interface we process:

    1. your public Wallet address,
    2. account balance,
    3. account activity, and
    4. Safe Account owner's Public wallet addresses.

9. When we decode Transactions from the Blockchain for the purpose of providing Transaction information in a conveniently readable format, we process:

    1. your public Wallet address,
    2. account balance, and
    3. account activity.

10. When we maintain a user profile to provide you with a good user experience through Profiles and an address book we process:

    1. your public Wallet address,
    2. label,
    3. smart contract address of Safe Account,
    4. Safe Account owner's public wallet addresses,
    5. last used Wallet (for automatic reconnect),
    6. last used chain id,
    7. selected currency,
    8. theme, and
    9. address format.

The legal base for all these activities is the performance of the contract we have with you (GDPR Art. 6.1b).

THE PERSONAL DATA WILL BE STORED ON THE BLOCKCHAIN. GIVEN THE TECHNOLOGICAL DESIGN OF THE BLOCKCHAIN, AS EXPLAINED IN SECTION 2, THIS PERSONAL DATA WILL BECOME PUBLIC AND IT WILL NOT LIKELY BE POSSIBLE TO DELETE OR CHANGE THE PERSONAL DATA AT ANY GIVEN TIME.

3.2. Tracking and analysis

3.2.1 We will process the following personal data to analyze your behavior:

1. IP address (will not be stored for EU users),
2. session tracking,
3. user behavior,
4. wallet type,
5. Safe Account address,
6. Signer wallet address,
7. device and browser user agent,
8. user consent,
9. operating system,
10. referrers, and
11. user behavior: subpage, duration, and revisit, the date and time of access.

The collected personal data is solely used in the legitimate interest of improving our services and user experience. Such personal data is stored only temporarily and is deleted after 14 months.

We do not track any of the following data:

1. wallet signatures, and
2. granular transaction details.

In the case you have given consent, we will additionally store an analytics cookie on your device to identify you as a user across browsing sessions. The lawful basis for this processing is your prior consent (GDPR Art.6.1a) when agreeing to accept cookies. You can revoke your consent at any time with effect for the future via the cookie banner. The withdrawal of your consent does not affect the lawfulness of processing based on your consent before its withdrawal.

3.2.2 For general operational analysis of the Safe{Wallet} app interface, monitoring transaction origins and measuring transaction failure rates to ensure improved service performance and reliability, we process information which constitutes the transaction service database, such as:

1. signatures,
2. signature_type,
3. ethereum_tx_id,
4. message_hash,
5. safe_app_id, and
6. safe_message_id.

We conduct this analysis in our legitimate interest to continuously improve our services and ensure increased service performance and reliability (GDPR Art.6.1f).

3.2.3 We conduct technical monitoring of your activity on the platform in order to ensure availability, integrity and robustness of the service. For this purpose, we process your:

1. IP addresses,
2. meta and communication data,
3. website access, and
4. log data.

The lawful basis for this processing is our legitimate interest (GDPR Art.6.1f) in ensuring the correctness of the service.

3.2.4 Anonymized tracking

We will anonymize the following personal data to gather anonymous user statistics on your browsing behavior on our website:

1. daily active users,
2. new users acquired from a specific campaign,
3. user journeys,
4. number of users per country, and
5. difference in user behavior between mobile vs. web visitors.

The lawful basis for this processing is our legitimate interest (GDPR Art.6.1f) in improving our services and user experience.

3.3. When participating in user experience research (UXR)

When you participate in our user experience research we may collect and process some personal data. Such personal data may include:

1. your name,
2. your e-mail,
3. your phone type,
4. your occupation, and
5. range of managed funds.

In addition, we may take a recording of you while testing the Safe Interfaces for internal and external use. The basis for this collection and processing is our legitimate business interest in monitoring and improving our services.

The lawful basis for this processing is your informed consent (GDPR Art.6.1f) as provided before participating in user experience research. You can revoke your consent at any time with effect for the future by email to privacy@safe.global. The withdrawal of your consent does not affect the lawfulness of processing based on your consent before its withdrawal.

3.4. Downloading the Safe{Mobile} app

3.4.1 Downloading the Safe{Mobile} app on Google Play Store.

We process the following information to enable you to download the Safe{Wallet} app on smartphones running Android:

1. google account, and
2. e-mail address.

3.4.2 Downloading the Safe{Mobile} app on Apple App Store

We process the following information to enable you to download the Safe{Mobile} app on smartphones running iOS:

1. apple account, and
2. e-mail address.

The lawful basis for these two processing activities is the performance of the contract we have with you (GDPR Art.6.1b).

3.5. Use of the Safe{Mobile} app

3.5.1 We provide the Safe{Mobile} app to you to enable you to use it. For this purpose we process your:

1. mobile device information,
2. http request caches, and
3. http request cookies.

3.5.2 In order to update you about changes in the Safe{Mobile} app, we need to send you push notifications. For this purpose we process your:

1. Transactions executed and failed,
2. assets sent, and
3. assets received.

3.5.3 To provide support to you and notify you about outage resulting in unavailability of the service, we process your:

1. pseudonymized user identifier.

3.5.4 In order to provide remote client configuration and control whether to inform about, recommend or force you to update your Safe{Mobile} app or enable/disable certain Safe{Mobile} app features we process your:

1. user agent,
2. Safe{Mobile} app information (version, build number etc.),
3. language,
4. country,
5. platform,
6. operating system,
7. browser,
8. device category,
9. user audience,
10. user property,
11. user in random percentage,
12. imported segment,
13. date/time,
14. first open, and
15. installation ID.

For all these activities (3.5.1-3.5.4) we rely on the legal base of performance of a contract (GDPR Art.6.1b) with you.

3.5.5 To report errors and improve user experience we process your:

1. user agent info (Browser, OS, device),
1. URL that you were on (can contain Safe Account address), and
2. error info: time, stacktrace.

We rely on our legitimate interest (GDPR Art.6.1f) of ensuring our service quality.

3.5.6 We process your personal data to allow you to authenticate using your gmail account or AppleID and to create a signer wallet/owner account. For that purpose following personal data is processed:

1. anonymised device information and identifiers, e.g. IP address, cookie IDs, device type,
2. user account authentication information (e.g. username, password),
3. unique user identifier (e.g. a random string associated with authentication, at times can be email. If so, sensitive strings are processed but hashed and not stored), and
4. connection and usage information (e.g. logins to the application).

For this processing, we rely on our legitimate interest (GDPR Art.6.1f) of facilitating the onboarding for users and ameliorating the user experience with regards to our services.

3.5.7 Providing on and off-ramp services to enable you to top up your Safe Account with e.g. bank transfer, debit card, credit card. For this purpose MoonPay may process your:

1. full name,
2. date of birth,
3. nationality,
4. gender,
5. signature,
6. utility bills,
7. photographs,
8. phone number,
9. home address,

10. email,
11. information about the transactions you make via MoonPay services (e.g. name of the recipient, your name, the amount, and/or timestamp),
12. geo location/tracking details,
13. operating system, and
14. personal IP addresses.

To conduct this activity we rely on our legitimate interest (GDPR Art.6.1f) of ameliorating the onboarding process and the user experience through providing an easier option to customers to fund their account.

3.5.8 Geofencing users in the US to prevent locking safe tokens, which may result in them being classified as securities. For this purpose, we process the following information relating to a user's device:

1. operating system,
2. browser and browser configuration,
3. IP address, and
4. approximate location.

We rely on our legitimate interest to ensure that our services or derivatives do not extend into sectors in which we are not licensed to operate in (GDPR Art.6.1f). Safe Labs is not licensed to provide or trade securities in the US and therefore cannot operate in the securities market.

3.5.9 We process personal data to detect use of VPN aimed at circumventing the restriction in section 3.5.8 above and to prevent fraud. Personal data processed include:

1. operating system,
2. browser and browser configuration,
3. IP address, and
4. approximate location.

We rely on our legitimate interest to ensure the prevention of fraud (GDPR Art.6.1f). This also helps us detect users who may want to circumvent the restriction on US users by the use of VPN.

3.6. Contacting us

It is possible to contact us on our Website by e-mail or via the contact form. When you contact us, we collect and process certain information in connection with your specific request, such as, *e.g.*, your name, e-mail address, and other data requested by us or personal data you voluntarily provide to us (hereinafter "**Contact Data**"). If you contact us as part of an existing contractual relationship or contact us in advance for information about our range of services, the Contact Data will be processed for the performance of a contract or in order to take steps prior to entering into a contract and to respond to your contact request in accordance with GDPR Art.6.1.b.

Otherwise, the legal basis for the processing of Contact Data is GDPR Art.6.1.f. The Contact Data is processed to pursue our legitimate interests in responding appropriately to customer/contact inquiries.

4. Data receivers

We may transfer your personal data to our business partners, administration centers, third party service providers, agents, subcontractors and other associated organizations for the purposes of completing tasks and providing our services to you.

In addition, we might transfer your personal data to certain data receivers if such transfer is necessary to fulfill our contractual and legal obligations.

In individual cases, we transfer personal data to our consultants in legal or tax matters, whereby these recipients act independently in their own data protection responsibilities and are also obliged to comply with the requirements of the GDPR and other applicable data protection regulations. In addition, they are bound by special confidentiality and secrecy obligations due to their professional position.

In the event of corporate transactions *(e.g.*, sale of our business or a part of it) or as part of any business restructuring or reorganization, we may transfer personal data to involved advisors or to potential buyers.

Additionally, we also use services provided by various specialized companies, *e.g.*, IT service providers, that process personal data on our behalf ("**Data Processor**"). We have concluded a data processing agreement according to GDPR Art.28 or EU standard contractual clauses of the EU Commission pursuant to GDPR Art.46.2.c with each service provider and they only process personal data in accordance with our instructions and not for their own purposes.

5. Use of Subprocessors

5.1. Blockchain

When using Safe Accounts your smart contract address, Safe Account Transactions, addresses of signer accounts and ETH balances and token balances will be stored on the Blockchain. See section 2 of this Policy

THE INFORMATION WILL BE DISPLAYED PERMANENTLY AND PUBLIC, THIS IS PART OF THE NATURE OF THE BLOCKCHAIN. IF YOU ARE NEW TO THIS FIELD, WE HIGHLY RECOMMEND INFORMING YOURSELF ABOUT THE BLOCKCHAIN TECHNOLOGY BEFORE USING OUR SERVICES.

5.2. Amazon Web Services

We use **Amazon Web Services (AWS)** to store log and database data as described in section 5.1.

5.3. Datadog

We use **Datadog** to store log data as described in section 5.1.

5.4. Mobile app stores

Safe{Mobile} mobile apps are distributed via **Apple AppStore** and **Google Play Store**. They most likely track user behavior when downloading apps from their stores as well as when using apps. We only have very limited access to that data. We can view aggregated statistics on installs and

uninstalls. Grouping by device type, app version, language, carrier and country is possible.

5.5. Fingerprint/Touch ID/ Face ID

We enable the user to unlock the Safe{Mobile} app via biometrics information (touch ID or face ID). This is a feature of the operating system. We do not store any of this data. Instead, the API of the operating system is used to validate the user input. If you have any further questions you should consult with your preferred mobile device provider or manufacturer.

5.6. Google Firebase

We use the following **Google Firebase** services:

- Firebase Cloud Messaging: Provide updates to the user about changes in the mobile apps via push notifications.
- Firebase remote config: Inform users about, recommend or force user to update their mobile app or enabling/disabling certain app features. These settings are global for all users, no personalization is happening.
- Firebase crash reporting: Report errors and crashes to improve our services and user experience.

5.7. WalletConnect

WalletConnect is used to connect wallets to dapps using end-to-end encryption by scanning a QR code. We do not store any information collected by WalletConnect.

5.8. Sentry

We use **Sentry** to collect error reports and crashes to improve our services and user experience.

5.9. Beamer

We use **Beamer** providing updates to the user about changes in the app.Beamer's purpose and function are further explained under the following link **https://www.getbeamer.com/showcase/notification-center**.

We do not store any information collected by Beamer.

5.10. Node providers

We use **Infura** and **Nodereal** to query public blockchain data from our backend services. All Safes are monitored, no personalization is happening and no user IP addresses are forwarded. Personal data processed are:

- your smart contract address of the Safe,
- transaction id/hash, and
- Transaction data.

5.11. Tenderly

We use **Tenderly** to simulate blockchain transactions before they are executed. For that we send your smart contract address of your Safe Account and transaction data to Tenderly.

1. Internal communication

We use the following tools for internal communication.

- **Slack**
- **Google Workspace**
- **Notion**

5.12. MoonPay

We use MoonPay to offer on-ramp and off-ramp services. For that purpose personal data is required for KYC/AML or other financial regulatory requirements. This data is encrypted by MoonPay.

5.13. Spindl

We use **Spindl**, a measurement and attribution solution for web3 that assists us in comprehending how users interact with different decentralized applications and our Safe{Mobile} app and to enhance your experience with Safe{Wallet}. For enhanced privacy, data is stored for a period of 7 days after which it is securely deleted.

5.14. Fingerprint

This tool enables the processing in sections 3.5.8 and 3.5.9.

6. Personal data transfers to third countries

Wherever possible we will choose service providers based in the European Economic Area ("**EEA**"). However, it may also be necessary for personal data to be transferred to recipients located outside the EEA, *i.e.*, to third countries, such as the USA. If possible, we conclude the currently applicable EU standard contractual clauses of the EU Commission pursuant to GDPR Art.46.2.c with all processors located outside the EEA. Otherwise, we ensure that a transfer only takes place if an adequacy decision exists with the respective third country and the recipient is certified under this, if necessary. We will provide you with respective documentation on request.

HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS EXPLAINED ABOVE IN THIS POLICY, THE BLOCKCHAIN IS A GLOBAL DECENTRALIZED PUBLIC NETWORK AND ACCORDINGLY ANY PERSONAL DATA WRITTEN ONTO THE BLOCKCHAIN MAY BE TRANSFERRED AND STORED ACROSS THE GLOBE.

7. Automated decision-making/profiling

We do not use automatic decision-making or profiling within the meaning of GDPR Art.22.1 when processing personal data.

8. Obligation to provide personal data

When you visit our Websites, use our mobile applications, services or contact us you may be required to provide us with certain personal data as described in this Privacy Policy. Beyond that, you are under no obligation to provide us with personal data. However, if you do not provide us with your personal data as required, you may not be able to contact us and/or we may not be able to contact you to respond to your inquiries or questions.

9. Storing personal data

We retain your information only for as long as is necessary for the purposes for which we process the information as set out in this Privacy Policy. However, we may retain your personal data for a longer period of time where such retention is necessary for compliance with a legal obligation to which we are subject, or in order to protect your vital interests or the vital interests of another natural person.

10. Your rights as a data subject

The following rights are available to you as a Data Subject in accordance with the provisions of the GDPR. If you wish to exercise your Data Subject rights, please contact us by post or at privacy@safe.global.

Right of access

Under the conditions of GDPR Art.15 you have the right to request confirmation from us at any time as to whether we are processing personal data relating to you. If this is the case, you also have the right within the scope of GDPR Art.15 to receive access to the personal data as well as certain other information about the personal data and a copy of your personal data. The restrictions of BDSG §34 apply.

Right to rectification

Under the conditions of GDPR Art.16 you have the right to request us to correct the personal data stored about you if it is inaccurate or incomplete.

Right to erasure (right to be ‘forgotten’)

You have the right, under the conditions of GDPR Art.17, to demand that we delete the personal data concerning you without delay. The restrictions of BDSG §35 apply.

HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN WE MAY NOT BE ABLE TO ENSURE THAT YOUR PERSONAL DATA IS DELETED. THIS IS BECAUSE THE BLOCKCHAIN IS A PUBLIC DECENTRALIZED NETWORK AND BLOCKCHAIN TECHNOLOGY DOES NOT GENERALLY ALLOW FOR DATA TO BE DELETED AND YOUR RIGHT TO ERASURE MAY NOT BE ABLE TO BE FULLY ENFORCED. IN THESE

CIRCUMSTANCES WE WILL ONLY BE ABLE TO ENSURE THAT ALL PERSONAL DATA THAT IS HELD BY US IS PERMANENTLY DELETED.

Right to restrict processing

You have the right to request that we restrict the processing of your personal data under the conditions of GDPR Art.18.

Right to object

You have the right to object to the processing of your personal data under the conditions of GDPR Art.21.

HOWEVER, WHEN INTERACTING WITH THE BLOCKCHAIN, AS IT IS A PUBLIC DECENTRALIZED NETWORK, WE WILL LIKELY NOT BE ABLE TO PREVENT EXTERNAL PARTIES FROM PROCESSING ANY PERSONAL DATA WHICH HAS BEEN WRITTEN ONTO THE BLOCKCHAIN. IN THESE CIRCUMSTANCES WE WILL USE OUR REASONABLE ENDEAVORS TO ENSURE THAT ALL PROCESSING OF PERSONAL DATA HELD BY US IS RESTRICTED, NOTWITHSTANDING THIS, YOUR RIGHT TO RESTRICT TO PROCESSING MAY NOT BE ABLE TO BE FULLY ENFORCED.

Right to data portability

You have the right, under the conditions of GDPR Art.20, to request that we hand over, in a structured, common and machine-readable format, the personal data concerning you that you have provided to us. Please note that this right only applies where the processing is based on your consent, or a contract and the processing is carried out by automated means.

Right to object to direct marketing (‘opting out’)

You have a choice about whether or not you wish to receive information from us. We will not contact you for marketing purposes unless:

- you have a business relationship with us, and we rely on our legitimate interests as the lawful basis for processing (as described above)
- you have otherwise given your prior consent (such as when you download one of our guides)

You can change your marketing preferences at any time by contacting us on the above details. On each and every marketing communication, we will

always provide the option for you to exercise your right to object to the processing of your personal data for marketing purposes (known as ‘opting-out’) by clicking on the ‘unsubscribe’ button on our marketing emails or choosing a similar opt-out option on any forms we use to collect your data. You may also opt-out at any time by contacting us on the below details.

Please note that any administrative or service-related communications (to offer our services, or notify you of an update to this Privacy Policy or applicable terms of business, etc.) will solely be directed at our clients or business partners, and such communications generally do not offer an option to unsubscribe as they are necessary to provide the services requested. Therefore, please be aware that your ability to opt-out from receiving marketing and promotional materials does not change our right to contact you regarding your use of our website or as part of a contractual relationship we may have with you.

Right of revocation

You may revoke your consent to the processing of your personal data at any time pursuant to GDPR Art.7.3. Please note, that the revocation is only effective for the future. Processing that took place before the revocation remains unaffected.

Right to complain to a supervisory authority

Subject to the requirements of GDPR Art.77, you have the right to file a complaint with a competent supervisory authority. As a rule, the data subject may contact the supervisory authority of his or her habitual residence or place of work or place of the alleged infringement or the registered office of Safe Labs. The supervisory authority responsible for Safe Labs is the Berliner Beauftragte für Datenschutz und Informationsfreiheit. A list of all German supervisory authorities and their contact details can be found here.

11. Changes to this Privacy Policy

We may modify this Privacy Policy at any time to comply with legal requirements as well as developments within our organization. When we do, we will revise the date at the top of this page. We encourage you to regularly review our Privacy Policy to stay informed about our Privacy Policy. The current version of the privacy notice can be accessed at any time at https://app.safe.global/privacy.

12. Contact us

Contact us by post or e-mail at:
Safe Labs GmbH
Unter den Linden 10
10117 Berlin

10115 Berlin, Germany
privacy@safe.global

Contact our Data Protection Officer by post or e-mail at:

TechGDPR DPC GmbH
Willy-Brandt-Platz 2
12529 Berlin-Schönefeld
Germany
privacy@safe.global

***