



## **PRIVACY NOTICE: REGISTRANTS, APPLICANTS AND REGULATED INDIVIDUALS**

### **THE KIND OF INFORMATION WE HOLD ABOUT YOU**

We collect, store and use personal data that you provide during the process of applying to be regulated by IPReg, when you initially populate your IPReg Pro account and when you update it. This includes information such as your contact details, date of entry to the Register(s), fee-paying category, qualifications, CPD compliance, whether you are an office holder (such as a Head of Legal Practice or a Head of Finance and Administration) and PII details. We also collect, store and use personal data when you contact us by email or by completing one of our website contact forms.

We process this personal data in order to comply with our legal obligations and perform a public task under various statutes and statutory instruments including the:

- Trade Marks Act 1994;
- Copyright, Designs and Patents Act 1988; and
- Legal Services Act 2007.

“Special categories” of particularly sensitive personal information require higher levels of protection. The GDPR classifies certain data as belonging to “special categories” as: racial origin; ethnic origin; political opinions; religious beliefs; membership of a trade union; genetic data; biometric data; health data; data concerning a person's sex life; and sexual orientation. We need to have further justification for collecting, storing and using this type of personal information. We have in place an appropriate policy and safeguards which we are required by law to maintain when processing such data. The GDPR requires that explicit consent is provided by the data subject for obtaining these special categories of data.

IPReg asks registrants to provide the following sensitive personal data about themselves on admission to the Register: ethnicity; religion or belief; gender; sexual orientation; whether their gender is the same as the gender they were assigned at birth; whether they consider themselves to be disabled. We ask you to provide this information in order to comply with our legal obligation under the Legal Services Act 2007 to encourage an independent, strong, *diverse* and effective legal profession (emphasis added). Registrants can decide not to provide information about sensitive personal data by indicating “prefer not to say”. Registrants may update or remove this data at any time.

Access to data relating to special categories is restricted to the IPReg Chief Executive and the IPReg Head of Registration.

### **HOW IS YOUR PERSONAL INFORMATION COLLECTED?**

We collect personal information about you through the application process for individuals and entities, the subsequent registration process, the annual re-registration process and any emails, website contact forms or letters that you send us. We may sometimes collect additional information from third parties including former or current employers, other regulators, credit reference agencies or other background check agencies.

We may also hold other information about you that you have not provided to us such as alternative contact details. We obtain these from sources such as LinkedIn, CIPA or CITMA or from an internet search. We process this data to comply with our legal obligations as set out above and because we have a legitimate interest in ensuring that we know where our registrants are working and can contact them.

## **HOW WE WILL USE INFORMATION ABOUT YOU**

We need personal data primarily to allow us to perform our statutory regulatory responsibilities and to enable us to comply with legal obligations. We also need this data because we have a legitimate interest in ensuring that the way we regulate is informed by our knowledge of the legal services market(s) and by the opinions of those we regulate. The situations in which we will process your personal information include:

- The maintenance of Register(s) of individual registrants and registered entities;
- Applications for admission to the Register(s);
- The administration and granting of licences and applications for licences;
- Monitoring compliance with our regulatory arrangements;
- The consideration and investigation of complaints;
- Formal enforcement action;
- Development of IPReg's policy on regulatory matters including diversity;
- Providing advice and information to those we regulate and consumers;
- To alert you to any proposals to change our regulatory arrangements and invite your views;
- To maintain our own accounts and records;
- To support and manage our employees;
- Undertake research into the way legal services are used or provided and thematic reviews into matters such as compliance with our regulatory arrangements or areas of risk to consumers;
- Internal support functions, corporate administration and all activities we are required to carry out as a data controller.

## **If you fail to provide personal information**

If you fail to provide certain information when requested, you may be in breach of IPReg's regulatory arrangements and this may have serious consequences – for example, you may be suspended or removed from the Register(s) and/or disciplinary action may be taken against you. However, for the avoidance of doubt, you are not under any obligation to provide special categories of personal data that relate to equality and diversity.

## **Keeping your information up to date**

IPReg will endeavour to keep your personal data up to date and accurate. We do this by the Annual Return process each year. You can also update your personal data at any time by logging on to your IPReg Pro account.

## **DATA SHARING**

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law. Your personal information on the Register(s) and our CRM system more generally will not be transferred outside the EU/EEA and in most cases is stored in the UK. Emails that you send us are stored by Microsoft in the UK. In some cases, for example, if emails are

exchanged as part of our consideration of a complaint, they may be backed-up on servers in the USA. These transfers are covered by the EU-US Privacy Shield Framework.

### **Why might you share my personal information with third parties?**

We will share your personal information with third parties where required by law. We will also share your personal information (for example with our IT contractor) where it is necessary to fulfill our legal obligations or where we have legitimate interest in doing so.

When there is no longer a service need, or the contract comes to an end, the third party will dispose of all personal data according to our procedures. Unless we are required do so by law, we will never share your personal data with other types of third parties (such as marketing agencies) unless we have received your consent.

### **How secure is my information with third-party service providers?**

All our third-party service providers are required to take appropriate security measures to protect your personal information. We do not allow our third-party service providers to use your personal data for their own purposes. We only permit them to process your personal data for specified purposes and in accordance with our instructions.

### **What about other third parties?**

We may share your personal information with other third parties such as other regulators who are investigating a potential breach of their regulatory arrangements or an application to be regulated by them, an insurer providing PII or run-off cover or to otherwise comply with the law.

## **DATA SECURITY**

We have put in place measures to protect the security of your information. Third parties will only process your personal information on our instructions and where they have agreed to treat the information confidentially and to keep it secure.

We have put in place appropriate security measures to prevent your personal information from being accidentally lost, used or accessed in an unauthorised way, altered or disclosed. In addition, we limit access to your personal information to those employees, agents, contractors and other third parties who have a business need.

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

## **INFORMATION ABOUT CRIMINAL CONVICTIONS**

We will only use information relating to criminal convictions where the law allows us to do so. This will usually be where such processing is necessary to carry out our obligations and providing we do so in line with our data privacy policy. Less commonly, we may use information relating to criminal convictions where it is necessary in relation to legal claims, where it is necessary to protect your interests (or someone else's interests) and you are not capable of giving your consent, or where you have already made the information public.

## **AUTOMATED DECISION-MAKING**

We do not envisage that any decisions will be taken about you using automated means, however we will notify you in writing if this position changes.

## **DATA RETENTION**

### **How long will you use my information for?**

We will only retain your personal information for as long as necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory or reporting requirements. Once you are no longer on the Register(s), we will retain your data on our CRM system but your details will not be displayed on our website.

To determine the appropriate retention period for personal data, we consider the amount, nature, and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal requirements.

In some circumstances we may anonymise your personal information so that it can no longer be associated with you, in which case we may use such information without further notice to you.

## **RIGHTS OF ACCESS, CORRECTION, ERASURE, AND RESTRICTION**

### **Your duty to inform us of changes**

It is important that the personal information we hold about you is accurate and current. Please keep us informed if your personal information changes during your working relationship with us; you can do this by updating your IPReg Pro account.

### **Your rights regarding personal information**

In certain circumstances, you have the right to:

- Request access to your personal information (commonly known as a “data subject access request”). This enables you to receive a copy of the personal information we hold about you and to check that we are processing it lawfully;
- Request correction of the personal information that we hold about you. This enables you to have any incomplete or inaccurate information we hold about you corrected;
- Request erasure of your personal information. This enables you to ask us to delete or remove personal information 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 information where you have exercised your right to object to processing. The right to erasure does not apply when IPReg is processing data to comply with a legal obligation;
- Object to processing of your personal information where we are relying on a legitimate interest (or those of a third party) and there is something about your particular situation which makes you want to object to processing on this ground;

- Request the restriction of processing of your personal information. This enables you to ask us to suspend the processing of personal information about you, for example if you want us to establish its accuracy or the reason for processing it;
- Request the transfer of your personal information to another party.

If you want to review, verify, correct or request erasure of your personal information, object to the processing of your personal data, or request that we transfer a copy of your personal information to another party, please contact us.

### **No fee usually required**

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

### **What we may need from you**

We may need to request specific information from you to help us confirm your identity and ensure your right to access the information (or to exercise any of your other rights). This is another appropriate security measure to ensure that personal information is not disclosed to any person who has no right to receive it.

### **RIGHT TO WITHDRAW CONSENT**

In certain circumstances where you have provided your consent to the collection, processing and transfer of your personal information for a specific purpose, you have the right to withdraw your consent for that specific processing at any time. To withdraw your consent, please contact us. Once we have received notification that you have withdrawn your consent, we will no longer process your information for the purpose or purposes you originally agreed to, unless we have another legal basis for doing so.

### **CONTACT DETAILS**

If you have any questions about this Privacy Notice or how we handle your personal information, please contact us. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK supervisory authority for data protection issues.

### **CHANGES TO THIS PRIVACY NOTICE**

We reserve the right to update this privacy notice at any time, and we will publish a new privacy notice when we make any substantial updates. We may also notify you in other ways from time to time about the processing of your personal information.

If you have any questions about this privacy notice, please contact us.

## Change history record

Issue	Description of Change	Approval	Date of Issue
1	First version	CEO	16 May 2018
2	Changes to reflect go live of new CRM system and related change to server provision	CEO	26 September 2019