

THE UAP GROUP – PRIVACY NOTICE

Introduction

This Privacy Notice explains how The UAP Group (“we”, “us” or “our”) handle any personal information about you. The UAP Group, registered office address: Cambridge House, Le Truchot, St Peter Port, Guernsey, GY1 1WD.

UAP is the data controller of your personal data and is subject to UK General Data Protection Regulation, 1 January 2021, the Data Protection (Bailiwick of Guernsey) Law, 2017 and General Data Protection Regulation, May 2018 for Malta.

Details on how to contact us are below.

UAP is committed to protecting your personal information and being transparent about what information we hold.

The purpose of this Notice is to give you a clear explanation about how UAP collects and uses the personal information you provide to us, whether online, via phone, email, in letters, in any other correspondence or from third parties.

We ensure that we use your information in accordance with all applicable laws concerning the protection of personal information.

When we refer to “personal information” or “personal data” in this Privacy Notice, we mean information which identifies you as an individual, or is capable of doing so. In the context of this Privacy Notice, the terms “personal information” and “personal data” may be used interchangeably.

This Notice explains:

- What personal information UAP may collect about you;
- How we might use that information;
- Our legal basis for contacting you and using your personal information;
- Whether we disclose your details to anyone else; and
- Your rights regarding personal information you provide to us.

What information do we collect?

In order to provide services to you, we need to collect certain personal information. We may also be required by law, or as a consequence of any contractual relationship we have, to collect your personal information. If you do not provide this information to us, it may prevent or delay us fulfilling our obligations or performing services.

We may collect the following information:

- Your contact details, such as your name, address, telephone number and email address;
- Your date of birth, nationality, country of birth, country of residence, employment status and tax identification number;
- Passport details, driving licence, ID cards and utility bills;

- Details of the services you request from us;
- Any records held by financial crime prevention agencies, on the Electoral Register and by providers of utility services; and
- Details of your employment status, income and source of wealth.

In some cases, you are not obliged to provide any personal data to us, but if you have requested information or a service from us, we will not be able to provide it without certain information, such as your contact details.

Before we can begin providing you with our services, we may need to obtain certain information about you, so that we can verify your identity in order for us to meet our obligations under the Anti Money Laundering and Counter-Terrorism Financing requirements and any other applicable legislation and for the purposes of crime prevention and fraud prevention in the relevant jurisdictions. You are obliged to provide this information and if you do not provide it, we will be unable to provide you with our services.

We may also collect and process information about your interactions with us, including details about our contacts with you for example through email on the phone or in person (such as the date, time, and method of contact). Please note phone calls are recorded. Skype, WhatsApp and other forms of mobile communication are not classed as data, unless expressly requested to be, or, at our discretion, reproduced in a reportable format such as email or File Note.

We do not normally ask you for any personal data which would fall into certain special categories (also known as 'sensitive personal data'), which include information revealing an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and genetic data, biometric data, data concerning health or data concerning an individual's sex life or sexual orientation.

However, as part of our supply of our services to you, you may voluntarily provide us with sensitive personal data. We will only process this data when we have your consent or we are otherwise allowed to by law. We would only collect sensitive personal data if there is a clear reason for doing so.

Why do we collect this information?

When we use your personal information the law says we have to be able to show that we have a lawful ground for doing so. Lawful grounds can include:

- When we have a legal obligation;
- When it is necessary to carry out a contract with you or to take steps to enter into a contract with you; or
- When it is in our legitimate interest.

When we process personal information on the basis that it is in our legitimate interests to do so we will have undertaken an assessment to ensure our processing is transparent, proportionate and does not unfairly prejudice your interests.

By providing personal data you consent to our processing of said data to the extent that we have lawful grounds to do so.

We use information held about you in the following ways:

- To process your application to use our services;
- To undertake checks such as identification verification checks with fraud prevention agencies to enable us to comply with our anti-money laundering obligations and for the purposes of crime prevention and fraud prevention;
- To comply with our obligations arising from any contracts entered into between you and us and to provide you with the information, products and services that you request from us;
- To help protect your information and prevent unauthorised access to it;
- To deal with any queries, complaints or problems reported by you;
- To provide additional requested services;
- If required to do so by law and to the extent necessary for the proper operation of our systems, to protect us/our clients, or for the enforcement of any agreement between you and us;
- To notify you of changes to our services; and
- To help improve the services we provide to you.

Unless otherwise stated in this Privacy Notice, the legal basis for our use of your personal data will be that this information is required to be processed on the lawful grounds described above.

Financial Crime Prevention Checks

As part of our application process we will carry out automated checks using your personal data, such as your name, postal address, date of birth, telephone numbers and employment status. These checks include identification verification checks and financial crime checks and involve us obtaining information from financial crime prevention agencies and any records held by financial crime prevention agencies and providers of utility services.

We need to carry out these checks in order to meet our obligations under any applicable legislation. The information obtained from these checks is used by us to determine if we can accept you as a client, whether further information is required or the application is rejected, based on factors such as whether we have been able to verify your identity.

We may make periodic searches with financial crime prevention agencies during the course of our relationship with you to verify the information we hold remains correct and that there has been no change in your status (for example when you are a politically exposed person or if you have been subject to a financial sanction). We and other organisations (who may be from other countries) may use and access the information recorded by financial crime prevention agencies.

To prevent or detect financial crime or to assist in verifying your identity we may make searches at financial crime prevention agencies. We may also provide information to financial and other organisations involved in financial crime prevention to protect ourselves and our clients from theft and/or financial crime. If false or inaccurate information is provided and financial crime is identified or reasonably suspected, details will be passed to financial crime prevention agencies who will record this. This information may also be accessed by law enforcement agencies. This information may be used by us, other Group companies and other organisations to prevent financial crime and money laundering, for example, when processing applications for services or for debt recovery.

When do we collect personal information?

We may collect personal information about you when you:

- Ask about our services;
- Register with us for information;
- Use our services;
- Sign up for publications or newsletters;
- Telephone, write, contact us online, or otherwise provide us with your personal information.

We may collect information about you directly whenever you interact with us. We may also receive information about you when you interact with third parties with whom we work. We may supplement what we know about you with information that is available to the public. Generally, our processing of your personal information as described in this Notice is allowed by applicable data privacy laws because we have a legitimate need to carry out the processing for the purposes described above.

Some processing may also be necessary so that we can perform a contract with you or because it is required by law. We will only use your information to send you marketing communications with your consent, and you can always opt out of receipt of marketing communications at any time.

How do we protect your personal information?

We take appropriate physical, electronic and managerial measures to ensure that we keep your information secure, accurate and up to date, and that we only keep it as long as is reasonable and necessary.

Although we use appropriate security measures once we have received your personal information, the transmission of information over the internet is never completely secure. We do our best to protect personal information, but we cannot guarantee the security of information transmitted to us, so any transmission is at the user's own risk.

Sharing your personal information

We make all reasonable efforts to keep your details secure. We will only share them with suppliers or professionals working on our behalf, or on a need to know basis for legal reasons. We carefully select suppliers and professionals and will only share information with them if we have confirmation that they will protect it, and we have an agreement in place with them that assures this.

We will only ever share your details with other organisations to use for their own purposes if:

- We are required to by law or by a regulator;
- We deem it necessary and appropriate to respond to a legitimate request of assistance from law enforcement agencies;
- We are seeking legal or financial advice e.g. in connection with litigation or suspected fraud;
- We deem it necessary for the provision of services that we are engaged to provide to you;
- Where appropriate, to enforce the rights of UAP and its employees; or

- Requested by our underwriters so that we can maintain appropriate insurance coverage.

We will not, under any circumstances, share with or sell your personal information to any third party for marketing purposes, and you will not receive offers from other companies or organisations as a result of giving your details to us.

We may also share your personal information where you ask us to do so.

Where personal information is stored?

Your personal information may be transferred to and stored in, countries which have less strict, or no data protection laws, when compared to those in force in member states of the European Union. In these cases, we will take appropriate steps to ensure that adequate safeguards are in place to protect your personal information and to make sure it is treated securely. You can contact us for information of the applicable safeguards.

We store our data in line with our Data Protection Policy, using secure physical safeguards (e.g. in locked filing cabinets in lockable offices) and secure IT systems, (e.g. password protected computers and systems). Hard copy data is held by us in the relevant jurisdiction where the client relationship is held.

How long we will keep your personal information?

The length of time we will retain your information will depend on how long our relationship lasts. We will retain your personal information whilst you have a relationship with us or whilst you hold a product with us. We will retain the information for up to 7 years after your relationship ends to allow us to respond to any questions or complaints, to maintain evidence we have treated you fairly and to maintain an effective records management approach.

We may also keep the information for longer than 7 years after our relationship ends, where necessary for legal or regulatory requirements or where the information is required in connection with any ongoing or outstanding claims or legal action. Where your information is no longer required, we will ensure it is disposed of in a secure manner or if we can't delete the information for technical reasons (in which case we will take appropriate measures to protect the information from further processing or use and will only process for those purposes).

Your rights and choices

Notwithstanding anything set out in this Privacy Notice, you have the right:

- To ask us not to process your personal data for marketing purposes;
- To access personal data held about you and to obtain a copy of it;
- To prevent any processing of personal data that is causing or is likely to cause unwarranted and substantial damage or distress to you or another individual;
- To request the rectification or completion of personal data which are inaccurate or incomplete;
- To require us to erase your personal data;
- To require us to restrict our data processing activities (and, where our processing is based on your consent, you may withdraw that consent, without affecting the lawfulness of our processing based on consent before its withdrawal);

- To receive from us the personal data we hold about you which you have provided to us, in a reasonable format specified by you, including for the purpose of you transmitting that personal data to another data controller; and
- To object, on grounds relating to your particular situation, to any of our particular processing activities where you feel this has a disproportionate impact on your rights.

When you contact us to exercise any of the rights above, we may ask you to provide some additional information in order to verify your identity, such as your name, your address and proof of identity by completing our Data Subject Access Request Form.

We will comply with our legal obligations in relation to such requests, but please be aware that we may not be able to supply some information for legal reasons, for example if there is ongoing litigation or a reasonable prospect of law enforcement action.

Should you wish to exercise the above rights, please provide as much information as possible about the nature of your contact with us, to help us locate your records, and details of in what ways you have had contact with us on our Data Subject Access Request Form.

We will request confirmation of your identity before we release the information if we reasonably believe this is necessary to safeguard the personal information. In certain situations, we may also charge a small fee or refuse should the request be manifestly unfounded, frivolous, vexatious, unnecessarily repetitive or otherwise excessive.

Please note that the above rights are not absolute, and we may be entitled to refuse requests where exceptions apply.

If you have given your consent and you wish to withdraw it, please contact us using the contact details set out below. Please note that where our processing of your personal data relies on your consent and where you then withdraw that consent, we may not be able to provide all or some aspects of our services to you and/or it may affect the provision of those services.

If you have concerns about the way in which we have handled your personal information, we ask that you contact us in the first instance by post or email (to the addresses below).

If you are still dissatisfied, you have the right to complain to the Office of the Data Protection Commissioner which oversees the protection of personal data in Guernsey.

Alternatively, you may choose to contact the Office of the Data Protection Commissioner directly about your complaint, regardless of whether you have raised it with us first.

Changes to this Privacy Notice

We may update the terms of this Notice at any time, so please do check it from time to time. We will notify you about significant changes in the way we treat personal information by sending a notice to the primary email address you have provided to us, by placing a prominent notice on our website, and through arrangements in our face-to-face services. By continuing to use our website or services, you will be deemed to have accepted such changes.

Contact details

If you would like to lodge a complaint or exercise any of your rights set out above, you can contact us at:

E-mail: enquiries@TheUAPGroup.com

Post: Data Subject Access Request, The UAP Group, Cambridge House, Le Truchot, St Peter Port, Guernsey, GY1 1WD.

Guernsey Office of the Data Protection Commissioner: <https://dataci.gg/>

Malta Information and Data Protection Commissioner: <https://idpc.org.mt/>

UK Information Commissioners Office: <https://ico.org.uk/>

Where we rely on your consent to use your personal data, you have the right to withdraw that consent at any time.