

Data Privacy and Cookie Policy

[\(Click for German version\)](#)

Content

1	Introduction	1
2	Personal data collected from data subjects	1
3	Personal data collected from other sources	2
4	Browsing Moss Websites	2
5	Purposes of and legal basis for processing personal data	2
6	Storage period.....	3
7	Disclosure to recipients or third parties	3
8	Data processing in the EU/EEA and UK; exceptions	4
9	Automated processing.....	4
10	Protection of personal data.....	4
11	Overview of rights	4

1 Introduction

1.1 Identity and contact details of the controller. Nufin GmbH, Saarbrücker Str. 37A, 10405 Berlin, Germany (together with its affiliated companies within the meaning of sections 15 et seq. German Stock Corporation Act (AktG) involved in providing our products and services, including, without limitation, Moss GmbH, Saarbrücker Str. 38, 10405 Berlin, Germany, "**Moss**", "**we**", "**our**", and "**us**") takes all legally required measures to protect personal data. Our data protection officer can be contacted at the postal address above or by e-mail (datenschutz@getmoss.com / privacy@getmoss.com).

1.2 Scope. We provide corporate card and expense management solutions exclusively to corporate customers, but these services will be used by natural persons. As a result, we process both company data and personal data. As our products and services may be available in the European Union (EU), the European Economic Area (EEA) or within the United Kingdom (UK), we process personal data in accordance with applicable data protection laws and this Data Privacy and Cookie Policy (the "**Policy**"). We comply in particular with the European Regulation (EU) 2016/679 (GDPR). Terms defined in the GDPR have the same meaning in this Policy unless otherwise defined herein. Please note, that this Policy does not apply as far as our products and services are governed by distinct privacy policies or when services are managed by a company other than ours.

1.3 Content. In this Policy, we explain in particular how we process personal data when using our websites (the "**Moss Websites**"), our web application (the "**Moss Platform**") and our iOS or Android mobile application (the "**Moss Mobile App**"; the services provided through the Moss Websites, the Moss Platform and the Moss Mobile App jointly the "**Moss Platform Services**"). We also address the utilisation of cookies and similar website technologies (the "**Cookies**"). Please read this Policy carefully, as it applies to your use of the Moss Platform Services (accordingly, "**you**" or "**your**" refers to the relevant data subject interacting with us).

1.4 Role. As part of your interaction with and use of the Moss Platform Services, we process specific personal data as a controller. In this capacity, we determine the purposes and means of the processing of personal data (e.g. to comply with legal obligations, such as requirements to detect and prevent financial crime) as explained in this Policy. Where two or more entities from Moss are involved in the provision of our services, we may control the processing jointly or have agreed to specific regulations regarding the processing. Additionally, we also process personal data as a data processor for our customers. In this role, we process personal data as instructed and on the basis of a data processing agreement concluded separately with our customers.

1.5 Reference. Using the Moss Platform Services, you may share with us personal data concerning you or other natural persons (e.g. as a component of the Moss Platform Services or in the context of referring potential new customers). By doing so, you confirm that you have all necessary rights and permissions to share such personal data with us. If you provide us with information about other data subjects, please make sure that such data subjects are informed

about the processing of such data, if required by the applicable data protection laws. You can also refer to this Policy for this purpose.

1.6 Changes. This Policy updates and replaces any prior policy. We may change, modify or update this Policy at any time without prior notice to adapt it to legal and regulatory developments, including requirements of supervisory authorities and consequences from relevant case law, and to align it to new technical implementations, products, and services. A change will only affect the processing of personal data for the future, a reduction of the level of data protection below the legal requirements is excluded. You may access the current version of this Policy on Moss Websites.

1.7 Categories of personal data. We may process the following categories of personal data:

- Contact data (e.g. first and last name, email and postal addresses and phone numbers or profiles on social media, if applicable);
- Professional data (e.g. job title, role and employer and in the case of job applications curriculum vitae and a cover letter with references);
- Communication data (e.g. personal data used for or embedded in any kind of communication and interaction, including calls, chats, emails or attachments to such communications);
- Identity data (e.g. additional to contact data, date and place of birth, nationality and residence, digital representations of passport or other national ID or driving license, and any information on such documents or conveyed through our ID verification process);
- Financial data (e.g. personal data relating to any bank account information of a customer, including account numbers, account balance or transaction history or any other financial information we receive);
- Transaction data (e.g. personal data linked to the usage of corporate cards issued by us (the "**Moss Cards**"), including the respective card number, cardholder's name, issuance date, expiry date, CVC code, together with other transaction-related details like date, time, amount, currency, exchange rate, recipient particulars, merchant information, references, location, payment device, and payment method);
- Accounting data (e.g. personal data generated by using the Moss Platform and the Moss Mobile App to prepare and conduct accounting operations or information included in any process, approval and payment flow, attachment or file for this purpose, in particular budgets, roles, or reimbursement information such as travel expenses, receipts or invoices);
- User data (e.g. personal data related to a personal profile on the Moss Platform and the Moss Mobile App (the "**Moss Account**"), e.g. the respective UserID, optional profile pictures, mobile phone numbers, or user-defined addresses for sending physical cards, personal IBAN for reimbursements, etc.);
- Marketing data (e.g. personal data including contact preferences or webinar/event registrations, attendances, and participation information);
- Traffic data (e.g. personal data about the device or browser, data volume, date, time and duration of access, and reference to the specific Moss Platform Services or Cookie information).

2 Personal data collected from data subjects

We process personal data when data subjects interact with the Moss Platform Services. The personal data we process depends on the specific service used. This includes:

2.1 Job applications. We process personal data candidates provide to us in the process of applying for a job at Moss. Personal data may in this case include contact data, professional data and communication data, together with the respective employment and education history, transcripts, or references, and traffic data. The same applies to cases where we communicate with job applicants via phone, email, or other means of communication.

2.2 Webchat/other communication. If you communicate or interact with us, including calls, chat, email, we may process contact, professional, communication and traffic data.

2.3 Intro. Scheduling and participating in a personal or self-guided demonstration of the Moss Platform Services, we process contact and professional data from the data subject requesting such product demonstration (e.g. representatives of (potential) customers) and, in individual cases, additional communication and traffic data.

2.4 Customer application. During the onboarding of our customers, we process contact data, identity data and communication data of data subjects filling out an application form, acting on behalf

or duly representing potential customers, including managing directors, board members, authorised employees, freelancers, or other individuals. We also process financial data, including personal data within bank account information or information about the company structure provided by potential customers. In this context, we may also process contact data and identity data about the owners of the potential customer, including the beneficial owners and other individuals within the scope of our Know-Your-Customer (KYC) policies, as well as contact and professional data of employees, freelancers or other individuals associated with the potential customer.

2.5 User registration/login. We may process contact, professional and user data to personalise individual Moss Accounts. We also process account/login credentials, including passwords (hashed) and information for authentication and account access. When accessing and using the Moss Platform and Moss Mobile App, we also process traffic data.

2.6 Moss Cards/other services. When using Moss Cards, our invoice management or reimbursement service, our budgetary control or other services provided through the Moss Platform or the Moss Mobile App, we process financial, transaction and accounting data. In this context, we further process contact, professional and user data. This personal data might also be referenced to a Moss Card transaction. We also process communication and traffic data when you interact with other users through the Moss Platform or the Moss Mobile App (e.g. when you request Moss Cards, submit a request to the administrator to approve a transaction or to increase a spending limit on your Moss Card).

2.7 Notifications. We process contact data, professional data, financial data, transaction data, accounting data, user data and traffic data to inform you via emails, in-App updates, push notifications or reminders to keep you informed about your Moss Account, all transaction with your or your companies' Moss Cards, and other pertinent information regarding the Moss Platform Services. Some communications are personalised based on recent user behaviour, including your interaction with the Moss Platform Services (e.g. transactions), or recent events (e.g. when the limit of a card or a budget has been reached).

2.8 Customer support and success. When communicating with our customer support or success team, we process contact, professional, communication, user and traffic data. This also applies to any participation in our customer trainings or in customer surveys related to the Moss Platform Services.

2.9 Integrations. We may process contact data, identity data, financial data, transaction, or accounting data using integrations to connect the Moss Platform Services with third party services determined by the customer (e.g. financial institutions, payment service providers or business software integrations (accounting, HR systems or Single-Sign On (SSO) service providers)).

2.10 Marketing. We may process contact data, marketing data and traffic data related to your consent for the purpose of receiving marketing communications or, for example, if you request marketing material from Moss.

2.11 Newsletter. When you subscribe to our newsletters, we process contact data along with professional, communication and traffic data. To verify ownership of the email-address provided and consent, we send an automated confirmation email after receiving the subscription request (double opt-in). After verification your contact data is added to our internal newsletter distribution list.

3 Personal data collected from other sources

We may also process personal data collected from other sources. These sources include:

3.1 Customers. We process personal data provided by the customer for onboarding and delivering the Moss Platform Services. This includes contact data and identity data of the customer's representatives, including managing directors, board members, authorised employees, freelancers, or other individuals, irrespective of the legal form, and beneficial owners and other individuals within the scope of our Know-Your-Customer (KYC) policies. We also process contact, professional and user data when a customer adds you as a user of the Moss Platform or a cardholder of a Moss Card.

3.2 Financial institutions/merchants. We process contact data, identity data as well as financial, transaction and accounting

data from financial institutions (e.g. the card network provider of Moss Cards, banks, or other payment processors) or merchants when processing your Moss Card transactions.

3.3 Compliance service providers. We may process contact, professional, identity, financial, transaction and accounting data from identity verification providers, services for fraud and compliance monitoring as well as financial and business information providers during and after the onboarding of our customers.

3.4 Other services providers. We may also process contact, professional, financial, transaction and accounting data from other third party integrations or service providers in relation to the Moss Platform Services.

3.5 Publicly available sources. We process contact, professional, financial, and marketing data available on the media or public domains to identify potential customers and partners or conduct due diligence or other risk management activities for existing and potential customers.

4 Browsing Moss Websites

4.1 Log Data. Accessing and browsing Moss Websites, we may process traffic data.

4.2 Cookies. Cookies are small data files stored on a device that serve to re-identify the device. Session cookies expire when you stop browsing on Moss Websites. Persistent cookies remain on your device and can be managed through your browser settings. It's important to distinguish further between first-party cookies, exclusively set by us as the provider of Moss Websites, and third party cookies set by other parties that enable certain features or content on Moss Websites (such as advertising, interactive content, and social sharing). The latter can recognise your device when you visit Moss Websites and other websites with which such parties have partnered. Furthermore, Cookies as defined in this Policy include similar technologies like pixel tags, web beacons, mobile identifiers, or JavaScripts when used for the same purpose.

4.3 Consent management. The Cookies we are using can be divided into two categories: consent-free and consent-requiring. Our consent management platform, which is automatically displayed and accessible at any time on Moss Websites, allows to manage these Cookies. It additionally provides further information, including the scope of data processing by the respective services. You can revisit the consent management platform at any time for updates and control of your settings.

4.4 Essential Cookies. Cookies that do not require consent are those that are necessary for the safe and secure provision of the Moss Platform Services. For example, we can detect and analyse malfunctions or cyber-attacks on our resources and prevent our systems and data from being compromised.

4.5 Non-essential Cookies. Cookies requiring consent make visiting Moss Websites and using the Moss Platform Services more pleasant and user-friendly. As we strive to increase the attractiveness of the Moss Platform Services, we would like to customise our content and tailor the information displayed specifically to the respective user. Non-essential cookies also help us to monitor our advertisements. Cookies requiring consent also serve to statistically record, bug fixing and evaluate the use of Moss Platform Services.

5 Purposes of and legal basis for processing personal data

We process personal data to provide corporate card and expense management solutions that align closely with our customers' needs. This involves:

5.1 Providing services. We use all categories of personal data for providing product information and offering Moss Platform Services to our customers. Our objective is to leverage the technical capabilities of the Moss Platform Services, enabling various functionalities and executing specific business processes related to the management and control of Moss Cards issued to our customers. This includes in particular monitoring payment transactions in real-time, providing customers with comprehensive insights into their expenses incurred with Moss Cards and other tools. We utilise contact, professional, communication, and traffic data to personalise the Moss Platform Services, enhancing the user interface to deliver a customised service. We rely on our legitimate interest in providing Moss Platform Services to our customers (Article 6 (1) (f) GDPR) and

we acknowledge our customers' legitimate interests (Article 6 (1) (f) GDPR) in managing their corporate expenses, overseeing how corporate funds are utilised. To the extent the processing of your personal data is necessary to take steps prior to entering into or for the performance of a contract with you, the legal basis for the processing is Article 6 (1) (b) GDPR.

5.2 Improving services. With the exception of identity data, we process all categories of personal data to gain insights into the use of the Moss Platform Services. This analysis encompasses activities like testing, research, and statistical analysis and serves the purpose of identifying trends, enhancing and improving performance, and developing and modifying (new) products and services. We rely on our legitimate interest in the development, promotion, and improvement of Moss Platform Services, as well as identifying future business opportunities (Article 6 (1) (f) GDPR). We may further ask for your consent in this regard as the legal basis (Article 6 (1) (a) GDPR).

5.3 Security. We process all categories of personal data to uphold and guarantee the functionality and security of our information technology systems. This includes investigations and countermeasures for technical issues, the identification of suspicious activities, fraud detection, enforcement of terms and policies, and safeguarding the rights of our customers, partners, and ourselves. We rely on our legitimate interest in ensuring the safety and security of the Moss Platform Services (Article 6 (1) (f) GDPR). This encompasses our interest in protecting our rights and those of our customers, affirming our zero-tolerance stance against any engagement in illicit or criminal activities. We also prioritise security measures to prevent any interference or breaches that could compromise the confidentiality of the data we handle. To this extent the processing may also be necessary for the performance of a contract with your company (Article 6 (1) (b) GDPR). If such data is required for the documentation of our technical or organisational security measures, legal basis may also be Article 6 (1) (c) GDPR.

5.4 Compliance. We process all categories of personal data to fulfil our legal and regulatory obligations, including preventing and detecting crime and averting misuse of the Moss Platform Services. Our responsibilities extend to safeguarding against fraudulent, unauthorised, or illegal activities. Further, we process personal data to protect our legal rights and pursue remedies to mitigate financial losses, claims, liabilities, or other damages. This includes complying with judicial proceedings, court orders, legal processes, or lawful requests. In cases of complying with court orders and similar legal processes, we uphold transparency and make reasonable efforts to inform our customers and users of any disclosure of their personal data, unless prohibited by law, court order, or exigent circumstances. The legal basis for the processing of personal data for this purpose rests on compliance with our legal and regulatory obligations (Article 6 (1) (c) GDPR), as well as our legitimate interests (Article 6 (1) (f) GDPR). Processing of personal data may also be in the public interest pursuant to Article 6 (1) (e) GDPR (e.g. preventing or detecting terrorism financing, money laundering and other financial crimes).

5.5 Efficient support/communication. We use all categories of personal data for enhancing communication with our customers and users (e.g. for sending confirmations, updates or reminders, providing customer care and handling complaints, troubleshooting issues, addressing inquiries, identifying and investigating security and technical incidents and, if applicable, sending technical notices and security alerts) and enhancing the knowledge and training of our employees. Legal basis for processing personal data in this regard is our legitimate interest (Article 6 (1) (f) GDPR) and in some cases, compliance with our regulatory obligations (Article 6 (1) (c) GDPR). Processing may also be necessary for the performance of a contract with your company (Article 6 (1) (b) GDPR).

5.6 Marketing. We use contact, user and traffic data to properly implement and execute events or webinars or to communicate with our customers. Additionally, we process traffic data for the display of marketing campaigns. Legal basis is our legitimate interest (Article 6 (1) (f) GDPR) in marketing the Moss Platform Services. We further rely on your consent (Article 6 (1) (a) GDPR) for specific marketing communications.

5.7 Consent. We may process personal data with your consent (Article 6 (1) (a) GDPR) or, if applicable, section 26 German Federal Data Protection Act (BDSG). You can withdraw your consent at any time without affecting the lawfulness of any prior processing of personal data. For Cookies, managing consent is easily done through

the consent management platform available on Moss Websites. Within e-mails we provide an unsubscribe link for this purpose. If storing your consent is necessary for processing your personal data, the legal basis is Article 6 (1) (c) GDPR.

6 Storage period

6.1 General principle. Personal data will be deleted as soon as it is no longer needed for the intended purpose mentioned above, its legal basis for processing no longer applies and the applicable retention periods have expired.

6.2 Legal obligations. We are required to retain personal data to comply with legal obligations, including those outlined in regulatory, tax, commercial and civil laws such as the German Commercial Code (HGB) and the German Fiscal Code (AO). These obligations necessitate data retention periods ranging from two (2) to ten (10) full calendar years. Additionally, we may store data as required to preserve evidence in compliance with applicable limitation periods, such as sections 194 et seq. German Civil Code (BGB). In some cases, these retention periods can extend from three (3) to as long as thirty (30) years. Regarding data related to legal claims, we will delete this information once the claim is fully resolved, unless it is subject to longer retention periods (e.g. as specified in the German Commercial Code (HGB) or the German Fiscal Code (AO), among others).

6.3 Newsletter. Data collected for our newsletter will be retained only for the duration required to send the newsletter. Furthermore, if we choose to cease sending the subscribed newsletter, the data will be promptly deleted.

6.4 Cookies. Session cookies are automatically deleted at the end of your browser session. Persistent cookies remain on your device for a specific duration after your browser session concludes. Personal data related to Cookies is finally deleted when it is no longer necessary for processing purposes. You can find detailed information about the retention periods for individual Cookies on our consent management platform, accessible on Moss Websites at any time.

6.5 Termination. If a customer terminates its contract with Moss, it results in the permanent loss of access to the Moss Account and associated personal data. Nevertheless, personal data may still be retained by us, but only when necessary to comply with legal obligations, fulfil contractual commitments, or conduct legitimate business activities.

7 Disclosure to recipients or third parties

7.1 General principle. In all cases, we ensure that data recipients or third parties only access personal data necessary for specific tasks to provide our customers with the best Moss Platform Services. We never sell your personal data to data recipients or third parties under any circumstances.

7.2 Moss Group. We may share all categories of personal data with our subsidiaries to enhance our customers' experience by providing and improving the Moss Platform Services, for marketing purposes, internal reporting, or when these subsidiary companies offer services to us.

7.3 External service providers. We partner with external services providers and may share personal data as specified above to fulfil contractual obligations to our customers and to ensure the security of our systems. These include, for example, our corporate card network, payment processors and other financial service providers, including services to comply with our regulatory obligations (e.g. identity verification providers or services for compliance monitoring). Such service providers also include technical services providers, for example, IT infrastructure and security providers such as hosting and cloud providers, or other data recipients or third parties such as accounting and expense integrators and solutions, services for customer communication and (technical) support, or data analytics tools. For job applications, we use software services to manage and optimise our recruiting and hiring processes. External service providers may also include advertising agencies and advertising technology providers with whom we share marketing data. Where processing of personal data is carried out on our behalf and at our instructions, personal data will only be transferred to external service providers as processors in accordance with Article 28 GDPR.

7.4 Public bodies and institutions. We may disclose all categories of personal data on request by law enforcement agencies, courts, or regulatory authorities, in full compliance with relevant laws.

7.5 **Fraud prevention.** Personal data may be exchanged between us and fraud prevention agencies, and if required, with law enforcement agencies for the purpose of detecting, investigating, and preventing crimes.

8 Data processing in the EU/EEA and UK; exceptions

The processing of personal data generally takes place within the member states of the EU/EEA and UK when Moss Platform Services are used there. We may transfer personal data to contractual and business partners in third countries (subject to the European Commission's adequacy decision or agreed standard contractual clauses) if necessary to execute orders of our customers, provide our products or services, or as required by law. We transmit a copy of these standard contractual clauses on request by the data subject.

9 Automated processing

In general, we do not take decisions based solely on automated individual decision-making and profiling within the meaning of Article 22 GDPR. Should we use such processes, we will inform about this separately and as required by law.

10 Protection of personal data

10.1 **Security.** We store personal data within highly secure networks, accessible solely by a designated group of our employees with specific access permissions. All employees are bound by strict confidentiality and data secrecy obligations. They also undergo comprehensive training and authorisation procedures. Additionally, we enforce robust technical and organisational safeguards to protect personal data against loss or any unauthorised processing.

10.2 **Data Breach.** In the event of a data breach, we will promptly notify the competent supervisory authority and any affected data subjects, without undue delay, and within the timeline set by the GDPR. This notification will be made as soon as practically possible unless the breach is unlikely to pose a risk to the rights and freedoms of natural persons. We will thoroughly document all data breaches, including pertinent details about the breach, its consequences, and the corrective measures implemented.

11 Overview of rights

11.1 **Rights.** In addition to the right to withdraw your consent at any time (Article 7 (3) GDPR), you are entitled to the following rights, subject to respective legal requirements:

- Right of access (Article 15 GDPR);
- Right to rectification (Article 16 GDPR);
- Right to erasure ('right to be forgotten') (Article 17 GDPR);
- Right to restriction of processing (Article 18 GDPR);
- Right to data portability (Article 20 GDPR);
- Right to object (Article 21 GDPR).

11.2 **Exercise.** To exercise your rights, you can contact our Data Protection Office at the address given in Section 1.1 of this Policy. In addition, you may contact or lodge a complaint with the competent supervisory authority (Article 77 GDPR).

11.3 **Contacting customer.** If personal data has been processed by us as a processor on behalf of our customers, and you intend to exercise your rights related to such data, please reach out directly to the relevant customer. If you prefer to contact us directly, kindly specify the name of the customer for whom we processed your personal data. We will then forward your request to our customer and assist them in responding to your request as required by applicable law.

11.4 **Continuance of processing.** Please be aware that we may continue processing personal data despite a request to the contrary, to comply with legal obligations and/or in accordance protect our legitimate interests if permitted by law. These purposes may include resolving disputes, preventing fraud and financial crimes, enforcing our contractual rights, and adhering to legal retention obligations.