

Privacy policy

At Mobile Arts AB, we protect your personal privacy and always strive for a high level of data protection (for example, we would never sell your personal data to another company). This privacy policy explains how we collect and use your personal information. It also describes your rights and how you can claim them.

It is important that you read and understand the privacy policy and feel secure in our processing of your personal data. You are always welcome to contact us if you have any questions. Using the table of contents below, you can easily navigate to the sections that are of special interest to you.

What is personal data and what is processing of personal data?

Personal data is any kind of information that can be directly or indirectly attributed to a natural person who is alive. This includes images and sound recordings that are processed in a computer, even if no names are mentioned. Encrypted information and various kinds of electronic identities (e.g. IP numbers) are personal data if they can be linked to natural persons.

Processing of personal data is everything that happens to the personal data. Every action taken with personal data constitutes processing, regardless of whether it is performed automatically or not. Examples of common processing includes collection, recording, organization, structuring, storage, adaptation, transmission and erasure.

Who is responsible for the personal data we collect?

Mobile Arts AB, corp. reg. no. 556609-4594, with address Tjärhovsgatan 56, SE-116 28 Stockholm, Sweden is controller for the company's processing of personal data.

Contact information:

Mobile Arts AB
Attention: Information Security Coordinator
Tjärhovsgatan 56
SE-116 28 Stockholm
Sweden

Mail address:

infosec@mobilearts.com

What personal information do we collect about you as a job seeker and for what purpose?

Purpose	Processing performed	Categories of personal data
Recruitment of human resources	Handling of applications.	Cover letter, CV
Legal basis: contract and/or legitimate interest.		
Storage period: During the recruitment period as well as possibly longer, e.g., employment.		

What contact information do we collect about you as a customer and for what purpose?

Purpose	Processing performed	Categories of personal data
To be able to manage offers, contracts, deployment and support.	Customer register, book-keeping documents, web services, time reporting, accounting. Project documentation. Payment processing (including obtaining credit information from credit agencies).	Name. Corporate registration number. Contact information (e.g. address, e-mail and telephone number). Payment history. Payment information. Credit information from credit agencies. End-customer data that might be send to us in the processing of support issues. System information.
Legal basis: contract and/or legitimate interest. This collection of your contact information is required in order for us to be able to fulfil our obligations under the agreement.		
Storage period: As long as the agreement is valid and possible longer to be able to manage any complaints and due to Companies Act, tax legislation, banking and money laundering legislation and the need for fabricating certificates. System login information is only stored for as long as necessary. Subscriber information and logs only stored at the customer, but if attached during support the subscriber logs and other logs are stored for a maximum of 29 days. No subscriber information should be sent to MA via bug reports or e-mail.		

What contact information do we collect about prospects and for what purpose?

Purpose	Processing performed	Categories of personal data
Marketing, recruiting new customers.	List of prospects, newsletters, trade show contacts, NDAs	Name. Contact information (e.g. address, e-mail and telephone number).
Legal basis: legitimate interest. The processing is necessary to satisfy our and possibly our new customers' legitimate interest in deepening contact.		
Storage period: As long as there is interest from any party. Deregistering at requests takes place on an ongoing basis.		

What contact information do we collect about you as a supplier and for what purpose?

Purpose	Processing performed	Categories of personal data
To be able to execute the company's procurement procedures and meet the requirements of ISO certification.	Necessary handling to fulfil the company's legal obligations or obligations arising from governmental decisions.	Name. Contact information (e.g. address, e-mail and telephone number).
Legal basis: contract and/or legitimate interest. This collection of your contact information is required in order be able to fulfil our obligations under the agreement		
Storage period: as long as the business relationship is active. Possibly longer due to Companies Act, tax legislation, banking and money laundering legislation.		

From which sources do we retrieve your personal data?

In addition to the information you provide to us yourself, we may also collect personal data from someone else (known as a third party). The data we collect from third parties is as follows:

- 1) Address information from public records to ensure we have the correct information for you.
- 2) Rating information from rating agencies, banks or credit agencies.
- 3) Information from social media for marketing purposes.

Who might we share your personal data with?

Processors. In cases where it is necessary for us to be able to offer our services, we share your personal data with companies who act as what are known as processors for us. A processor is a company that processes the information on our behalf and according to our instructions. We have processors that help us with:

- 1) Accounting
- 2) Suppliers which provide services to our company and employees.
- 3) IT services (companies that manage the necessary operations, technical support and maintenance of our IT solutions).

When your personal data is shared with processors, this only takes place for purposes compatible with the purposes for which we have collected the information (e.g. to fulfil our commitments under the purchase agreement). We check all processors to ensure that they can provide adequate guarantees regarding security and the confidentiality of personal data.

Independent controllers. We also share your personal data with some companies that are independent controllers. The fact that the company is an independent controller means that it is not us who control how the information provided to the company will be processed.

Independent controllers with whom we share your personal data are:

- 1) State authorities (police, tax authorities or other authorities) if we are obliged to do so by law or on suspicion of a crime.
- 2) Companies that arrange general goods transport (logistics companies and freight forwarders).
- 3) Companies that offer payment solutions (card-acquisition companies, banks and other payment service providers).

When your personal data is shared with a company that is an independent controller, we control that company's privacy policy and personal data management apply.

Where do we process your personal data?

We always strive for your personal data to be processed within the EU/EEA, and all our own IT systems are located within the EU/EEA. However, for systems support and maintenance, we may have to transfer the data to a country outside the EU/EEA, e.g. if we share your personal data with a processor that, either itself or through a subcontractor, is established or stores data in a country outside the EU/EEA. In these cases, the processor may only access the data that is relevant for the purpose (e.g. log files).

Regardless of in which country your personal data is processed, we take all reasonable legal, technical and organizational measures to ensure that the level of protection is the same as in the EU/EEA. In cases where personal data is processed outside the EU/EEA, the level of protection is guaranteed either by a decision from European Commission that the country in question ensures an adequate level of protection, or through the use of what are known as appropriate safeguards. Examples of these are an approved code of conduct in the recipient country, standard contractual clauses, binding corporate rules or Privacy Shield. If you want a copy of information on the safeguards that have been established or information about where these have been made available, you are welcome to contact us.

How long do we store your personal data?

We never store your personal data for longer than is necessary for each purpose. See more about the specific storage periods under each purpose.

What rights do you have as a data subject?

Right of access (known as a database extract). We are always open and transparent with how we process your personal data, and if you want to gain a deeper insight into the personal data we process about you, you can request access to the data (the data is provided in the form of a database extract indicating purposes,

categories of personal data, categories of recipients, storage periods, information about from where the information has been collected and the occurrence of automated decision-making). Please note that if we receive a request for access, we may ask for additional information to ensure the efficient handling of your request and that the data is provided to the right person.

Right to rectification. You can request that your personal data be rectified if the information is incorrect. Within the scope of the stated purpose, you also have the right to supplement any incomplete personal data.

Right to erasure. You can request the erasure of personal data we process about you if:

The data is no longer necessary for the purposes for which it has been collected or processed.

You object to a balancing of interests we have performed based on legitimate interest and your reason for the objection outweighs our legitimate interest. You object to processing for direct marketing purposes.

Personal data is being processed in an illegal manner. The personal data must be erased in order to fulfil a legal obligation to which we are subject.

Please note that we may be entitled to deny your request if there are legal obligations that prevent us from immediately deleting certain personal data. These obligations come from accounting and tax legislation, banking and money laundering legislation, as well as from consumer protection legislation. It may also be the case that processing is necessary for us to be able to establish, exercise or defend legal claims. Should we be prevented from meeting a request for deletion, we will instead prevent the personal data from being used for purposes other than the purpose that prevents the requested deletion. This means that you can request that we do not delete your data.

Right to restriction. You have the right to request that our processing of your personal data be restricted. If you dispute that the personal data we are processing is accurate, you may request limited processing during the time we need to check whether the personal data is accurate. If we no longer need the personal data for the stated purposes, but you on the other hand need them to be able to establish, enforce or defend legal claims, you may request limited data processing. If you have objected to a balancing of legitimate interests that we have performed as a legal basis for a purpose, you can request limited processing for the time we need to check whether our legitimate interests outweigh your interests in having the data deleted. If the processing has been restricted according to any of the situations above, we can only, in addition to the storage itself, process the data to establish, enforce or defend legal claims, to protect someone else's rights or if you have given your consent.

Right to object to a certain type of processing. You are always entitled to avoid direct marketing and to object to any processing of personal data based on a balancing of interests.

Balancing of interests: In cases where we use a balancing of interests as a legal basis for a purpose, you have the opportunity to object to the processing. To be able to continue processing your personal data after such an objection, we must be able to demonstrate a compelling legitimate reason for the processing in question that outweighs your interests, rights or freedoms. Otherwise, we may only process the data to establish, exercise or defend legal claims.

Direct marketing (including analytics performed for direct marketing purposes): You have the opportunity to object to your personal data being processed for direct marketing purposes. The objection also includes the analyses of personal data (known as profiling) that are performed for direct marketing purposes. Direct marketing refers to all types of outreach marketing measures (e.g. via mail, e-mail and text message). Marketing measures where you as a customer actively chose to use one of our services or otherwise contacted us to find out more about our services are not considered direct marketing (e.g. product recommendations or other features).

If you object to direct marketing, we will stop processing your personal data for that purpose and discontinue all types of direct marketing measures. Remember that you always have the opportunity to influence which channels we should use for mailings and personal offers. E.g. you can choose to only receive offers from us via email.

Right to data portability. If our right to process your personal data is based either on your consent or fulfilment of an agreement with you, you are entitled to request that the information that concerns you and that you

have provided to us be transferred to another controller (known as data portability). A prerequisite for data portability is that the transfer is technically possible and can be automated.

How do we handle social security numbers?

We will only process your social security number when it is clearly justified considering the purpose, necessary for secure identification or if there is some other noteworthy reason. We always minimize the use of your social security number to the greatest extent possible by, in cases where this is sufficient, using your birth registration number instead.

What are cookies and how do we use them?

Cookies are a small text file consisting of letters and numbers sent from our web server and saved on your browser or device.

<https://bugs.mobilearts.com> and our product OAM GUI uses cookies for its trouble report system and Operations, Administration and Management system, respectively. No other MA services uses cookies.

- 1) Session cookies (a temporary cookie that expires when you close your browser or device).
- 2) Persistent cookies (cookies that remain on your computer until you remove them or they expire).
- 3) First-party cookies (cookies set by the website you visit).
- 4) Third-party cookies (cookies set by a third-party website. We use these primarily for analyses, e.g. Google Analytics.).

Cookies improves the services we offer. Some of our services need cookies to work properly, while others improve the services for you.

<https://mobilearts.com> does not use any cookies.

Social media

Mobile Arts does not use any social media, such as Twitter, Facebook or YouTube, as communication channels to provide information on Mobile Arts's operations.

Exceptions are *LinkedIn*.

Can you control the use of cookies yourself?

Yes! Your browser or device allows you to change the usage settings and the scope of cookies. Go to your browser or device settings to learn more on how to adjust your cookie settings. Examples of things you can adjust are blocking all cookies, only accepting first-party cookies or deleting cookies when you close your browser. Keep in mind that some of our services may not work if you block or delete cookies. You can read more about cookies on the Swedish Post and Telecom Authority's website, www.pts.se.

How is your personal data protected?

We use IT systems to protect confidentiality, privacy and access to personal data. We have taken special security measures to protect your personal data from illegal or unauthorized processing (such as illegal access, loss, destruction or damage). Only the people who actually need to process your personal data so that we can fulfil our stated purposes have access to it.

What does it mean that the Swedish Authority for Privacy Protection (Integritetsskyddsmyndigheten) is a supervisory authority?

The Swedish Authority for Privacy Protection is responsible for monitoring the application of the legislation, and whoever considers that a company is incorrectly handling personal data can file a complaint with the Authority.

Web: www.imy.se

How can you most easily reach us with questions about data protection?

As we take data protection very seriously, we have assigned a role at the company who manage this area. We may make changes to our privacy policy. The latest version of the privacy policy is available on request, see

contact information in first page. We will do our best to inform each party in our in company register when changes are made.