# The Right Will and Estate Planning Limited

## Self-Assessment Document

## 22nd May 2018

As of May 25th, the General Data Protection Regulation (GDPR) will replace the Data Protection Act.

Whilst The Right Will and Estate Planning Ltd is happy to offer reasonable support to ensure that you can become compliant with GDPR, the ultimate responsibility for compliance with GDPR lies with each Firm and, in particular, you as Data Controller.

As such, we have put together this self-assessment document, so that you can ensure you have completed all necessary actions to ensure you are ready for the introduction of GDPR and are suitably equipped to comply with this regulation going forward. If any of these actions have not been completed, you should look to do so as soon as possible.

Please see next page for the checklist:

| Action | Completed? |
|---|---|
| I have read and understood the GDPR information on The Right Will and Estate Planning Ltd and ICO websites. | |
| I have conducted a data audit to establish the personal data that I hold, process, and share. I have ascertained who I hold personal data on, why I hold it, how accurate it is, how I came by it, and how long I have held it for. | |
| I have established the 'Lawfulness of Processing' basis for holding personal data in line with the 6 basis from the ICO, namely:<br>1. Consent<br>2. Contractual<br>3. Legal Obligation<br>4. Vital Interest<br>5. Public Interest<br>6. Legitimate Interest | |
| I have reviewed and updated my Data Protection Policy to ensure this is GDPR compliant. | |
| I have put in place procedures to ensure I can obtain and evidence consent to contact clients that is compliant with GDPR | |
| After May 25th, I will not contact any client or potential client that I have not obtained prior consent to contact unless there is a necessary reason to do so. | |
| I have put in place a privacy policy for clients that is to be provided when receiving their personal data. | |
| I have put in place policies to ensure that I can comply with Subject Access Requests within one month of such a request. | |
| I have ensured that all devices used for the processing of personal data are password protected and suitably encrypted; and that where my data is stored remotely or in physical form, that this complies with GDPR. | |
| Where information is transmitted electronically (e.g. email) I have ensured that my means of transmitting such information is suitably secure in line with GDPR. | |
| I have set a data retention policy for the personal data I hold, and have put in place suitable systems to ensure that this policy can be followed | |
| I have trained my staff on the requirements of GDPR and our new policies resulting from this. This training has been documented to ensure I can provide evidence of procedures to the ICO. | |
| I have put in place procedures to detect, investigate and report a personal data breach, and understand my responsibilities to clients when this happens. | |
| Where introduced (or referred) customer leads are provided, I am aware that it is my responsibility to establish that the customer has provided their consent to be contacted prior to such contact. | |