PRIVACY POLICY

Document Changes

S/N	Name	Change Summary	Date
1	First release – v1.0	First release	16/10/2024
2			
3			

Document Reviewers

S/N	Role	Name
1	Head of Compliance	Angeliki Georgiou
2	Executive Director	Sergey Tsipko
3	Executive Director	Michale Capone

Next Scheduled Review

S/N	Role	Frequency	Date
1	Head of Compliance and AML Department	On an annual basis	16/10/2025

Document Approvers

S/N	
1	Board of Directors

Document Release Versions

Version	Version Summary	Approval	Date
V1.0	First Release	Approved	16/10/2024

Contents

Contents 3
1. Introduction 4
2. Scope of the Privacy Policy 5
3. Consent 6
4. Personal Information/Data the Company may collect 7
5. How the Company Collects Personal Data 9
6. Duties and Responsibilities of the Data Protection Officer 9
7. Use of Personal Information/Data 10
8. Statistical Data 12
9. Retention of Personal Data - (Article 7(h) of Law 87(I)2017) 13
10. Protection and Security of Personal Data 13
11. IT Department 14
12. Changes in Personal Information/Data 15
13. Your Rights in Relation to Your Personal Data and Information 15
14. Company's Ventors and Third-Party Associates 18
15. Non-Affiliate Third Parties 18
16. Warranties 18
17. Links to Other Websites 19
18. Use of Cookies 19
19. Setting your Cookie Preferences 21
20. Contact Clients and Recordings 21
21. Clients' Rights 21
22. Data Protection Impact Assessment ("DPIA") 25
23. Amendment/Review of the Policy 26
24. General Information 26
25. How to Make a GDPR Complaint? 26
26. Governing Law 26
27. Definitions 27
28. Monitoring and Review 27

1. Introduction

1.1 **Xtellus Europe Limited** (hereinafter, "the Company" and/or "we") is an Investment Firm regulated by the Cyprus Securities and Exchange Commission (hereinafter, "CySEC") with License number 446/24, having its principal place of business at 26 Spyrou Kyprianou, 4040, Limassol, Cyprus and is registered with the Registrar of Companies in Nicosia under the number HE 447781.

1.2 The Company is compliant with the requirements of the Markets in Financial Instruments Directive (MiFID II), Investments Services Law 87(I) 2017, the Laws for the Prevention of Money Laundering and Terrorist Financing, Market Abuse and Insider Dealing, the General Data Processing Regulation [1](GDPR) as well as other legislation applicable in the Republic of Cyprus.

1.3 The Company needs to collect and use certain types of information about the Clients whom the Company come into contact to the extent that is necessary to perform its services to its clients in connection with its Products and Services. This personal information must be collected and dealt appropriately, whether is collected on paper, stored in computer database, or recorded on other material and there are safeguards to ensure this are under the Protection of Natural Persons Against the Processing of Personal Data and the Free Circulation of such Data Law L.125(I)/2018[2] and under the General Data Protection Regulation 2016/679 (2018).

1.4 The Company has established a Privacy Policy (the "Policy") appropriate to the size and organization of the Company and the nature, scale and complexity of the Company's business.

1.5 This Policy applies to former, existing and potential Clients (hereinafter referred to as the "Client(s)" and/or "you") as well as to any Company's inhouse employees, Third Party Associates and/or Providers, Custodians, Liquidity Providers and Execution Brokers.

1.6 Client means any natural or legal person who has entered a client relationship with the Company and is actively using, or has used, the services of the Company until the termination of the Client relationship. A prospective Client is a natural or legal person who intends to use our services and has made the initial registration for such use of services without concluding the Client relationship.

[1] https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/all/DB87F8669B782F68C22582630035BFF1/$file/Regulation%202016_679_ENG.pdf?openelement

[2] https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/2B53605103DCE4A4C225826300362211/$file/Law%20125(I)%20of%202018%20ENG%20final.pdf

2. Scope of the Privacy Policy

2.1 With the implementation of the Privacy Policy the Company aims to outline the Company's responsibility to manage and ensure the protection of privacy and the clients' personal and financial information and to behave in a fair and moral manner concerning the gathering, storing and handling of data. This process will be carried out with transparency and respect towards the rights of individuals who entrust it with their information.

2.2 For this Privacy Policy, Data Protection Legislation means: the General Data Protection Regulation (EU) 2016/679 (the "GDPR") applicable in the European Union, including Cyprus until any Cyprus data protection legislation replaces the GDPR and then such Cyprus data protection legislation replacing the GDPR once in force and applicable. For the Data Protection Legislation, the data controller is the Company.

The clients' privacy is considered and treated by Company with utmost importance and highest priority and this Policy applies to former, existing and potential clients as well as to any visitors of the Company's website.

2.3 This Privacy Policy:

a) provides an overview of how the Company collects, processes and uses the clients' personal data and informs the client about his rights under the GDPR;

b) is directed to natural persons who are either existing or potential Clients of the Company, or are authorized representatives/agents or beneficial owners of legal entities or of natural persons which/who are current or potential Clients of the Company;

c) is directed to natural persons who had such a business relationship with the Company in the past;

d) contains information about when the Company shares the Clients' personal data with other third parties, where applicable according to the GDPR and/or any legal framework issued by the Cyprus Securities and Exchange Commission (for example, the Company's counterparties and/or vendors).

2.4 Through this Policy the clients' data may be called either "personal data" or "personal information". The Company may also sometimes collectively refer to handling, collecting, protecting and storing the clients' personal data or any such action as "processing" such personal data.

2.5 For the purposes of this Privacy Policy, personal data shall mean any information relating to the client which identifies or may identify any potential and/or existing client.

3. Consent

3.1 Consent refers to the client's right as a data subject to freely and unambiguously agree to a specific condition related to the Company's primary or supporting services by making a positive action. Such action might be a tick box in the client's area, signature on a document, electronic signature or name placement in online questionnaires or other similar action. Most of the services provided by the Company do not require a separate or explicit consent by data subjects to process their information in connection to the core services of the company when requesting to become a client of a regulated Cyprus Investment Firm based on the definitions for legal grounds of processing found in Article 6 of the GDPR.

3.2 By, registering with the Company or submitting information to the Company, any client consents and agrees with the terms of this Policy and hereby consents to the collection, process, storage, use and disclosure of the clients' personal data by the Company whether such use is by the Company or by another third party associate which may be required by them in order to effectively perform Services in connection with the Company's Terms of Business or effectively execute any related operational function performed by the Company to its Clients, and as explained below herein

3.3 The Company acknowledges its engagement with certain Third-Party Associates, which include, but are not limited to, software platform providers, financial services providers, data and/or media providers, and regulatory reporting providers relating to EMIR and MIFIR, screening providers (collectively referred to as "Third Party Associates"). Such cooperation is undertaken for the purpose of providing financial services in compliance with the applicable licensing provisions under the First Appendix of Law 87(I)/2017 as issued by the Cyprus Securities and Exchange Commission.

Consequently, the relevant Third Party Associates may have access to certain personal information concerning clients, as necessary for the performance of their services:

For Individuals

- Full Name
- Personal Address
- Date of Birth
- Passport Number
- Nationality
- Email Address

- Phone Number

For Legal Entities

- Company's Name
- Incorporation Number
- LEI Number
- Registered and/or Business Address
- Full Name of the Signatory(ies)
- Email Address
- Phone Number

3.4 If any potential client does not agree with this Policy, the use of the Company's Website and/or access to the Company's services or the submit of any personal information by any potential client is prohibited.

4. Personal Information/Data the Company may collect

4.1 The Company will only use clients' personal data in accordance with the Regulations mentioned within Sections 1.2. and 1.3 of this Policy. In particular, the Company is registered as a Data Controller with the Office of the Commissioner for Personal Data Protection[3] and will collect, process, maintain, store, use and handle clients' personal information in accordance with the provisions of the Law 125(I)/2018, the GDPR, Investments Services Law 87(I) 2017, MiFID II, this Privacy Policy and the Company's Terms of Business (available within the Company's website).

4.2 During and/or following the completion of the online registration procedure potential and/or existing clients are required to provide personal information and to attach a series of required documents.

4.3 The Company may collect such Personal Information from other persons including, for example, online anti-money laundering or fraud prevention agencies or online screening services providers, banks, other financial or credit institutions, third authentication service providers and the providers of public registers or such other services that may from time to time be required for Company's legitimate purposes.

4.4 Personally identifiable information (or "Personal Information"), according to Article 4 of the GDPR means any information that may be used, either alone or in combination with other information, to personally identify directly or indirectly, contact or locate any potential or existing Clients of the Company.

[3] https://www.dataprotection.gov.cy/dataprotection/dataprotection.nsf/home_el/home_el?opendocument

4.5 Personal Information includes, but is not limited to:

a. First and Last name
b. ID/Passport/Driving License numbers
c. Nationality
d. Physical address
e. Date of Birth
f. Contact information (such as telephone number and email address)
g. Identity and Address verification documents such as passport and ID, utility bills and/or bank statements
h. Employment status
i. Tax information such as tax identification numbers
j. Company information concerning activities of the company, company incorporation documents/certificates in case of a corporate account
k. Financial data such as estimated annual income and net worth, trading experience and investment knowledge including but not limited to trading data, deposits, withdrawals, and credit.
l. Payment details and bank account details

4.6 The Company is required by the Prevention and Suppression of Money Laundering and Terrorist Financing Laws of 2007-2021 (as amended from time to time) issued by the CySEC, to identify any potential client, if the relevant client is opening a trading account or adding a new signatory or representative to an existing account. The above-mentioned Anti-money laundering Laws require the Company to sight and record details of certain documents (i.e. photographic and non-photographic documents) to meet the standards, set under those laws. Identification documentation, as required under anti-money laundering legislation or any other legislation issued by CySEC relevant to the services the Company provides to clients, includes, but not limited to information and/or documents mentioned within Section 4.5 of this Policy or any other information the Company considers necessary to its functions and activities.

4.7 Where it is necessary to do so, the Company also collects data regarding the following individuals:

a) trustees;
b) partners;
c) legal entities ultimate beneficial owners, directors and legal representatives;
d) officers of co-operatives and associations; or
e) client agents.

4.8 When an existing client of the Company wishes to have online access to view statements and other information relating to his account, the Company may request the relevant client to provide some

information about himself for security, identification and verification purposes.

5. How the Company Collects Personal Data

5.1 The Company may collect and process the personal data when:

a) The client contacts the Company, whether through the Company's Website (by e-mail, post or phone), as the Company may keep a record of that correspondence: For example, when any client submits a complaint, report a problem with the Company's services or our website or otherwise liaise with any Company's Department with the Company.

b) When the relevant client updates his details provided to the Company during the onboarding process (by completing the relevant Questionnaires provided by the Company).;

c) The existing clients use their trading account to login to and use the Company's platform, technology and other features and functionalities. Under no circumstances are these details disclosed to any third party other than those who need to know this information in the context of the services the Company provides.

6. Duties and Responsibilities of the Data Protection Officer

6.1 The Company has appointed Mrs. Angeliki Georgiou (email address: compliance@xtelluseurope.com) as the Data Protection Officer.

6.2 Main duties, responsibilities and powers of the DPO:

a) Provide advice and guidance to the Company and its employees on the requirements of the GDPR.

b) Monitor the organization's compliance with the GDPR provisions.

c) Be consulted and provide advice during Data Protection Impact Assessments.

d) Decide if the DPIA is necessary based on the specific conditions.

e) Be the point of contact for data subjects and for cooperating and consulting with national supervisory authorities, such as the Office of the Commissioner for Data Protection.

f) Provide training to employees and awareness of how their duties are connected to the protection of rights of data subjects.

g) to hold a register of all categories of processing activities carried out on behalf of the Company.

h) To create and hold a register of all complaints, responses and results.

i) To create, update and improve regularly the procedures and policies relating to the compliance with GDPR and other local data protection principles and laws.

j) To create a procedure of reporting directly to the Commissioner of Data Protection.

k) To deal and respond to all data subjects' complaints and be the main contact point for GDPR.

l) DPOs should also take responsibility for carrying out data audits and oversee the implementation of compliance tools.

m) The DPO must be able to act independently, be adequately resourced and be able to report directly to senior management to raise concerns.

6.3 Responsible for all changes, deletion and protection of rights. In the event that clients' personal information changes at any given time, clients are responsible to inform the Company by emailing the Compliance Officer at compliance@xtelluseurope.com.

7. Use of Personal Information/Data

7.1 The collection personal Information (not in the public domain or already possessed by us without a duty of confidentiality) which the Company holds is to be treated by us as confidential and will not be used for any purpose other than in connection with the provision, administration and improvement of the Company's Services to existing clients or the furthering of the Company's Terms of Business between the Company and any existing client, establishing and managing the client's Trading Account or any business relationship between the Company and the existing client, reviewing the clients' ongoing needs, enhancing clients' services and/or financial products, providing ongoing information that the Company believes may be relevant to its clients, improving the Company's relationship, anti-money laundering and due diligence checks, as applicable.

7.2 The Company will use any client's personal information for the purposes of providing the services the relevant client has requested, for administration, for anti-money laundering and appropriateness test scoring and to ensure that the content and services that we offer are tailored to the clients' needs and interests. We may keep the clients' information for a reasonable period for these purposes, as defined within the Law 87(I)2017. The Company may need to share the Clients' information with its vendors and/or service providers for these purposes.

7.3 In assessing the potential client onboarding application to open an account, to prevent fraud, to check client's identity and to prevent money laundering, the Company may search the files of credit reference or screening providers that will record any credit searches on the clients' file.

7.4 In order for the Company to provide, monitor and improve the quality service and security to its clients, the Company may use the clients' personal information/data for one or more of the following purposes:

a. Verify the identity of clients;

b. To maintain clients' personal profile;

c. Assess and improve the services provided to clients;

d. To such an extent as reasonably required so as to execute Orders and for purposes ancillary to the provision of the Services;

e. Company's transmission/execution and post transaction/order services;

f. Analysis of statistical data which will aid the Company to provide clients with better suited products and services in the future;

g. To other service providers who create, maintain or process databases (whether electronic or not), offer record keeping services, email transmission services, messaging services or similar services which aim to assist the Company collect, storage, process and use Client information to improve the provision of the Company's services;

h. To a Trade Repository (for EMIR or MiFIR Reporting purposes) or similar under the Regulation (EU) No 648/2012 of the European Parliament and of the Council of 4 July 2012 on OTC derivatives;

i. Inform clients of additional products, services or promotions relevant to its clients.

7.5 In regards to point (k) above and should for any reason clients do not consent to receive information of this nature, the client can inform us accordingly by contacting the Company on the contact details provided by the Company on its Terms of Business or at the following address: compliance@xtelluseurope.com.

7.6 We may disclose personal data to comply with a legal or regulatory obligation.

7.7 We may contact the client by mail, telephone, e-mail or other electronic messaging service with offers of services or information that may be of interest to the Client. By providing the Company

with the client's telephone numbers or email address, the client consents to being contacted by these methods for these purposes.

7.8 Any information, which we send to the client by email, will not be encrypted. We cannot guarantee confidentiality of emails that the client sends to us.

7.9 The client may ask the Company to provide him/her with information about our services by sending us an email to michael.capone@xtelluseurope.com.

The client has the following Rights:

a. The right to be informed
b. The right of access
c. The right to rectification
d. The right to erasure
e. The right to restrict processing
f. The right to data portability
g. The right to object
h. Rights in relation to automated decision making and profiling

7.10 Those clients whose Personal Data we keep, have the right at any time to obtain confirmation of the existence of the same from the Data Protection Officer, to know the content and origin, to check its accuracy or request its integration, updating, rectification, erasure, or blocking of Personal Data processed in violation of law, and to oppose in any case, for legitimate reasons, to their treatment, only if the above request is in line with the applicable GDPR, Law 87(I)2017 and/or any other Regulation issued by the CySEC.

7.11 To make a request, the client can contact us, verifying his identity and specifying what information requires.

7.12 Data controller and Data processor is the Company.

7.13 The Company does not provide any services to children, nor processes any personal data in relation to children, where 'children' are individuals who are under the age of eighteen (18).

8. Statistical Data

8.1 The Company may, from time to time, combine clients' personal information/data to create impersonalized statistical data. The Company may use this data for statistical purposes and to better improve the provision of the Company's investment and ancillary services and to the extent allowed by the Company's Terms of Business already accepted by the clients.

8.2 The Company will take all reasonable measures to ensure that in no circumstances will clients be identifiable from this statistical data and consequently for clients to remain anonymous.

9. Retention of Personal Data - (Article 7(h) of Law 87(I)2017)

9.1 In accordance with the Company's regulatory requirements and as required by Article 17(7)(h) of the above titled Law issued by the CySEC, all clients' personal information/data will be required to be kept and retained on record for a minimum period of five (5) years, and, where requested by the CySEC for a period of up to seven years, which will commence on the the date of which the business relationship between both parties is terminated in accordance to the Company's Trading Terms and Conditions.

10. Protection and Security of Personal Data

10.1 The Company takes reasonable precautions to protect personal information/data from loss, theft, misuse, unauthorized access or disclosure, alteration, or destruction. The Company employs physical, electronic, and procedural safeguards to protect personal information/data and it does not store personal information/data for longer than necessary for the provision of services or as permitted by law, as per Article 7(h) of Law 87(I)2017.

10.2 The Company's may utilize services that are managed by outsourced service providers. Reasonable actions are taken to ensure that the environments that support and deliver these services have adequate security measures taken to protect the data and maintain the integrity, confidentiality, and availability of the Company's information. These security measures include, but are not limited to, encryption, access controls, regular security audits, and monitoring. Any personal information/data provided by clients to the Company will be strictly protected under enhanced measures of security, protected against loss, misuse, unauthorized access or disclosure, alteration, or destruction with use of security measures, such as strong authentication mechanisms and separation of machines and data to provide secure areas in order to protect clients' personal information from unauthorised users and such personal information will be treated as confidential and shared only with the Company's authorised employees and/or authorised outsourcing service providers and shall not be disclosed to any third parties except, and without notice, in accordance with the provisions of this Policy as well as under any regulatory or legal proceedings.

10.3 The Company also advices all clients to serve and protect their personal data, to maintain confidentiality and not share with any other third party its usernames and passwords provided by the Company. The Company bears no responsibility for any unlawful or unauthorised use of

clients' personal information due to the misuse or misplacement of clients' access codes (i.e. passwords/credentials), irrespective of the way such use was conducted including without limitation negligent or malicious use.

10.4 We will use reasonable endeavors to implement appropriate internal policies, rules and technical measures to protect the personal data that we have under our control (having regard to the type and amount of that data) from unauthorized access, improper use or disclosure, unauthorised modification, unlawful destruction or accidental loss. Examples of our security measures include, but are not limited to:

a) educating our employees as to their obligations with regard to your personal data;
b) requiring our employees to use passwords and two-factor authentication when accessing our systems;
c) employing firewalls, intrusion detection systems and virus scanning tools to protect against unauthorised persons and viruses entering our systems;
d) using dedicated secure networks or encryption when we transmit electronic data for purposes of outsourcing, where necessary;
e) practicing a clean desk policy in all premises occupied by us and our related bodies corporate and providing secure storage for physical records; and
f) employing physical and electronic means such as alarms, cameras and guards (as required) to protect against unauthorized access to buildings.

10.5 We will ensure that the clients' personal data and information will not be disclosed to government institutions or authorities except if required by Law, taking into consideration Article 6, Article 23 and Article 58 of the GDPR Regulation and Article 5 and 25 of Law 125(I) of 2018.

11. IT Department

11.1 The Company requires that all computer equipment is connected to a Firewall, anti-malware software, and automatic updating facilities that are all up to date and meet the corporate minimum business standards acceptable in the financial industry. The Company also requires:

a) Deployment of the corporate principle on usernames and passwords, to have a password protected screensaver, and to password protect and encrypt all folders containing confidential corporate information, sensitive personal information, personably identifiable information, and to disable folder and printer sharing.

b) All notebook computers (if any) and/or laptops that carry personal data or can connect to systems that store or process personal data, use full-disk encryption.

c) The notebook computers and/or laptops are physically protected against theft and damage

while in transit, in storage or in use and that, in cases of loss or theft.

d) That the IT Department ensures that all the recent operating system and application security-related patches, fixes and updates have been installed.

e) Employees to comply with the corporate requirements on the means of connecting to public access points and accessing corporate information.

f) That all computers and laptops are protected by an anti-virus and antimalware software.

12. Changes in Personal Information/Data

12.1 Under the Terms of Business between the Company and its clients, we have the right to disclose the clients' Personal Data or Information (including recordings and documents of a confidential nature, card details) in certain circumstances:

a) Protect the Company's rights and/or to comply with judicial proceedings and/or court order;
b) Protect and defend the rights or property of the Company's website;
c) Protect the safety of Company's clients, all users of the Company's website and/or the public.
d) Where required by law or a court order by a competent Court;
e) Where requested by the Cyprus Securities and Exchange Commission or any other regulatory authority having control or jurisdiction over the Company or the Client or their associates or in whose territory the Company has Clients;
f) To relevant authorities to investigate or prevent fraud, money laundering or other illegal activity;
g) To credit reference and fraud prevention agencies, third authentication service providers, banks and other financial institutions for credit checking, fraud prevention, anti-money laundering purposes, identification or due diligence checks of the Client. To do so they may check the details the Client supplied against any particulars on any database (public or otherwise) to which they have access. They may also use Client details in the future to assist other companies for verification purposes. A record of the search will be retained by the Company;
h) Where necessary in order for the Company to defend or exercise its legal rights to any court or tribunal or arbitrator or Ombudsman or governmental authority;
i) At the Client's request or with the Client's consent;
j) To successors or assignees or transferees or buyers, with ten Business Days prior Written Notice to the Client.

13. Your Rights in Relation to Your Personal Data and Information

13.1 The Company may, from time to time, combine clients' personal data and information with

information from other users of the Company's website to create impersonalized statistical data. The Company will use the above-mentioned information solely for statistical purposes and to better improve Company's services, the extent allowed by the Company's Trading Terms and Conditions already accepted by the clients.

13.2 The Company will take all reasonable measures in order to ensure that in no circumstances will clients be identifiable from this statistical data and consequently for clients to remain anonymous.

13.3 Under the Article 20 General Data Protection Regulation (GDPR 679/2016), you have the right, in certain circumstances, to obtain personal information you have provided us with (in a structured, commonly used and machine-readable format) and to re-use it elsewhere or ask us to transfer this to a third party of your choice.

13.4 Please note that the above-mentioned rights do not apply in all circumstances. More specifically, you are entitled to:

a) request access to your personal data (commonly known as a "data subject access request" described in Article 15 of the GDPR);
b) request correction of the personal data that we hold about you;
c) request erasure of your personal data. 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;
d) object to processing of your personal data where we are relying on a legitimate interest (or those of a third party associate) and there is something about your situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information, which override your rights and freedoms;
e) 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:
    i. if you want us to establish the data's accuracy;
    ii. where our use of the data is unlawful, but you do not want us to erase it;
    iii. 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
    iv. you have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it;
f) request the transfer of your personal data to you or to a third party. We will provide you, or a third party you have chosen, your personal data in a structured, commonly used,

machine-readable format. Note that this right only applies to automated information (i.e. not to hard copies) which you initially provided consent for us to use or where we used the information to perform a contract with you; and

g) withdraw consent at any time where we are relying on consent to process your personal data. 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. Please email us at compliance@xtelluseurope.com.

13.4 You will need to quote your name and address and also provide via the email address provided to the Company during the onboarding process, brief details of the data that you would like a copy of or which you would like to be corrected.

13.5 We will require you to confirm your identity before providing you with details of any personal data we may hold about you.

13.6 We try to respond to all legitimate requests within 10 (ten) business days. Occasionally, it may take us longer than 10 (ten) business days if your request is particularly complex or you have made more than one requests. In this case, we will notify you within 10 (ten) business days of the receipt of your request and keep you updated.

13.7 We may charge a reasonable fee to you when a request is manifestly unfounded, excessive or repetitive, or we receive a request to provide further copies of the same data via the post. Any fees will be disclosed to you before the relevant Department of the Company takes any additional actions of your request. Alternatively, we may refuse to comply with your request in these circumstances.

13.8 Not all types of data can be deleted or amended per request of the data subject. The Company may retain your data, information, and documentation for a minimum period of five (5) years. Upon request, this period may be extended to up to seven (7) years. The retention period begins upon the termination of the business relationship between both parties, in accordance with the Company's Terms of Business and on the below legal requirements:

a) The Investment Service Law 87(I)/2017, or any subsequent amendment or change of this legislation.
b) The Prevention and Suppression of Money Laundering and Terrorist Financing Law of 2007 to 2023 (as amended from time to time).
c) Directive for the Prevention and Suppression of Money Laundering and Terrorist Financing (as amended from time to time).
d) Any Regulation issued by the Tax Department of the Republic of Cyprus.
e) Any legislation issued by the Unit for Combating Money Laundering (MOKAS), the Cyprus Securities and Exchange Commission, the Office of the Commission of Data protection in Cyprus or any other legislative or supervisory authority, which may be empowered by Law

to supervise us.

14. Company's Ventors and Third-Party Associates

14.1 The Company uses clients' Bank Account Information for clients' deposits and withdrawals, to and from clients trading account.

14.2 Clients acknowledge and consent that the Company and its vendors and/or third-party associates may share information in a manner that is useful and relevant only to do so and in relation to one of the following purposes:

a. Reasonably required by such vendor and/or third-party associate of the Company to provide products and services to its clients;
b. To offer additional similar products and services that meet clients' needs.

14.3 The Company may disclose clients' personal information to any organization at the clients' request or to any persons legally acting on behalf of clients, including clients' financial adviser, solicitor or accountant.

14.4 The Company may disclose clients' personal information other legal entities hired by the Company to provide limited services on behalf of the Company, including but not limited to packaging, mailing and delivering purchases, postal mail. The Company will take all reasonable measures to ensure that the said legal entities will be subject to such personal information/data necessary to deliver the service and are prohibited from using personal information for any other purpose.

15. Non-Affiliate Third Parties

15.1 The Company may disclose information to non-affiliated third parties where necessary in order to carry out the following internal functions of the Company:

a. Service providers such as third parties providing internal audit, risk management, accounting or any other services that we may require from time to time;

b. Use of specialized agencies to help carry out certain internal functions such as account processing, client service or other data collection activities relevant to our business.

16. Warranties

16.1 For any purpose mentioned above the use of shared information is strictly limited to the performance of the services expected and assigned to be undertaken by all third parties or non-

affiliated with which the Company.

16.2 All the above-mentioned third-party providers or non-affiliated third parties (see Sections 14 and 15) are required and shall ensure that:

a. Their employees are informed of the confidential nature of the personal information/data and that usage of the shared information is strictly limited to the performance of the relevant services expected and assigned to be undertaken on behalf of the Company.

b. Processing of personal information/data is in accordance and in compliance with all relevant legislation, applicable laws and regulation mentioned in Section 13.8 of this Policy.

c. All third-party providers or non-affiliated third parties agree and consent to indemnify and keep indemnified at their own cost and expense the Company against all costs, claims, damages or expenses incurred by the Company or for which the Company may become liable due to any failure by any third-party providers or non-affiliated third parties or their employees to comply with any of their obligations under this Policy as well as with all relevant legislation, applicable laws and regulation under Section 13.8 of this Policy.

d. The Company will not share personal information with third parties which it considers will not provide its clients with the required level of protection similar to that of its own and in compliance with all relevant legislation, applicable laws and regulation.

17. Links to Other Websites

17.1 The Company's website will *not* be normally linked to other websites. Hence, this Policy is not applicable to any other sites. The Company recommends and encourages clients to read, understand and familiarize themselves with the privacy policies (if any) available on these other sites.

17.2 The Company cannot be held responsible or liable for the privacy policies or content of other sites and therefore has no control over the protection and use of information provided by the clients on such sites.

17.3 In case the Company's website contains any hyperlinks to websites owned and operated by third parties, we urge you to review the equivalent data protection, privacy and cookie policy available on such websites. We do not accept any responsibility or liability for the data protection of privacy practices of third parties in relation to such websites and your use of third-party websites is entirely at your own risk.

18. Use of Cookies

18.1 The Company may use cookies to assess and improve the performance of the website and its services offered to its clients. Cookies are used by most internet browsers and are small pieces of information which use a unique identification tag and are stored on clients' device as a result of clients using the Company's website or other services the Company provides to its clients.

18.2 Clients may be able to refuse to have cookies stored on their device they may be able to change the setting of their browser to refuse all cookies, and/or have their device to notify them each time a cookie is sent to their device. By controlling their cookies in this way may impair the quality of service provided by the Company to its clients and therefore, it is recommended for clients to allow cookies on their device to ensure the best possible experience and quality services provided by the Company.

18.3 *What is a cookie*?

Cookies are text files containing small amounts of information which are downloaded to your device when you visit a website. Cookies are then sent back to the originating website on each subsequent visit, or to another website that recognises that cookie. Cookies are useful because they allow a website to recognise a user's device.

Cookies do lots of different jobs, like letting you navigate between pages efficiently, remembering your preferences, and generally improve the user experience. They can also help to ensure that adverts you see online are more relevant to you and your interests.

18.6 The categories of cookies we use are:

a) **Essential cookies** are required for the operation of the Company's website. These cookies allow clients to access various secured areas of the Company's website. Clients by opt to disable these cookies, this may have a negative impact on their browsing experience and in particular, they will not be able to fully access secure areas of the Company's website.

b) **Analytical/performance cookies** are used to recognize, monitor and track the number of visitors, how clients use the Company's website and for how long. This helps the Company to improve the way its website works and consequently to improve how the Company provides the Company's website content to clients. These cookies are not used to determine the personal identity of clients.

c) **Functionality cookies** are used to allow the Company to remember clients' preferences and to recognize when a client returns to the Company's website. This helps the Company to personalize its website content for clients. For example, these cookies remember clients' username and the customization preference previously selected by clients such as language of region.

d) **Targeting cookies** are cookies that record clients' visits on Company's website, other pages visited, and links followed, related to the Company (if any). This information may be shared with third parties such as advertising and social media websites for the provision of services for example:

   a. Use information about clients' visits to target advertising to clients on other websites
   b. Use information about clients' visits in order to present clients with advertisements that might be in clients' interest
   c. Use information about clients' visits for the purposes of matching, audience research and creation of audience segments. Outsourcing

19. Setting your Cookie Preferences

19.1 You can control how cookies are placed on your device from within your own browser. You can also delete existing cookies from your browser. However, refusing and/or deleting cookies may mean some sections of our site will not work properly.

20. Contact Clients and Recordings

20.1 The Company may contact clients via its official telephone line, email, or other communication channels to provide additional information regarding its investment services or to inform clients about new financial products. By registering and agreeing to the Company's Terms of Business, clients consent to such communications from the Company's employees, as necessary. The Company remains fully compliant with Article 25(1) of Law 87(I)2017, ensuring that it acts honestly, fairly, and professionally when providing investment or, where applicable, ancillary services to clients, always in alignment with the clients' best interests.

20.2 For regulatory and quality assurance purposes and/or as per Article 17(6) and 17(7)(a) - (d) any type of communication between the clients and the Company whether in writing or by telephone or other means of medium shall be monitored by the relevant Department and recorded by the Company without any warning (unless required to do so by the applicable rules and regulations). Clients acknowledge and accept that such recordings are the sole property of the Company. Clients further accept that such recordings constitute conclusive evidence of the Orders/Instructions/Requests or conversations so recorded.

20.3 Any person who wishes not to be contacted further by telephone or email, can inform the Company accordingly by contacting the Company at the following address: compliance@xtelluseurope.com.

21. Clients' Rights

21.1 Right to Access

a) You have the right to request copies of your personal data. Information must be provided without delay and at the latest within ten (10) business days of receipt. The Company will be able to extend the period of compliance by a further one (1) month where requests are complex or numerous. If this is the case, we will inform the individual within one month of the receipt of the request and explain why the extension is necessary.

b) We must provide a copy of the information free of charge. However, the Company can charge a "reasonable fee" when a request is manifestly unfounded or excessive, particularly if it is repetitive. The fee if applied will be based on the administrative cost of providing the information.

c) If at any time we refuse to respond to a request, we will explain in writing the reasons to the clients, informing them of their right to complaint to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

21.2 Right for Rectification

a) The GDPR includes a right for individuals to have inaccurate personal data rectified or completed if it is incomplete. You can make a request for rectification in writing via email to the Data Protection Officer of the Company (compliance@xtelluseurope.com).

b) If we have disclosed the personal data in question to others, we must contact each recipient and inform them of the rectification - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients.

c) The Company will respond within 10 (ten) working days after your request for rectification has been submitted. This can be extended by 1 (one) month where the request for rectification is complex.

d) Where the Company is not acting in response to a request for rectification, an explanation to the individuals will be provided, informing them of their right to complain to the supervisory authority and to a judicial remedy.

21.3 Right to Erasure

The right to erasure does not provide an absolute 'right to be forgotten'. Individuals have a right to have personal data erased and to prevent processing only in specific circumstances and in line

with Article 17(7)(h) of Law 87(I)2017:

a) Where the personal data is no longer necessary in relation to the purpose for which it was originally collected/processed.
b) When the individual withdraws consent.
c) When the individual objects to the processing and there is no overriding legitimate interest for continuing the processing.
d) The personal data was unlawfully processed (i.e. otherwise in breach of the GDPR).
e) The personal data must be erased to comply with a legal obligation issued by any regulation within the Republic of Cyprus.
f) The personal data is processed in relation to the offer of information society services to a child, under 18 (eighteen) years old.
g) There are some specific circumstances where the right to erasure does not apply, and we can refuse to deal with a request.

We can refuse to comply with a request for erasure where the personal data is processed for the following reasons:

- to comply with a legal obligation for the performance of a public interest task or exercise of official authority.
- the exercise or defense of legal claims.

If we have disclosed the personal data in question to others, we will contact each recipient and inform them of the erasure of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients.

21.4 Right to Restrict Processing (Article 18 of GDPR)

a) We will be required to restrict the processing of personal data in the following circumstances:
   i. Where an individual contests the accuracy of the personal data, we should restrict the processing until you have verified the accuracy of the personal data.
   ii. Where an individual has objected to the processing (where it was necessary for the performance of a public interest task or purpose of legitimate interests), and we are considering whether our Company's legitimate grounds override those of the individual.
   iii. When processing is unlawful, the individual opposes erasure and requests restriction instead.
   iv. If the Company no longer needs the personal data but the individual requires the data to establish, exercise or defend a legal claim.

b) We may need to review procedures to ensure we are able to determine where we may be required to restrict the processing of personal data.

c) If the Company has disclosed the personal data in question to others, we must contact each recipient and inform them of the restriction on the processing of the personal data - unless this proves impossible or involves disproportionate effort. If asked to, we must also inform the individuals about these recipients.

d) The Company must inform individuals when we decide to lift a restriction on processing.

e) When processing is restricted, the data will only be stored and won't be processed further without the individual's consent, unless it's for legal claims, protecting the rights of others, or for reasons of important public interest.

21.5 Right to Data Portability (Article 20 of GDPR)

a) The right to data portability allows the clients to obtain and reuse their personal data for their own purposes across different services.
b) It allows them to move, copy or transfer personal data easily from one IT environment to another in a safe and secure way, without hindrance to usability.
c) It enables Clients to take advantage of applications and services which can use this data to find them a better deal or help them understand their spending habits.
d) We will respond without undue delay, and within 10 (ten) working days. This can be extended by one (1) month where the request is complex or where the Company may receive several requests. We will inform the client within one month of receipt of request and explain why the extension is necessary, if applicable.
e) Where we are not acting in response to a request, we will explain why to the clients, informing them of their right to complain to the supervisory authority and to a judicial remedy without undue delay and at the latest within one month.

21.6 Raising a concern (Article 77 of GDPR)

a) You have the right to be confident that we handle your personal information responsibly and in line with good practice and the best interest of any Company's client.

b) If you have a concern about the way we are handling your information, for example if you feel we may not be keeping your information secure or holding inaccurate information about you or have disclosed information about you or keeping information about you for longer than is necessary or have collected information for one reason and are using it for something else you can contact us. We take all concerns seriously and will work with you to resolve any such concerns.

c) In case any of the clients' personal information have changed at any given time or they wish from the Company to delete any personal data, they may do so by informing the Company via email at compliance@xtelluseurope.com. The Company to the extent permitted by any regulatory framework issued within the Republic of Cyprus and/or in the European Union, including those cases where the Company is required to hold clients' personal data for regulatory and legal purposes for the provision of services and/or maintenance of adequate business records, will proceed with changing or deleting clients' personal data in accordance with the instructions received.

22. Data Protection Impact Assessment ("DPIA")

22.1 Based on Article 35 of the GDPR, the Company must perform a Data Protection Impact Assessment ("DPIA") for any and all new projects and/or new uses of personal data which involve the use of new technologies, and the processing involved is likely to result in a high risk to the rights and freedoms of data subjects under the GDPR.

22.2 The Company is responsible for ensuring that the DPIA is carried out. The DPO is responsible for performing necessary checks on personal data to establish the need for conducting a DPIA.

22.3 The Company must also seek the advice of the DPO, where designated and this advice, and the decisions taken by the Company, should be documented within the DPIA. The DPO should also monitor the performance of the DPIA. The Company's DPO will be responsible for checking appropriate controls are implemented to mitigate any risks identified as part of the DPIA process and subsequent decision to proceed with the processing.

22.4 The Company should document its actions and decisions regarding DPIAs in order to be in a position to prove its compliance with the GDPR.

a) Identify the need for a DPIA
b) Describe the information flow
c) Identify data processing and related risks
d) Identify solutions to reduce or eliminate these risks
e) Sign off the outcomes of the DPIA
f) Integrate data protection solutions into the project

22.5 Why should we conduct a DPIA?

The GDPR mandates a DPIA to be conducted where data processing "is likely to result in a high risk to the rights and freedoms of natural persons". The three primary conditions identified in the GDPR are:

a) A systematic and extensive evaluation of personal aspects relating to natural persons, which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person.

b) Processing of special categories of data or personal data relating to criminal convictions and offences on a large scale.

c) Systematic monitoring of a publicly accessible area on a large scale.

Examples of personal data processing where a DPIA is likely to be required:

a) The archiving of pseudonymised sensitive data from research projects or clinical trials.
b) The Company using an intelligent video analysis system to single out cars and automatically recognise registration plates.
c) The Company systematically monitoring its employees' activities, including their workstations and Internet activity.
d) The gathering of public social media data for generating profiles.
e) An institution creating a national-level credit rating or fraud database.

23. Amendment/Review of the Policy

23.1 The Company reserves the right to review and amend this Policy at any given time it deems suitable and appropriate without giving notice to the Clients. The Policy is available for review by clients upon request and it is uploaded on the Company's website.

24. General Information

24.1 For further details with regards to the Company's Privacy Policy and procedures, clients may contact compliance@xtelluseurope.com.

25. How to Make a GDPR Complaint?

25.1 If you have a complaint about the way in which your personal data is being processed, please email compliance@xtelluseurope.com. In the event that you are not satisfied with our handling of your complaint, you have the right to report your concern to the Data Protection Commissioner at **1, Iasonos Street, 1082 Nicosia, P. O. Box 23378, 1682 Nicosia** Tel: (+357) 22818456, Fax: (+357) 22304565 email: commissioner@dataprotection.gov.cy

26. Governing Law

26.1 Use of this site shall be governed by the Laws of the Republic Cyprus.

26.2 By accessing the Company ("We" or "us" or "the Company") website and any pages linked thereto, you the Client agree to be bound by the terms and conditions as described above. By continuing to use this website you are also consenting for the use of cookies.

27. Definitions

a) **consent** of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

b) **CySEC** means the Cyprus Securities and Exchange Commission.

c) **GDPR** – General Data Protection Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016.

d) **Personally identifiable information** (or "Personal Information" or "Personal Data") means any information that may be used, either alone or in combination with other information, to personally identify, contact or locate any Customer of the Company.

e) **You, data subject, client(s), customer** refers to you as the party agreeing to becoming a client and use the investment services of the Company.

f) **We, the company, controller** refers to Xtellus Europe Limited (see Section 1.1.).

g) **EMIR** refers to the European Market Infrastructure Regulation (EU) No 648/2012.

h) **MiFIR** refers to the Markets in Financial Instruments Regulation EU) No 600/2014.

i) **DPIA** Data Protection Impact Assessment.

j) **DPO** Data Protection Officer.

k) **IT** Information Technology.

28. Monitoring and Review

28.1 The Company will monitor the effectiveness of this Policy on a regular basis, at least annually. The review will also be carried out whenever any material changes occur.

28.2 The existing Clients will be notified of any material changes or amendments to this Policy which may be made from time to time. The latest version of the document will also be available at the Company's website.