PRIVACY POLICY

iPWC Ltd (iPWC), on behalf of The Knight inde, are committed to protecting your privacy and confidentiality. This privacy policy sets out how iPWC uses and protects the information that you provide to us when you contact us or use our website.

iPWC is committed to ensuring that your privacy is always protected. Should we ask you to provide certain information by which you can be identified, you can be assured that it will only be used in the ways set out in this privacy policy.

iPWC may change this policy from time to time by updating this page. You should check this page from time to time to ensure that you are happy with any changes. This policy is effective from 25/05/18 and complies with the EU General Data Protection Regulation (GDPR) as from May 25th 2018.

What information do we collect?

We may collect the following information in order to provide you with a service:

- Your name
- Business/company name
- Job title
- Contact information such as your email address and telephone number
- Industry information

Additionally, when you visit our website we may collect information about your visit such as your IP address, your browser and device, and the pages you have viewed and when.

By using our services or submitting personal information through our services, you expressly consent to the processing of your personal information, according to this privacy policy.

How do we collect your information?

We may collect your information if you:

- Make an enquiry about a service
- Meet with staff in the course of business or exchange business cards
- Become a client
- Speak to us in a phone conversation
- Send us emails or letters
- Interact with us on social media
- Participate in client feedback surveys to help improve our own business operations
- Use our website

We may require this information to understand your needs and to provide you with the information that you have requested.

We will take all reasonable steps to ensure that we fully protect your rights and comply with our obligations under the Data Protection Act 1998, the Privacy and Electronic Communications (EC

Directive) Regulations 2003, as amended in 2004, 2011, and 2015, and the General Data Protection Regulation (GDPR) which comes into force from 25th May 2018.

Our legal basis for processing your information

We have a number of lawful reasons that we can use to process your personal information.

These include processing personal information where we have a legitimate interest to do so, where it is necessary to fulfil a contract, or where we are required to as a legal obligation.

Broadly speaking, legitimate interests means that we can process your personal information if:

- We have a genuine and legitimate reason to do so and we are not harming any of your rights and interests.

We will always carry out an assessment prior to processing your information to ensure it falls within the parameters set under legitimate interests.

We process personal information in order to run our business and to provide our services to you. If you choose not to provide us with this information, or do not wish us to collect and use this information in these ways, it may mean we will be unable to provide you with a service.

How do we use your information?

We may use your information in order to respond to your requests, or to provide you with a service.

We may use information collected by Google Analytics during your visit to iPWC.eu in order to help us improve the experience for visitors and develop new features for the future.

We may use your information to contact you from time to time to inform you about services and information about iPWC that may be of interest to you.

You can opt out of this at anytime by contacting us at info@ipwc.co.uk.

How do we share your data?

We do not share your data with any other company unless a project we are undertaking for you requires third party support, and you have given us permission to disclose your details.

In certain circumstances, we may be legally required to share certain data held by us, which may include your personal information, for example, where we are involved in legal proceedings, where we are complying with the requirements of legislation, a court order, or a governmental authority. We do not require any further consent from you in order to share your data in such circumstances and will comply as required with any legally binding request that is made of us.

How long we keep your information?

We will keep your personal information only where it is necessary to provide you with our products or services as a customer, where required to meet our legal or regulatory obligations, and/or for as long as we have your permission to keep it.

Security

Data security is of great importance to us, and to protect your data we have put in place suitable physical, electronic and managerial procedures to safeguard and secure the data we collect.

Notwithstanding the security measures we take, please remember data transmission via the internet may not be completely secure. We advise you to take suitable precautions when transmitting data to us via the internet.

Other websites

This privacy policy applies only to The Knight Index website and the information you provide to The Knight Index. There may from time to time be links on our website to third-party websites over which we have no control. When you click on these links, you will leave this website, and thereafter the third-party's privacy policy will apply.

Use of data processors

We use the following data processors who provide us with services to our business. We ensure they have the highest levels of reliability, security, and accreditation.

- Qualtrics, an external supplier that we use to host our survey applications and databases.

In addition, we have our main server, where all project-related data is stored securely.

Any consent records provided to us are also stored securely as an electronic copy.

Where is your information processed?

Information we may collect from you is processed in the UK and European Economic Area (EEA). Where information is processed by suppliers outside the EEA, we aim to ensure these suppliers have accreditations sufficient to acknowledge the safe handling and storage of data from the EEA.

How we use cookies

Cookies are small text files that are sent by web servers to web browsers and can be used by web servers to identity and track users as they view different pages on a website or return to a website. They may be either persistent cookies or session cookies and may contain unique identifiers.

A persistent cookie will be stored by the browser and will remain valid until its set expiry date (unless deleted by the user before this date). A session cookie, on the other hand, will expire at the end of the user session when the web browser is closed.

The types of cookies we use are:

- *Functional*
  These cookies are used to ensure you can correctly navigate our websites and play videos, listen to podcasts or share pages via social media.

- *Performance*
  These cookies are used to analyse trends, administer the website, track visitor movements and gather broad demographic information for aggregate use. We use the information to compile reports and to help us improve our websites. These cookies are not linked to personally identifiable information.

The Knight Index website uses the following cookies.

- XSRF-TOKEN
- bSession
- HS
- svSession
- Google Analytics

Managing cookies

If you don't want to receive cookies, you can modify your browser so that it notifies you when cookies are sent or refuse cookies altogether. You can also delete cookies that have already been set. You can do this through your browser settings.

If you'd like to learn more about cookies in general and how to manage them, visit aboutcookies.org

Your individual rights

You have several rights in relation to how we use your information. They are:

- *Right to be informed*

  You have a right to receive clear and easy-to-understand information on what personal information we have, why, and who we share it with – we do this in our privacy policy and privacy notices.

- *Right of access*

  You have the right of access to your personal information.

  If you wish to receive a copy of the personal information we hold on you, you may make a data subject access request at no expense by contacting us at info@iPWC.co.uk.

- *Right to request that your personal information be rectified*

  If your personal information is inaccurate or incomplete, you can request that it is corrected. If the request concerns sensitive data, we will update the necessary databases and store your request as a hard copy in a locked filing cabinet as well as a soft copy on our protected server.

- *Right to request erasure*

  You can ask for your information to be deleted or removed if there is not a compelling reason for iPWC to continue to hold it.

  We will supply a request form for the erasure of personal data that doesn't need to be maintained for legal obligations or exercise of official authority. To erase this data, we will delete all soft copies off of our server and hard copies will be shredded and disposed of safely.

- *Right to restrict processing*

  You can ask that we limit the processing of your personal information for certain reasons. This means that we are still permitted to keep your information – but only to ensure we don't use it in the future for those reasons you have restricted.

- *Right to object*

  You can object to iPWC processing your personal information where:

  - It's based on our legitimate interests.
  - It may be used for direct marketing.
  - If we were using it for scientific/historical research and statistics.

In which circumstances do we report a data breach?

A loss of personal data does not result in a data breach unless the breach results in a risk to the rights and freedoms of an individual, a detrimental effect on their reputation, financial loss, loss of confidentiality, discrimination, or any significant economic or social disadvantage.

Should a data breach occur, we will:

- Report internally to the directors of iPWC Ltd: David George, Mark Bradshaw
- Report back directly to the individual exposed if there is a high risk to rights & freedoms
- Report to the appointed Data Protection Officer (DPO) and/or data protection team
- Report to the Information Commissioner's Office with 72 hours

If the breach occurs or is discovered outside normal working hours, it must be reported as soon as is practicable. The DPO or response team lead will act as a point of contact to coordinate a response team in carrying out the following procedure:

- Begin implementation of appropriate counter-measures whilst maintaining quality of service. Depending on the severity of the incident, it may be appropriate to temporally withdraw service.
- Notify the client that an incident has taken place and appraise them of the situation.

- If required by the client, we will notify affected users and appraise them of the situation. We will establish what, if any, data has been accessed or modified and promptly notify the client as to the extent of the incident. We will reset the authentication for affected users. We can also reset the authentication of all users of the service.
- Where appropriate, we will provide a time-scale for the restoration of service and notify the client.
- Following a full system test, service will be restored.

How to make a complaint

We will always strive to collect, use and safeguard your personal information in line with data protection laws and our Privacy Policy.

If you are still unhappy, you can complain to our Supervisory Authority. You can find their contact details on the ICO website.

How to contact us

If you have any other questions about your personal information, please contact us.

iPWC Ltd

T: 020 3026 0778

E: info@ipwc.co.uk

W: www.ipwc.co.uk

Address: 71-75 Shelton Street, Covent Garden, London, WC2H 9JQ