

# AMDAX Privacy Statement



# Contents

1	Welcome to AMDAX.....	3
2	Personal Information We Collect.....	3
2.1	Personal Information we collect from you.....	3
2.2	Personal Information we collect automatically.....	3
2.3	Personal Information we collect from third parties.....	4
2.4	Accuracy and retention of Personal Information .....	4
3	How We Use Your Personal Information .....	4
4	How We Share Your Personal Information.....	5
5	Cookies.....	5
6	Direct Marketing.....	6
7	Information Security .....	6
8	Contact Us .....	6
	Annex I - General Data Protection Regulation Statement.....	7
	Annex II - Procedure relating to rights of the data subjects .....	16



## 1 Welcome to AMDAX

Welcome! Thank you for visiting Amdax, a digital asset platform operated by and proprietary to Amdax B.V. Use of the words “Amdax,” “we,” “us,” or “our” refers to Amdax B.V. This Privacy Statement explains what Personal Information (as defined below) we collect, why we collect it, how we use and disclose it. Furthermore, the GDPR Policy (as defined below) annexed to this Privacy Statement describes the GDPR-related requirements in more detail.

Your privacy matters to us so whether you are new to AMDAX or a long-time client, please do take the time to get to know and familiarize yourself with our policies and practices. Feel free to print and keep a copy of this Privacy Statement, but please understand that we reserve the right to change any of our policies and practices at any time. But don't worry, you can always find the latest version of this Privacy Statement on our website.

## 2 Personal Information We Collect

As used in this Privacy Statement, “**Personal Information**” means information that identifies or is reasonably capable of identifying an individual, directly or indirectly, and information that is being associated with an identified or reasonably identifiable individual.

This Privacy Statement describes how Personal Information is collected, processed and stored and how we comply with applicable legislation and the data protection standards set by AMDAX.

### 2.1 Personal Information we collect from you

We may collect the following categories of Personal Information directly from you:

- identification information, such as name, email, phone number, postal address, government identification numbers (which may include social security number or equivalent, driver's license number, passport number);
- commercial information, such as trading activity, order activity, deposits, withdrawals, account balances;
- financial information, such as bank account information, source of wealth, routing number;
- correspondence, including information provided during account opening and customer support;
- sensory information, such as images collected for identity verification, audio recordings left on answering machines;
- employment information, such as job title, name of employer; and
- company information, such as the company's legal name, employer identification number or any comparable identification number issued by a government, proof of legal existence (which may include articles of incorporation, certificate of formation, business license, trust instrument, or other comparable legal document).

### 2.2 Personal Information we collect automatically

We may collect the following categories of Personal Information automatically through your use of our services:

- online identifiers, such as IP address; domain name;
- device information, such as hardware, operating system, browser;
- usage data, such as system activity, internal and external information related to AMDAX pages that you visit, clickstream information; and
- geolocation data.



Our automatic collection of Personal Information may involve the use of cookies (see below).

### 2.3 Personal Information we collect from third parties

We may collect and/or verify the following categories of Personal Information relating to you from third parties:

- identification information, such as name, email, phone number, postal address, government identification numbers (which may include social security number or equivalent, driver's license number, passport number);
- financial information, such as bank account information, source of wealth, routing number;
- transaction information, such as public blockchain data (bitcoin, ether, and other digital assets are not anonymous). We can match your public digital asset address to other Personal Information about you and may be able to identify you from a blockchain transaction because - in some circumstances - Personal Information published on a blockchain (such as your digital asset address and IP address) can be correlated with Personal Information that we may have. Furthermore, by using data analysis techniques on a given blockchain, it may be possible to identify other Personal Information about you; and
- additional information, as requested by and at the discretion of our compliance team (which may include criminal records or alleged criminal activity).

Personal Information you provide during the registration process may be retained, even if your registration is left incomplete or abandoned.

### 2.4 Accuracy and retention of Personal Information

We take reasonable and practicable steps to ensure that your Personal Information (i) is accurate with regard to the purposes for which it is used, and (ii) is not kept longer than is necessary for the fulfillment of the purpose for which it is used.

## 3 How We Use Your Personal Information

The Personal Information we collect and the practices described above are for the purpose of providing you with the best experience possible, protecting you from risks related to improper use and fraud, and helping us maintain and improve AMDAX. We may use your Personal Information to:

- Provide you with our services.** We use your Personal Information to provide you with our services pursuant to the terms of your agreement with us. For example, in order to facilitate fiat transfers to or from your account, we need to know your bank account information.
- Comply with legal and regulatory requirements.** We process your Personal Information as required by applicable laws and regulations. For example, we have identity verification requirements to fulfill our obligations under anti-money laundering laws.
- Detect and prevent fraud.** We process your Personal Information to detect and prevent fraud on your account, which is especially important given the irreversible nature of crypto-asset transactions.
- Protect the security and integrity of our services.** We use your Personal Information to enhance our security-first mentality. Maintaining the security of your account and the platform requires us to process your Personal Information,



including information about your device and your activity on the platform, and other relevant information.

- E. **Provide you with customer support.** We process your Personal Information anytime you reach out to our customer support team.
- F. **Optimize and enhance our services.** We use your Personal Information to understand how our products and services are being used to help us improve our services and develop new products.
- G. **Market our products to you.** We may contact you with Personal Information about our products and services. We will only do so with your permission, which can be revoked at any time.
- H. **Other business purposes.** We may use your Personal Information for additional purposes if that purpose is disclosed to you before we collect such Personal Information or if we obtain your consent.

## 4 How We Share Your Personal Information

We will not share your Personal Information with third parties, except as described below:

- A. **Service Providers.** We may share your Personal Information with third-party service providers for business or commercial purposes. Your Personal Information may be shared so that they can provide us with services, including identity verification, fraud detection and prevention, security threat detection, payment processing, customer support, data analytics, information technology, advertising, marketing, data processing, network infrastructure, storage, transaction monitoring, and tax reporting. We share your Personal Information with these service providers only so that they can provide us with services, and we prohibit our service providers from using or disclosing your Personal Information for any other purpose. Our third-party service providers are subject to strict confidentiality obligations.
- B. **Law Enforcement.** We may be compelled to share your Personal Information with law enforcement, government officials and/or regulators.
- C. **Corporate Transactions.** We may disclose Personal Information in the event of a proposed or consummated merger, acquisition, reorganization, asset sale, or similar corporate transaction, or in the event of a bankruptcy or dissolution.
- D. **Professional Advisors.** We may share your Personal Information with our professional advisors, including legal, accounting, or other consulting services for purposes of audits, business purposes or to comply with our legal obligations.
- E. **Consent.** We may share or disclose your Personal Information with your consent.

If we decide to modify the purpose for which your Personal Information is collected and used, we will amend this Privacy Statement.

## 5 Cookies

When you access AMDAX, we may make use of the standard practice of placing tiny data files called cookies, flash cookies, pixel tags, or other tracking tools ("**Cookies**") on your computer or other devices used to visit AMDAX. We use Cookies to:

- help us recognize you as a client;
- collect information about your use of AMDAX to better customize and improve our services and content for you;
- collect information about your computer or other access devices to ensure compliance with our Client Acceptance Procedure and Anti-Money Laundering Compliance Program;



- ensure that your account security has not been compromised by detecting irregular, suspicious, or potentially fraudulent account activities; and
- assess and improve our advertising campaigns.

You also can learn more about cookies by visiting <http://www.allaboutcookies.org>, which includes additional useful information on Cookies and how to block Cookies on different types of browsers and mobile devices. Please note that if you reject Cookies, you will not be able to use some or all parts of AMDAX software.

## **6 Direct Marketing**

Subject to applicable laws and regulations, we may from time to time send direct marketing materials promoting services, products, facilities, or activities to you using information collected from or relating to you. You may also opt-out of such communications by following the directions provided in any marketing communication. It is our policy to not provide your Personal Information for those third parties' direct marketing purposes without your consent.

## **7 Information Security**

We cannot guarantee absolute security, but we work hard to protect AMDAX and you from unauthorized access to or unauthorized alteration, disclosure, or destruction of the Personal Information we collect and store. Measures we take include:

- encryption of the AMDAX website communications with SSL;
- require two-factor authentication for all sessions;
- periodic review of our Personal Information collection, storage, and processing practices; and
- restricted access to your Personal Information on a need-to-know basis for our employees, contractors and agents who are subject to strict contractual confidentiality obligations and may be disciplined or their engagement terminated if they fail to meet these obligations.

## **8 Contact Us**

If you have questions or concerns regarding this Privacy Statement or our processing of your Personal Information, please feel free to email us at: [hello@amdax.com](mailto:hello@amdax.com), call us at our telephone number (to be found on our website), or write to us at: AMDAX, Gustav Mahlerplein 45, 1082 MS Amsterdam, the Netherlands.

If you are a European resident and you believe that we have not adequately resolved any such issues, you have the right to contact the local supervisory authority.



## Annex I - General Data Protection Regulation Policy

We adhere to EU data protection laws as stated in the General Data Protection Regulation (EU) 2016/679 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data ("**GDPR**"). The GDPR describes how companies such as AMDAX must collect, process and store personal data. These rules apply regardless of whether the data is processed electronically, on paper or in another way.

Below is our GDPR Policy, outlining how we implement the GDPR. This GDPR Policy ensures that AMDAX:

- complies with laws and regulations regarding the protection of personal data;
- protects the rights of customers, employees, partners and suppliers;
- is transparent in the way in which it stores and processes personal data; and
- mitigates the risk of infringement with regard to personal data as much as reasonably possible.

### Data protection risks

This GDPR Statement helps protect AMDAX against data security risks such as:

- the risk of a breach of trust, for example because the data has been unlawfully made public;
- the risk that the rights of an individual are not respected, for example the right to access or rectify his or her personal data; and
- the risk of reputation damage, for example because hackers have successfully gained unlawful access to privacy sensitive information.

### Responsibilities

Everyone who works at or for AMDAX has a responsibility to ensure that data collection, processing and retention is done properly. Everyone within AMDAX who comes into contact with personal data must guarantee that processing such data is in line with this GDPR Policy and the data protection principles.

### Definitions

The definitions we use in our Privacy Statement are in line with the definitions used in the GDPR.

Defined term	Definition
<b>personal data</b>	any information relating to an identified or identifiable natural person.
<b>data subject</b>	an identified or identifiable natural person. An identifiable natural person is one who can be identified directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.
<b>processing</b>	any operation or set of operations which is performed on personal data or on sets of personal data, whether or not



	carried by automated means, such as collecting, recording, organisation, structuring, storage, adaption or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.
<b>controller</b>	a natural or legal person, public authority, agency or other body, which, alone or jointly with others, determines the purposes of and means of the processing of personal data; where the purposes and means of such processing are determined by EU or national law, the controller or the specific criteria for its nomination may be provided by EU or national law.
<b>processor</b>	a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

#### Principles regarding the processing of personal data

To comply with laws and regulations, the following principles regarding the processing of personal data must be met:

- The personal data must be processed in a manner that is lawful, proper and transparent with regard to the data subject (*legality, fairness and transparency*).
- The personal data must be collected for specified, explicit and legitimate purposes and may not be further processed in a way incompatible with those purposes (*purpose limitation*).
- The personal data must be adequate, relevant and limited to what is necessary for the purposes for which they are processed (*data minimisation*).
- The personal data must be accurate and, where necessary, kept up to date; all reasonable measures must be taken to ensure that personal data that are inaccurate, with a view to the purposes for which they are processed, is erased or rectified without delay (*accuracy*).
- The personal data must be kept in a form that makes it possible to identify the data subjects for no longer than is necessary for the purposes for which the personal data is processed (*storage limitation*);
- By taking appropriate technical or organizational measures, personal data must be processed in such a way that appropriate security of the personal data is guaranteed, including protection against, inter alia, unauthorized or unlawful processing and against accidental loss, destruction or damage (*integrity and confidentiality*). AMDAX has taken various measures to this end.

#### Regularity

Personal data may only be processed if at least one of the following conditions is met:





- The data subject has given permission for the processing of his or her personal data for one or more specific purposes.
- The processing is necessary for the performance of an agreement to which the data subject is party, or to take measures at the request of the data subject prior to entering into an agreement.
- The processing is necessary for compliance with a legal obligation to which the controller is subject.
- The processing is necessary to protect the vital interests of the data subject or another natural person.
- The processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
- The processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except such interests are overridden by the interests or fundamental rights and fundamental freedoms of the data subject which require protection of personal data, in particular when person is a child.

If the lawfulness of processing is 'consent' (first bullet above), AMDAX must be able to demonstrate that the person concerned has given permission, for example by means of a written record. The consent must be given by the person concerned in a free, specific, informed and unambiguous manner.

Permission to process personal data can be withdrawn by the data subject. Such a withdrawal has no retroactive effect. The processing must be stopped after withdrawal of the permission, unless the processing can be based on another basis as referred to in the list above.

#### Transparency

AMDAX provides the person concerned with the following information:

- the identity and contact details of AMDAX;
- the processing purposes for the personal data, as well as the legal basis for processing;
- the recipients or categories of recipients of the personal data;
- if applicable, the intention to transfer the personal data to a third country or an international organization;
- the period during which the personal data will be stored, or if that is not possible, the criteria for determining that period;
- information about the data subject's right to request AMDAX to inspect and rectify or erase the personal data or limit the processing concerning him or her, as well as the right to object to the processing and the right to data transferability;
- that the person concerned has the right to lodge a complaint with a supervisory authority; and
- whether the provision of personal data is a legal or contractual obligation or a necessary condition for entering into an agreement, and whether the data subject is obliged to provide the personal data and what the possible consequences are if this data is not provided.

The above information is provided in writing or by other means, including, if appropriate, electronic means.

#### Right of inspection of the person concerned

The data subject has the right to obtain information from AMDAX about whether or not they are processing personal data concerning him or her and, if that is the case, to have



access to such personal data, including the information stated under the section Transparency (above).

When personal data is transferred to a third country or an international organization, the data subject has the right to be informed of the appropriate safeguards regarding the transfer.

AMDAX provides the data subject with a copy of the personal data that is being processed at the request of the person concerned. If the person concerned requests additional copies, AMDAX may charge a reasonable fee based on the administrative costs. If the person concerned submits his or her request electronically, and does not request another method of delivery, the information is provided in a conventional electronic form.

We refer to Annex II – Procedure for rights of data subjects for our procedure with regard to the processing of requests from data subjects.

#### Purpose limitation

AMDAX only collects and processes personal data for specific, explicitly described and justified purposes. AMDAX will not use the personal data for a purpose other than the predetermined purpose, unless the use is compatible with the original purpose for which the data was collected. Whether or not there is compatibility depends on:

- the relationship between the purposes for which the data was collected and the purposes of further processing;
- the context in which the data was collected and the reasonable expectations of the parties involved with regard to further use;
- the nature of the data and the impact of further processing on the data subjects; and
- the safeguards applied by the controller to ensure fair processing and to prevent inappropriate consequences for data subjects

#### Minimum data processing

AMDAX only processes personal data to the extent that this is necessary for processing purposes. This means that AMDAX only uses the personal data that is necessary to achieve the goal. Subsidiarity is also taken into account: if the goal can also be achieved through another way, with less infringement of privacy, AMDAX will use this other way.

#### Correctness

The GDPR requires AMDAX to take reasonable measures to ensure that the data is accurate and correct. The more important the personal data is, the more effort is required from AMDAX to ensure accuracy.

It is AMDAX's responsibility to take reasonable measures to ensure that the data is as accurate and accurate as reasonably possible. To this end, they take the following measures:

- the data is stored in as few different places as possible. That way it is easier to maintain the data;
- employees will use every opportunity to update the data, for example in (daily) contact with the customer;
- if inaccuracies are found in the data, the data must be adjusted accordingly. For example, if a customer or supplier is no longer available on the telephone number known to AMDAX, it will be removed from the database and / or replaced by a correct telephone number.



The data subject can also request AMDAX to rectify it with regard to incorrect personal data without delay. Taking into account the purposes of the processing, the data subject has the right to complete incomplete personal data.

We refer to Annex II – Procedure for rights of data subjects for our procedure with regard to the processing of requests from data subjects.

#### Storage restriction

AMDAX stores the personal data in a form that makes it possible to identify the data subjects no longer than is necessary for the purposes for which the personal data is processed.

The person concerned can also request AMDAX to delete his or her personal data. AMDAX must then delete the personal data without unreasonable delay, for example when the personal data is no longer needed for the purposes for which it was collected or otherwise processed.

We refer to Annex II – Procedure for rights of data subjects for our procedure with regard to the processing of requests from data subjects.

#### Other general guidelines

The following other general guidelines apply within AMDAX:

- Employees or other persons working for AMDAX only have access to personal data that they need to perform their work.
- Employees protect personal data by taking reasonable precautions.
- Employees use strong passwords and do not share their password with others. A strong password contains the following elements:
  - At least 1 capital letter;
  - At least 1 lowercase letter;
  - At least 1 digit;
  - At least 1 symbol;
  - At least 8 characters;
- Employees do not provide data to unauthorized persons, both within and outside the AMDAX organization.
- Employees periodically update the data if it appears that they are no longer accurate.

#### Appropriate protection measures

This section describes the protection measures that AMDAX has taken with a view to protecting personal data.

##### Electronic storage of data

When data is stored electronically, data must be protected against unauthorized access, accidental deletion of data and malicious hacking of the electronic storage location. The following assumptions apply to electronic storage:

- **Access security:** authentication (who) and authorization (was the person allowed to) are essential. The authentication and authorization of every employee must be recorded, so that when the employee leaves AMDAX, his or her rights can be withdrawn from the AMDAX systems. All data is protected with a combination of login and a strong password, which is periodically changed and not shared with unauthorized persons. When data is stored on an external carrier (such as a USB), this carrier must be stored in a closed cupboard with lock. If external data carriers



are no longer in use, they must be destroyed or formatted. When formatting, the carrier must be formatted several times to avoid reconstructing data is possible after formatting.

- **Management of technical vulnerabilities:** all servers and computers are protected with security software, virus scanners, anti-malware and/or a firewall. All software, including browsers, virus scanners and operating systems are held up to date. Data must always be stored on designated disks/servers, and may only be uploaded to AMDAX approved cloud computing servers, (managed) hosting parties or third-party software. Systems that are 'end-of-support' or 'end-of-life' are being replaced by AMDAX for other systems. In this way it is prevented from working with systems for which support is no longer available and where the security is not maintained.
- **Continuity management:** personal information may be lost due to natural disasters, accidents, equipment failure or intentional acts. To mitigate this risk, backups are made of all relevant data. The frequency and retention period of the backups must be appropriate for the data that is being backed up. For the storage location, the backup is not stored on the same location as where the original data is stored.

#### Paper storage of data

Data stored on paper is stored in a place where unauthorized persons cannot view, reproduce or take the papers. The following principles apply to paper storage:

- If the papers are not used, they must be kept in a closed cupboard with a lock;
- If the paper storage is no longer used, it must be destroyed with the paper shredder or discarded in lockable trash bins for confidential documents, the contents of which are removed and destroyed by a specialized company.
- At the end of each working day, every employee must store confidential papers.

#### Special personal data

AMDAX does not, in principle, process special categories of personal data as referred to in the GDPR. Special categories of personal data include a person's race or ethnic origin, political views, religious or philosophical beliefs, union membership, and genetic data, biometric data for the unique identification of a person, or data on health or relating to a person's sexual orientation. Nevertheless, if special personal data is processed, this will only be done under the following conditions:

- AMDAX has explicitly requested permission from the person concerned;
- The data has been provided by the person concerned; and
- An exception as included in the GDPR is met.

#### Information security incidents

AMDAX has established the following procedure for the timely and effective handling of information security incidents and security vulnerabilities as soon as they are reported. The lessons learned from the incidents handled are used to structurally improve security where possible.

If a follow-up procedure following an information security incident includes legal measures (civil or criminal), the evidence is collected, stored and presented in accordance with the rules for evidence established for the relevant jurisdiction. The board of AMDAX will be responsible for these tasks and, if necessary, be assisted with external expertise for this.

Following an information security incident, the board of AMDAX assesses the risks for those involved. It is also considered whether the incident must be reported to the person(s) involved and/or the relevant supervisor.



### Infringement in connection with personal data

Under the GDPR, there is a 'personal data breach' in the event of a security breach that accidentally or unlawfully leads to the destruction, loss, alteration or unauthorized disclosure of or unauthorized disclosure access to personal data transmitted, stored or otherwise processed.

### Report to the Dutch Data Protection Authority

If an infringement involving personal data has taken place, AMDAX will report this without unreasonable delay and, if possible, no later than 72 hours after having become aware of it, to the Dutch Data Protection Authority (and also to the AFM if the infringement also qualifies as an 'incident' 'in accordance with AMDAX's incident statement), unless it is unlikely that the personal data breach would pose a risk to the rights and freedoms of natural persons.

Whether the personal data breach constitutes a risk to the rights and freedoms of natural persons depends on the following factors:

- The type of infringement (for example, unlawful access or loss of personal data);
- The nature, sensitivity and amount of personal data;
- Simple identification of individuals (how easy it is to identify a natural person from the data);
- The severity of consequences for individuals;
- Special characteristics of the individual (children and vulnerable groups entail a higher risk); and
- The number of people affected.

If the report to the Dutch Data Protection Authority does not take place within 72 hours, AMDAX provides a good explanation for the delay.

The notification shall at least describe or communicate the following:

- The nature of the personal data breach, where possible specifying the categories of data subjects and personal data records involved and, approximately, the number of data subjects and personal data records involved;
- The name and contact details of a contact person for more information;
- The likely consequences of the personal data breach;
- The measures proposed or taken by AMDAX to address the personal data breach, including, where appropriate, the measures to limit any adverse effects thereof.

### Communication to the person(s) involved

If the personal data breach is likely to pose a high risk to the rights and freedoms of natural persons, AMDAX shall immediately inform the data subject of the personal data breach.

The communication to the person concerned contain a description, in clear and simple language, of the information provided to the Dutch Data Protection Authority (see above).

The communication to the data subject is not required if one of the following conditions is met:

- AMDAX has taken appropriate technical and organizational protection measures and these measures have been applied to the personal data covered by the personal data breach, in particular those that make the personal data incomprehensible to unauthorized persons, such as encryption;
- AMDAX has taken retrospective measures to ensure that the high risk to the rights and freedoms of those involved is unlikely to occur;



- The communication would require disproportionate efforts. In that case, a public announcement or similar measure replaces data subjects with the same effectiveness.

The Dutch Data Protection Authority may oblige AMDAX to report the data subject infringement to the data subject.

#### Procedure for the infringement of personal data.

The following procedure is used within the organization with regard to a personal data breach:

- If discovered by an employee: every employee who suspects an infringement with regard to personal data must immediately report this to management;
- If discovered by a client: a client sends a message or contacts us by telephone. The person at AMDAX who receives the report from the client must immediately report this to management;
- If discovered by a third party: a third party sends a message or contacts us by telephone. The person at AMDAX who receives the report from the third party must immediately report this to management;
- Management (and possibly a third party involved) investigate the scope and technical aspects of the infringement:
  - Which breach of security measures has occurred and when?
  - Which part of the IT system is involved and/or which equipment? For example, where is equipment lost/stolen?
  - Which data is (possibly) involved?
  - What are the (expected) consequences of the incident?
- Management (and possibly a third party involved) ensures that measures are taken to restore security;
- AMDAX keeps records of the infringement (facts, data and communication regarding the infringement). Other internal security incidents are also recorded, regardless of whether the infringement is reported to the supervisor and/or the person(s) involved.

#### Data processing outsourcing

##### Enable processors

AMDAX also outsources the processing of personal data to processors. AMDAX ensures that these processors offer sufficient guarantees with regard to technical and organizational security measures with regard to the processing of personal data.

AMDAX enters into a processor agreement with each processor, stating that the processing is done in accordance with the GDPR, that the processor has implemented sufficient technical and organizational security measures, and that the processor informs AMDAX of any information security incidents.

#### International data traffic

Because AMDAX uses one or more processors, it is possible that data will be transferred to countries outside the Netherlands. Within the European Union and the European Economic Area, the level of data protection is similar and personal data can easily be transferred, provided that all other legal obligations are met by AMDAX and the processor.

Data traffic to countries outside the European Union and the European Economic Area is only permitted by law if that country guarantees an adequate level of protection. The European Commission has published a list of countries that offer an adequate level of



protection. One of the countries on the list is the United States, but only for transfer of data on the basis of the 'EU-US privacy shield'. Companies in the US can be certified under the privacy shield since August 1, 2016, after which they are entered in a register. Every certified company in the US is deemed to have an appropriate level of protection for the duration of the certification.

Data traffic with countries without an adequate level of protection is only possible under certain conditions as stated in the GDPR, for example with the express consent of the person(s) involved.



## Annex II - Procedure relating to rights of the data subjects

Under the GDPR, persons whose data is processed have various rights with respect to such processing. AMDAX has set up a procedure so that requests from clients exercising their rights can be handled correctly. Under the GDPR, the data subjects have the following rights:

- Right to access
- Right to rectification and alteration
- Right to object
- Right to limit processing
- Right to data portability
- Right to erasure (*right to be forgotten*)
- Right with regard to automated decision-making and profiling

In respect of all these rights, a data subject can invoke his or her right by contacting AMDAX (for example by telephone, in person or by email). We will first verify whether the person making the request is actually the person concerned, for example by asking for identification. If this is proven, AMDAX will proceed with the relevant procedure.

AMDAX will respond as quickly as possible, but in any event no later than 1 month after the request. If it takes more time to process the data subjects' request, AMDAX will inform the data subject accordingly.

### Right to view

AMDAX will provide the following information in writing and in a safe manner to the person concerned:

- The processing purposes;
- The categories of personal data concerned;
- The recipients or categories of recipients to whom the personal data have been or will be provided, in particular recipients in third countries or international organizations;
- If possible, the period during which the personal data is expected to be stored, or if that is not possible, the criteria to determine that period;
- That the data subject has the right to request AMDAX that personal data be rectified or deleted, or that the processing of personal data concerning him or her is restricted, and the right to object to such processing;
- That the person concerned has the right to lodge a complaint with a supervisory authority;
- If the personal data is not collected from the data subject, all available information about the source of that data;
- The existence of automated decision-making, including profiling referred to in the GDPR, and, at least in those cases, useful information about the underlying logic, as well as the importance and the expected consequences of that processing for the data subject.

The data subject can also request AMDAX for access to the personal data that is processed from him or her. AMDAX then provides the data subject with a copy of the personal data that is being processed. If the person concerned requests additional copies, AMDAX may charge a reasonable fee based on the administrative costs. If the person concerned submits his or her request electronically and does not request another arrangement, the





information is provided in a conventional electronic form (if possible and/or necessary also secured).

#### Right to rectification

A data subject can request AMDAX to rectify his or her personal data. AMDAX will ask the data subject which information is inaccurate and/or incomplete and how this information must be corrected.

Any changes will be clearly documented by AMDAX and submitted to the person concerned for assessment and approval. If approval is received, the document will be added to the file of the person concerned and the data must be corrected in accordance with such documentation.

If AMDAX has provided incorrect or incomplete personal data to third parties, AMDAX will pass on the corrected data to the third party involved. If requested by the data subject, AMDAX will inform the data subject of the name of such third party.

#### Right to object

The data subject has the right, at any time, to object, on grounds relating to his or her particular situation, to processing of personal data concerning him or her. AMDAX will ask the data subject against which processing of which personal data the data subject specifically objects. Unless AMDAX has compelling legitimate grounds for the processing of the personal data which overrides the interests, rights and freedoms of the data subject, or for the establishment, exercise or defence of legal claims, AMDAX will stop the processing against which the data subject objects. As long as it is not clear whether the grounds of AMDAX overrides the rights of the data subject, AMDAX may not process the relevant data. AMDAX will then set a processing limit. If the person concerned objects to the processing of personal data for direct marketing, AMDAX will stop processing for marketing purposes immediately.

If AMDAX has provided personal data to third parties, AMDAX will inform these third parties that the data subject has objected to the processing of his or her personal data. If a person asks for it, AMDAX will inform the data subject of the name of such third party.

#### Right to restriction of processing

The data subject has the right to obtain from AMDAX restriction of processing if one of the following applies:

- **Data may be incorrect:** if the person concerned indicates that AMDAX uses incorrect personal data, AMDAX may not use this data as long as AMDAX has not yet verified that the data is correct.
- **The processing is unlawful:** AMDAX is not allowed to process certain data and the data subject does not want AMDAX to erase the personal data. For example, because he or she wants to request the data at a later moment.
- **Data is no longer needed:** AMDAX no longer needs the personal data for the purpose for which AMDAX has collected it, but the data subject still needs the personal data for legal action.
- **The person concerned objects:** The data subject objected to processing of its personal data and AMDAX is in the process of determining whether the legitimate grounds of AMDAX override those of the data subject.

If AMDAX has provided personal data to third parties, AMDAX will inform these third parties that the data subject has objected to the processing of his or her personal data. If a person asks for it, AMDAX will inform the data subject of the name of such third party.



### Right to data portability

The right to data portability means that people have the right to receive the personal data that AMDAX has from them, for example to be able to easily transfer the data to a third party. Data subjects can also request that data be transferred directly to a third party (if this is technically possible).

AMDAX will ask with regard to which personal data he or she makes the request for data portability. The right of the person concerned only relates to digital data (not physical files) that AMDAX processes with the permission of the person concerned or that are processed to carry out an agreement with the person concerned. In addition, only data that clients have provided to AMDAX (directly or by using the services or products of AMDAX) needs to be made available. The right to data portability does not relate to derived data that AMDAX itself has generated, such as a profile that AMDAX has drawn up of the data subject. However, the data subject has the right to view this data (see above).

AMDAX provides the data in a structured, commonly used and machine-readable format.

### Right to erasure (right to be forgotten)

The data subject has the right to request AMDAX to erase the personal data processed by AMDAX. AMDAX will ask the data subject to specify which personal data the data subject wishes to be deleted. The personal data will be deleted if one of the following grounds applies:

- the personal data is no longer necessary for the purpose for which the data was collected and there is no other reason to store this personal data;
- the purpose for processing the personal data is based on the consent of the data subject and the data subject who withdraws consent;
- the person concerned objects to the processing and AMDAX has no compelling reasons to process the data;
- the personal data has been processed unlawfully;
- the personal data must be deleted in order to comply with a legal obligation laid down in European or national law.

AMDAX will comply with the data subject's request without undue delay, unless processing is necessary:

- for exercising the right of freedom of expression and information;
- for compliance with a legal obligation which requires processing in connection with the public interest;
- in connection with any legal proceeding;
- for reasons of public interest in the area of public health.

If AMDAX has provided personal data to third parties, AMDAX will inform these third parties that the data subject has requested the deletion of personal data. If a person asks for it, AMDAX will inform the data subject of the name of such third party.

### Right not to be subject to automated decision making

The person concerned has the right not to be subjected to a decision based solely on automated processing, including profiling, which has legal consequences for him or her or that otherwise significantly affects him or her. If the person concerned invokes this right, AMDAX will assess the processing of personal data. AMDAX will ask the person concerned to specify with regard to which decision AMDAX has taken, he or she makes the request. If



AMDAX honors the request, AMDAX will assess the processing of personal data again and make a new decision.