



Rosetta Consulting Ltd.

Main Complex, Cockleton Lane, Cowes, PO31 8QE
01983 220 210, info@rosettaconsulting.co.uk

- Investigative & Litigation Support Service Provider -
data protection supervisory authority
www.ico.org.uk

Data Protection

UK General Data Protection Regulation

PART 1: Privacy Notice

Glossary of Terms

Data Protection Principles

PART 2: Cookie Policy

PART 3: Record of Processing Activities

PART 1: Privacy Notice

1. The purpose of this Privacy Notice is to protect the rights and privacy of living individuals and to ensure that personal data is not processed by Rosetta Consulting Ltd., hereinafter known as Rosetta Consulting, without the person's knowledge or consent, unless otherwise permitted. The Privacy Notice also sets out individuals' rights under the data protection legislation.
2. This document sets out the Data Protection Policy for Rosetta Consulting and should be read in conjunction with Rosetta Consulting's record of processing activities annexed hereto.
3. Rosetta Consulting complies with the requirements of the prevailing data protection legislation with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the core data protection principles.
4. Rosetta Consulting is committed to a policy of protecting the rights and privacy of individuals (including staff, course delegates, trainees and trainers, clients, subjects of investigations and others) in accordance with the data protection legislation.
5. Rosetta Consulting needs to process certain information about its staff, trainees and trainers, sub-contractors and other individuals it has dealings with such as clients, and to comply with legal obligations and government requirements.
6. During the course of its core business activities Rosetta Consulting will be instructed to process the personal data of individuals who are identified in clients' instructions or during the course of the investigation undertaken pursuant to such instructions. Rosetta Consulting will not process any personal data without first having established the lawful basis on which to process personal data, which when necessary will be recorded in a Data Privacy Impact Assessment.
7. To comply with the law, information processed about individuals must be kept to the minimum, collected and used fairly, be accurate, used solely for the purpose intended, stored safely, securely including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical measures such as encryption or in password protected devices, retained for no longer than necessary and not disclosed to any third party unlawfully.
8. The policy applies to all Data Subjects. In the event of a breach of the data protection legislation or this Privacy Notice by a member of staff, Rosetta Consulting employment disciplinary procedures will apply otherwise it will constitute a breach of contract.
9. As a matter of good practice, other agencies and individuals working with and thus affiliated to Rosetta Consulting and who have access to personal information, will be expected to have read and comply with this Privacy Notice, the terms of which form part of the consultancy/agency

agreement between Rosetta Consulting and that affiliate.

10. It is expected that departments who deal with external agencies will take responsibility for ensuring that such agencies contract to abide by this policy.
11. Rosetta Consulting is the Controller under the data protection legislation, when dealing with its core business activity as an Investigative, Risk Management & Litigation Support Service Provider. However, in certain circumstances Rosetta Consulting will be Joint Controller with the instructing client. There may be instances when acting under strict instructions, which also cover the purpose (the why) and means (the how) for the processing of all the personal data in the client provided case scenario, that Rosetta Consulting will be the Processor.
12. Rosetta Consulting is the Controller under the data protection legislation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of Rosetta Consulting
13. The Senior Management and Heads of Departments and all those in managerial or supervisory roles are responsible for developing and encouraging good information handling practice within Rosetta Consulting
14. Compliance with data protection legislation is the responsibility of all members and affiliates of Rosetta Consulting who process personal information.
15. Each member of staff, clients, contractors, trainees and any other member or affiliate of Rosetta Consulting is responsible for ensuring that any personal data supplied to or handled by Rosetta Consulting is accurate and up-to-date.
16. Data Subjects have the following rights regarding data processing and the data that are recorded about them:
 - To make subject access requests regarding the nature of information held and to whom it has been disclosed.
 - To prevent processing likely to cause damage or distress.
 - To prevent processing for purposes of direct marketing.
 - To be informed about mechanics of automated decision taking process that will significantly affect them.
 - Not to have significant decisions that will affect them taken solely by automated process.
 - To sue for compensation if they suffer damage by any contravention of the prevailing data protection legislation.
 - To take action to rectify, block, erase or destroy inaccurate data.
 - To request the Information Commissioner to assess whether any provision of the prevailing data protection legislation has been contravened.

17. For criminal data, explicit written consent of the Data Subject must be obtained unless an alternative lawful basis for processing exists and Rosetta Consulting has ensured that it has an additional condition for processing this type of data, under Schedule 1 of the Data Protection Act 2018, for example, to safeguard vulnerable individuals or children, assess people's suitability for employment, or assess whether a person can access services such as housing or insurance.
18. Rosetta Consulting will not keep any comprehensive register of criminal convictions.
19. For special category data processing is prohibited, unless the Data Subject has given explicit consent or one of the permitted conditions set out in the data protection legislation are met.
20. Rosetta Consulting understands "consent" to mean that the Data Subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
21. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from no response to a communication.
22. In most instances consent to process personal, special category or criminal data is obtained routinely by Rosetta Consulting (e.g. when a member of staff or consultant signs a Service or Consultancy Agreement).
23. Any Rosetta Consulting forms (whether paper-based or electronic-based), that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe.
24. If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place, unless an exemption applies.
25. **CONSENT GIVEN CAN BE WITHDRAWN AT ANY TIME BY GIVING ROSETTA CONSULTING WRITTEN NOTICE.**
26. If any member or affiliate of Rosetta Consulting is in any doubt about these matters, they should consult a director or senior manager.
27. All staff and affiliates of Rosetta Consulting are responsible for ensuring that any personal data (on others), which they hold are kept securely and that they are not disclosed to any unauthorised third party.

28. All personal data should be accessible only to those who need to use it. Those concerned should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:
- In a lockable room with controlled access, or
 - In a locked drawer or filing cabinet, or
 - If electronic, password protected, or
 - Kept on disks which are themselves kept securely.
29. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised persons.
30. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be wiped clean before disposal.
31. This Privacy Notice also applies to staff and affiliates of Rosetta Consulting who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and affiliates of Rosetta Consulting should take particular care when processing data at home or in other locations outside the offices of Rosetta Consulting or its affiliated locations.
32. Members of Rosetta Consulting and / or other Data Subjects have the right to access any personal data which are held by Rosetta Consulting in electronic format and manual records which form part of relevant filing system held by Rosetta Consulting about that person.
33. Any individual who wishes to exercise this right should apply in writing to a director or senior management. Rosetta Consulting will make no charge for data subject access requests. Any such request will normally be complied with within 30 days of the receipt of the written request supported by proof of identity and address.
34. Rosetta Consulting must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police, unless authorised under the terms of the prevailing data protection legislation or other statute or Court Order or where disclosure of data is required for the performance of Rosetta Consulting contractual duty or otherwise exempt. All staff and affiliates should exercise caution when asked to disclose personal data held on another individual to a third party.
35. The prevailing data protection legislation permits certain disclosures without consent to a Competent Authority, such as law enforcement agencies.

36. Rosetta Consulting undertake their services in accordance with the data protection good practice policies and guides published by the Association of British Investigators.

37. For reasons of personal security and to protect Rosetta Consulting premises and the property of staff, trainees and other visitors, close circuit television cameras may be in operation in several areas. The presence of these cameras may not be obvious. This Privacy Notice determines that personal data obtained during monitoring will be processed as follows:

- Any monitoring will be carried out only by a limited number of specified senior managers;
- The recordings will be accessed only by a director or an appointed senior manager;
- Personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
- Staff involved in monitoring will maintain confidentiality in respect of personal data.

Glossary of Terms

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the Controller, includes name, address, telephone number, identity number. Also includes expression of opinion about the individual, and of the intentions of the Controller in respect of that individual.

Special category or criminal data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Special category or criminal data are subject to much stricter conditions of processing.

Data Subject

Refers to any individual person who can be identified, directly or indirectly, via an identifier such as a name, an ID number, location data, or via factors specific to the person's physical, physiological, genetic, mental, economic, cultural, or social identity.

Controller or Joint Controller

Means the natural or legal person, agency, or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Put simply, the Controller determines what information is needed and why.

Processor

Is a person or organization who deals with personal data as instructed by a Controller for specific purposes and services offered to the Controller that involve personal data processing. The service provider could act on instructions both as to the purpose and manner of the processing to maintain the Processor status. However, such is the nature of the work and methodologies, that a service provider, who is very often the professional party in processing personal data, (in the relationship with the client), will determine what information is needed and why, activities which will determine the service provider's role is that of Controller or possibly Joint Controller with the client.

Third Party

Any individual/organisation other than the Data Subject, the Controller, Joint Controller, Processor, or the agents/sub-contractors appointed by any of them when permitted by the Controller or the client.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data. Accessing, altering, adding to, merging, deleting data. Retrieval, consultation or use of data. Disclosure or otherwise making available of data.

Relevant Filing System

Any paper filing system or other manual filing system, which is structured so that information about an individual is readily accessible. Please note that this is the definition of "Relevant Filing System". Personal data as defined, and covered, by the prevailing data protection legislation can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.

Investigative Service Provider ('Professional Investigation')

The Private Security Industry Act 2001 defines investigations as:

... to any surveillance, inquiries or investigations that are carried out for the purpose of:

*obtaining information about a particular person or about the activities or whereabouts of a particular person; or
obtaining information about the circumstances in which or means by which property has been lost or damaged*

Litigation Support Services

An investigation agency client portfolio will inevitably include members of the legal profession and thus potentially forms part of the judicial process. Lawyers rely on outsourced investigative services for a number of reasons; primarily as part of their own case handling for lay, professional or commercial clients in contentious scenarios in contemplation of, or part of on-going legal proceedings. This work is referred to within the judicial system as "Litigation Support" and often includes activities that process personal data.

Privacy

Privacy, in its broadest sense, is about the right of an individual to be left alone. It can take two main forms, and these can be subject to different types of intrusion: **Physical privacy** - interference such as surveillance and the taking of biometric information, and **Informational privacy** - the ability of a person to control, edit, manage, and delete information about themselves and to decide how and to what extent such information is communicated to others.

Data protection law

The UK General Data Protection Regulation as applied in the UK and The Data Protection Act 2018.

[BACK TO TOP](#)

Data Protection Principles

All processing of personal data must be done in accordance with the six data protection principles, which collectively demonstrates Rosetta Consulting accountability.

1. Personal data shall be processed fairly, lawfully and transparently.

Data processing will not be lawful unless it satisfies at least one of the following processing conditions:

- **Consent** - The Data Subject has provided valid consent for the processing.
- **Contract** - The processing is necessary for the performance of a contract.
- **Legal obligation** - The processing is necessary for compliance with a legal obligation to which the Controller is subject.
- **Legitimate interest** - The processing is necessary for the purposes of the legitimate interests pursued by the Controller, the client or Rosetta Consulting except where such interests are overridden by the interests or fundamental rights of the Data Subject. Fraud prevention, cybersecurity and direct marketing are examples of the type of activities that might constitute legitimate interests.
- **Vital interest** - The processing is necessary to protect the Data Subject's vital interests, such as in a medical emergency.
- **Public interest** - Processing is necessary for a task carried out in the public interest.

2. Purpose limitation - Data processing must relate to a specific, explicit and legitimate purpose. Data must not be processed in a manner that is incompatible with the stated purpose/s. Generic purpose statements will not be compatible with the data protection legislation.

3. Data minimisation - Data collected must be limited to what is necessary. It must be adequate, relevant and not excessive, having regard to the stated purpose for which data is being processed.

4. Accuracy - Data must be kept accurate and up to date. Controllers must be able to correct personal data 'without undue delay'.

5. Storage limitation - Data should not be kept for any longer than is necessary. Data retention policies should establish time limits for erasure, although it is permissible to retain data for longer periods for archive or statistical purposes only.

6. Integrity and confidentiality - Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical or organisational measures.

[BACK TO TOP](#)

PART 2: Cookie policy

1. Introduction

This Policy covers our use of cookies, IP addresses, and other technologies.

2. What are Cookies?

Cookies and other online tracking technologies are small bits of data or code that are used to identify your devices when you use and interact with our website and other services. They are often used for remembering your preferences, to identify popular web site or apps pages.

3. What Cookies may we use and how would we use them?

i. Essential cookies and similar technologies

These are vital for the running of our services on our website and apps. Without the use of these cookies parts of our website would not function. For example, the use of cookies may help us identify the location and or authenticity of a site visitor, protect Rosetta Consulting from misuse, malice or fraud.

ii. Analytics cookies and similar technologies

These collect information about your use of our website and apps, and enable us to improve the way it works. For example, analytics cookies show us which are the most frequently visited pages on the website allowing us to provide the most popular news articles further up the page. They help us record how you interact with our website, such as how you navigate around pages and from page to page; identifying improvements we can make to the visitor's journey. They also help identify any difficulties you have accessing our services, so we can fix any problems. Additionally, these cookies allow us to see overall patterns of usage at an aggregated level.

iii. Functional/preference cookies and similar technologies

These cookies collect information about your choices and preferences, and allow us to remember things like language, text size, and location, so we can show you relevant content to where you are. They allow us to customize the pages, products or services you have accessed.

iv. Tracking, advertising cookies and similar technologies

These types of technologies provide advertisements that are more relevant to your interests. This can be done by delivering online adverts based on your previous web browsing activity, known as "online behavioural advertising" (OBA). Cookies are placed on your browser, which will remember the websites you have visited. Advertising based on what you have been looking at is then displayed to you when you visit websites who use the same advertising networks.

v. Web beacons

These are bits of data that count the number of users who access a website or webpage and can also allow us to see if a cookie has been activated. Web beacons used on web pages or in emails allow us to see how successful an article has been or that an email message was successfully delivered and read in a marketing campaign or newsletter. Web beacons are also used to verify any clicks through to links or advertisements contained in emails. We may use this information to help us identify which emails are more interesting to you and to inform advertisers how many customers have clicked on their adverts (this information is aggregated and does not identify you individually).

vi. Flash cookies

We may, in certain situations, use Adobe Flash Player to deliver special content, such as video clips or animation. To improve your user experience, Local Shared Objects (commonly known as Flash cookies) are used to provide functions such as remembering your settings and preferences. Flash cookies are stored on your device, but they are managed through an interface different from the one provided by your web browser.

vii. Tracking URLs

Tracking URLs are a special web link that allows us to measure when a link is clicked on. They are used to help us measure the effectiveness of campaigns and advertising and the popularity of articles that are read.

viii. We also use cookies and similar technologies:

When you access and interact with our services cookies may collect certain information about those visits. For example, in order to permit your connection to our website, our servers receive and record information about your computer, device, and browser, including potentially your IP address, browser type, other software or hardware information, and your geographic location.

ix. If you access our services from a mobile device

We may collect a unique device identifier assigned to that device, geo-location data, and other transactional information for that device.

x. Usage of services

To collect, use and store information about your usage of our services, website and apps, such as pages you have visited, content you have viewed, search queries you have run, and advertisements you have seen or interacted with.

XI. To provide relevant content

The content on our website and in our communications with you may be adjusted depending on what we know about the content, products and services that you like. This means we can highlight content and articles that we believe will be of interest to you. We provide personalisation by using cookies, IP addresses, web beacons, URL tracking and mobile app settings.

4. Third party advertisers

- a. We may sell space on our website to advertisers. The adverts they display on our website will often contain cookies. Our advertisers may use cookies or similar technologies to provide you with advertisements that they believe are relevant. They may use browsing data obtained to restrict the number of times you see particular adverts (frequency capping). You may also see adverts from these advertisers on other websites you visit.
- b. Third parties that support our services by serving advertisements or providing other services, such as allowing you to share content or tracking aggregate service usage, may also use cookies and other technologies to collect information relevant to the provision of those services.
- c. We do not control third-party cookies or other technologies. Their use is governed by the privacy policies of third parties using such technologies. You should make sure you are aware of how third parties will use cookies by checking the third party's cookie policy.

5. Mobile applications

By downloading our apps, we will require access to the following services on your device: unique identifier (UDID), MAC address or other applicable device identifier and location. Other services may also be required in order for the apps to function. We may use this information to validate free trials. Our apps may also provide push notifications to your device. You may control these through using the tools on your device, such as turning off push notification and location services.

6. Managing cookies

Most modern browsers are set to accept cookies by default, but you can change your settings to notify you when a cookie is being set or updated, or to block cookies altogether. Please consult the "Help" section of your browser.

7. Controlling OBA cookies

The "Your Online Choices" website <http://www.youronlinechoices.com> provides more information about controlling cookies. It also provides an easy way to opt out of behavioural advertising from each (or all) of the networks represented by the European Interactive Digital Advertising Alliance <http://www.youronlinechoices.com/uk/your-ad-choices>.

8. Controlling Flash cookies

You can manage the use of Flash technologies with the Flash management tools available at Adobe's website, at <http://www.adobe.com/devnet/flashplayer/articles/privacy.html>.

9. Controlling web beacons

You can prevent web beacons from tracking your activity, although you won't be able to decline receiving them in emails. For information about managing your cookie options, please click here. <http://www.allaboutcookies.org/>. Please note that by blocking any or all cookies you may not have access to certain features, content, or personalisation available on our website, or apps.

[BACK TO TOP](#)

PART 3: Record of processing activities

- Investigative & Litigation Support Service Provider -
data protection supervisory authority is the Information Commissioner's Office (ICO)

www.ico.org.uk

1. **Nature of work - Professional investigation in the private sector, risk management and litigation support services.**
2. **Date: 01/01/2021**
3. **Description of processing**
 - 3.1. The following is a broad description of the way this organisation processes personal information. To understand how your own personal information is processed you may need to refer to any personal communications you have with the organisation, check the [Privacy Notice](#) that the organisation has provided above, or contact the organisation to ask about your personal circumstances.
 - 3.2. Reasons/purposes for processing information
We process personal information to enable us to:
 - provide investigatory, risk management & litigation support services on the written instructions of a client;
 - to maintain our own accounts and records;
 - and to support and manage our employees, trainees and contractors.
4. **Type/classes of information processed**
 - 4.1. We process information relating to the above reasons/purposes. This information may include:
 - personal details
 - the investigation brief, results and related information
 - lifestyle and social circumstances
 - family details
 - goods and services
 - financial details
 - education and employment and/or business details
 - 4.2. We also process special category or criminal classes of information that may include:
 - physical or mental health details
 - racial or ethnic origin
 - trade union membership
 - religious or other beliefs

- criminality

5. **Who the information is processed about**

5.1. We process personal information about:

- customers and clients, including prospective clients
- witnesses
- the subjects of investigations
- business contacts
- advisers and other professional experts
- suppliers/contractors
- employees

6. **Who the information may be shared with**

6.1. We sometimes need to share the personal information we process with the individual themselves and also with other organisations. Where this is necessary we are required to comply with all aspects of the data protection legislation. What follows is a description of the types of organisations we may need to share some of the personal information we process with for one or more reasons.

6.2. Where necessary or required we share information with the following, which may include our clients and/or contractors:

- financial organisations
- credit reference, debt collection and tracing agencies
- law enforcement
- professional investigators
- government
- business associates and other professional bodies and advisers
- suppliers/contractors
- current, past or prospective employers
- education and examining bodies
- family, associates or representatives of the person whose personal data we are processing

7. **Trading and sharing personal information**

7.1. Personal information is traded and shared as a primary business function. For this reason the information processed may include name, contact details, family details, financial details, employment details, and goods and services and where appropriate special category or criminal data. This information may be about customers and clients.

7.2. The information may be traded or shared with business associates and professional advisers, agents, service providers, customers and clients, and traders in personal data.

8. **Undertaking research**

- 8.1. Personal information is also processed in order to undertake research.
- 8.2. For this reason the information processed may include name, contact details, family details, lifestyle and social circumstances, financial details, goods and services.
- 8.3. The special category or criminal data types of information may include sexuality, physical or mental health details, racial or ethnic origin and religious or other beliefs.
- 8.4. This information is about survey respondents. Where necessary or required this information may be shared with clients, contractors, other service providers, survey and research organisations.

9. **Consulting and advisory services**

- 9.1. Information is processed for consultancy and advisory services that are offered.
- 9.2. For this reason the information processed may include name, contact details, family details, financial details, and the goods and services provided.
- 9.3. This information may be about clients.
- 9.4. Where necessary this information is shared with the data subject themselves, business associates and other professional advisers, current, past or prospective employers and service providers.

10. **Transfers**

- 10.1. It may sometimes be necessary to transfer personal information overseas.
- 10.2. When this is needed information may be transferred to countries or territories around the world.
- 10.3. Any transfers made will be in full compliance with all aspects of the data protection law.

[BACK TO TOP](#)