

Computer Forensics Online Limited's Privacy Policy

Introduction

Contained within this narrative is the privacy policy of Computer Forensics Online Limited (CFO from this point forward). This policy refers directly to your personal data and what we do with it when you consent to its collection.

As an organisation, CFO are committed to the privacy protection of your personal data. We encourage you to take some time to read our privacy policy in order to fully to understand how your personal data is captured, protected and used.

Whenever you give us personal data, you are consenting to its collection and use in accordance with this privacy policy.

Information about CFO Ltd

Company. CFO Limited is a company registered in England and Wales under company number 06487033. Our registered office is at Old Court Buildings, Regent House, 2 Regent Road, Lowestoft, Suffolk, NR321PA. Our contact telephone number is (0800) 9996432 and our e-mail address is enquiries@computerforensicsonline.co.uk.

Contacting us about data privacy. Please use these details to contact us about any of the topics set out in this Privacy Policy. If you have any questions, or want more details about how we use your personal data, you can ask us by using our secure online enquiry form. If you are not satisfied with any response you may receive, please contact our Data Protection Officer

Website. CFO operates a website on the world wide web with the URL <https://www.computerforensicsonline.co.uk>. CFO also operates other websites which can be viewed with the URLs <http://www.iamconcerned.co.uk> and <http://www.cf-online.co.uk>.

Website Hosting: Our website is hosted by Ionis (Formerly One and One Internet) in Germany (An EU country).

Purpose of our Website. Our website is published online for our existing and prospective customers to obtain information and contact us regarding our services. It is not intended to be directed at data subjects aged under 16 years of age; however, CFO recognise that such data subjects can freely visit and view our content.

VAT Registration: The VAT registration number for CFO is 929441701.

ICO Registration: CFO is registered as a Data Controller with the Information Commissioners Office (ICO) with the registration number: ZA375766

How the Data Protection Act (2018) protects you

This section sets out the legal reasons we rely on, for each of the ways we may use your personal data. As well as our Privacy Promise, your privacy is protected by law. This section explains how that works.

The Data Protection Act (2018) says that we are allowed to use personal data only if we have a proper reason to do so. This includes sharing it outside the company. The law says we must have one or more of these reasons:

1. To fulfil a contract we have with you, or
2. When it is our legal duty, or
3. When it is in our legitimate interest, or
4. When you consent to it.

When we have a business or commercial reason of our own to use your personal data, this is called a 'legitimate interest'. We will tell you what that is, if we are going to rely on it as the reason for using your data. Even then, it must not unfairly go against your interests.

The Data Protection Act (2018) treats some types of sensitive personal data as 'special'. This includes data about racial or ethnic origin, sexual orientation, religious beliefs, trade union membership, health data, and criminal records. We will not collect or use these types of data without your consent unless the law allows us to do so. If we do, it will be afforded additional security only be processed when it is absolutely necessary:

1. **For reasons of substantial public interest, or**
2. **To establish, exercise or defend legal claims.**

What personal data is collected?

This explains what all the different types of personal data mean, that are covered by the Data Protection Act (2018).

We use different kinds of personal data. They are grouped together like this. The groups are all listed here so that you can see what we may know about you, even if we obtain it from public sources such as the world wide web. We don't use all this data in the same way.

Some of it is useful for marketing, or for providing services to you. But some of it is private and sensitive and we treat it that way by affording it the security it requires.

Where do we collect your personal data from?

This section lists all the places where we get data that counts as part of your personal data. We may collect personal data about you (or your business) from publicly available areas and any of these sources:

Part A – Personal Data you give to us:

1. When you apply for services;
2. When you talk to us on the phone and the notes we make;
3. When you use our websites;
4. In emails and letters and any other documents;
5. In recruitment / attachment interviews;
6. In online customer surveys;
7. Data we collect when you use our services.

Part B – Personal Data from outside organisations:

1. Companies that introduce you to us, such as our official partners;
2. Social networks (for instance, when you click on one of our Google ads);
3. Employers (for instance, to get a reference);
4. Payroll and Pension service providers;
5. Publicly available information sources such as Companies House;
6. Agents, suppliers, sub-contractors and advisers;
7. These can be types of companies we use to help us provide our services. They can also be specialist companies who advise us on ways to develop and improve our business;
8. Medical professionals*;
9. Government and law enforcement agencies.

* For HR purposes, we may ask your GP or other medical practitioner to send us a report. We will only do this if we get your consent first.

Data collected during visit to www.computerforensiconline.co.uk & www.iamconcerned.co.uk

When the above CFO websites are visited, a log is maintained of your visit. This includes your IP Address at the time of visiting. This data is used for maintaining website statistical analysis in such areas as:

- Page loading - This tells us what your machine has looked at, whether the page request was successful or not and which browser your machine used to view the pages
- Helping us understand which areas of the Site are of particular interest
- Understanding which pages are not being requested
- How many people are visiting the website in total

IP Address data is also used for reason such as:

- Restrictions on the use of the website are being broken
- To block IP addresses where there is a breach of the website use terms and conditions

Also generated during a visit to our website are cookies. These are small text files that are loaded into the storage of your device via your internet browser to store information that can later be retrieved. Cookies enable us to analyse the interests of our visitors in order to improve the users' browsing experience.

How long do we keep your personal data?

This section explains how long we may keep your personal data for and why. We will keep your personal data for as long as you are a customer CFO. For several reasons, we may keep your data for up to 10 years after you stop being a customer.

1. To respond to a question or complaint, or to show whether we gave you fair treatment
2. To study customer data as part of our own internal research
3. To obey rules that apply to us about keeping records

We may also keep your data for longer than 10 years if we cannot delete it for legal, regulatory or technical reasons. We will only use your personal data for those purposes and will make sure that your privacy is protected.

What if I choose not to provide you with my personal data?

You can choose not to give us personal data. In this section we explain the effects this may have. We may need to collect personal data by law, or to enter into or fulfil a contract we have with you.

If you choose not to give us this personal data, it may delay or even prevent us from fulfilling our contract with you, or doing what we must do by law. It could mean that we cancel a service you have with us.

We sometimes ask for information that is useful, but not required by law or a contract. We will make this clear when we ask for it. You do not have to give us these extra details and it won't affect the services you have with us.

MY RIGHTS AS A DATA SUBJECT

What if you want us to stop using your personal data? This section explains about your right to object and other data privacy rights you have – as well as how to contact us about them. You can object to us keeping or using your personal information. This is known as the 'right to object'. You can also ask us to delete, remove, or stop using your personal information if there is no need for us to keep it. This is known as the 'right to erasure' or the 'right to be forgotten'.

Please note that there may be legal or other official reasons why we need to keep or use your data. But please tell us if you think that we should not be using it. We may sometimes be able to restrict the use of your data. This means that it can only be used for certain things, such as legal claims or to exercise legal rights.

You can ask us to restrict the use of your personal information if:

1. It is not accurate;
2. It has been used unlawfully but you don't want us to delete it;
3. It is not relevant anymore, but you want us to keep it for use in legal claims;
4. You have already asked us to stop using your data but you are waiting for us to tell you if we are allowed to keep on using it

If we do restrict your personal data in this way, we will not use or share it in other ways while it is restricted. If you want to object to how we use your data, or ask us to delete it or restrict how we use it or, please contact using our secure online contact form on our website.

EXERCISING YOUR RIGHTS AS A DATA SUBJECT

How to complain

This section gives details of how to contact us to make a complaint about data privacy. It also shows you where you can get in touch with the government regulator. Please let us know if you are unhappy with how we have used your personal data. You can contact us using our secure online contact form on our website.

You also have the right to complain to the UK regulator, the Information Commissioner's Office (ICO) and to lodge an appeal if you are not happy with the outcome of a complaint.

How to withdraw your consent

This section explains what to do if you no longer want us to hold or use your personal data.

You can withdraw your consent at any time. Please contact us using our secure online contact form on our website (found in the "Contact Us" section of the website), should you want to do so. Please note that this will only affect the way we use personal data when our reason for doing so is that we have your consent.

If you withdraw your consent, we may not be able to provide certain services to you. If this is so, we will tell you.

Making sure that your personal data is correct and accurate

Here you can find out how to contact us if you think the information we hold for you is wrong, incomplete or out of date. You have the right to question any information we have about you that you think is incorrect. We'll take reasonable steps to check this for you and correct it. If you want to do this, please contact us using our secure online contact form on our website or contact our headquarters on (0800) 9996432.

How to get a copy of your personal data

This section tells you where to write to us to get a copy of your personal data, and how to ask for a digital file you can use yourself or share easily with others. You can do this online or by writing to us.

You can get a copy of all the personal data we hold about you by writing to us at this address:

The Data Protection Officer

Computer Forensics Online Limited, Old Court Buildings, Regent House, 2 Regent Road, Lowestoft, Suffolk, NR321PA.

When you want to share your data with outside companies

You also have the right to get certain personal data from us as a digital file, so you can keep and use it yourself, and give it to other organisations if you choose to. If you wish, we will provide it to you in an electronic format that can be easily re-used, or you can ask us to pass it on to other organisations for you.

If you want to do this, please contact us using our secure online contact form on our website.

HOW PERSONAL DATA IS USED

Who we share your personal data with

We may share your personal data with outside organisations such as our official partners or governmental / law enforcement agencies. This is so that we can provide our services, run our business, and obey rules that apply to us. Below is a list all the types of organisation that we may share your personal data with.

Authorities

This means official bodies that include:

1. Central and local government agencies;
2. Registered charities mandated to undertake investigational activities in the public interest;
3. HM Revenue & Customs, regulators and other tax authorities;
4. Law enforcement and fraud prevention agencies.

Banking and financial services

1. Official partner companies we work with to provide services to you and to run our business;
2. Someone linked with you or your business's product or service#;
3. This could mean a joint account holder, trustee, or fellow company director;
4. Other financial services companies (to help prevent, detect and prosecute unlawful acts and fraudulent behaviour);
5. Employers (for instance, to confirm a reference);
6. Companies you ask us to share your data with.

General Business

1. Partner and associate companies we use to help grow and improve our business;
2. Organisations that introduce you to us.

HOW WE USE YOUR PERSONAL DATA TO MAKE AUTOMATED DECISIONS

CFO presently does not utilise any processing that involves automated processing.

SENDING DATA OUTSIDE OF THE EEA / EU / Adequacy Agreement Country List

This section tells you about the safeguards that keep your personal data safe and private, if it is sent outside the countries deemed to have similar controls to those contained within the GDPR / Data Protection Act (2018).

We will only send your data outside of this area to:

1. Follow your instructions;
2. Comply with a legal duty;
3. Work with our suppliers who help us to run your accounts and services.

If we do transfer your personal data outside the EEA to our suppliers, we will make sure that it is protected to the same extent as in the EEA. We'll use one of these safeguards:

1. Transfer it to a country with privacy laws that give the same protection as the EU;
2. Put in place a contract with the recipient that means they must protect it to the same standards as expected under the GDPR / Data Protection Act (2018);
3. Transfer it to organisations that are part of Privacy Shield. This is a framework that sets privacy standards for data sent between the US and EU countries. It makes sure those standards are similar to what is used within the EEA. You can find out more about data protection on the European Commission Justice website.

Notification of changes

This privacy policy was last updated on 29 Mar 2019. We reserve the right to amend or vary this policy at any time and the revised policy will apply from the date posted on the Site. You accept that by doing this, we have provided you with sufficient notice of the amendment or variation.