Foris DAX Middle East FZE Privacy Notice

Last update: 15 July 2024

Welcome to Foris DAX Middle East FZE Privacy Notice ("Privacy Notice"). Please spend a few minutes to read it carefully before providing us with any information about you or any other person. If you are a resident of any country other than the UAE, please refer to our privacy and data practices which apply in your country of residence.

Contents

1. Introduction 2
2. Purpose 2
3. Who we are 2
4. What data we collect about you 3
5. How we collect your data 6
6. How we use your data 7
7. Disclosures of your data 14
8. International transfers 14
9. Data security 15
10. Data retention 16
11. Your legal rights 16

1. Introduction

We respect your privacy, and we are committed to protecting your personal data. This Privacy Notice applies to the processing of personal data by Foris DAX Middle East FZE ("Crypto.com", "we", "us", "our") in connection with:

- use of any of our products, services or applications (together the "Services"),
- visit or use of our website including the Exchange subdirectory ("Sites") or, main mobile application ("Crypto.com App") or exchange mobile application ("Crypto.com Exchange App") (together, the "Apps").

Please note that our Services, Sites and Apps are not intended for minors below 18 years of age and we do not knowingly collect data relating to minors.

For services provided by other Crypto.com companies, please carefully read the respective privacy notice or policy available on the Sites or in the Apps.

2. Purpose

This Privacy Notice aims to give you information on how we collect and process your personal data.

This Privacy Notice informs you about your privacy rights and how the data protection principles set out in the Federal Decree-Law No. 45 of 2021 On the Protection of Personal Data ("Data Protection Code") of the United Arab Emirates outside any of the UAE financial free zones ("UAE") protect your personal data as a UAE resident.

It is important that you read this Privacy Notice together with any other notice we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of how and why we are using your data. This Privacy Notice supplements other notices and is not intended to override them.

Please note that all or part of our Services may not be available in your region.

3. Who we are

Data Controller

The controller of your personal data is the legal entity that determines the purposes, conditions and manner of any processing activities that it carries out. Foris DAX Middle East FZE is the data controller and is responsible for the processing of your personal data.

Foris DAX Middle East FZE is established as a Free Zone Establishment in the Dubai World Trade Centre fee zone in the Emirate of Dubai, the United Arab Emirates, with limited liability ("we" or "us"), with company registration number 2125 and registered address at: the 8th floor, offices 4, One Central, Dubai World Trade Centre, Dubai, United Arab Emirates.

Data Protection Officer

We have appointed a Data Protection Officer ("DPO") who is responsible for overseeing questions in relation to this Privacy Notice. If you have any questions or complaints related to this Privacy Notice or our privacy practices, or if you want to exercise your legal rights, please contact our

DPO at dpo@crypto.com.

Complaints

You have the right to make a complaint to the UAE Data Office about the way we process your personal data. The UAE Data Office is the UAE supervisory authority for data protection issues.

We would, however, appreciate the chance to deal with your concerns before you approach the UAE Data Office or other relevant authority, so please feel free to contact us in the first instance.

Our duties and your duties in case of changes

We keep our Privacy Notice under regular review. This version was last updated on the date above written. Please check from time to time for new versions of the Privacy Notice. We will also additionally inform you on material changes of this Privacy Notice in a manner which will effectively bring the changes to your attention.
It is important that the personal data we hold about you is accurate and up-to-date. Please keep us informed if your personal data changes during your relationship with us.

Third-party links

The Sites and any applicable web browser, the Apps or application programming interface required to access the Services ("Applications"), may include links to third-party websites, plug-ins and applications ("Third-Party Sites"). Clicking on those links or enabling those connections may allow third-parties to collect or share data about you. We do not control these Third-Party Sites and are not responsible for their privacy statements and policies. When you leave our Sites or Applications, we encourage you to read the privacy notice or policy of every Third-Party Site you visit or use.

4. What data we collect about you

Personal data

Personal data, or personal information means any information relating to an identified natural person (a "Data Subject"), or one who can be identified directly or indirectly by way of linking data, using identifiers such as name, voice, picture, identification number, online identifier, geographic location, or one or more special features that express the physical, psychological, economic, cultural or social identity of such person. It does not include data where the identity has been removed (anonymous data).

It also includes Sensitive Personal Data which is any data that directly or indirectly reveals a natural person's family, racial origin, political or philosophical opinions, religious beliefs, criminal records, biometric data, or any data related to the health of such person, such as his/her physical, psychological, mental, genetic or sexual condition, including information related to health care services provided thereto that reveals his/her health status.

Different pieces of information, which collected together can lead to the identification of a particular person, also constitute personal data. It does not include data where the identity has been removed (anonymous data).

Depending on whether and how you use our Services, Sites or Apps, we will collect, use, store and transfer different kinds of personal data about you which we have grouped in categories as

follows:

Category of Personal Data	Examples of specific pieces of personal data
Identity Data	● first name; ● maiden name; ● last name; ● username or similar identifier; ● title; ● employment status; ● date of birth and gender; ● biometric information, including a visual image of your face, ● video and voice recording; and ● national identity card, passport, driving license or other form of identification document.
Social Identity Data	● your group/company data; ● information on referrals related to you; ● political background; ● close connections; ● behavioral data; ● risk assessment; and ● compliance assessment.
Contact Data	● residence details; ● billing address; ● delivery address; ● home address; ● work address; ● email address and telephone number(s); and ● proof of address documentation.

Financial Data	● bank account; ● payment card details; ● virtual currency account(s); ● stored value account(s); ● amounts associated with account(s); ● external account details; ● annual income range; and ● source of funds and related documentation.
Transactional Data	● details about payments to and from you; and ● other details of any transactions you enter into using the Services, Sites or Apps.
Investment Data	● information about your: ○ investment objectives (e.g. expected annual transaction volume range); ○ investment experience; and ○ prior investments.
Technical Data	● internet connectivity data; ● internet protocol (IP) address; ● operator and carrier data; ● login data; ● browser type and version; ● device type, category and model; ● time zone setting and location data; ● language data; ● application version and SDK version; ● browser plug-in types and versions; ● operating system and platform; ● diagnostics data such as crash logs and any other data we collect for the purposes of measuring technical diagnostics; and ● other information stored on or available regarding the devices you allow us access to when you visit the Sites, or use the Services or the Apps.

Profile Data	• your username and password; • your identification number as our user; • information on whether you have an account and the email associated with your accounts; • requests by you for products or services; • your interests, preferences and feedback; and • other information generated by you when you communicate with us, for example when you address a request to our customer support.

Usage Data	• information about how you use the Sites, the Services, the Apps and other offerings made available by us, including:
	  ○ device download time;
	  ○ install time;
	  ○ interaction type and time; and
	  ○ event time, name and source.

Marketing and Communications Data	• your preferences in receiving marketing from us or third-parties, your communication preferences; and • your survey responses.

As explained above under Identity Data, we may also collect a visual image of your face which we will use, in conjunction with our sub-contractors (see Section 7), to check your identity for onboarding purposes. This data falls within the scope of Sensitive Personal Data (a.k.a. special categories of personal data) which warrants extra protection.

We may also ask you to prove ownership or control of a particular blockchain address. We are required to ask for certain information to comply with anti-money laundering and counter-financing of terrorism requirements, and to ensure we safeguard against and report any suspicious activity.

If you refuse to provide personal data

Where we need to collect personal data by law, or under the terms of a contract we have with you and you refuse to provide that data when requested, we may not be able to perform the contract we have or are trying to enter into with you – for example, to provide you services. In this case, we may have to cancel a product or service you have with us, but we will notify you if this is the case at the time.

5. How we collect your data

We use different methods to collect data from and about you including through:

Direct interactions. You may give us your Identity Data, Social Identity Data, Contact Data, Financial Data, Profile Data and Marketing and Communications Data by filling in forms, providing a visual image of yourself via the Services, by email or otherwise. This includes personal data you provide when you:

- visit our Sites or Apps;
- apply for our Services;
- create an account;
- access or make use of any of our Services;
- request marketing to be sent to you, for example by subscribing to our newsletters;
- enter a competition, promotion or survey, including through social media channels;
- give us feedback or contact us.

Automated technologies or interactions. As you interact with us via our Sites or Apps, we will automatically collect Technical Data about your equipment, browsing actions and patterns. We collect this personal data by using cookies, server logs and other online identifiers. We will also collect Transactional Data, Investment Data and Usage Data. We may also receive Technical Data and Marketing and Communications Data about you if you visit other websites employing our cookies. You may find more information about how we use cookies through the Cookie Preferences.

Third parties or publicly available sources. We also obtain information about you, including Social Identity Data, from third parties or publicly available sources. These sources may include:

- fraud and crime prevention agencies,
- a customer referring you,
- public blockchain,
- publicly available information on the Internet (websites, articles etc.)

6. How we use your data

Lawful basis

We will only use your personal data when the applicable legislation allows us to. In other words, we have to ensure that we have a lawful basis for such use. We rely for the processing your personal data on the principles and legal bases provided by the Data Protection Code for the processing of your personal data.

Most commonly, in the absence of your consent, we will use your personal data on the legal bases provided for under the Data Protection Code which includes (among others) the following relevant legal bases:

- **public interest**: means processing your data where it is necessary to protect the public interest;
- **legal proceedings**: means processing your data where it is necessary to initiate or defend legal proceedings or in relation to judicial or security procedures;

- **protection of your interests**: means processing your personal data where it is necessary to protect your interests;
- **performance of a contract**: means processing your data where it is necessary for the performance of a contract to which you are a party or to take steps at your request before entering into such a contract; we use this basis for provision of our Services; and
- **compliance with a legal obligation**: means processing your personal data where we need to comply with a legal obligation we are subject to.

Purposes for which we use your personal data

We have set out below a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so.

Note that we may process your personal data on more than one lawful ground depending on the specific purpose for which we are using your data. We establish the applicable legal basis prior to the processing activity and in relation to the specific purpose. Please contact us if you need details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To register you as a new customer	• Identity Data • Social Identity Data • Contact Data • Financial Data	• Performance of a contract
To carry out and comply with anti-money laundering requirements	• Identity Data • Social Identity Data • Contact Data • Financial Data	• Compliance with a legal obligation
To process and deliver our Services and any of our Apps' features to you, including to execute, manage and process any instructions or orders you make	• Identity Data • Contact Data • Financial Data • Transactional Data • Technical Data • Marketing and Communications Data	• Performance of a contract

To prevent abuse of our Services and promotions	• Identity Data • Contact Data • Financial Data • Transactional Data • Technical Data • Marketing and Communications Data	• Public interest • Consent, if required
To manage our relationship with you which will include asking you to leave a review, take a survey or keeping you informed of our company's business and product development	• Identity Data • Contact Data • Profile Data • Transactional Data • Marketing and Communications Data	• Performance of a contract • Consent, if required
To keep our records updated and to study how customers use our products/services	• Identity Data • Contact Data • Profile Data • Transactional Data • Marketing and Communications Data	• Consent, if required
To manage, process, collect and transfer payments, fees and charges, and to collect and recover payments owed to us	• Identity Data • Contact Data • Financial Data	• Performance of a contract
To obey applicable legislation and handle complaints, including: manage risk and crime prevention involving performance of anti-money laundering, counter terrorism, sanction screening, fraud	• Identity Data • Social Identity Data • Contact Data • Financial Data • Technical Data • Transactional Data • Investment Data • Sensitive Personal Data (a.k.a. Special Categories	• Compliance with a legal obligation • Performance of a contract • Consent, if required

and other background checks detect, investigate, report and prevent financial crime in the broad sense ensure your account's security, in order to honour requests regarding information and/or changes to your account	Data) data that you give us directly or that we receive from third-parties and/or publicly available sources: - data which might be revealed by KYC or other background checks (for example, because it has been reported in the press or is available in public registers); - data that is incidentally revealed by photographic ID although we do not intentionally process this personal data;	
To enable you to partake in a prize draw, competition or survey	● Identity Data ● Contact Data ● Profile Data ● Usage Data ● Marketing and Communications Data	● Performance of a contract ● Consent, if required
To gather market data for studying customers' behaviour including their preference, interest and how they use our products/services, determining our marketing campaigns and growing our business	● Identity Data ● Contact Data ● Profile Data ● Usage Data ● Marketing and Communications Data	● Consent
To administer and protect our business, our Sites, Apps and social media channels including bans, troubleshooting, data analysis, testing, system maintenance, support, reporting, hosting of data	● Identity Data ● Contact Data ● Financial Data ● Technical Data ● Transactional Data ● Investment Data	● Performance of a contract • Consent

To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	• Identity Data • Contact Data • Profile Data • Usage Data • Technical Data • Marketing and Communications Data	• Consent
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	• Technical Data • Usage Data	• Consent
To make suggestions and recommendations to you about goods or services that may be of interest to you	• Identity Data • Contact Data • Technical Data • Usage Data • Profile Data • Investment Data • Marketing and Communications Data	• Consent
To use the services of social media platforms or advertising platforms some of which will use the personal data they receive for their own purposes, including marketing purposes	• Technical Data • Usage Data	• Consent

To use the services of financial institutions, crime and fraud prevention companies, risk measuring companies, which will use the personal data they receive for their own purposes in their capacity of independent controllers	• Identity Data • Social Identity Data • Contact Data • Financial Data • Transactional Data • Investment Data • Technical Data • Usage Data	• Performance of a contract
To record voice calls for compliance, quality assurance and training purposes	• Identity Data • Social Identity Data • Contact Data • Financial Data • Transactional Data	• Performance of a contract

Automated Decision Making

What is an automated decision?

Automated decision is usually a decision that may impact you and is made automatically based on software algorithms, without human intervention. As an illustrative example, we use automated decisions to complete the onboarding process of a new customer or to perform anti-fraud monitoring.

Why is an automated decision important to you?

Depending on the particular case, using your personal data may lead to automated decisions being taken (including profiling) that legally affect you or similarly significantly affect you.

How do we protect your interests regarding automated decisions?

The rights and interests of individuals whose personal data undergoes automated decision-making is safeguarded through appropriate measures. When an automated decision is made about you, you have the right to oppose the decision, to express your opinion, and to require human intervention regarding the decision. If you need more detailed information or wish to exercise this right, please contact us.

Marketing

We may use your Identity Data, Contact Data, Technical Data, Transactional Data, Usage Data, Investment Data and Profile Data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you (we call this marketing).

You will receive marketing communications from us if you have requested information from us and consented to receive marketing communications, or if you have purchased from us and you have not opted out of receiving such communications. We will use your Marketing and Communications Data for our respective activities.

Third-party marketing

We will get your opt-in consent before we share your personal data with any third party for marketing purposes.

Opting out

You can ask us to stop sending you marketing messages at any time by following the opt-out links on any marketing message sent to you.
Further, you can let us know directly that you prefer not to receive any marketing messages by emailing dpo@crypto.com.

Where you opt out of receiving marketing messages, this will not apply to service messages which are directly related to the use of our Services (e.g. maintenance, change in the terms and conditions and so forth).

Cookies

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of the Services or Sites may become inaccessible or not function properly. For more information about the cookies we use, please review the Cookie Preferences.

Change of purpose

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. If you wish to get an explanation as to how the processing for the new purpose is compatible with the original purpose, please contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Sale or transfer of business

We may also need to process your data in connection with or during the negotiation of any merger, financing, acquisition, bankruptcy, dissolution, transaction or proceeding involving all or a part of our shares, business or assets in which case we may need to seek your consent.

7. Disclosures of your data

We share your personal data with our third-party service providers, agents, subcontractors and other associated organisations, our group companies and affiliates in order to complete tasks and provide the Services to you on our behalf. When using third-party service providers, they are required to respect the security of your personal data and to treat it in accordance with the law.

We may pass your personal data to the following parties:

- companies and organisations that assist us in processing, verifying or refunding transactions/orders you make and in providing any of the Services that you have requested;
- identity verification agencies to undertake required verification checks;
- a global, secure, and industry-driven solution designed to comply with a requirement known as the Travel Rule;
- fraud or crime prevention agencies to help fight against crimes including fraud, money-laundering and terrorist financing;
- anyone to whom we lawfully transfer or may transfer our rights and duties under the relevant terms and conditions governing the use of any of the Services;
- any third-party because of any restructure, sale or acquisition of our group or any affiliates, provided that any recipient uses your information for the same purposes as it was originally supplied to us and/or used by us; and
- regulatory and law enforcement authorities, whether they are outside or inside of the UAE, where the law allows or requires us to do so.

Regarding the Travel Rule, we and other custodial cryptocurrency exchanges and financial institutions share certain basic information about their customers when handling a cryptoasset transfer over a certain amount to another financial institution.

Specifics regarding the use of the blockchain
The blockchain technology used in the provision of certain Services operates on a decentralised network, where transactions are recorded in an immutable and transparent manner. This characteristic ensures the integrity and security of the data stored on the blockchain. However, it also means that once data is added to the blockchain, it becomes virtually impossible to remove or delete it.

8. International transfers

As part of our operations, your personal data may be processed by entities within our group or by external third parties located outside the UAE. To safeguard your data in these instances, we adhere to stringent measures in line with UAE regulations:

- We prioritize transferring personal data to countries recognized by the UAE as providing adequate data protection. This includes nations listed by the UAE for their data protection standards or those engaged in bilateral or multilateral data protection

agreements with the UAE.

- For countries not meeting these criteria, we ensure one of the following safeguards is in place:
    - Binding contractual agreements with the data-receiving parties, obligating them to adhere to the UAE Data Protection Code standards.
    - Transfers serving specific purposes, such as:
        a. Fulfilling legal obligations or defending legal rights.
        b. Contractual necessities involving you or a third party for your benefit.
        c. Engaging in international judicial cooperation.
        d. Upholding public interest.
- In certain situations, we may transfer personal data outside the UAE if we determine that there are sufficient legal grounds under the UAE Data Protection Code.
- Alternatively, transfers may occur based on your explicit written consent.

For more details on the mechanisms, we use for international data transfers, please feel free to contact us.

9. Data security

While there is an inherent risk in any data being shared over the internet, we have put in place appropriate security measures to prevent your personal data from being accidentally lost, used, damaged, or accessed in an unauthorised or unlawful way, altered, or disclosed. In addition, we limit access to your personal data to those employees, agents, contractors and other third parties who have a legitimate business need to know. They will only process your personal data on our instructions, and they are subject to a duty of confidentiality.

Depending on the nature of the risks presented by the proposed processing of your personal data, we will have in place the following appropriate security measures:

- **organisational measures** (including but not limited to staff training and policy development);
- **technical measures** (including but not limited to physical protection of data, pseudonymization and encryption); and
- **securing ongoing availability, integrity, and accessibility** (including but not limited to ensuring appropriate back-ups of personal data are held).

We have put in place procedures to deal with any suspected personal data breach and will notify you and any relevant regulator of a breach where we are legally required to do so.

If you want to know more about our security practice, please visit this link.

10. Data retention

The UAE Data Protection Code does not specify a fixed duration for retaining personal data. Our approach to determining the retention period considers various factors, such as the volume, type, and sensitivity of the personal data, the risk of harm from unauthorized access or disclosure, the objectives of processing your data and if these can be achieved through other means, and relevant legal, regulatory, tax, accounting, or other obligations.

Upon concluding that your personal data is no longer necessary for the purposes for which it was collected, we will either delete or anonymize it.

Here are key considerations influencing our decision on the duration of data retention:

- In case of a complaint, we may retain relevant data.
- If there's a reasonable chance of litigation related to our relationship with you, or for defending potential future legal claims, we may keep certain data (like email addresses, chat content, letters) for up to 8 years after our relationship ends, in line with the UAE's limitation period.
- To comply with legal and regulatory requirements, certain data (e.g., for audit purposes) may be retained as needed.
- We may retain data in accordance with industry standards or guidelines.
- For our legitimate business interests, such as preventing abuse in promotions, we retain customer data for the duration of the promotion and a specified period thereafter to deter abusive practices.

Please note that under certain condition(s), you can ask us to delete your data: see Section Your Legal Rights for further information. We will honor your deletion request ONLY if the condition(s) is/are met. However, when interacting with any blockchain, we may not be able to ensure that your personal data is deleted. This is because blockchains are public decentralised networks and blockchain technology does not generally allow for data to be deleted and your right to erasure may not be able to be fully enforced. In these circumstances, we will only be able to ensure that all personal data that is held by us is permanently deleted.

11. Your legal rights

You have rights we need to make you aware of. The rights available to you depend on our reason for processing your personal data. If you need more detailed information or wish to exercise any of the rights set out below, please contact us.

You may, among other things:

- request access to your personal data, which enables you to obtain confirmation of whether we are processing your personal data, to receive a copy of the personal data we hold about you and information regarding how your personal data is being used by us;
- request rectification of your personal data by asking us to rectify information you think is inaccurate and to complete information you think is incomplete, though we may need to verify the accuracy of the new data you provide to us;

- request erasure of your personal data by asking us to delete or remove personal data we hold about you; note, however, that we may not always be able to comply with your request of erasure for specific legal reasons which will be notified to you;
- object to or require that decisions be reconsidered if they are made solely by automated means, without human involvement; we use automated tools to make sure that you are eligible to be our customer taking into account our legal obligations; if these automated tools indicate that you do not meet our acceptance criteria, we will not onboard you as our customer;
- request restriction of processing your personal data, which enables you to ask us to suspend the processing of your personal data, if you want us to establish the data accuracy; where our use of the data is unlawful, but you do not want us to erase it; where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims, or if you have objected to our use of your data;
- object to and request that the processing of your personal data, if the processing is unlawful, or for the purposes of direct marketing (including profiling) or conducting statistical surveys (provided the survey is not necessary to achieve the public interest);
- request the transfer of your personal data to you or to a third party, and we will provide to you, or a third party you have chosen (where technically feasible), your personal data in a structured, commonly used, machine-readable format; note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a contract with you;
- withdraw consent at any time where we are relying on consent to process your personal data; however, this will not affect the lawfulness of any processing carried out before you withdraw your consent; if you withdraw your consent, we may not be able to provide certain products or services to you, but we will advise you if this is the case at the time you withdraw your consent;
- complain to the UAE Data Office or any relevant authority about any perceived violation and to seek compensation for damages in the courts.

No fee usually required

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is not of the type which is required to be provided free of charge under the Data Protection Code. Alternatively, we could refuse to comply with your request in these circumstances.

Time limit to respond

We try to respond to all legitimate requests within one month. Occasionally, it could take us longer than one month if your request is particularly complex or you have made several requests, also if more time is required to consult with a third party or other data controller (if needed) before we can reply to your request; In this case, we will notify you and keep you updated.