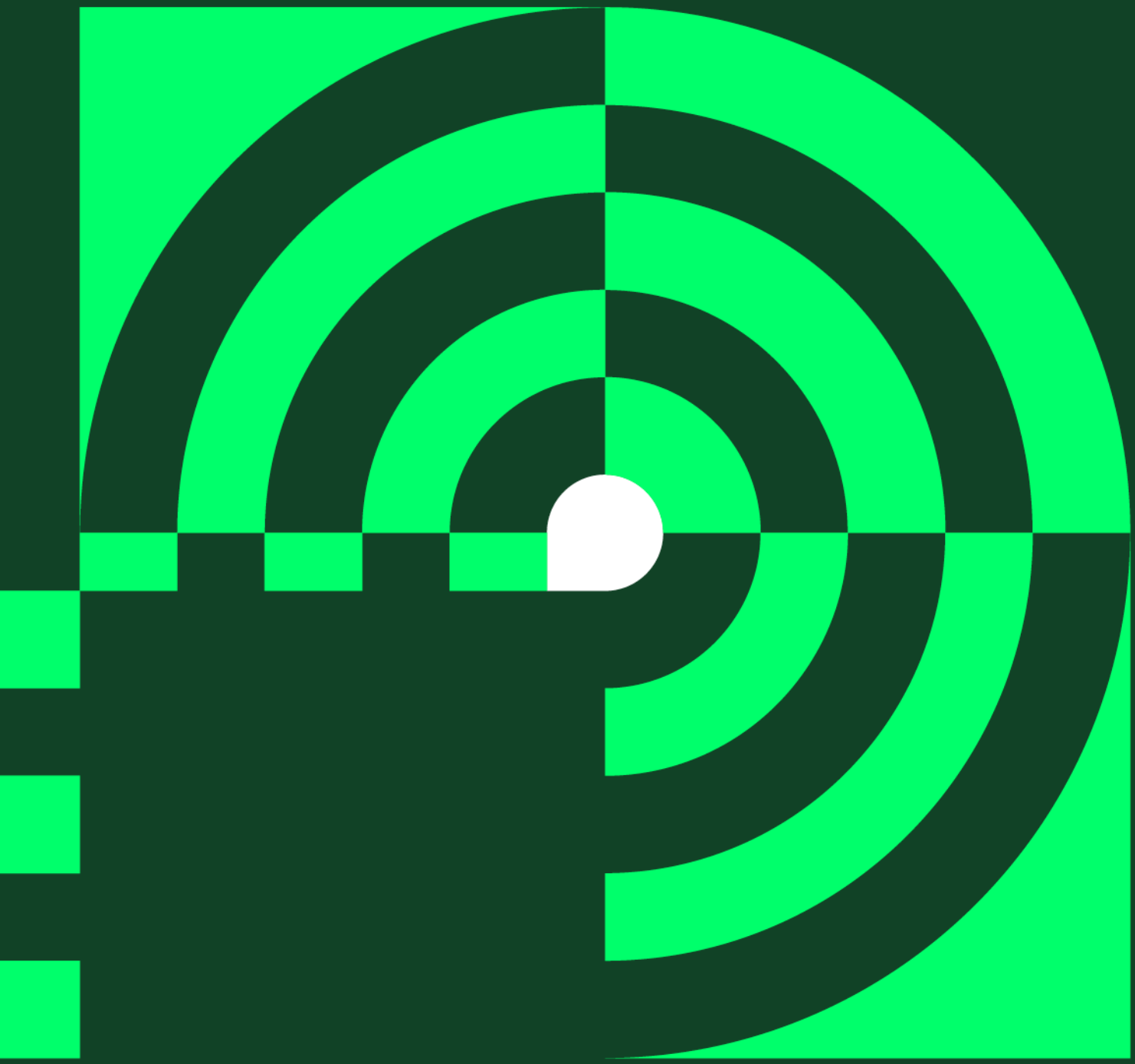
eightcap

Eightcap Global Services Privacy Policy



1 Introduction

This Privacy policy is issued by Eightcap Global Services Ltd (Registration Number 2025-00652). Our registered address is Ground Floor, Rodney Court Building, Rodney Bay, Gros Islet, St. Lucia. In this policy, we use the terms '**we**', '**our**', '**us**' or '**Eightcap**' to refer to Eightcap Global Services Ltd, and as the case requires, its affiliated entities.

Protecting your privacy and keeping your information confidential is important to us. We are committed to managing your personal and sensitive information in an open and transparent way. This Policy outlines how Eightcap manages, handles and protects the personal data it collects and holds about you in accordance with the Data Protection Legislation.

Before onboarding you as a client we are legally required to collect identifying information from you. This is also a precondition of entering into our client Agreement. We collect personal and sensitive information to provide you with products and services that you ask for and information about products and services offered by us or third parties. We may also use your information to administer our services, for corporate risk management, and unless you tell us otherwise, to provide you with marketing material.

Eightcap is part of a multinational group of companies called the Eightcap Group. The Eightcap Group works on a shared services model where different offshore entities will process your data for the purposes of providing our services and products to you. These relationships, including those with Third Parties, are governed by Data processing Agreements. These Data processing Agreements set out enforceable standards which our processors and Sub-processors must follow when processing your personal data on our behalf.

We expect that all Third Parties, clients, Employees, suppliers, subcontractors or agents that have access to your personal data, will abide by this Policy.

2 European and United Kingdom Representative

2.1 Our role as a Controller

We act as a Controller of EU and UK client personal data. Because we are not incorporated in the EU or UK, we are required to appoint an in-region representative for any EU or UK based client to deal with. This representative also acts as our representative when dealing with Supervisory Authorities.

2.2 Our role as a processor

We may act as a processor of some EU and UK client personal data for a number of Eightcap Group Controllers, including:

(a) Eightcap Group Limited – registered in the United Kingdom

(b) Eightcap EU Limited – registered in Cyprus

(c) Eightcap Global Limited – registered in the Bahamas

(d) CL Markets Limited – registered in the SVG

(e) GC Group Limited – registered in Seychelles

(f) Eightcap International Trading Limited – registered in Mauritius

2.3 Appointed Entities

Eightcap has authorised the following Eightcap Group Entities to act as it's EU and UK representative:

(a) United Kingdom Representative

Entity: Eightcap Group Limited
Registration Number: 12448314
Contact Details:

- **Address -** 40 Gracechurch Street, London, EC3V 0BT
- **Phone** - +44 333 1503 027
- **Email** - customerservice-uk@eightcap.com

(b) European Union and European Economic Area Representative

Entity: Eightcap EU Limited
Registration Number: 246/14
Contact Details:

- **Address -** Aiolou & Panagioti Diomidous 9, Katholiki, 3020, Limassol, Cyprus
- **Phone** - +357 25 060 006
- **Email** - support@eightcap.eu

2.4 Our UK and EU Data Protection Officers

You may address any communications to the applicable Data Protection Officer, by using the contact details above.

3 Collection of personal data

3.1 Why we collect your personal data

We only collect your personal data when its reasonably necessary for us to provide you with our products or services. To open a trading account with us and deposit funds, we are required under AML/CTF Laws to collect certain information to verify your identity, such as your driver's licence or passport.

3.2 personal data we may collect

When we deal with you as a current or prospective client, we may collect personal data directly from you, most of the time. However, we may also collect information about you from other organisations and/or people. We collect information when you:

(a) apply for or enquire about our products or services;

(b) contact us to make an enquiry, complain or provide feedback;

(c) enter into transactions on ours (or a third parties) trading platform;

(d) interact with our website or other digital services owned by us or our affiliated entities;

(e) participate in other activities with us such as seminars or education session; and

(f) talk to us or enter into a business partnership with us.

We only collect information where it is necessary for us to provide you the products or services you require. Depending on your relationship with us and the products and services you receive, we may collect the following information:

Types of personal data	Kind of personal data Involved

Personal and contact details	Name, address, date of birth, email address, phone number
Government Issued Identity Documents	We may request government issued identity documents, such as: (a) passport; (b) drivers licence; (c) proof of age card; and (d) other government issued photo identity document If you request to change your details (including country of citizenship), we may request: (a) change of name/marriage certificate; (b) death certificates; (c) citizenship certificate; and (d) any other document necessary to prove the change of details.
Financial information	We may request documents to prove your source of wealth or funds. We may also require your financial information to process payments. This may include: (a) bank account information; (b) credit card details; (c) transaction history; (d) trading statements or statements of entitlement; (e) details of your employment, income, assets, liabilities; and (f) bank statements, account statements or ledgers from financial institutions.
Socio-economic and demographic information	We may request information for us to determine whether you are suitable for our products or services. This could include details about your age, gender, occupation, literacy, housing status etc.
Digital information	We collect information from your interactions with our online services. This includes: (a) location information (where you enable this on your device); (b) IP address; and (c) details regarding access of our digital services. We may collect similar data where you interact with our social media channels. You can control our access to some details through accepting or rejecting cookies upon entering our website.
Behavioural information	We will collect and maintain data relating to how you use our products and services. This will assist us to improve the design of our products and services.

Recordings and transcripts	Any interaction you have with an Eightcap staff member through official channels (i.e. publicly available phone numbers, emails and live chats) are recorded. These records may be accessed for monitoring as part of our quality assurance programme.
Sensitive information	There are limited circumstances where Eightcap will acquire sensitive data about you. However, some instances include: (a) where we have conducted a screening check and have been alerted to your criminal history; (b) you provide us health information to prove your suitability to trade with us; (c) where you provide details to us about your religion to access specific religion-friendly accounts; and (d) biometric data collected as part of our KYC process. Where we require sensitive information outside the scope of the above, we will request your consent before collecting this from you.
Publicly available information	In many instances Eightcap may collect information about you from publicly available sites. This includes: (a) social media platforms, online forums and profession networking sites; and (b) publicly accessible registers (bankruptcy registers, corporate databases etc)

3.3 Purposes and Basis for processing your personal data

We processes your personal data to facilitate the provision of our products and services. We will process, or appoint others to process your data for the following purposes:

Types of personal data	Kind of personal data Involved
Compliance with legal obligations	We are bound to abide by specific legislation and to the scrutiny and expectations, within the legal boundaries, of Supervisory Authorities and other relevant stakeholders. We, among other things, help to prevent terrorist financing, money laundering, financial crime and fraud, for instance by reporting unusual transactions or by identifying and stopping potentially fraudulent transactions and, where necessary, verifying transactions. We at times, may be required to disclose your information to a regulator, if this disclosure is inconsistent with the Data Protection Laws that apply to you, we will make the necessary disclosures to the Supervisory Authorities.

Legitimate Interests	(a) Eightcap Group Entities use personal data to study possible market trends, problems, and identify root causes of errors and risks within our business. (b) personal data may be used in a qualitative or quantitative format to facilitate any research objective, so long as that objective is ethical and has a reasonable basis. (c) We may use a client's personal data, to the extent reasonably necessary, to provide them with their products and services (d) client personal data may be used to verify whether our products or services are still meeting your wishes and expectations. (e) client personal data may also be used for the development, release and/or updating of new and existing products or services. (f) personal data may be used to form large data sets which allow an us to understand our client base and who is using our products and services. These findings may then be used as the basis for targeting and distributing our products and services to other prospective clients. (g) We will use client personal data to process any requests the client provides to us, including but not limited to, a client exercising a right under this Policy, a general enquiry, or a client exercising rights under Local Laws.
Security, Integrity and Operational Resilience	(a) personal data may be used to prevent or combat attempted or actual criminal acts, including, hacking, Distributed Denial-of-Service Attacks, and any other applicable cyberattack. (b) From time-to-time we may use client data to perform simulated cyber or physical events to assess its preparedness in the event of some attack or disruption to business continuity. (c) To the extent allowed or required under Local Laws, we may use personal data for the generation and maintenance of warning systems designed to detect and ensure the integrity of our technological infrastructure.
Improving the Eightcap Group Entities	We may collect, process, store, and utilise client personal data for the purpose of improving business efficacy, operational efficiency, and day-to-day activities. This includes, but is not limited to, enhancing quality, optimising internal processes, refining risk management

	practices, and ensuring compliance with internal policy and/or procedure requirements.
Monitoring	Monitoring, assurance and audit are critical functions within every our business. We use client personal data to fulfil our monitoring, assurance and audit functions/requirements. Any information, document, report or set of data is to be classified, at a minimum, as 'confidential' in accordance with the Information Classification Policy.
Marketing	We may provide information, offers or news on relevant products to clients, their representatives or related persons. (a) This includes the processing of personal data in order to establish a relationship with a Data Subject and/or continuing as well as extending a relationship with a client or with the representatives or related individuals of such client, which can be a business.

3.4 Grounds for processing personal data

(a) personal data will only be processed if at least one of the following grounds applies:

(i) the processing is necessary for the performance of a contract, including a client agreement, to which you are a party or to take steps at your request prior to entering into a contract;

(ii) the processing is necessary for compliance with a legal obligation to which an Eightcap Group Entity is subject;

(iii) the processing is necessary to protect your vital interests.

(iv) the Data Subject has given their consent to the processing; or

(v) the processing is necessary for the purposes of the legitimate interests pursued by us, except where such interests are overridden by your interests or fundamental rights and freedoms.

(b) Legitimate interests under clause 3.4(a)(v) can include, but are not limited to:

(i) the protection of property and personal data of clients, Employees, Eightcap Group Entities or others;

(ii) the protection of Eightcap Group's financial position (for example, by undertaking financial risk assessments) the interests of client and employees and the interests of others (including creditors in the event of an insolvency);

(iii) carrying out fraud detection activities so that clients and Employees of Eightcap Group do not suffer losses as a result of fraud and to contribute to and preserve the integrity of the Eightcap Group; and

(iv) to conduct statistical and scientific research for example to understand how products perform, whether they should be modified or how they should be updated. Such research my also include research using advanced analytics on Employee personal data to identify the impact of management decisions as long as permitted as per the terms of this Policy and applicable local

legislation. It also makes use of service providers that help in such efficient organisation.

3.5 How we collect your data

Unless you post us physical documents, all data you provide us will be through electronic means. Most personal data you provide us is provided during your application process.

Any subsequent interactions, calls, chats or emails you engage with us are retained for the periods required under the applicable laws.

There may be times where the data we collect about you is not directly provided by you. These cases include:

(a) accessing publicly available information;

(b) conducting manual or automated due diligence checks, including by accessing third party credit reporting agencies;

(c) using cookies to collect information about your interests and history to tailor our marketing (you will be prompted to agree or reject the use of cookies upon entering our website).

We will not collect any data where it would not be necessary for the provision of our products and services to you.

3.6 Dealing with Unsolicited personal data

If you provide personal data that we have not requested, we will only retain it in limited circumstances. We will only retain the information if it is reasonably necessary for us to provide you with products and services, and you have consented to the information being collected, or it was not practical or reasonable for us to obtain your consent under the circumstances. If these conditions are not met, we will destroy the information where it is reasonably practical for us to do so.

If the unsolicited information we receive about you is sensitive information, we will always obtain your consent.

3.7 How and where we store your data

We use secure systems and buildings to hold your information. Most information you provide to us is stored electronically in Australian based server.

We maintain some overseas servers to ensure that we have copies of you information in the event of a system outage or disaster. We take all reasonable measure to ensure that your person information is stored safely to protect it from misuse, loss, unauthorised access, modification or disclosure, including electronic and physical security measures.

3.8 Retention of your data

To comply with our legal record keeping obligations, we and our processors will store your data for a period of 5 years. After this period your personal data will be destroyed or de-identified.

4 Your Data Rights

Unless otherwise required by Law or we are entitled to do so, we will not reject an exercise of your data rights, unless the request is:

(a) manifestly unfounded; or

(b) excessive.

4.2 Access and rectification

You may request access to the personal data we hold about you. If the information we hold is inaccurate, incomplete, outdated or otherwise unreliable, please let us know so that we can correct it. We will action you request within 30 days of receiving it.

However, there may be some circumstances where Eightcap is legally prevented from providing you access to your data. In these cases, we may be restricted from informing you of the reasons for denying your request.

For example, we may have used your personal data to make a commercially sensitive decision about providing you with a product or service. We may choose to provide you with this information, or provide you limited (or no) access to the specific information connected with our decision.

4.3 Deletion – right to be forgotten

Any client may request to have their personal data deleted at any time. However, in most circumstances, Eightcap is prevented from deleting your data. We must comply with our Anti-Money Laundering and Counter-Terrorism Financing Obligations. This requires us to retain any know your client information (***KYC Information***) for a period of 5 years after you cease to be a client with us. You may still raise a request with us and our Privacy Team will take steps to limit access to your personal data on our internal systems.

Where you request for your data to be deleted, and you have not provided us with any KYC Information, we will delete all records of your personal data. If you have provided us with KYC Information including identity documents, statements of wealth/funds or proof of address documentation, we will remove any employee facing records in our customer relationship management software and cycle your data through our database in accordance with our data lifecycle policy. After 5 years, these records will be destroyed.

4.4 Right to object to processing

You have an absolute right to reject to our processing of your personal data if it is used for direct marketing purposes. You may also object to our processing if:

(a) it is carried out in the public interest

(b) we are exercising an official authority which has vested in us; or

(c) we are processing on the basis of our legitimate interests.

Your rights may be limited depending upon the processing activity you are objecting to. We will provide reasons for our decision when actioning your request.

4.5 Right to Restrict processing

You may request that we restrict the processing of your personal data. This includes limiting the ways in which we can use your data or prevent us from using it entirely. You may only exercise this right where:

(a) you contest the accuracy of the personal data and we are taking steps to verify its accuracy;

(b) the data has been unlawfully processed and you oppose its erasure and instead request restriction;

(c) we no longer require the personal data but you require us to keep it to establish, exercise or defend a legal claim; or

(d) you have objected to the processing of your data, and we are considering whether our legitimate interests override your legitimate interests.

4.6 Right to Data Portability

You have the right to receive your personal data in a structure and commonly used machine-readable format. Where you request, we will help to facilitate the transfer of this data from us to another Controller, where this is technically feasible.

4.7 Right to Withdraw Consent

You may withdraw your consent at any time where the basis of our processing Activity relies on your consent. We will make available to you a simple process which allows you to withdraw consent as easily as it is to give it.

4.8 Anonymity and pseudonymity

Due to the nature of the products and services that we provide, and our associated legal and regulatory obligations, we are unable to allow you to deal with us on an 'anonymous' basis.

5 Dealing with Unsolicited personal data

If you provide personal data that we have not requested, we will only retain it in limited circumstances. We will only retain the information if it is reasonably necessary for us to provide you with products and services, and you have consented to the information being collected, or it was not practical or reasonable for us to obtain your consent under the circumstances. If these conditions are not met, we will destroy the information where it is reasonably practical for us to do so.

If the unsolicited information we receive about you is sensitive information, we will always obtain your consent.

6 Sharing your personal data

Depending on the product or service concerned and particular restrictions on sensitive information, where necessary, we may need to share or disclose personal data about you to the following organisations:

(a) any related entities of Eightcap in Australia and elsewhere in the world which provide financial and other services for Eightcap;

(b) credit reporting or reference agencies;

(c) an agent, contractor or service provider we engage to carry out our functions and activities, such as our lawyers, accountants, debt collectors or other advisers;

(d) organisations involved in managing payments, including payment merchants and other financial institutions, such as banks;

(e) regulatory bodies, government agencies, law enforcement bodies and courts;

(f) financial product issuers and credit providers;

(g) if you were introduced to Eightcap by a third-party, we may disclose personal and account information about you to them, their related companies and licensees or authorised representatives;

(h) organisations involved in a transfer or sale of all or part of our assets or business;

(i) anyone else to whom you authorise us to disclose it or is required by law or contract.

If we disclose your personal data to service providers that perform business activities for us, they may only use your personal data for the specific purpose for which we supply it. We will ensure that all contractual arrangements with third parties adequately address privacy issues, and we will make third parties aware of this Privacy Policy.

6.1 Disclosure for AML/CTF Compliance

To open a trading account with us and deposit funds, we are required under the Anti-Money Laundering and Counter-Terrorism Financing Act to collect certain information to verify your identity, such as your driver's licence or passport.

We may need to disclose your full name, residential address, and date of birth to a service provider, who may provide this information to a credit reporting agency. This disclosure is solely for the purpose of assessing whether your identification information matches (in whole or in part) personal data held by the credit reporting agency.

We may need to conduct further checks on your information in accordance with out obligations under the AML/CTF Legislation. This may involve providing your information to an additional third party to be checked against publicly available databases or records maintained by the document issuer or official record holder.

6.2 Disclosure to overseas non-affiliated parties

Your personal data may be disclosed to third party provides located in a jurisdiction which is not the subject of an EU or UK adequacy decision. We will not disclose your data unless:

(a) we have taken reasonable steps to ensure that the recipient has the necessary controls in place to comply with our privacy standards and the necessary agreements are put in place; or

(b) you have consented to the disclosure.

Before we disclose personal data to an overseas recipient, we will take reasonable steps to ensure that the recipient does not breach this Policy or our standards in relation to that information.

6.3 Countries where your data is likely to be shared

The following are countries where Eightcap's affiliated entities, contractors and main vendors may access, inspect, use or store your data to provide you with products or services:

(a) Australia;

(b) United Kingdom;

(c) Cyprus;

(d) Bulgaria;

(e) Philippines;

(f) United States;

(g) Japan;

(h) Vietnam;

(i) Guatemala; and

(j) Thailand.

We conduct security audits and checks on all of our offshore affiliated entities and contractors as part of our quality assurance programme.

7 Contacting us and Complaints

7.1 Contact

If you have any questions or would like further information about our privacy and information handling practices, please contact us using:

(a) Email: privacy.lead@eightcap.com

(b) Phone: (03) 8375 9700

7.2 Making a complaint

We offer an internal complaint resolution scheme to all of our clients. If you have a privacy complaint, please contact us using the details above to discuss your concerns.

We will aim to respond within 48 business hours to let you know who is responsible for managing your complaint (this is ordinarily the Privacy Officer or their delegate) and will try to resolve your complaint within 10 business days. When this is not possible, we will contact you within that time to let you know how long it will take to resolve your complaint.

The Privacy Officer or their approved delegate will investigate your complaint thoroughly and write to you explaining the decision. All reasonable and appropriate steps will be taken to ensure the information you provide us in relation to the complaint is handled in accordance with the applicable laws.

7.3 Making a complaint to the supervisory authorities – EU and UK clients

Where you are unsatisfied with our handing of your data you may contact the following supervisory authorities to lodge you complaint:

(a) European Union

Authority: Office of the Commissioner for personal data Protection
Location: Cyprus
Phone: +357 2281845
Address: P.O.Box 23378, 1682 Nicosia, Cyprus
Fax: +357 22304565
Email: commissioner@dataprotection.gov.cy

(b) United Kingdom

Authority: Information Commissioner's Officer
Location: United Kingdom
Phone: 0303 123 1113
Website: https://ico.org.uk/make-a-complaint/


eightcap