Crypto.com Non-custodial Wallet (NCW) Privacy Notice

Last Material Update: 14 May 2020

We ask that you please read this Privacy Notice before providing us with any information about you or any other person. If you do not agree to this Privacy Notice and any revisions that may be made to it, you should discontinue your use of this Site and our Services.

Introduction

Welcome to Crypto.com NCW's Privacy Notice.

This Privacy Notice tells 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 a resident of the European Union, including Iceland, Liechtenstein and Norway (EU) or resident of the United States (US) State of California, please refer to the relevant sections below.

Please also use the Glossary to understand the meaning of some of the terms used in this Privacy Notice.

Contents

1. Important information and who we are

Purpose of this Privacy Notice

This Privacy Notice aims to give you information on how we collect and process your personal data when you visit our Site, or through your use of the Services (see the Glossary) and any data you may provide when you register for or use the Services, sign up for alerts or newsletters, contact us with a question or request for help and/or participate in any renewals, promotions or surveys.

The Site and the Services are not intended for minors below the age of 18 and we do not knowingly collect data relating to minors.

It is important that you read this Privacy Notice together with any other privacy notice or fair processing 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 policies and privacy notices and is not intended to override them.

As a best practice approach, we usually explain through understandable and common means the terms and conditions of our Services, renewals, promotions or surveys, please read them carefully before submitting your personal data.

Controller

DeFi Labs, is a company limited by shares and incorporated in the Cayman Islands ("we" or "us"), with our registered address at 94 Solaris Avenue Camana Bay PO Box 1348 Grand Cayman KY1-1108 Cayman Islands.

DeFi Labs is the data controller and responsible for the processing of your personal data.

Data Protection Officer, Complaints and Contact details

We have appointed a Data Protection Officer (DPO) who is responsible for overseeing questions in relation to this Global Privacy Notice. If you have any questions or complaints about this notice, our privacy practices or if you have a request to exercise your rights, please contact our DPO Team in the following ways:

Email: DPO@Crypto.com

You have the right to make a complaint to the Cayman Islands Ombudsman ("**Ombudsman**") about the way we process your personal information. The Ombudsman is the Cayman Islands supervisory authority for data protection issues. Further detail about making a complaint to the Ombudsman is available here: https://ombudsman.ky/make-a-complaint.

If you are an EU resident, click here.

If you are a resident of the US State of California, please click here.

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.

Changes to the Privacy Notice and your duty to inform us of changes

We keep our Privacy Notice under regular review. This version was last updated on the date above written. The Privacy laws around the globe change regularly, please check from time to time for new versions of the Privacy Notice.

It is important that the personal data we hold about you is accurate and current. 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 app 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. When you leave our Site or Applications, we encourage you to read the privacy notice of every Third Party Site you visit or use.

2. The data we collect about you

Personal data, or personal information means any information about an 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:

https://ombudsman.ky/data-protection-organisation/what-information-does-the-dpl-apply-to

If you are an EU resident, click here.

If you are a resident of the US State of California, please click here.

We may collect, use, store and transfer different kinds of personal data about you which we have grouped in categories as follows:

Category of Personal Information	Specific Pieces of Personal Information
Identity Data	• first name, • maiden name, • last name, • username or similar identifier, • title, • date of birth and gender, • a visual image of your face, • tax identification number, • national identity cards,

	• passports or other form of identification documents including proof of address such as utility bill or bank statement. * For the registration and use of the NCW itself, only email address is required. The ID data are only relevant if the user connect the NCW with the App. The ID data will not be transferred from the App to the NCW technically, but it will associate the KYC identity with the NCW.
Contact Data	• billing address, • delivery address, • home address, • work address, • email address and telephone numbers.
Financial Data	• bank account, • payment card details, • external e-money wallet details.
Transactional Data	• details about payments to and from you, • other details of any transactions you enter into using products and services you have purchased from us.

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

Technical Data	• internet protocol (IP) address, • your login data, • browser type and version, • time zone setting and location data, • browser plug-in types and versions, • operating system and platform, and • other technology or information stored on the devices you allow us access to when you visit the Site or use the Services, such as friends lists or other digital content.
Profile Data	• your username and password, • requests by you for products or services, • your interests, preferences, feedback and survey responses.

Usage Data	• information about how you use:
	  ○ our Site,
	  ○ App,

	○ products and services.
Marketing and Communications Data	• your preferences in receiving marketing from: ○ us ○ our third parties ○ your communication preferences.

We will only ask for your Identity Data if it is necessary to provide you with the Services.

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

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

Sensitive data (a.k.a. Special Categories data) includes details about your racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning your sex life or sexual orientation, as well as details of criminal records or any proceedings for any offence committed or alleged to have been committed, including the disposal of any such proceedings or any sentence of a court in the Cayman Islands or elsewhere.

We will only collect, use, store and transfer your sensitive data, if we are able to satisfy both the lawful basis requirements (see Section 4 and the Glossary), as well as at least one of the following additional conditions:

- **Consent**: you have given consent to the processing of your sensitive data;
- **Information made public by yourself**: the information contained in 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;
  is necessary for the purpose of obtaining legal advice; or is otherwise necessary for the purposes of 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;

If you are an EU resident, click here.

If you are a resident of the US State of California, please click here.

We also collect, use and share **Aggregated Data** such as statistical or demographic data for any purpose. Aggregated Data could be derived from your personal data but is not considered personal data in law as this data will not directly or indirectly reveal your identity. For example,

we may aggregate your Usage Data to calculate the percentage of users accessing a specific website feature. However, if we combine or connect Aggregated Data with your personal data so that it can directly or indirectly identify you, we treat the combined data as personal data which will be used in accordance with this Privacy Notice.

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 (where the personal data is necessary for the performance of that contract), 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.

3. How is your personal data collected?

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

Direct interactions. You may give us your Identity and Contact Data 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 products or services;
- create an account;
- subscribe to our services or publications;
- make use of any of our Services;
- request marketing to be sent to you;
- enter a competition, promotion or survey;
- 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. We may also receive Technical Data about you if you visit other websites employing our cookies. On our main website you will be informed about how we use cookies through the Cookie Settings.

Third parties or publicly available sources. We also obtain information about you from third parties or publicly available sources (credit reference agencies, fraud and crime prevention agencies, public blockchain).

4. How we use your personal data

We will only use your personal data when the DPL, the EU General Data Protection Regulation (GDPR) (if applicable) or the California Consumer Privacy Act (if applicable) allows us to. Most commonly, we will use your personal data in the following circumstances:

- For the provision of the Services.

- Where we need to comply with a legal obligation.
- Where it is necessary for our legitimate interests (or those of a third party) and your interests and individual rights do not override those interests.

Please refer to the Glossary, lawful basis sections to find out more about the types of lawful bases that we will rely on to process your personal data.

Generally, we do not rely on consent as a legal basis for processing your personal data although we will get your consent before sending third party direct marketing communications to you via email or text message. You have the right to withdraw consent to marketing at any time by contacting us. See below for further details on marketing.

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 on 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.

No	Purpose/Activity	Categories of personal information	Lawful basis for processing including basis of legitimate interest
i.	To register you as a new customer	• Identity • Contact	• Performance of a contract with you • Necessary to comply with a legal obligation (e.g. to comply with Anti-Money Laundering requirements)
ii.	To process and deliver our Services to you including: • Execute, manage and process any instructions or orders, you make	• Identity • Contact • Transactional • Technical • Marketing and Communications	• Performance of a contract with you • Necessary for our legitimate interests (e.g. to prevent abuse of our Services and promotions)
iii.	To manage our relationship with you which will include: • Asking you to leave a review	• Identity • Contact • Profile • Transactional	• Performance of a contract with you • Necessary for our legitimate interests (to keep our records updated and to study how customers use our products/services)

	or take a survey	• Marketing and Communications		
iv.	To manage risk and crime prevention including: • Detect, investigate, report and prevent financial crime in broad sense • Obey laws and regulations which apply to us • Responding to complaints and resolving them	• Identity • Contact • Technical • Transactional • 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: ○ special categories 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); ○ special categories data that is revealed by photographic ID although we do not intentionally process this personal data;	• Performance of a contract with you • Necessary to comply with a legal obligation • Necessary for our legitimate interests (to develop and improve how we deal with financial crime) • For Sensitive Data (a.k.a. Special Categories Data) it's necessary for reasons of substantial public interest under 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').
v.	To enable you to			

	partake in a prize draw, competition or complete a survey	• Identity • Contact • Profile • Usage • Marketing and Communications • Technical data	• Performance of a contract with you • Necessary for our legitimate interests (to gather market data for studying customers' behavior including their preference, interest and how they use our products/services, determining our marketing campaign and growing our business)
vi.	To administer and protect our business, our Site and Applications including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data	• Identity • Contact • Technical • Transactional	• Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security, to prevent fraud and in the context of a business reorganisation or group restructuring exercise) • Necessary to comply with a legal obligation
vii.	To deliver relevant website content and advertisements to you and measure or understand the effectiveness of the advertising we serve to you	• Identity • Contact • Profile • Usage • Marketing and Communications • Technical	Necessary for our legitimate interests (to study how customers use our products/services, to develop them, to grow our business and to inform our marketing strategy)
viii.	To use data analytics to improve our website, products/services, marketing, customer relationships and experiences	• Technical • Usage	Necessary for our 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)
ix.	To make suggestions and recommendations to you about goods or services that may be of interest to you	• Identity • Contact • Technical • Usage • Profile • Marketing and Communications	Necessary for our legitimate interests (to develop our products/services and grow our business)

Marketing

We strive to provide you with choices regarding certain personal data uses, particularly around marketing and advertising.

Promotional offers from us

We may use your Identity, Contact, Technical, Transactional, Usage 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 or purchased from us and you have not opted out of receiving that marketing.

Third-party marketing

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

Opting out

You can ask us or third parties 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 these marketing messages, this will not apply to personal data provided to us as a result of a product/service purchase, warranty registration, product/service experience or other transactions.

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. On our main website you will be informed about how we use cookies through the Cookie Settings.

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.

5. Disclosures of your personal data

We may share your personal data with our third-party service providers, agents, subcontractors and other associated organisations, our group companies and Affiliates (as described below) 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 do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

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;
- organizations which assist us with customer service facilities;
- 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 as a result 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.

6. International transfers

We may 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 paragraph 5 above) are based outside the Cayman Islands so their processing of your personal data will involve an international transfer of your data.

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:

1. 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
2. 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:

https://ec.europa.eu/info/law/law-topic/data-protection/international-dimension-data-protection/adequacy-decisions_en. On the basis of our own adequacy assessment regarding the applicable country or territory pursuant to Schedule 1, Part 2(4) of the DPL. This adequacy assessment will involve an assessment of the following elements to determine if the other country or territory is deemed to have an adequate level of protection:
    - the nature of the personal data (e.g. "Are there sectorial data protection laws that apply?");
    - the country or territory of origin of the information contained in the data;
    - the country or territory of final destination of that information;
    - the purposes for which and the period during which the personal data is intended to be processed;
    - the law in force in the country or territory in question;
    - the international obligations of that country or territory;
    - any relevant codes of conduct or other rules that are enforceable in that country or territory, whether generally or by arrangement in particular cases; and
    - any security measures taken in respect of the data in that country or territory.
3. Where the Ombudsman has authorised the international transfer:
    - pursuant to Schedule 4(9) of the DPL having taken into consideration the elements described in item 2 above;
    - required under international cooperation arrangements between intelligence agencies or regulatory agencies, if permitted under an enactment or order issued by the Grand Court; or
    - made on terms approved by the Ombudsman (e.g. pursuant to data transfer agreements which replicate the rights of the GDPR or are based on or contain standard contractual clauses (as and when they are made available by the Ombudsman).
4. Where the safeguards described in items 1 to three above cannot be satisfied, we are still able to internationally transfer your personal data if one of the following exemptions apply:
    - made with your consent;
    - necessary for the performance of a contract between us, or for pre-contractual steps taken at your request;
    - necessary for the performance of a contract made in the interests of yourself between us and another person;
    - necessary for important reasons of substantial public interest;
    - necessary for the establishment, exercise or defence of legal claims;
    - necessary to protect the vital interests of the data subject; or
    - made in regard to public data on a public register, and any conditions subject to which the register is open to inspection are complied with.
5. If you are an EU resident, click here.

7. Data security

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:

a. organizational measures (including but not limited to staff training and policy development);
b. technical measures (including but not limited to physical protection of data, pseudonymization and encryption); and
c. 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 the following link: https://crypto.com/security

8. Personal Data Retention

How long will you use my personal data for?

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 will 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:

a. in the event of a complaint;
b. 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;
c. to comply with any applicable legal and/or regulatory requirements with respect to certain types of personal data (e.g. information needed for audit purposes etc); or
d. in accordance with relevant industry standards or guidelines;
e. 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 in order to prevent the appearance of abusive behavior.

Please bear in mind that the **right to deletion/erasure** of your personal data **is not absolute** which means that in some circumstances, you can ask us to delete your data: see Section Your Legal Rights for further information. 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.

9. Your legal rights

Under certain circumstances, you have rights under the data protection laws in relation to your personal data:

- Right to be informed.
- Request access to your personal data.
- Request correction of your personal data.
- Request erasure of your personal data.
- Object to the processing of your personal data.
- Right to stop direct marketing.
- Rights in relation to automated decision making.
- Request restriction/stop of processing your personal data.
- Request transfer of your personal data.
- Right to withdraw consent.
- Right to complain/seek compensation.

Please refer to the GLOSSARY at paragraph 10 below for further detail on each of these rights. If you wish to exercise any of the rights set out above, please contact us.

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.

What we may need from you

We may need to request specific information from you to help us confirm your identity and ensure your right to access your personal data (or to exercise any of your other rights). This is a security measure to ensure that personal data is not disclosed to any person who has no right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

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 a number of 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.

10. EU Residents

As an EU Resident the EU General Data Protection Regulation (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 about an 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: https://ec.europa.eu/info/law/law-topic/data-protection/reform/what-personal-data_en

Additional condition for processing of special categories of personal data

Processing of your personal data is necessary for reasons of substantial public interest, on the basis of 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.

See also row iv in 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 GDPR 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.

Lodging a complaint with a data protection authority

If you are an EU resident, you can also lodge a complaint with your local data protection authority. A detailed list is available here:

https://edpb.europa.eu/about-edpb/board/members_en

We would, however, appreciate the chance to deal with your concerns before you approach the relevant 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 4 and 5) 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.

Another example relates to 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 in order to prevent the appearance of abusive behavior.

International Transfers

The delivery of our Services sometimes involves the transfer of your personal information out of EU countries. Laws in these countries may differ from the laws applicable to your country of residence. Where we transfer, store and process your data outside of the EU we have ensured that appropriate safeguards are in place to ensure an adequate level of data protection. This may be an adequacy decision of the European Commission confirming an adequate level of data protection in the respective non-EU country or an agreement on the basis of the EU Model Clauses (a set of clauses issued by the European Commission).

Further information on these EU Model Clauses (a.k.a Standard Contractual Clauses) and the rights they provide to data subjects can be found on the European Commission website.

Please contact us if you require further information on the specific mechanism used by us when transferring your personal data outside of the EU.

11. Glossary

Lawful Basis

Legitimate Interest means the interest of our business in conducting and managing our business to enable us to give you the best service/product and the best and most secure experience. We make sure we consider and balance any potential impact on you (both positive and negative) and your rights before we process your personal data for our legitimate interests. We do not use your personal data for activities where our interests are overridden by the impact on you (unless we have your consent or are otherwise required or permitted by law). You can obtain further information about how we assess our legitimate interests against any potential impact on you in respect of specific activities by contacting us.

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.

Comply with a legal obligation means processing your personal data where it is necessary for compliance with a legal obligation that we are subject to.

Site

"Site" means the relevant sections of the website under which DeFi Labs provides all or part of its Services: https://crypto.com.

Services

"Services" means the services provided by DeFi Labs through the Site, or through such other facility provided by (or on behalf of) DeFi Labs.

12. Legal Rights Explained

You have the right to:

- Request information in relation to the collection and use of your personal data. This enables you to be informed at all times about who we are and the purposes for processing your personal data.
- Request access to your personal data (commonly known as a "Data Subject Access Request"). This enables you to receive a copy of the personal data we hold about you and to check that we are lawfully processing it.
- Request correction of the personal data that we hold about you. This enables you to have any incomplete or inaccurate data we hold about you corrected, though we may need to verify the accuracy of the new data you provide to us.
- Request erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. 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, if applicable, at the time of your request. If a valid erasure request is received, we will take steps to ensure erasure from back-up systems as well as live systems. You will be informed after your personal data has been erased.
- Object to processing of your personal data (in whole or in relation to certain purposes or in certain manners) 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 individual 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.
- Request to stop direct marketing of your personal data. Where we are processing your personal data for direct marketing purposes, you have the right to notify us in writing requesting that we cease or do not begin processing your personal data for direct marketing purposes.
- Right to require that decisions be reconsidered if the decision is made solely by automated means (without human involvement). You will be notified when decisions are made solely on an automated basis.
- Request restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
    1. If you want us to establish the data's accuracy.
    2. Where our use of the data is unlawful, but you do not want us to erase it.

3. 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.
4. 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. 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 by contacting us through dpo@crypto.com. 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. We will advise you if this is the case at the time you withdraw your consent.
- Right to complain to the Ombudsman or any relevant authority about any perceived violation and to seek compensation for damages in the courts.