Privacy Policy for CFC Security Limited

1. About us

1.1 In this Privacy Policy references to "we" or "us" or "our" are to CFC Response, a trading name of CFC Security Limited, registered company number 13497455, registered address 85 Gracechurch Street, London EC3V 0AA.

This Privacy Policy (the "Policy") sets out how we process the personal data of our customers and, where relevant, website visitors and CFC Response app users, including in the European Union and the United Kingdom ("Users").

1.2 If you have any questions about this Policy, please contact our data protection officer ("DPO") by clicking here.

2. What information do we process

Personal Data

2.1 We will process personal data when you are introduced to us for one of our products of services, or in the course of providing you with one of our products of services.

The types of information we process under paragraph 2.1 above may include:

2.1.1 Information you provide us when you are introduced to us, including names, phone number, email address or other information provided by you connection with our potential engagement;

2.1.2 Information you provide us to help us carry out our obligations under any contract in place between us and you; and

2.1.3 Information you provide us through our CFC Response app.

2.2 We may also process personal data as part of CFC Response's Forensics and Security Information Response Services, from your hard drives, servers, networks and/or computer systems to enable us to:

2.2.1 carry out our obligations under any contract in place between us and you; and

2.2.2 find patterns and correlations in data sets through the use of data mining technology.

2.2.3 The types of personal data that we may process under paragraph 2.3 above will depend upon what data is stored on your computer hard drives, servers, networks and/or computer systems and may include:

2.2.4 Information that is visible to us from the live customer environment;

2.2.5 Any information that you hold (which may include personal data) or which can otherwise by accessed on your services, hard drives, networks and/or computers (including but not limited to employee data and communications);

2.2.6 Information that is contained within personnel email accounts to which we are granted administrative access;

2.2.7 Information that is copied from your server in the course of our forensic investigation.

2.3 Where such information is present on your hard drives and/or computer systems, we may also process special categories of personal data about your employees, customers and/or other third parties which may include without limitation information about:

2.3.1 the physical or mental health condition of one of your employees or (where relevant) customers or other third parties;

2.3.2 the religious or philosophical beliefs of your employees or (where relevant) customers or other third parties;

2.3.3 the political opinions or trade union membership of your employees or (where relevant) customers or other third parties; and/or

2.3.4 any criminal offence or alleged criminal offence committed by one of your employees or (where relevant) customers or other third parties.

2.4 The processing of special categories of personal data under paragraph 2.4 will only be incidental to the services we provide to you. Such processing may be necessary where we have been instructed to carry out data mining activities for you, to identify what data has potentially been exposed in a data breach. The processing of special categories of personal data may also take place in connection with any Forensics and Security Information Response Services that we provide to you and will only be processed for the purposes of the provision by us of those Forensics and Security Information Response Services.

2.5 We may also collect data (such as IP and/or infrastructure data) which is sufficiently anonymised and/or aggregated such that the data subject cannot be identified directly or indirectly from it. Further information about our use of cookies is included in [reference Cookie Policy].

3. Grounds for processing

3.1 To process your data lawfully we need to rely on one or more valid legal grounds. Our primary legal ground is that we need the data to fulfil our contract with you or to take certain steps prior to entering our contract with you. However, there may be circumstances where we also rely on other valid legal grounds, such as:

3.1.1 our legitimate interests as a business (except where your interests or fundamental rights override these). For example, it is within our legitimate interests to use your data to prevent or detect fraud or abuses of our CFC Response app and/or website; or

3.1.2 your consent, or the consent of your employees, customers and/or other third parties, where legally required to obtain consent; or

3.1.3 our compliance with a legal obligation to which CFC Response is subject. For example, if we have a duty to provide information pursuant to a Court order and need to process your data as part of such request.

3.1.4 In addition to the above legal grounds, where we process special categories of personal data as part of our data mining activities and/or Forensics and Security Information Response Services such processing will be incidental to the services we provide and we may do so where the processing is necessary:

3.1.5 to comply with, or assist you to comply with, a regulatory requirement to take steps to establish whether a person has committed an unlawful act or been involved in seriously improper conduct and consent cannot reasonably be expected to be obtained and it is necessary for reasons of substantial public interest; or

3.1.6 for an insurance purpose and for reasons of substantial public interest and such processing can reasonably be carried out without data subject consent.

4. Disclosure of your information

4.1 There are circumstances where we may wish to disclose or are compelled to disclose your personal data to third parties. This will only take place in accordance with the applicable law and for the purposes listed above. These scenarios include disclosure:

4.1.1 to members of the CFC Group and their and our respective branches or associated offices including CFC regional incident response labs where data will be stored physically;

4.1.2 to our outsourced service providers or suppliers to facilitate the provision of our services or products to you including to external forensic vendors where their engagement is necessary in connection with our provision of services to you;

4.1.3 to third party service providers and consultants in order to protect the security or integrity of our business, including our databases and systems and for business continuity reasons;

4.1.4 to online incident response share repositories;

4.1.5 to another legal entity, on a temporary or permanent basis, for the purposes of a joint venture, collaboration, financing, sale, merger, reorganisation, change of legal form, dissolution or similar event. In the case of a merger or sale, your personal data will be permanently transferred to a successor company;

4.1.6 to legal advisors who you have instructed in connection with any cyber incident;

4.1.7 to public authorities where we are required by law to do so; and

4.1.8 to any other third party where you have provided your consent.

5. International transfer of personal data

5.1 We may transfer your personal data to a third party in countries outside the UK for further processing in accordance with the purposes set out in this policy. Your personal data may be transferred throughout the CFC Group, including within the UK, and to third parties located abroad as envisaged by paragraph 4 above.

In these circumstances we will, as required by applicable law, ensure that your privacy rights are adequately protected by appropriate technical, organisation, contractual or other lawful means. Please contact the DPO for a copy of the safeguards which we have put in place to protect your personal data and privacy rights in these circumstances.

6. Retention of personal data

6.1 If you are, or have previously been, a customer of ours then we may continue to hold and process your information for the purpose of continuing to carry out our obligations in connection with the contract between us and you. We will continue to hold and process your information for the duration of the contract and for a reasonable period of time afterwards as required by law.

6.2 We may keep an anonymised form of your personal data, which will no longer refer to you, for statistical purposes without time limits, to the extent that we have a legitimate and lawful interest in doing so.

7. Data subject rights

7.1 Data protection law provides individuals with numerous rights, including the right to: access, rectify, erase, restrict, transport, and object to the processing of, their personal data. Individuals also have the right to lodge a complaint with the relevant data protection authority if they believe that their personal data is not being processed in accordance with applicable data protection law.

7.1.1 Right to make subject access request (SAR). Where we are processing your personal data as a data controller you may, where permitted by applicable law, request copies of your personal data. If you would like to make a SAR, i.e. a request for copies of the personal data we hold about you, you may do so by writing to the DPO whose contact details are in paragraph 1.2 above. The request should make clear that a SAR is being made. You may also be required to submit a proof of your identity and a fee.

7.1.2 Right to rectification. You may request that we rectify any inaccurate and/or complete any incomplete personal data.

7.1.3 Right to withdraw consent. You may, as permitted by applicable law, withdraw your consent to the processing of your personal data at any time. Such withdrawal will not affect the lawfulness of processing based on your previous consent. Please note that if you withdraw your consent, we may not be able to provide all of the services under the contract entered into between us and you for which the processing of your personal data is essential.

7.1.4 7.1.4 Right to object to processing. You may, as permitted by applicable law, request that we stop processing your personal data.

7.1.5 7.1.5 Right to erasure. You may request that we erase your personal data and we will comply, unless there is a lawful reason for not doing so. For example, there may be an overriding legitimate ground for keeping your personal data, such as a legal obligation that we have to comply with, or if retention is necessary for us to comply with our legal obligations.

7.1.6 7.1.6 Your right to lodge a complaint with the supervisory authority. We suggest that you contact us about any questions or if you have a complaint in relation to how we process your personal data. However, you do have the right to contact the relevant supervisory authority directly. To contact the Information Commissioner's Office in the United Kingdom, please visit the ICO website for instructions.

8. Linked websites

Please note that any websites that may be linked to our websites are subject to their own privacy policy.

9. Changes to this policy

We may update this Policy from time to time to ensure that it remains accurate. Please check back regularly so you are fully aware of any changes.

This Policy was last updated on: 7 December 2021.