NEWGATE COMPLIANCE

NEWGATE NEWS

UP TO DATE COMPLIANCE NEWS FOR
FIRMS IN THE FINANCIAL SERVICES SECTOR

Newgate Compliance Limited
20 Ropemaker Street
London. EC2Y 9AR
Phone: +44 (0)20 3696 8750
Email: info@newgatecompliance.com

The General Data Protection Regulation – Are you Ready?

With MiFID II fully implemented many firms' attention is understandably now being focused on ensuring that they are ready for the next regulatory change on the horizon, namely The General Data Protection Regulation ("GDPR") 2018.

GDPR comes into force on the 25th May 2018 and is being introduced as an update to personal data privacy laws across all EU member states and replaces the Data Protection Directive 95/46/EC. GDPR governs the processing, such as the use or holding, of personal data, which is essentially any information about identifiable living individuals. This also gives those individuals certain rights and remedies in respect of that information.

In February 2018 the Information Commissioners Office ("ICO"), as the supervisory Authority who will be enforcing GDPR, and the FCA published a joint update out that compliance with GDPR is now a board level responsibility. Firms must be able to produce evidence to demonstrate the steps that they have taken to comply. Both the FCA and ICO recognised that there will be ongoing discussions to ensure specific details of the GDPR can be implemented consistently within the wider regulatory landscape.

The FCA up until this point, had remained relatively quiet publicly on GDPR, however they have clearly stated that a firm's compliance with the GDPR requirements is something the FCA will consider under their rules. Again, citing governance as being a crucial aspect, the FCA state that areas such as The Senior Management Arrangements, Systems and Controls (SYSC) module is one example of an area impacted with firms being required to establish, maintain and improve appropriate technology and cyber resilience systems and controls.

Although not strictly a traditional role of the compliance function within financial services firms, we do recognise the impact that this new regulation will have across all firms range of services and internal procedures. Consequently, we stand ready to help.

NEWGATE COMPLIANCE

NEWGATE NEWS

UP TO DATE COMPLIANCE NEWS FOR FIRMS IN THE FINANCIAL SERVICES SECTOR

Newgate Compliance Limited
20 Ropemaker Street
London. EC2Y 9AR
Phone: +44 (0)20 3696 8750
Email: info@newgatecompliance.com

Preparing for GDPR

The following are key areas you should be looking to address and in which Newgate is happy to provide assistance:

Accountability and Governance: As we have already touched on, governance is going be crucial under GDPR. The ICO can implement fines against firms found to have breached GDPR which depending on the seriousness, duration, and nature of infringement can be severe. A two-tiered sanction regime is applied:

- Up to €20 Million or 4% of global annual turnover for the preceding financial year, whichever is the greater;
- Up to €10 Million or 2 % of global turnover, whichever is greater.

The governing bodies of firms therefore need to have in place proportionate but robust policies and procedures to address all of its obligations. This may also include staff training, internal audits of processing activities, and reviews of internal HR policies.

Contracts: Data controllers who use data processors need to have a written contract in place. This contract is to ensure both parties understand their responsibilities and liabilities. This is no longer a way of demonstrating compliance with data protection laws, but a general requirement under GDPR and all firms should be looking to review and update data contracts, as there are specific aspects which must be addressed.

Data Protection Officer: As a firm that processes personal data, for example KYC Anti-Money Laundering Information, you will already be registered with the ICO as a Data Controller and may even have registered a Data Protection Officer for your firm. Although appointing and registering a DPO is not an essential requirement for all firms we believe it to be good practice and governance to do so.

Data Protection Impact Assessments: Under GDPR, Data Protection Impact Assessments ("DPIA") are an essential compliance tool which are primarily aimed at identifying risks relating to personal data. It is mandatory that a DPIA is undertaken when designing or modifying a process that involves the processing of personal information. Examples of areas where a DPIA must be carried out are:

- Changes to customer KYC and suitability checks;
- Changes to marketing processes;
- Changes to storage procedures or systems;
- Changes to internal HR administrative procedures.

Newgate Compliance Limited
20 Ropemaker Street
London. EC2Y 9AR
Phone: +44 (0)20 3696 8750
Email: info@newgatecompliance.com

We believe that all firms should be looking to undertake a DPIA to review how, where, when and on who they hold personal data. This will give firms a refreshed and clear understanding of the risks that a firm faces and allow your firm to put in place a programme of work to address them.

Identify the Lawful Basis you use for Processing Personal Data: For processing of personal data to be lawful under GDPR, firms will need to identify a lawful basis before it is able to process personal data and it is vitally important that documentation is held to support this. There are 4 key areas which you are likely to rely on in lawfully processing personal data:

- Processing takes place with the **explicit consent** of the Data Subject;
- Processing is necessary for the **performance of a contract** or to take steps to enter into a contract;
- Processing is necessary for compliance with a **legal obligation**;
- Processing is necessary for the purpose of **legitimate interests** of the firm, EXCEPT where such interests are overridden by the interest, rights, or freedoms of the data subject.

Subject Access Requests: Under GDPR a key right of individuals data subjects is that of being able to learn and have access to what personal information is held on them and by whom. This is known as a subject access request ("SAR"). Firms will need to have procedures in place to identify and deal with subject access requests, as in the main, responses are required without delay and at the latest within one month of receipt.

Sharing Data and Cross Border Transfers: If as a firm you share personal data with third parties it is vital that the lawful basis for doing so is identified. DPIAs will be crucial in identifying processes within your firm which this impacted by this and it is vitally important that documentation is held to support this. There are no restrictions on sharing personal data between EEA member states, however GDPR has imposed greater restrictions on the transfer of personal data outside the EU. Again, the completion of a DPIA will help identify areas of risk and help you address the extra requirements firms will need to meet.