FORSTERS

Forsters LLP 31 Hill Street London W1J 5LS **| DX:** 82988 Mayfair
T: +44(0)20 7863 8333 **| F:** +44(0)20 7863 8444 **| W:** www.forsters.co.uk

Data Protection Statement

Compliance with the EU General Data Protection Regulation (GDPR)

Forsters takes the security and privacy of data seriously. This document sets out our approach to compliance with the EU General Data Protection Regulation and provides information about how we will manage our data privacy and security obligations.

Collection and processing of personal and/or sensitive data

We will collect and process personal data, including sensitive data, in order for us to carry out our contractual responsibilities with our clients and legal obligations with our regulators and/or insurers. We will collect data on behalf of ourselves and/or third parties directly related to the performance of a contract with our clients. We will not pass client data to unrelated third parties other than as required for the provision of our services. We do not normally copy such information to anyone outside the European Economic Area. However, we may do so when the particular circumstances of a matter so require.

Personal data that we collect for the purposes of compliance with our money laundering obligations will be processed only for the purposes of preventing money laundering and terrorist financing, or as otherwise permitted by law or with your express consent. Such data will generally be retained for five years, but may be retained for longer in certain circumstances.

Use of personal data for marketing purposes

Personal data will only be used for marketing purposes where we have the consent of the person(s) to whom the data relates, or where there is a legitimate business reason for us to do so. In situations where the latter is applicable, individuals will always be given the opportunity to opt-out of receiving further communications. We will not initiate unsolicited contact with any individuals.

Authorised access to Personal Data

Only partners and staff of Forsters LLP and Forsters Service Company Limited and approved third parties – where it is necessary for the performance of our contract with our clients – will have access to the personal data we hold.

Vetting and due diligence procedures for employees and providers

Pre-employment vetting, including criminal background checks, is conducted on all employees and references are obtained from previous employers.

Due diligence on third parties and suppliers

We undertake due diligence on a risk based approach when engaging with potential suppliers or other third parties.

In accordance with Article 28 of the GDPR, we are currently in the process of reviewing our internal supplier management policies. We are in discussions with each of our key suppliers (those who process personal data on our behalf) to seek clarification of the steps being taken to ensure they are GDPR compliant and to ensure that our agreements with those suppliers provide adequate protection for data they process on our behalf.

Training

In accordance with our GDPR implementation process, online training will be rolled out to all staff via a mandatory training module through our online training provider during May 2018.

Remote policy

We have an agile working policy which allows, where appropriate, employees to work remotely. The same technological measures are in place to protect remote workers from viruses and social engineering. Remote access to our network is controlled via secure authentication, including password protection for firm issued devices as well as our cloud platform.

Receiving Personal Data

We receive personal data throughout the course of performing our contract with clients via electronic means, mail, telephone, or as a result of notes taken during face to face meetings.

Personal Data back ups

Our key business service systems, within which personal data is held, are backed up to disk every evening and we perform a full back up once per month. Our services are mirrored across two sites.

Physical security measures

Secure entry systems are in place across all of our offices. There is a manned reception presence at each office as well as on-site security guards, and CCTV where appropriate.

Technological security measures

Our online platform is password protected and we operate a "need to know" access control policy where appropriate. We are currently in the process of reviewing our access control policy in line with a firm wide information security review. Our network is secured by managed firewalls and anti-virus software. Internal and external vulnerabilities, including those on remote devices, are identified and remediated on a daily basis. Penetration testing has been carried out and we are currently developing a regular schedule for this to be conducted on an ongoing basis.

Destruction of physical data

Physical records are stored securely on site and with our data storage provider. Data held on client files will be subject to file retention and destruction policies in line with the GDPR. Such files will be reviewed at appropriate intervals and destroyed accordingly. Secure destruction bins are available on each floor and we use a certified secure destruction provider.

Detecting and reporting breaches

We are developing a new breach response procedure, which will be incorporated into our updated data protection procedures. We will be providing firm wide training in due course to ensure that our staff are aware of the process to follow should a breach occur.

Data Subject Rights

The GDPR provides data subjects with certain rights. These include the right to access the data we are processing, the right to request that data be destroyed, the right to correct the data and the right to object to further data processing.

In most situations, we will not rely on consent as a lawful ground to process client data. If we do however request consent to the processing of personal data for a specific purpose, that consent can be withdrawn at any time.

Any questions or concerns regarding our data processing activities should be directed to the relevant matter partner in the first instance.

Data subjects additionally have the right to complain to the Information Commissioner. Full contact details including a helpline number can be found on the Information Commissioner's Office website (www.ico.org.uk). This website also has further information on data subject rights and our obligations.