Foris DAX KY Group Privacy Notice

Last Material Update: 3 September 2021
Introduction

Welcome to Foris DAX KY Group 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.

Contents

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 KY Group ("Crypto.com", "we", "us", "our") in connection with:

- use of services through our Applications or through other facilities provided by or on behalf of Foris DAX KY Group ("Services"),
- visit or use of the relevant sections of the website ("Site") under which Foris DAX KY Group promotes all or part of its Services.

Please note that our Services and Site are not intended for minors below the age of 18 years 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 Crypto.com or in the Crypto.com App.

2. Purpose

This Privacy Notice aims to give you information on why and 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 Data Protection Law, 2017 of the Cayman Islands ("DPL") protect you.

If you are resident of the European Economic Area ("EEA") or the United Kingdom ("UK"), please make sure that you review also Section 12 below.

It is important that you read this Privacy Notice together with any other notice or policy we may provide on specific occasions when we are collecting or processing personal data about you so that you are fully aware of why and how we are using your data. This Privacy Notice supplements other notices and policies 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 KY Group is the data controller and is responsible for the processing of your personal data.

Foris DAX KY Group is an exempted company incorporated in the Cayman Islands with limited liability, with company registration number QH-331723 and registered address at: 94 Solaris Avenue Camana Bay PO Box 1348 Grand Cayman KY1-1108 Cayman Islands.

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 Cayman Islands Ombudsman ("Ombudsman") about the way we process your personal data. The Ombudsman is the Cayman Islands supervisory authority for data protection issues. Further details about making a complaint to the Ombudsman are available on its official website.

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

If you are a resident of the EEA or the UK, please make sure that you review also Section 12 below.

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 Site and any applicable web browser, smartphone application 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 Site 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 about a living individual from which that person can be identified. It does not include data where the identity has been removed (anonymous data). More information could be found here.

If you are a resident of the EEA or the UK, please make sure that you review also Section 12 below.

Depending on whether and how you use our Services, Site or Crypto.com App, 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	Specific Pieces of Personal Data
Identity Data	• first name, • maiden name, • last name, • username or similar identifier, • title, • date of birth and gender, • biometric information, including a visual image of your face, • national identity cards, • passports, driving licences or other forms of identification documents.

Category of Personal Data	Specific Pieces of Personal Data
Social Identity Data	• your group/company data, • information on referrals related to you, • political background, • close connections, • behavioural data, • risk assessment, • compliance assessment.
Contact Data	• residence details, • billing address, • delivery address, • home address, • work address, • email address and telephone numbers, • proof of address documentation.
Financial Data	• bank account, • payment card details, • virtual currency accounts, • stored value accounts, • amounts associated with accounts, • external account details, • source of funds and related documentation.
Transactional Data	• details about payments to and from you, • other details of any transactions you enter into using the Services, Site or Applications.

Investment Data	• information about your:
	  ○ investment objectives,
	  ○ investment experience,
	  ○ prior investments.

Category of Personal Data	Specific Pieces of Personal Data
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 Site, or use the Services or the Applications.
Profile Data	• your username and password, • your identification number as our user, • your Crypto.com App account and the email associated with your accounts, • requests by you for products or services, • your interests, preferences and feedback, • 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 Site, the Services, mobile applications and other offerings made available by us, including:
	  ◦ device download time,
	  ◦ install time,
	  ◦ interaction type and time,
	  ◦ event time, name and source.

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

As explained above under Identity Data, we will also collect a visual image of your face which we will use, in conjunction with our sub-contractors (See Section Disclosures of Your Data below), to check your identity for onboarding purposes. This data falls within the scope of sensitive personal data.

Sensitive personal data

In addition, the DPL also treats certain categories of personal information as sensitive and accordingly such sensitive data warrants extra protection.

We will only collect, use, store and transfer your sensitive data, if we are able to satisfy both the requirement of a lawful basis and at least one among specific additional conditions.

For more information on the lawful bases, please see How we use your data section below.

The additional conditions include:

- **circumstances prescribed by regulations**: personal data are processed in such circumstances prescribed by regulations;
- **consent**: you have given consent to the processing of your sensitive data;
- **information made public by yourself**: the sensitive data has been made public as a result of steps you have taken;
- **legal proceedings**: the processing is necessary for the purpose of, or in connection with any legal proceedings, for obtaining legal advice, or is otherwise necessary for establishing, exercising, or defending legal rights;
- **public functions**: the processing is necessary for the exercise of any functions conferred on any person by or under an enactment.

See also the respective row in the table below which describes the purposes for which we will use your personal data.

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 directly interacting with us, including by filling in forms, providing a visual image of yourself via the Service, by email or otherwise. This includes personal data you provide when you:

- visit our Site or Applications;
- apply for our Services;
- create an account;
- 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 Site or Applications, 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 similar technologies. 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 personal 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. If you are located in the EEA or the UK, we rely on the principles and legal bases provided by the GDPR for processing your personal data.

Most commonly, we will use your personal data in the following circumstances:

- **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;
- **legitimate interests**: means our interests (or those of a third party), where we make sure we use this basis as far as your interests and individual rights do not override those interests;
- **compliance with a legal obligation**: means processing your personal data where we need to comply with a legal obligation we are subject to;
- **consent**: means freely given, specific, informed and unambiguous indication of your wishes by which you, by a statement or by a clear affirmative action, signify agreement to the processing of personal data relating to you.

Purposes for which we will use your personal data

We have set out below, in a table format, 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. We have also identified what our legitimate interests are where appropriate.

Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. 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 Crypto.com App 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	• Legitimate interests
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

Purpose and/or activity	Categories of personal data	Lawful basis for processing
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	• Legitimate interests • 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 ensure good management of our payments, fees and charges and collection and recovery of payments owned to us	• Identity Data • Contact Data • Financial Data	• Legitimate interests

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To manage risk and crime prevention including performing anti-money laundering, counter terrorism, sanction screening, fraud and other background checks, detect, investigate, report and prevent financial crime in broad sense, obey laws and regulations which apply to us and response to complaints and resolving them	• Identity Data • Social Identity Data • Contact Data • Financial Data • Technical Data • Transactional Data • Investment Data • Sensitive Data (a.k.a. Special Categories 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	• Compliance with a legal obligation • We may also process such data in connection with these purposes if it is necessary for the performance of our contract with you • In addition to our legal obligations, we may process this personal data based on our legitimate interest in ensuring that we are not involved in dealing with the proceeds of criminal activities and do not assist in any other unlawful or fraudulent activities, as well as to develop and improve our internal systems for dealing with financial crime and to ensure effective dealing with complaints • For Sensitive Personal Data (a.k.a. Special Categories Data), it is necessary for reasons of substantial public interest under EU Anti-Money Laundering Legislation as the Cayman Islands are subject to the Council Decision 2013/755/EU on the association of the overseas countries and territories with the European Union ("Overseas Association Decision")

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To enable you to partake in a prize draw, competition or complete a 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' behavior 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	• Legitimate interests: understanding our customers and improving our products and services
To administer and protect our business, our Site, App(s) 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	• Legitimate interests: to run our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganization or group restructuring exercise
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	• Legitimate interests: to study how customers use our products/services, to develop them, to grow our business and to form our marketing strategy • Consent, if required

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	• Technical Data • Usage Data	• Legitimate interests: to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to form our marketing strategy • Consent, if required
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	• Legitimate interests: to develop our products/services and grow our business • Consent, if required
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	• Legitimate interests: to conduct our business activities on the market of financial services, to participate actively in the prevention of crime and fraud

Purpose and/or activity	Categories of personal data	Lawful basis for processing
To record voice calls for compliance, quality assurance and training purposes	• Identity Data • Social Identity Data • Contact Data • Financial Data • Transactional Data	• Legitimate interests: to comply with the industry standards and requirements in payments services, to ensure quality of our service, including by proper training of our personnel

Marketing

We may use your Identity Data, Contact Data, Technical Data, Transactional Data, Investment Data, Usage 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 Site 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. This will be based on our legitimate interests in carrying out such transaction, or to meet our legal obligations.

7. Disclosures of your data

We share your personal data with our third-party service providers, agents, subcontractors and other associated organizations, our group companies, and affiliates (as described below) in order to complete tasks and provide the Services and use of the Crypto.com App 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 entities:

- companies and organizations 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;
- 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 Cayman Islands, where the law allows or requires us to do so.

8. International transfers

We share your personal data within our group. This will involve transferring your data outside the Cayman Islands or the origin of where your data is collected.

Many of our external third parties (described in Section 7 above) are based outside the Cayman Islands so their processing of your personal data will involve an international transfer of your data.

Safeguards

Whenever we transfer your personal data out of the Cayman Islands, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- Where the applicable country or territory is deemed to provide an adequate level of protection for personal data. For the purposes of this requirement, the Ombudsman considers the following countries and territories as ensuring an adequate level of protection:
    - Member States of the European Economic Area (that is, the European Union plus Lichtenstein, Norway, and Iceland) where Regulation (EU) 2016/679 (the General Data Protection Regulation or "GDPR") is applicable. The list of applicable countries and territories can be accessed [here](https://www.gov.uk/eu-eea; or
    - Any country or territory in respect of which an adequacy decision has been adopted by the European Commission pursuant to Article 45(3) GDPR or remains in force pursuant to Article 45(9) GDPR. The list of applicable countries and territories can be accessed here.
- Based on our own adequacy assessment regarding the applicable country or territory pursuant to Schedule 1, Part 2(4) of the DPL.
- Where the Ombudsman has authorised the international transfer.

If you are a resident of the EEA or the UK, please make sure that you review also Section 12 below.

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 DPL does not dictate how long any personal data is required to be kept. To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

If we determine that we no longer need your personal data to fulfil the purposes we collected it for, we will either erase (delete) it or anonymize it.

Here are some exemplary factors which we usually consider when determining how long we need to retain your personal data:

- in the event of a complaint;
- if we reasonably believe there is a prospect of litigation in respect to our relationship with you or if we consider that we need to keep information to defend possible future legal claims (e.g. email addresses and content, chats, letters will be kept up to 6 years following the end of our relationship, in accordance with the limitation period applicable in the Cayman Islands);
- to comply with any applicable legal and/or regulatory requirements with respect to certain types of personal data (e.g. information is needed for audit purposes and so forth);
- in accordance with relevant industry standards or guidelines;
- in accordance with our legitimate business need to prevent abuse of the promotions that we launch. We will retain a customer's personal data for the time of the promotion and for a certain period after its end to prevent the appearance of abusive behaviour.

Please note that under certain condition(s), you can ask us to delete your data: see your legal rights below for further information. We will honor your deletion request ONLY if the condition(s) is met.

If you are a resident of the EEA or the UK, please make sure that you review also Section 12 below.

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:

- 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 the processing of your personal data, where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms; in some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms; you also have the right to object where we are processing your personal data for direct marketing purposes;
- 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 interests and 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, but we need to verify whether we have overriding legitimate grounds to use it;
- 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 Ombudsman 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 manifestly unfounded or excessive. 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 30 days. Occasionally, it could take us longer than 30 days 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.

As per the Guidance of the Ombudsman, for some requests the period for us to reply is 21 days:

- request based on the right to stop or restrict processing,
- request based on the rights in relation to automated decision making.

The said period could be expanded on the same conditions as described in the first paragraph.

If you are a resident of the EEA or the UK, please make sure that you review also Section 12 below.

12. EEA and UK residents

As an EEA resident the EU General Data Protection Regulation (GDPR) applies to you. As a UK resident the post-Brexit privacy law publicly known as the UK GDPR applies to you. In some sections throughout this Privacy Notice we encourage you to check this content as it provides you with certain specificities, please read it carefully.

What is personal data

Personal data, or personal information means any information that relates to an identified or identifiable living individual. This is a broad definition which includes the specific pieces of personal data which we have described below. It does not include data which cannot be used to identify an individual person, such as a company registration number.

A "data subject" is an individual who can be identified, directly or indirectly, by personal data. This is usually by reference to an identifier such as a name, identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

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).

More information could be found here.

Additional condition for processing of special categories of personal data

Certain types of sensitive personal data are subject to additional protection under the legislation applicable to you. They are called "special categories" of personal data. The special categories are:

- Personal data revealing racial or ethnic origin.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.

- Genetic data and biometric data processed for the purpose of uniquely identifying a natural person.
- Data concerning health.
- Data concerning a natural person's sex life or sexual orientation.

We will only use special categories of personal data for a specific purpose and if we are able to satisfy both the lawful basis requirements, as well as at least one of the following additional conditions:

- You have given explicit consent.
- Processing relates to personal data which are manifestly made public by you.
- Processing is necessary for the establishment, exercise of defence of legal claims.
- Processing is necessary for reasons of substantial public interest based on EU or EU Member State law. In particular, processing of your personal data is necessary for reasons of substantial public interest, based on the EU Anti-Money Laundering legislation as the Cayman Islands are subject to the Council Decision 2013/755/EU on the association of the overseas countries and territories with the European Union ("Overseas Association Decision"). Hence, we are required to process for instance information from your ID documents including a photographic picture of you and a visual image of your face (the so called "liveness check").

Please also refer to the table which describes the purposes for which we will use your personal data.

Period for replying to a legitimate request

The statutory period under the applicable legislation for us to reply to a legitimate request is one month. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests.

Please note that we may request that you provide some details necessary to verify your identity when you request to exercise a legal right regarding your personal data.

Lodging a complaint with a data protection authority

If you are an EEA resident, you have the right to make a complaint about the way we process your personal data to the supervisory authority in the EEA Member State of your habitual residence, place of work or place of the alleged infringement. Information about your supervisory authority could be found here.

If you are a UK resident, you may contact the Information Commissioner's Office.

We would, however, appreciate the chance to deal with your concerns before you approach a data protection regulatory authority, so please feel free to contact us in the first instance.

Retention period

Under the EU Anti-Money Laundering legislation (Anti-Money Laundering Directives) we are obliged to retain your personal data for a period of 5 years after the end of the relationship

between us as a company and you as a customer. This period may be further extended in certain cases if so provided by and in accordance with the applicable legislation.

International transfers

We share your personal data within our group. This will involve transferring your personal data outside the European Economic Area (EEA) or the UK.

Many of our external third parties are based outside the EEA or the UK so their processing of your personal data will involve a transfer of data outside the EEA or the UK.

Whenever we transfer your personal data out of the EEA or the UK, we ensure a similar degree of protection is afforded to it by ensuring at least one of the following safeguards is implemented:

- the country to which we transfer your personal data has been deemed to provide an adequate level of protection for personal data by the European Commission;
- a specific contract approved by the European Commission which gives safeguards to the processing of personal data, the so called Standard Contractual Clauses.

Please contact us if you want further information on the specific mechanism used by us when transferring your personal data out of the EEA or the UK. Please also note that future changes to the Standard Contractual Clauses are expected for transfers from the UK. When this situation arises, we will comply with the guidance provided by the UK supervisory authority in this regard.