

## PRIVACY NOTICE

Phoenix Project Solutions Ltd is committed to protecting the privacy and personal information of all individuals it engages with and in doing so, complying with the EU General Data Protection Regulation 2016/679 (GDPR) and the Data Protection Act 2018. We would ask you to read this Notice carefully as it contains important information about the type of personal details we collect, how we collect it, what we might do with that information, how we protect it and how you might request details of the personal information we hold.

We may need to make changes to this Notice from time to time and will contact you if there are important changes to how your personal data will be processed, otherwise a current version of the Notice can always be viewed on our website, [www.phoenixps.co.uk](http://www.phoenixps.co.uk). This Notice was last updated on 24<sup>th</sup> May 2018.

### **1. Background to the General Data Protection Regulation ('GDPR')**

The EU General Data Protection Regulation 2016/679 replaces the EU Data Protection Directive of 1995 and supersedes the laws of individual Member States that were developed in compliance with the Data Protection Directive 95/46/EC. Its purpose is to protect the “rights and freedoms” of living individuals, and to ensure that personal data is not processed without their knowledge. There are 6 lawful bases for processing personal data which have been detailed in point **3. Collection of Data**.

### **2. Key definitions drawn from the GDPR**

**Personal data** – any information relating to an identified or identifiable living natural person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

**Special categories of personal data** – personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

**Data controller** – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data. Where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

**Data subject** – any living individual who is the subject of personal data held by an organisation.

**Processing** – any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**Profiling** – is any form of automated processing of personal data intended to evaluate certain personal aspects relating to a natural person, or to analyse, or predict that person's performance at work, economic situation, location, health, personal preferences, reliability, or behavior. This definition is linked

to the right of the data subject to object to profiling and a right to be informed about the existence of profiling, of measures based on profiling and the envisaged effects of profiling on the individual.

**Personal data breach** – a breach of security leading to the accidental, or unlawful, destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. There is an obligation on the controller to report personal data breaches to the supervisory authority and where the breach is likely to adversely affect the personal data or privacy of the data subject.

**Data subject consent** – Phoenix Project Solutions Ltd understands “consent” to mean that data subject has been fully informed of the intended processing of their personal information and has signified their agreement. That it has been freely given, is specific, informed and there is an unambiguous indication of the data subject’s wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

**Child** – the GDPR defines a child as anyone under the age of 16 years old. The processing of personal data of a child under 13 years of age is only lawful if parental or custodian consent has been obtained.

**Third party** – a natural or legal person, public authority, agency or body other than the data subject, controller, processor and persons who, under the direct authority of the controller or processor, are authorised to process personal data.

**Filing system** – any structured set of personal data, which are accessible according to specific criteria, whether centralised or de-centralised.

### 3. **Collection of data**

We will collect and use different personal information about you for different reasons depending on our relationship with you be that prospective client, client or supplier. Were you to provide personal information to us about other individuals (for example direct contact details for a colleague) we will also be data controller of their personal information and we are responsible for protecting their personal information and using it appropriately. This notice will therefore apply to those individuals and you should refer them to this notice.

#### **How we might collect personal data**

Information obtained from any written or verbal communication with you;

Information collected through any meeting with you;

Information you might provide in a survey, review or in response to a newsletter;

Information obtained through audit or processed whilst ensuring regulatory obligations are met.

#### **What personal information may we collect?**

General information such as your name, address, job title, place of employment, phone numbers and email addresses.

We do not have any cookies operating on our site and therefore will not obtain any information this way.

#### **What special categories of information may we collect?**

Depending on the nature of the service you receive from us we may process sensitive details which might include any criminal conviction(s) and any related information relevant to the service you are receiving which you have chosen to disclose.

### **How we might use your personal data**

There are a number of reasons we might use your personal information and for each use we need to have a “lawful” basis to do so. We will rely on one or more of the following “lawful bases” when we process your “personal information”:

**Consent:** the individual has given clear consent for you to process their personal data for a specific purpose

**Contract:** the processing is necessary to service a contract you have with the individual, or because they have asked you to take specific steps before entering into a contract

**Legal or regulatory obligation:** the processing is necessary for you to comply with the law (not including contractual obligations)

**Vital Interests:** the processing is necessary to protect someone’s life.

**Public task:** the processing is necessary for you to perform a task in the public interest or for your official functions, and the task or function has a clear basis in law.

### **Example of purpose for processing your personal data**

Registering you as a client or supplier

You have given us your permission (consent) to send you information about services, ICO updates and/or blog/news updates

To maintain satisfactory records/fulfil the obligations of a contract with you/your organisation

To comply with our legal or regulatory obligations

For communications purposes including handling complaints and dealing with any other communications

### **Who we might share your personal information with?**

We will not sell or transfer your personal information to anyone unless we have a valid purpose as set out above and we would only disclose it to the following parties:

Regulatory and government bodies, where we have a legal obligation to do so;

Data Protection authorities;

Third party suppliers/controllers/processors who have entered into a contractual arrangement with us to provide a service we need to carry out our everyday business such as IT suppliers, accountants, lawyers; web/database design and management;

Third party suppliers/controllers/processors who deliver a product/service you have requested;

Your employer.

### **How long do we keep your personal information for?**

We will only keep your personal information for so long as it is reasonably necessary to fulfil the purposes set out above and/or to comply with our legal and regulatory obligations or for as long as necessary to respond to concerns you have raised – this period would usually be 7 years after the last time you interacted with us. The length of time we keep your information for these purposes will vary depending on the obligations we are required to meet but, where possible, information needing to be retained will be anonymised.

### **What is our approach to sending your personal information overseas?**

It is the policy of Phoenix Project Solutions Ltd not to engage with any third party controller/processors who operate outside of the European Economic Area (“EEA”), therefore when undertaking GDPR due diligence with processor suppliers and/or third party controller/suppliers we look to ensure they also have the same policy. Personal data shall not be transferred to a country or territory outside the European Union unless a data subject specifically requests it in relation to a service they require. The country or territory must then ensure one or more of the specified safeguards is in place to provide an adequate level of protection for the ‘rights and freedoms’ of the data subject in relation to the processing of personal data as per the GDPR regulation.

#### 4. Data subjects' rights

Data subjects have the following rights regarding data processing, and the data that is recorded about them:

- **The right to be informed**  
You have the right to receive clear and easy to understand information on what personal information we have, where we hold it, why we hold it and who we share it with.
- **The right of access to personal information**  
You have the right to access any personal data (i.e. data about them) which is held by the firm in electronic format and manual records, which form part of a relevant filing system. Information should be provided within one calendar month, free of charge. We reserve the right to charge a fee if you are requesting information previously provided.
- **The right to rectification**  
If you believe there are any inaccuracies, discrepancies or gaps in any of the personal information we hold on you, you have the right to request it be corrected.
- **The right to erasure**  
You are entitled to request that we erase, cease processing and/or delete your information. If there is a regulatory requirement to hold information please see your "right to restricted access" below:
- **The right to restricted access** (where regulatory requirements prohibit erasure)  
You can ask that we block or suppress the processing of your personal information in certain circumstances.
- **The right to portable data**  
You have the right for personal data to be provided in a secure, structured, commonly used and machine-readable format, and the right to have that data transmitted to another controller.
- **The right to object/withdraw consent**  
The consent of the data subject can be withdrawn at any time from the processing of their personal data.
- **The right not to be subject to automated decision-making**  
You have the right to object to any automated profiling.

#### 5. Cookies

We do not have cookies operating within our website.

If you would like information on Cookies, please visit [www.youonlinechoices.com](http://www.youonlinechoices.com)

Our website may, from time to time, contain links to and from third party websites, including social media sites. If you follow a link to any of these websites, please note that these sites have their own privacy notices and that Phoenix Project Solutions Ltd do not accept any responsibility or liability for those notices. Please check these policies before you submit any information to these websites.

#### 6. Security of data

Phoenix Project Solutions Ltd take IT and security of data very seriously. Employees are responsible for ensuring that any personal data, which the firm holds and for which they are responsible, is kept securely. Any personal information will be held securely, within the EU or a country which the EU has deemed to have adequate security measures in place.

Internally we will have appropriate safeguards and procedures in place aligned with good practice standards to protect all information held and all staff with access to personal data will have been issued with the IT Policy which they are required to comply with.

## **7. Disclosure of data**

Phoenix Project Solutions Ltd must ensure that personal data is not disclosed to any unauthorised third parties.

In certain circumstances, we may process your personal information without further notification to you. This applies, for example, where we make a report in good faith under the Terrorism Act 2000 or Proceeds of Crime Act 2002. Such processing is justified under data protection law on the basis that it is in the substantial public interest.

## **8. Access to Information**

Under GDPR you can exercise your right of access by making a written request to receive copies of some or all information we hold on you. Please contact: Lara Bull, Director, 2 Dumbleton Close, Pinewood Park, Southampton, SO19 6AP/lara@phoenixps.co.uk. Proof of identify or authority if making a request on behalf of someone else will be required.

## **9. Complaints**

If you wish to contact us with any questions about our Privacy Notice or, to make a complaint you may contact our Lara Bull, Director, 2 Dumbleton Close, Pinewood Park, Southampton, SO19 6AP/lara@phoenixps.co.uk

If you have any concerns or complaints as to how we have handled your personal data you may lodge a complaint with the UK's data protection regulator, the ICO, who can be contacted through their website at <https://ico.org.uk/global/contact-us/> or by writing to the Information Commissioner's Office, Wycliffe House, Water Lane, Wilmslow, Cheshire, SK9 5AF.

Where data subjects wish to complain about how their complaint has been handled, or appeal against any decision made following a complaint, they may lodge a further complaint to the Board of Directors. The right to do this will be included in the GDPR section of our complaints procedure.