Financial Advice

Paul Wellington
Financial Advisor
Harwicke House
Green Barn Farm
Selborne
Alton
Hants
GU34 3HL

How our Principal Firm Ensures We Comply With the GDPR and DPA 2017

With forthcoming European legislation coming into effect and the passage of an additional UK data protection Bill through Parliament, this paper highlights what we and our Principal are undertaking in readiness for new requirements, ensuring that we can demonstrate compliance and protect the rights, freedoms and interests of data subjects. At the end of the paper, there is a section providing the contact details of our Principal's Data Protection Officer should you have any further questions.

Compliance Audit Visits

Our Principal firm carries out on-site compliance audit checks which specifically focus on areas such as data protection. We have to ensure that we have technical and organisational measures in place which are appropriate to meet the risk posed by the type of data we process, or by the process itself. Our contract stipulates that we must comply with all relevant data protection legislation, and sanctions can be raised if we fail to adhere to these expectations.

Personal Data is Processed Securely by our Principal

Given that we input client personal data into our Principal's systems, security measures have been deployed to transfer, process, encrypt and store data. Connection to the Principal's website is via a TLS 1.2 secure connection.

Forthcoming GDPR and UK Legislation Module

Whilst the GDPR has already been written into UK law, it will officially apply from 25th May 2018. In order to demonstrate compliance, understand the risks associated with processing, and produce its GDPR Article 30 document of processing activities, each firm will undertake an online audit and submission of its data protection processes.

This will include detail of:

- Policies adopted.
- Organisational and technical measures implemented.
- Processes of activities carried out.
- Types of data processed.
- Categories of data subject.
- Source and format of the data.
- How the accuracy of data is maintained.
- The legal basis for each processing activity.
- Automated decision making processes and safeguards.
- Third party processors and compliant contracts.
- Transfers to third countries.
- How data is stored and what determines the length of storage.

- Risks associated with specific processing and the actual mitigation in place to reduce crystallisation of the risk.

Client Agreements and Privacy Notices

Our current client agreements and privacy notices are being revised by our Principal in accordance with GDPR Articles 13 and 14.

Evidence of Explicit Consent

Consent by the data subject is freely given, specific, informed and unambiguous and can be easily withdrawn.

GDPR Article 9 Processing Special Categories of Personal Data

Processing special categories of personal data is undertaken only where the law allows. Such data includes:

- Personal data revealing racial or ethnic origin.
- Personal data revealing political opinions.
- Personal data revealing religious or philosophical beliefs.
- Personal data revealing trade union membership or non-membership.
- Personal data relating to inherited or acquired genetic characteristics.
- Biometric data for the purpose of uniquely identifying a natural person.
- Personal data concerning health.
- Personal data concerning a person's sex life or sexual orientation.

GDPR Article 10 Criminal Conviction Data

Processing personal data concerning criminal convictions is undertaken only where the law allows.

GDPR Article 8 Processing Children's Personal Data

Consent is obtained from the holder of parental responsibility before processing the personal data of children under the age of 16.

Further New Data Subject Rights

GDPR Article 15 Data Subject Access Rights:

Our Principal handles all subject access requests and has, to date, delivered all requests within time constraints. The forthcoming legislation does reduce time limits to one calendar month with an option to request an extension, and it is expected that these new time limits will be met without serious impact on the business. In most cases there will now not be a charge for subject access requests.

Furthermore, the following rights are being incorporated into our Principal's systems, and will form part of forthcoming policies and privacy notices:

- The right to be informed - providing statutory information via privacy notices (Articles 12-13, GDPR).
- The right of access to personal data (Article 15, GDPR, *see above*).
- The right to rectification of personal data (Article 16, GDPR).
- The right to erasure of personal data (Article 17, GDPR).
- The right to restriction of processing (Article 18, GDPR).

- The right to data portability – receiving personal data in a standard format or to have it transmitted to another data controller (Article 20, GDPR).
- The right to object to processing, including direct marketing (Article 21, GDPR).
- The right not to be subject to decisions based solely on automated processing (Article 22, GDPR).

Technical and Organisational Measures

Appropriate technical and organisational measures, including policies, have been implemented and are regularly reviewed; (GDPR Article 24).

Data Protection is Implemented by Design and Default

Consideration to data protection is given before new processes are implemented or personal data is collected; (GDPR Article 25).

Data Protection Impact Assessments

GDPR Article 35 introduces a requirement to carry out a data protection impact assessment under certain circumstances. Our Principal will be making an online form available for us to record such assessments, where we can evidence that due regard is given to the risk associated with processing operations.

Third Party Processors

When engaging the services of another party to process data, an appropriate written contract protecting the rights and freedoms of data subjects is always put in place before any data transfer, in line with GDPR Article 28.

Transfers to Countries Outside the UK

Our Principal's forthcoming policy states:

"Data will not be transferred to countries outside the European Economic Area unless:

- *The law allows us to because there are adequacy decisions, appropriate safeguards or binding corporate rules as detailed in Articles 45-47, or;*
- *We have the explicit informed consent of the individual and we have informed them of the risks, or;*
- *The transfer is necessary to perform a contract between us and the data subject, or;*
- *The transfer is necessary to implement pre-contractual measures at the data subject's request, or;*
- *The transfer is necessary to perform or conclude a contract in the data subject's interest where the contract is between us and a third party, or;*
- *The transfer is necessary for important reasons of public interest, or;*
- *The transfer is necessary for the establishment, exercise or defence of legal claims, or;*
- *Another reason permitted by law.*

When such transfers must take place, we will document the reasons and legal basis for doing so.

We will take particular care to be aware of this when publishing information on our website/s, which can be accessed from anywhere in the globe. This is because the transfer includes placing data on a website that can be accessed from

outside the European Economic Area. Access to the organisation's website from certain countries has been automatically barred.

We will pay particular regard to any request for information that contains personal data where the request has come from any of our parent undertakings."

Resource Centre

The online GDPR module will contain the following resources:

- Industry relevant training in bite-sized chunks.
- A DPO blog.
- Links to relevant articles.
- Examples of documents, policies and forms.
- A GDPR search and lookup form.

Breach Register and Reporting

In accordance with GDPR Articles 33 and 34, data breaches will be reported to the regulator and those which pose a high risk will be reported to the data subject. In addition to the GDPR requirements, other medium or low risks may be also reported to the data subject to promote transparency and fairness in processing, and to demonstrate a firm's ability to detect breaches and mitigate risk.

Our Principal will require us to submit breaches to their online breach register so that they may review and audit our processes, offer advice, or reaffirm good practice.

The Data Protection Bill 2017-2019 (aka The Data Protection Act 2017)

Our Principal is monitoring the passage of the Bill through Parliament and has noted in particular the following additions to the GDPR:

1. When processing sensitive data in the realms of employment law or substantial public interest:

    - There must be a written policy document which explains procedures in place for securing compliance with Article 5 of the GDPR when processing this data, and this must be reviewed.
    - The policy must also explain the Company rules regarding the retention and erasure of this data and gives an indication of how long such data is likely to be retained.
    - The policy document must be retained for 6 months after processing stops and be made available to the regulator.

(Processing in the substantial public interest includes preventing dishonesty, preventing / detecting unlawful acts, equal opportunity monitoring, and preventing fraud, suspicion of terrorism or money laundering).

2. Criminal offences and unlimited fines of persons for:

    - Re-identifying de-identified data.
    - Processing re-identified data.
    - Preventing disclosure for a SAR request or data portability request.

3. Punishment for directors, officers or managers whose consent or negligence causes a corporate body to commit an offence under the GDPR.

4. Requirement to include additional information in the Article 30 document regarding the processing of sensitive data in (1) above.

5. Compensation is introduced for all other data protection legislation breaches under this Act and not just the GDPR.

Contact Our Principal's Data Protection Officer

Our Principal's Data Protection Officer is involved properly and in a timely manner in all issues which relate to data protection. CIPM and CIPP/E qualified, the DPO is available for contact using the details below:

- *In writing:*

  The Data Protection Officer,
  In Partnership Financial Advisers Ltd,
  On-Line House, 50-56 North Street,
  Horsham, West Sussex, RH12 1RD

- *Telephone:*

  01403 214200

- *Email:*

  dpo@inpartnership.net