

PRIVACY POLICY

Kyber Network International Limited, registered in Malta at 66, Old Bakery Street, Valletta, Malta (“Kyber”) is the Controller of Data under the terms of the Malta Data Protection Act (2018) and Regulation (EU) 2016/679.

Kyber is committed to protecting and respecting your privacy and managing your personal data transparently and in a fair and lawful manner. This policy (together with our terms of use and any other documents referred to herein) sets out the basis on which any personal data we collect from you, or that you provide to us, will be processed by us. Please read the following carefully to understand our practices in processing your data, as well as your rights regarding your personal data and how we will treat it.

Should you have any queries, concerns, requests or complaints in relation to the manner in which we process your personal data, you may contact our Data Protection Officer by email on dpo@kyber.network. You also have the right to lodge a complaint before the Office of Information and Data Protection Commissioner with regard to matters concerning your personal data.

By visiting <https://kyber.network> (“Website”) and submitting data to us, you are accepting and consenting to use of your personal data as described in this policy. If you do not agree with the terms of this Privacy Policy please do not use the Website or otherwise provide us with your personal data.

We may change our privacy policy from time to time. Any changes we may make to our Privacy Policy in the future will be posted on this page and any such changes will become effective upon posting of the revised Privacy Policy. Please check back frequently to see any updates or changes to our privacy policy. If we make any material or substantial changes to this Privacy Policy we will use reasonable endeavours to inform you by email.

For the avoidance of doubt, this Privacy Policy forms a part of the terms and conditions governing your relationship with us and should be read in conjunction with the Kyber relevant terms and conditions.

Your Personal Data

We may collect and process personal data provided directly by you; we also process, insofar as necessary, personal data provided to us by third parties, including publicly accessible data, personal data legitimately provided by other group companies and personal data provided by other trusted third parties. You are responsible to provide us with personal data that is correct and inform us of any changes occurring in your data in writing, in order that we may take all reasonable measures to keep our records in your regard correct and up to date. You have the choice, at any time, not to provide your Personal Data to Kyber; however, do note that failure to provide such Personal Data for us to process may result in Kyber being

unable to continue to provide our products or services to you or pursue any contractual relationship which may be in place between us.

Personal Data you give us

You may give us personal data about you by filling in forms on the Website or by corresponding with us by phone, e-mail or otherwise. This includes personal data you provide when you register on the Website, use our services and to purchase and exchange currency, or when you report a problem with the Website. Examples of such Personal Data you may provide to us may include (depending on the nature of your interaction with us) your name, passport or other identification number, telephone number(s), mailing address, email address, identification data (such as copies of your identification document or personal photograph) and financial and credit card information, and any other information relating to any individuals which you have provided us in any forms you may have submitted to us, or via other forms of interaction with you. You may also provide us with Personal Data of your officers, employees, agents and customers in order for us to provide you with our products and services.

Personal Data and information we collect about you

With regard to each of your visits to our site we may automatically collect the following information:

- technical information, including the Internet protocol (IP) address used to connect your computer to the Internet, your login information, browser type and version, time zone setting, browser plug-in types and versions, operating system and platform. An IP address is a number that is automatically assigned to your computer when you signed up with an Internet Service Provider. When you visit our website, your IP address is automatically logged in our server. We use your IP address to help diagnose problems with our server, and to administer our website.
- information about your visit, including the full Uniform Resource Locators (URL) clickstream to, through and from our site (including date and time); products you viewed or searched for; page response times, download errors, length of visits to certain pages, page interaction information (such as scrolling, clicks, and mouse-overs), and methods used to browse away from the page and any phone number used to call our customer service number.
- If you contact us or we contact you using the telephone, we may monitor or record the phone call for quality assurance, training and security purposes.

Personal Data we receive from other sources

We may receive personal data about you if you use any of the other websites we operate or other services we provide. In this case we will have informed you when we collected that data that it may be shared internally and combined with data collected on this site. We are also working closely with third parties (including, for example, business partners, sub-contractors in technical, payment and delivery services, advertising networks, analytics providers, search information providers, credit reference agencies) and may receive information about you from them.

Apart from Personal Data, we may collect other types of information which is not related to an individual and which is anonymous. For example, the number of website visitors and the number of website users using a particular service. In this way, we hope to improve our customer services.

Processing your personal data

We collect and process your personal data, including data provide by yourself, data we collect about you and data provided by third parties in accordance with the provisions of the General Data Protection Regulation (GDPR) and the Malta Data Protection Act (2018) in the following ways and upon the following grounds:

- For the fulfilment of contractual obligations entered into between you and us and to provide you with the information, products and services that you request from us;
- For the fulfilment of legal obligations and legal compliance;
- to notify you about changes to our service;
- to ensure that content from our site is presented in the most effective manner for you and for your computer;
- to provide you with information about other goods and services we offer that are similar to those that you have already purchased or enquired about;
- to provide you, or permit specific third parties to provide you, with information about goods or services we feel may interest you. If you are an existing customer, we will only contact you by electronic means (e-mail or SMS) with information about goods and services similar to those which were the subject of a previous sale or negotiations of a sale to you, subject to your

consent. If you are a new customer, and where we permit selected third parties to use your data, we (or they) will contact you by electronic means only subject to your consent.

If you do not want us to use your data in this way, or to pass your details on to specific third parties for marketing purposes, you have to the right to withdraw your consent at any time by writing to our Data Protection Officer by email on dpo@kyber.network. Withdrawal of consent does not affect the legality of data processed prior to such withdrawal.

- to safeguard legitimate company interests which require processing beyond the fulfilment of contractual obligations such as:
 - processing of personal data for the purposes of our daily operations including billing and debt collecting;
 - processing of personal data for market research, statistical purposes and service and product development;
 - processing of your data for the protection of the company's legal position in the event of legal proceedings;
 - processing for the purposes of ensuring network and information security, including preventing unauthorised access to electronic communications networks and stopping damage to computer and electronic communication systems;
 - processing for the purpose of reporting possible criminal acts or threats to public security to competent authorities;
 - to administer our site and for internal operations, including troubleshooting, data analysis, testing, research, statistical and survey purposes;
 - to improve our site to ensure that content is presented in the most effective manner for you and for your computer;
 - to allow you to participate in interactive features of our service, when you choose to do so;
 - as part of our efforts to keep our site safe and secure;
 - to measure or understand the effectiveness of advertising we serve to you and others, and to deliver relevant advertising to you;
 - to make suggestions and recommendations to you and other users of our site about goods or services that may interest you or them;
 - for accurately carrying out and confirming your instructions, for training purposes and/or in order to improve the quality of our customer services. Such data shall include calls, email communication and online chats.

You shall have the right to object to any of the above-mentioned legitimate company interests as a basis for the processing of personal data by contacting our Data Protection

Officer by email on dpo@kyber.network. If you submit an objection, we will no longer process your personal data unless we can give evidence of mandatory or legitimate reasons for processing, or processing serves the enforcement, exercise, or defence of our company's legitimate interests.

Disclosure of your personal data

As part of our due diligence process Kyber may forward your data to trusted third parties to be verified for identification purposes; this personal data shall include sensitive personal data such as a picture of your passport. Your personal data may also be provided to trusted third-party processors for the customer care and client communication services, credit reference, fraud prevention, business scoring, credit scoring, placing of monetary deposits, transfer of payments, debt collection and recovery. Such processing shall be conducted in compliance with all legal requirements as well as our Privacy Policy and strict retention policies and codes of conduct. We will ensure that all companies to which we disclose your Personal Data will only process it in accordance with our instructions and on our behalf, and that they shall only use such data to the extent to which we ourselves are entitled.

We may share your personal data with any member of our group of companies, which means our subsidiaries and our ultimate holding company and its subsidiaries.

We may share your personal data with selected third parties including:

- Business partners, suppliers and sub-contractors for the performance of any contract we enter into with them.
- Analytics and search engine providers that assist us in the improvement and optimisation of our site.
- Credit reference agencies, due diligence agencies or ID verification agencies for the purpose of verifying your identity where this is a condition of us entering into a contract with you.

We may disclose your personal data to third parties for the purpose of fulfilling legitimate company interests:

- In the event that we sell or buy any business or assets, in which case we may disclose your personal data to the prospective seller or buyer of such business or assets;
- If Kyber Network International Limited or substantially all of its assets are acquired by a third party, in which case personal data held by it about its customers will be one of the transferred assets;
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, or in order to enforce or apply our terms of use and other agreements; or to protect the rights, property, or safety of Kyber Network International Limited, our customers, or others. This includes exchanging data with other companies and organisations for the purposes of fraud protection and credit risk reduction;

- For the purposes of billing, debt collecting credit rating and verification and fraud prevention;
- For the protection of the company's legal position in the event of legal proceedings.

The trusted third parties we work with may be outside of the European Economic Area: your personal data will only be transferred to third countries or territories providing sufficient and appropriate safeguards to your personal data in compliance with all legal requirements as well as our Privacy Policy and strict codes of conduct.

We will ensure that all companies to which we disclose your Personal Data will only process it in accordance with our instructions and on our behalf, and may only use such data to the extent to which we ourselves are entitled. All such companies and third parties will further be required by us to meet the requirements of data protection legislation and our strict privacy and retention policies to keep your data secure at all times.

We may, if necessary or authorised by law, provide customer data to law enforcement agencies, regulatory organisations, courts or other public authorities. We attempt to notify our customers about legal demands for their Personal Data unless prohibited by law or court order or when the request is an emergency. We may dispute such demands when we believe that the requests are disproportionate, vague or lack proper authority, but we do not promise to challenge every demand.

Your personal data shall not be processed for purposes other than those it was collected for; should further processing be required, you will be informed of that purpose and provided with all necessary information.

You shall have the right to object to any of the above-mentioned legitimate company interests as a basis for the processing of personal data and to forward any queries you may have by contacting our Data Protection Officer by email on dpo@kyber.network. If you submit an objection, we will no longer process your personal data unless we can give evidence of mandatory, legitimate reasons for processing, which outweigh your interests, rights, and freedoms, or processing serves the enforcement, exercise, or defence of interests.

Where we store your personal data

The security of your Personal Data is our priority. Kyber takes all physical, technical and organisational measures needed to safeguard Personal Data. We will use all reasonable efforts to protect your information in a highly secure data centre, adhering to strict computer security standards. We have put in place, privacy protection control systems designed to ensure that our customers' information remains safe, secure and private.

Access to Personal Data is only limited to authorised personnel of Kyber who are fully trained in handling your information. These authorised personnel are required to ensure the confidentiality of your information and to respect your data protection rights at all times. Personnel who have access to your information will be subjected to disciplinary action

should they fail to observe this Privacy Policy and other guidelines, codes or policies which we may issue to them from time to time.

The data that we collect from you may be transferred to, and stored at, a destination outside the European Economic Area ("EEA"). It may also be processed by staff operating outside the EEA who work for us or for one of our suppliers. Such staff maybe engaged in, among other things, the fulfilment of your order, the processing of your payment details and the provision of support services. By submitting your personal data, you agree to this transfer, storing or processing. We take all steps reasonably necessary to ensure that your data is treated securely using sufficient and appropriate safeguards and in compliance with all legal requirements as well as this Privacy Policy and our strict codes of conduct.

All personal data you provide to us is stored on our secure servers. Any payment transactions will be encrypted using SSL technology. Where we have given you (or where you have chosen) a password which enables you to access certain parts of our site, you are responsible for keeping this password confidential. We ask you not to share a password with anyone.

Unfortunately, the transmission of information via the internet is not completely secure. Although we will do our best to protect your personal data, we cannot guarantee the security of your data transmitted to our site; any transmission is at your own risk. Once we have received your data, we will use strict procedures and security features to try to prevent unauthorised access.

In line with applicable law, we shall, where lawfully obliged, notify the competent authorities and/or you in cases of personal data breach and will keep a log of any such breaches.

For how long will your data be stored?

We will process and store your personal data for as long as it is necessary in order to fulfill our contractual, regulatory and statutory obligations. We will assess and respond to requests to delete data and we shall accordingly delete data provided that the data is no longer required in order to fulfill contractual, regulatory or statutory obligations, or the fulfillment of any obligations to preserve records according to law.

We will normally retain your records for a minimum of five years to comply with legal, regulatory and contractual requirements unless there is a particular reason to hold the records for longer; your personal data may be retained for longer periods in the event of prospective or pending debt collecting, legal or law-enforcement proceedings and until such proceedings are formally and definitively concluded.

Your rights

In relation to your personal data, you have the right to:

- access to your personal data;
- the rectification of your personal data;
- restrict processing;
- object to processing;
- data portability;
- request erasure of your personal data.

You shall also have the right to ask us not to process your personal data for marketing purposes. We will seek your explicit consent (before collecting your data) if we intend to use your data for such purposes or if we intend to disclose your information to any third party for such purposes. You can exercise your right to prevent such processing by checking certain boxes on the forms we use to collect your data. You can also withdraw your consent by contacting our Data Protection Officer by email on dpo@kyber.network. You also have the right to lodge a complaint before the Office of Information and Data Protection Commissioner with regard to matters concerning your personal data.

Our site may, from time to time, contain links to and from the websites of our partner networks, advertisers and affiliates. If you follow a link to any of these websites, please note that these websites have their own privacy policies and that we do not accept any responsibility or liability for these policies. Please check these policies before you submit any personal data to these websites.

Access to Data

You have the right to request, free of charge, access to and a copy of your personal data as processed by us.

Automatic Decision Making

In establishing and carrying out our business relationship, we generally do not make use of fully automated decision making. If we use this procedure in individual cases, we shall inform you of this separately, provided it is a legal requirement.

Contact

Questions, comments and requests regarding this privacy policy are welcomed and should be addressed to our Data Protection Officer on dpo@kyber.network.