

# ZENTEK DIGITAL INVESTIGATIONS LTD

## DATA PROTECTION POLICY

### Introduction

Zentek Digital Investigations Ltd is a digital forensics investigations service provider registered in England and Wales with company number 13430600 and registered office at 28 Bentham Road, Lancaster, Lancashire, LA1 4JX.

### Purpose and Principles

This policy is intended to ensure that personal information is dealt with correctly and securely and in accordance with the General Data Protection Regulations 2018 and other related legislation. Zentek Digital Investigations Ltd is a “data controller” registered with the Information Commissioner’s Office (“ICO”) with registration number 00017078195. The Data Controller will comply with their legal obligations to keep personal data up to date; to store and destroy it securely; to not collect or retain excessive amounts of data; to keep personal data secure, and to protect personal data from loss, misuse, unauthorised access and disclosure and to ensure that appropriate technical measures are in place to protect personal data.

All persons involved with the collection, processing and disclosure of personal data will be aware of their duties and responsibilities by adhering to these guidelines, they will be known as ‘Data Processors’.

We will use personal data for some or all of the following purposes:

- To enable us to meet all legal and statutory obligations;
- To maintain our own accounts and records in line with legal requirements including professional, financial, case, sensitive, criminal, technical and usage data;

Type of Data	Description and examples
Identity Data	Data used to personally identify you such as your full name (including name prefix or title) or similar identifier, date of birth, title and maiden name.
Contact Data	Data required to communicate with you during the course of our relationship with you to include address(es), email address(es), telephone number(s) and mobile phone number(s) – this may include both your business/work and personal contact details.
Professional Data	Data that relates to your position and profession such as job title, professional qualifications and experience, regulatory body, the entity that you work for and details of your professional online presence (such as your LinkedIn profile and business website(s)).
Financial Data	Data necessary for processing payments (such as bank account details and billing address(es)), fraud prevention and other related billing information.
Case Data	Data provided to us by you on your behalf, which will include details about your contact with us, information relating to the case(s) that we are dealing with including data extracted from devices and/or obtained from IT systems and/or Cloud (which may include data in the form of text, images, videos, audio recordings). The data under this category will vary depending on the nature of the services we provide and your specific instructions and

	requirements.
<b>Sensitive Data</b>	<p>(also known as “special category data”) may be obtained and/or processed depending on the services that we are providing and/or the relevant circumstances but may including information in relation to:</p> <ul style="list-style-type: none"> <li>- Health and medical records</li> <li>- Genetic data</li> <li>- Biometric data for the purpose of uniquely identifying a natural person</li> <li>- Membership of a professional trade association or union</li> <li>- Racial and/or ethnic origin</li> <li>- Political opinions</li> <li>- Sex life and sexual orientation; and/or</li> <li>- Information regarding religious and philosophical beliefs.</li> </ul> <p>(We may collect Sensitive Data in the following circumstances – from data provided to us by client(s), where it is necessary when carrying out our services to meet our contractual obligations and when making arrangements for you to attend a meeting, training session and/or interview and ensuring accessibility and catering for your dietary requirements).</p>
<b>Criminal Data</b>	<p>Such data may be processed within Case Data depending on the services that we are providing and the relevant client that we are instructed by and may include personal data relating to the alleged commission of offences by a data subject, proceedings for the offence and disposal of such proceedings including sentencing, criminal records and details of convictions, proceedings, allegations, investigations, offences and cautions.</p> <p>(We only collect and process Criminal Data when instructed to lawfully do so on behalf of our duly authorised client(s) and on their specific instructions in accordance with our contract with them and, in doing so, we act as a data processor in relation to such Criminal Data. Our processing of Criminal Data is only carried out under the control of an official authority and/or as authorised by law).</p>
<b>Technical Data</b>	<p>Internet protocol (IP) address, your login data (if access is provided to our Cloud platform in relation to some services, browser type and version, time zone setting and location, browser plug-in types and versions, operating system and platform and other technology on the devices you use to access our website.</p>
<b>Usage Data</b>	<p>Information about how you use our website and (if you are an existing client) our services, and/or your communication preferences.</p>

- We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. It may not always be apparent at the outset what data we may require, who we may need to obtain it from and/or share it with as this will depend on the nature of the work and how the case progresses. If you wish to have an explanation as to how the processing for the new purpose is compatible with the original purposes please do contact us.
- If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so. Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **Marketing Communications**

As part of the services we provide to our clients, we may use personal data to form a view on what we think you may want or need, or what may be of interest to you. This is how we decide which products, services and offers may be relevant for you and/or your business.

We have a legitimate interest in processing your personal data and information for our business development. We will only send marketing communications to you if you have requested information from us and you have not opted out of receiving that marketing.

We will only share your personal data with third parties for marketing purposes with your express consent and you can withdraw that consent (if provided) at any time by contacting us.

You can ask us or third parties to stop sending you marketing messages at any time by contacting us.

Where you opt out of receiving these marketing messages, this will not apply to personal data provided to us as a result of your use of our services and/or under a contract that you have entered into with us.

## **Change of purpose**

We will only use your personal data for the purposes for which we collected it, unless we reasonably consider that we need to use it for another reason and that reason is compatible with the original purpose. It may not always be apparent at the outset what data we may require, who we may need to obtain it from and/or share it with as this will depend on the nature of the work and how the case progresses.

If you wish to have an explanation as to how the processing for the new purpose is compatible with the original purpose then please do contact us.

If we need to use your personal data for an unrelated purpose, we will notify you and we will explain the legal basis which allows us to do so.

Please note that we may process your personal data without your knowledge or consent, in compliance with the above rules, where this is required or permitted by law.

## **Cookies**

You can set your browser to refuse all or some browser cookies, or to alert you when websites set or access cookies. If you disable or refuse cookies, please note that some parts of our website may become inaccessible or not function properly. For more information about the cookies we use please contact us.

## Data Sharing

### *Who do we share your data with?*

We may (depending on the nature of the services we are providing, and the work involved) have to share personal data with other third parties and they may also share the personal data they hold about you with us. This may include:

- Solicitors, accountants, legal counsel, and other professionals when providing our services;
- Courts, tribunals, arbitrators and/or mediators where we are asked to provide our expert witness and other services;
- If we are under a duty to disclose or share your personal data in order to comply with any legal obligation, to protect the rights, property, or safety of Zentek Digital Investigations Ltd, our clients, or others;
- Our IT and telecommunications system providers acting as data processors as a consequence of them providing support to us;
- Analytics and search engine providers that assist us in the improvement and optimisation of our website;
- Our third-party service providers to include external consultants, contractors, couriers and suppliers;
- If in our reasonable opinion disclosure is required in relation to any criminal investigation or prosecution;
- Disclosures to law enforcement agencies, tax authorities, the National Crime Agency or other public or government authorities or regulators where in our reasonable opinion the disclosure is required or permitted by law or applicable regulation; and/or
- In the event that Zentek Digital Investigations Ltd sell or buy any business or assets, with the prospective seller or buyer of such business or assets. If a change happens to the ownership of our business, then the new owners may use your data in the same way as set out in this policy/privacy notice.

We require all third parties with whom your data is shared to respect the security and integrity of your personal data and to treat it in accordance with the law. We also impose contractual obligations on service providers to ensure they can only use your personal information to provide services to us and to you.

We do not allow our third-party service providers to use your personal data for their own purposes and only permit them to process your personal data for specified purposes and in accordance with our instructions.

We will not share your information with third parties for marketing purposes (unless you expressly consent to this).

## **Information we collect about you from others**

Information about you may be passed to us by third parties and/or obtained from publicly available sources in the course of providing our services and/or complying with our legal obligations. Typically, these sources may include:

- Professional advisors (such as accountants, legal counsel); and
- Public sources where this relates to you or your organisation (e.g. internet searches, your organisation's website and public social media accounts).

## **Transfer of Data Abroad**

We will hold your personal data on secure servers within the European Economic Area (EEA), we do not routinely transfer personal data outside of the EEA.

Some of the external parties in relation to a case may be based outside the EEA so their processing of personal data may involve a transfer of data outside the EEA.

Whenever we transfer your personal data out of the EEA, we will seek to ensure a similar degree of protection is afforded to it by ensuring that appropriate safeguards are implemented. In some circumstances (particularly where data is to be transferred outside of the EU where data protection laws are not as strict), we may need your express consent to the transfer unless there is an overriding legal requirement to transfer the information.

## **Information collected from you about others**

In the course of providing our services to you, we may need you to provide us with personal data about others (such as directors and employees in your organisation and/or persons to which your case relates).

When you provide personal information to us relating to others, you must ensure that you are legally permitted to share this with us and all data disclosed should be complete, accurate and up to date. You should ensure that those individuals understand how their data may be shared and used by us.

## **Data Security**

We have put in place appropriate security measures to prevent your personal data from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal data to those members of staff and other third parties who have a business need to know. They will only process your personal data on our instructions and they are subject to a duty of confidentiality.

We will hold your personal data on secure servers with all reasonable technological and operational measures to safeguard unauthorised access to include firewalls, gateways, security configuration and malware protection.

If we provide you with a username and password which enables you to access certain parts of our systems you are responsible for keeping such log-in details confidential. You must not share such information with anyone.

We have put in place procedures to deal with any suspected personal data breach and will notify you and any applicable regulator of a breach where we are legally required to do so.

## **Data Retention**

We will only retain your personal data for as long as necessary to fulfil the purposes we collected it for, including:

- For the purposes of satisfying any legal, accounting and/or reporting requirements;
- To investigate and defend any complaints and/or legal claims alleged and/or made against us (such as professional negligence claims);
- To carry out our services under our contract with you; and
- To comply with our legal and/or reporting obligations.

In some circumstances you can ask us to delete your data. See your rights later in this document for further information.

If we are hosting and/or holding data on your behalf, we will contact you and obtain your instructions before destroying any such data.

## **Your Data Protection Rights**

Under certain circumstances, you have rights under data protection laws in relation to your personal data. You have the right to request:

- Access to your personal data (commonly known as a “data subject access request”). This enables you to receive details of the personal data we hold about you and to check that we are lawfully processing it;
- Correction of the personal data that we hold about you. This enables you to have any incomplete, inaccurate or out-of-date data we hold about you corrected and/or updated, though we may need to verify the accuracy of the new data that you provide to us;
- Erasure of your personal data. This enables you to ask us to delete or remove personal data where there is no good reason for us continuing to process it. You also have the right to ask us to delete or remove your personal data where you have successfully exercised your right to object to processing (see below), where we may have processed your information unlawfully or where we are required to erase your personal data to comply with local law. Note, however, that we may not always be able to comply with your request of erasure for specific legal reasons (as explained above in relation to data retention) which will be notified to you, if applicable, at the time of your request;
- Object to processing of your personal data where we are relying on a legitimate interest (or that of a third party) and there is something about your particular situation which makes you want to object to processing on this ground as you feel it impacts on your fundamental rights and freedoms. You also have the right to object where we are processing your personal data for direct marketing

purposes. In some cases, we may demonstrate that we have compelling legitimate grounds to process your information which override your rights and freedoms;

- Restriction of processing of your personal data. This enables you to ask us to suspend the processing of your personal data in the following scenarios:
  - (i) If you want us to establish the data's accuracy;
  - (ii) Where our use of the data is unlawful, but you do not want us to erase it;
  - (iii) Where you need us to hold the data even if we no longer require it as you need it to establish, exercise or defend legal claims; or
  - (iv) You have objected to our use of your data, but we need to verify whether we have overriding legitimate grounds to use it; and
- Transfer of your personal data to you or to a third party. We will provide to you, or a third party you have chosen, your personal data in a structured, commonly used, machine-readable format. Note that this right only applies to automated information which you initially provided consent for us to use or where we used the information to perform a retainer with you.

### **Rights of access to information**

The following rights to access with regards to personal data are listed below, in order to process any request we would need to verify the identity of the individual making the request for security purposes. In such cases we will need the individual to respond with proof of identity before any rights can be exercised, e.g. passport, driving licence, utility bills with the current address, birth/marriage certificates, P45/P60, credit card or mortgage statement (this is not an exhaustive list). This is a security measure to ensure that personal data is not disclosed to any person who may not have a right to receive it. We may also contact you to ask you for further information in relation to your request to speed up our response.

You will not have to pay a fee to access your personal data (or to exercise any of the other rights). However, we may charge a reasonable fee if your request is clearly unfounded, repetitive or excessive. Alternatively, we may refuse to comply with your request in those circumstances.

We try to respond to all legitimate requests within one month. Occasionally it may take us longer than a month if your request is particularly complex or you have made a number of requests. In this case, we will notify you and keep you updated.

Please note that if you:

- Want us to restrict or stop processing your data;
- Fail to provide data that we have reasonably requested from you; or
- Withdraw consent at any time where we are relying on consent to process your personal data.

This may impact on our ability to provide our services to you and/or contract with you. Depending on the extent of your request and/or the importance of any information we request from you that you do not provide, we may be unable to continue providing our services to you. We will notify you if this is the case at the time. This will not affect the lawfulness of any processing carried out before your withdrawal of consent. In these situations you would remain liable for the cost of our services up until the date of your request and/or refusal to provide information.

## **Are there any restrictions on exercising your rights?**

You should be aware that when providing our services to law enforcements agencies, regulatory authorities and/or legal representatives in the context of litigation and/or potential litigation (both civil and criminal), there may be restrictions on the rights of data subjects (where appropriate and necessary) as follows:

- Where such data is subject to legal privilege;
- To avoid obstructing an investigation or enquiry;
- To avoid prejudicing the prevention, detection, investigation or prosecution of criminal offences or the execution of criminal penalties;
- To protect public security;
- To protect national security; and/or
- To protect the rights and freedoms of others.

In addition, it may be that we are not the data controller of your personal data (particularly, in relation to Case Data, Sensitive Data and/or Criminal Data) and so requests to exercise your rights should be made to the relevant data controller.

In the event that any of the above restrictions apply to your rights, we will confirm this to you (to the extent that we are able to without breaching our legal obligations).

## **Changes to our Data Protection Policy and/or Privacy Notice**

Any changes that are made in the future will be posted on our website and where appropriate. Please check back frequently to see any updates or changes.

It is important that the personal data we hold about you is accurate and current. Please keep us informed if your personal data changes during your relationship with us.

## **Complaints**

If you wish to raise a complaint on how we have handled your personal data, you can contact us to have the matter investigated by writing to or emailing our DPO – Zentek Digital Investigations Ltd, Office 1, 3 Hampson Lane, Hampson, Lancaster, LA2 0HY or [dpo@zentekforensics.co.uk](mailto:dpo@zentekforensics.co.uk).

If you are not satisfied with our response or believe we are not processing your personal data in accordance with the law you can complain to the ICO, the UK supervisory authority for data protection issues. Further details can be found at [www.ico.org.uk](http://www.ico.org.uk) or by calling 0303 123 1113. We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

## **Review**

This policy will be reviewed on a regular basis.