

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

Privacy Policy

Effective Date 08 December, 2025

Introduction

Netmore Group AB (including all its subsidiaries, collectively “Netmore” or “we”) is responsible for the processing of personal data within the company and its subsidiaries. Netmore is committed to protecting personal privacy and always processes personal data with a high level of protection, in accordance with applicable data protection laws and regulations. For operations in the European Union (EU), we comply with the EU General Data Protection Regulation (GDPR), formally Regulation (EU) 2016/679. This policy describes what personal data we process about you, the purposes of processing, and your rights. It applies globally and includes region-specific provisions for the EU (GDPR), the United Kingdom (UK GDPR and Data Protection Act 2018), the United States, Brazil (*Lei Geral de Proteção de Dados – LGPD*), and Indonesia (Personal Data Protection Law).

Personal Information We Collect

We process personal data that you as a customer, supplier, or user provide to us, such as name and contact details (phone number, email). We also process information generated during your relationship with us, such as usage data (e.g. data traffic logs, IP addresses, device coordinates). We do not collect sensitive personal data.

Purpose of Processing

Personal data is processed by Netmore for the following purposes:

- To communicate with you as a representative of a customer, potential customer, or supplier.
- To administer and fulfil contracts or agreements between your organization and Netmore.
- To enable billing and payment processing.
- To provide customer support and handle support requests.
- To comply with Netmore’s legal obligations.
- For marketing purposes, where permitted by law and subject to your rights.

We only process personal data for these specified and legitimate purposes. We do not process your data in a manner incompatible with these purposes.

Legal Basis for Processing (EU)

Within the EU, our processing of personal data is based on at least one of the legal grounds permitted by GDPR: most often, processing is necessary to fulfil our contract with your organization or to take steps at your organization’s request before entering into a contract. In other cases, processing may be based on legal obligations, your consent (which you can withdraw at any time), or Netmore’s legitimate interests balanced against your data protection rights and freedoms. We will explicitly inform you when consent is required and ensure any necessary consent is obtained in accordance with GDPR.

Disclosure of Personal Data

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

Netmore utilizes your personal information with the entirety of the Netmore Group organization for the purposes stated above. We also use trusted external service providers (“processors”) to perform tasks on our behalf, for example, IT service providers, payment processors, or installation contractors. When we share data with such third parties, we ensure through contracts that they only process your data under our instructions and with appropriate security to protect your information, consistent with this policy and applicable laws. We may also disclose personal data to government authorities or law enforcement if required by law or legal process. Netmore will not transfer or store your personal data outside of the jurisdictions mentioned in this policy unless appropriate safeguards are in place, as detailed in the “International Data Transfers” section below.

Security of Personal Data

Netmore protects personal data by implementing appropriate technical and organizational security measures to prevent unauthorized access, alteration, disclosure, or destruction. These measures include access controls, encryption where appropriate, network security protections, and regular training for staff on data protection. We continuously review and enhance our security measures in line with industry standards and legal requirements.

Data Retention Period

We retain personal data only for as long as necessary to fulfil the above-stated purposes and if there is a legal basis (and, where applicable, a legal obligation) for doing so. This means data will be kept for the duration of your organization’s contract or relationship with us and thereafter for the period required or permitted by local laws. Personal data that is no longer needed, or where we no longer have a lawful basis to retain it, will be securely deleted or anonymized.

Your Rights and How to Exercise Them

Access and Correction: You have the right to request confirmation of whether we process personal data about you, and to obtain a copy of the data, as well as information about how we use it (a “subject access request”). You also have the right to request correction of any inaccurate personal data.

Deletion: You may ask us to delete personal data when it is no longer needed for the purposes for which it was collected, or if processing is unlawful, or if we have no legal basis to retain it. Note that we cannot delete data required by law to keep, and certain other exceptions may apply (for example, if the data is needed to establish or defend legal claims).

Restriction: You can request that we restrict (temporarily halt) processing of your personal data if you contest its accuracy, or object to processing, or if you need us to preserve the data for legal claims. When restricted, your data will only be processed with your consent or for certain legal reasons.

Objection: You have the right to object to processing of your personal data that is based on Netmore’s legitimate interests or for direct marketing. If you object to direct marketing, we will stop processing your data for those purposes. If you object to other legitimate interest processing, we will evaluate whether Netmore’s reasons override your privacy rights.

Data Portability: For data you provided to us and which we process by automated means on the basis of contract or consent, you have the right to request a copy in a structured, commonly used, machine-readable format, and/or to have that data transmitted to another controller where technically feasible.

Withdrawal of Consent: Where we process your personal data based on your consent, you have the right to withdraw that consent at any time, without affecting the lawfulness of processing based on consent before its withdrawal.

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

To exercise any of these rights, please contact us using the contact information in the “Contact Information” section below. We will respond to your request in accordance with applicable law. You also have the right to lodge a complaint with a supervisory authority in your jurisdiction if you believe your data has been handled unlawfully.

International Data Transfers and EU-U.S. Data Privacy Framework

Netmore is a global organization, and the personal data we collect may be transferred to and processed by Netmore entities or service providers in countries outside of your home jurisdiction. In particular, personal data collected in the European Economic Area (EEA) or UK may be transferred to our operations or subprocessors in the United States and other countries. We only transfer personal data internationally in compliance with applicable data transfer laws. This means that:

- Within the EU/EEA and UK: Your data may be transferred outside the EU/EEA/UK only if an approved safeguard or exemption applies. Netmore relies on mechanisms such as the European Commission’s adequacy decisions and the EU-U.S. Data Privacy Framework (DPF) for transfers to the U.S., or Standard Contractual Clauses where appropriate, to ensure an equivalent level of data protection.
- EU-U.S. and UK-U.S. Data Privacy Framework: Netmore Group AB (via its U.S. affiliate, Netmore, Inc.) complies with the EU-U.S. Data Privacy Framework and the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework (Swiss-U.S. DPF) as set forth by the U.S. Department of Commerce. We have certified to the Department of Commerce that we adhere to the DPF Principles with respect to all personal data received from the EU/EEA and the UK in reliance on the Data Privacy Framework. This includes the seven core principles (Notice; Choice; Accountability for Onward Transfer; Security; Data Integrity and Purpose Limitation; Access; Recourse, Enforcement and Liability) and the Supplemental Principles of the Framework. If there is any conflict between this privacy policy and the Data Privacy Framework Principles, the Principles shall govern. Netmore’s commitment under the DPF extends to personal data transferred from the United Kingdom as well, consistent with the UK Extension to the EU-U.S. DPF. Netmore has certified to the U.S. Department of Commerce that it adheres to the Swiss-U.S. Data Privacy Framework Principles (Swiss-U.S. DPF Principles) with regard to the processing of personal data received from Switzerland in reliance on the Swiss-U.S. DPF. If there is any conflict between the terms in this privacy policy and the EU-U.S. DPF Principles and/or the Swiss-U.S. DPF Principles, the Principles shall govern. To learn more about the Data Privacy Framework program and to view Netmore’s certification once approved, please visit the official Data Privacy Framework website, <https://www.dataprivacyframework.gov/>, maintained by the U.S. Department of Commerce.
- Accountability for Onward Transfers: When Netmore transfers personal data received under the DPF to third-party agents or service providers, we remain responsible and liable under the DPF Principles if those third parties process your personal data in a manner inconsistent with the Principles, unless we prove we are not responsible for the event giving rise to the damage. We contractually require that our service providers who receive personal data from us protect it in accordance with standards at least as strict as those required by the DPF.
- Recourse and Enforcement (DPF): In compliance with the DPF, Netmore commits to resolve complaints about our collection or use of your personal data. EU, UK, and Swiss individuals with inquiries or complaints regarding this policy or our data handling practices should first contact us at gdpr@netmoregroup.com. We will investigate and attempt to resolve any complaints or disputes regarding the use or disclosure of your personal data within 45 days. If you have an unresolved privacy concern related to EU/UK/Swiss personal data that we have not addressed satisfactorily, you have the right to escalate the matter. In compliance with the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF, Netmore commits to refer unresolved

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

complaints concerning our handling of personal data received in reliance on the EU-U.S. DPF and the UK Extension to the EU-U.S. DPF and the Swiss-U.S. DPF to [the International Centre for Dispute Resolution - American Arbitration Association](#) (ICDR-AAA), an alternative dispute resolution provider based in the United States. If you do not receive timely acknowledgment of your DPF Principles-related complaint from us, or if we have not addressed your DPF Principles-related complaint to your satisfaction, please visit the [ICDR-AAA's website](#) for more information or to file a complaint. The services of ICDR-AAA are provided at no cost to you.

- **U.S. Regulatory Oversight:** Netmore's U.S. operations are subject to the investigatory and enforcement powers of the United States Federal Trade Commission (FTC). We understand that if we or any third-party handling data on our behalf misrepresent our privacy practices or fail to comply with the DPF Principles, we may be subject to enforcement action under U.S. law, including Section 5 of the FTC Act which prohibits unfair or deceptive acts in commerce. In other words, Netmore's commitment to the DPF is enforceable under U.S. law.

We ensure that any transfer of your personal data is lawful and that your rights remain protected by equivalent high standards of privacy protection in the recipient country through the frameworks and measures described above. If you need more information about our transfer mechanisms or a copy of the relevant safeguards, please contact us.

Region-Specific Provisions

To address varying laws in different jurisdictions, the following additional provisions apply:

European Union (EU)

Our core practices outlined in this policy are designed to meet the requirements of the EU GDPR. Netmore Group AB is the controller of personal data for our EU operations. We rely on the GDPR legal bases as described above and uphold all data subject rights under GDPR (see "Your Rights" section). We have appointed a Data Protection Officer/Responsible contact (see Contact Information below) for GDPR compliance inquiries. If you believe our processing of your personal data is not compliant with GDPR, you have the right to lodge a complaint with an EU supervisory authority (e.g., Sweden's Authority for Privacy Protection (IMY) in our home jurisdiction). We remain committed to the fundamental principles of GDPR including lawfulness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity/confidentiality, and accountability. We do not process EU personal data except as permitted by GDPR and this policy. International transfers from the EU are handled as described under the Data Privacy Framework and other safeguards.

United Kingdom (UK)

For our subsidiaries or operations in the UK, we comply with the UK data protection regime, which includes the UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018. The UK GDPR is essentially the EU GDPR as incorporated into UK law, and our commitments and processes for EU data apply equally to UK personal data. In the UK, references in this policy to the GDPR should be understood as references to the UK GDPR. Netmore's UK-affiliated entities follow the requirements of the Data Protection Act 2018 in processing personal data and have the same legal bases for processing and providing individual rights as described for the EU. We have designated the same contact (see Contact Information) for UK data protection inquiries. UK personal data may be transferred outside the UK under either adequacy regulations or the UK Extension to the EU-U.S. DPF, as discussed above.

United States (US)

In the United States, we adhere to applicable federal and state privacy laws in the jurisdictions where we operate. While the U.S. currently lacks a single comprehensive federal data protection law equivalent to the

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

GDPR, Netmore complies with state and federal laws that apply to our activities. For example, if you are a California resident, you have specific rights under the CCPA, including the right to know what personal information we collect, the right to request deletion of your personal information, the right to opt-out of the “sale” or sharing of personal information, and the right to non-discrimination for exercising these rights (Cal. Civ. Code § 1798.100 et seq.). This Privacy Policy is intended to disclose the categories of personal information we collect and the purposes for which we use it, in accordance with CCPA requirements. Netmore does not sell personal information as defined under CCPA. If you are a California resident, you or your authorized agent can make requests to access or delete your information by contacting us as described below. We will verify your request according to CCPA’s requirements and respond within the timeframe set by law. We also honor applicable opt-out preference signals (such as a “Do Not Sell or Share” browser signal) as required. Aside from California, we will also comply with other U.S. state privacy laws (such as those in Virginia, Colorado, Connecticut, Utah, etc.) to the extent they apply to our operations, affording individuals the rights provided by those laws. We will update this policy or provide region-specific privacy notices as needed to reflect U.S. legal developments. U.S. residents may contact us for any questions about their personal data or to exercise applicable rights.

Note on U.S. Children’s Privacy: Our services are not directed to children under the age of 13, and we do not knowingly collect personal information from children under 13 without parental consent, in compliance with the U.S. Children’s Online Privacy Protection Act (COPPA). If we need to process personal data of minors in other contexts, we will ensure compliance with relevant laws such as requiring parental consent when mandated.

Brazil

For our operations in Brazil, we comply with the Brazilian General Data Protection Law, *Lei Geral de Proteção de Dados Pessoais* (Law No. 13,709/2018, commonly known as LGPD). The LGPD governs how we process personal data of individuals in Brazil or collected in Brazil, and establishes principles similar to the GDPR, such as necessity, transparency, security, non-discrimination, data subject rights, etc. Under LGPD, Brazilian data subjects have rights including confirmation of processing, access to data, correction of incomplete or inaccurate data, anonymization or deletion of unnecessary data, data portability, and information about data sharing with third parties. Netmore will facilitate these rights for Brazilian individuals in line with LGPD’s provisions (Arts. 18 and 19 of LGPD). We process Brazilian personal data only for lawful purposes and on appropriate legal bases as defined by LGPD (for example, with consent, or to fulfil a contract, or to comply with legal obligations, among others as listed in Article 7 of LGPD). Where consent is required, we will obtain it separately and allow revocation. Our Country Manager for Brazil also functions as the data protection officer (*Encarregado*) for Brazil as required and can be contacted via the contact information below. Netmore ensures that transfers of personal data from Brazil to other countries will observe the requirements of LGPD Chapter V on international transfers. We also implement security measures as required by LGPD to protect personal data from unauthorized access and incidents (Art. 46 of LGPD). Brazilian users can contact us with any questions or requests regarding their personal data and also have the right to petition the ANPD if needed.

Indonesia

For our operations in Indonesia, we comply with the *Undang-Undang Pelindungan Data Pribadi* (Law of the Republic of Indonesia No. 27 of 2022 on Personal Data Protection, “Indonesian PDP Law”). In accordance with the PDP Law, we process personal data of individuals in Indonesia lawfully, fairly, and transparently. We will only collect personal data for purposes directly related to our legitimate business functions and use it in a manner that is compatible with those purposes. We respect the rights granted to data subjects under the Indonesian PDP Law, which include (as per Chapter III of the law) the right to access personal data, the right to correct or update personal data, the right to delete or destroy personal data under certain conditions, the right to withdraw consent (when consent was the basis of processing), and the right to information about the personal data processing. Netmore will provide contacts and mechanisms for

netmore	Title: Privacy Policy and GDPR		Information Classification: Public	
	Publish Date: 08-Dec-25	Author: Joshua Mitchell; Björn Klug		Version: 1.0

Indonesian data subjects to exercise these rights. We also ensure compliance with the data localization or transfer requirements of Indonesian law. If personal data is transferred outside of Indonesia, we will do so only for jurisdictions that enforce equal or higher personal data protection standards, or we will ensure that adequate safeguards (such as agreements) are in place, in accordance with Article 55 of the PDP Law and related regulations. We implement technical and organizational measures required by the law to ensure the security and protection of personal data, and we will report any serious personal data breaches to the Indonesian authorities and affected individuals as required by law. Our appointed contact for personal data issues (see below) can be reached by Indonesian individuals for inquiries or complaints.

Contact Information

Data Protection Contact (EU, Switzerland, and UK): If you would like further information about how Netmore processes your personal data, or if you wish to exercise any of your rights described in this policy, please contact us at gdpr@netmoregroup.com and mention you are contacting us in reference to EU, Switzerland or UK data protection matters.

Brazil Encarregado: For Brazil, please contact us at gdpr@netmoregroup.com. Please mention you are contacting us in reference to Brazilian LGPD matters.

Indonesia Contact: Indonesian data subjects may contact us at gdpr@netmoregroup.com and mention you are contacting us in reference to Indonesia PDP matters. We will provide assistance in Bahasa Indonesia if needed when handling requests from individuals in Indonesia, in accordance with local law requirements.

United States Data Protection Contact: For inquiries involving data privacy and protections within the United States and individuals' rights in specific states, please contact us at gdpr@netmoregroup.com and mention you are contacting us in reference to US data privacy matters

We are committed to resolving any concerns about privacy and data protection. If you contact us with a privacy question or complaint, our privacy team will investigate and attempt to address it. If you are not satisfied with the response, you may escalate as described in the above sections.

Changes to This Policy

We update this Privacy Policy from time to time to reflect changes in our practices, legal requirements, or for other operational reasons. When we make changes, we will revise the "Effective Date" at the top of the policy. We encourage you to review this Privacy Policy periodically to stay informed about how we are protecting your personal data.