Strafford

Presenting a live 90-minute webinar with interactive Q&A

Compliance With New EU GDPR: Steps Investment Funds, Banks, Advisers and Financial Intermediaries Should Take Now

Revising Service Agreements and Internal Controls; Enhanced Disclosures, Higher Penalties

WEDNESDAY, APRIL 25, 2018

1pm Eastern | 12pm Central | 11am Mountain | 10am Pacific

Today's faculty features:

Gretchen E. Scott, Partner, **Goodwin Procter**, London

Kelly McMullon, Atty, **Proskauer Rose**, London

The audio portion of the conference may be accessed via the telephone or by using your computer's speakers. Please refer to the instructions emailed to registrants for additional information. If you have any questions, please contact **Customer Service at 1-800-926-7926 ext. 1**.

Tips for Optimal Quality

FOR LIVE EVENT ONLY

Sound Quality

If you are listening via your computer speakers, please note that the quality of your sound will vary depending on the speed and quality of your internet connection.

If the sound quality is not satisfactory, you may listen via the phone: dial **1-888-450-9970** and enter your PIN when prompted. Otherwise, please **send us a chat** or e-mail **sound@straffordpub.com** immediately so we can address the problem.

If you dialed in and have any difficulties during the call, press *0 for assistance.

Viewing Quality

To maximize your screen, press the F11 key on your keyboard. To exit full screen, press the F11 key again.

Continuing Education Credits

FOR LIVE EVENT ONLY

In order for us to process your continuing education credit, you must confirm your participation in this webinar by completing and submitting the Attendance Affirmation/Evaluation after the webinar.

A link to the Attendance Affirmation/Evaluation will be in the thank you email that you will receive immediately following the program.

For additional information about continuing education, call us at 1-800-926-7926 ext. 2.

Program Materials

FOR LIVE EVENT ONLY

If you have not printed the conference materials for this program, please complete the following steps:

- Click on the ^ symbol next to “Conference Materials” in the middle of the left-hand column on your screen.
- Click on the tab labeled “Handouts” that appears, and there you will see a PDF of the slides for today's program.
- Double click on the PDF and a separate page will open.
- Print the slides by clicking on the printer icon.

GDPR Compliance for Investment Funds Industry

Presented by:

Kelly McMullon

kmcmullon@proskauer.com

Gretchen Scott

gscott@goodwinlaw.com

25 April, 2018

GOODWIN

Proskauer

Today's Presenters

Kelly McMullon is an associate in the Labor & Employment Law Department and member of the International Labor & Employment Group and Privacy & Cybersecurity practices at Proskauer Rose.

Kelly assists clients in a wide range of contentious and non-contentious employment law matters. She also assists multinational organisations to understand their data privacy obligations in the UK and across Europe with a particular focus on employee data matters including regarding lawful data processing, the use of social media and covert recordings. She helps corporate clients across a range of sectors including asset management, hospitality, retail and information technology.

She is currently assisting many clients in becoming compliant with the General Data Protection Regulation, which comes into force in May 2018.

Gretchen Scott is a partner in Goodwin's Business Law Department and a member of the Strategic Technology Transactions and Licensing Group and Privacy + Cybersecurity Group.

Ms. Scott's technology transactions practice is sector agnostic and reaches across key industry verticals, such as software and SaaS, e-commerce, hardware and equipment, IT services, consumer goods, clean tech and energy and fintech.

She focuses on technology transfer and the exploitation of intellectual property rights, as well as on data protection compliance, including the GDPR and ePrivacy Directive, and on specialist commercial contracts involving distribution, agency and franchising. Ms. Scott also advises on intellectual property, IT and data protection issues in joint ventures, mergers, acquisitions and venture capital and private equity transactions.

General Data Protection Regulation (GDPR)

- **Enters into full force 25 May 2018**
- **Applies** to businesses that “process” EU personal data
- **Harmonizes** EU data protection law
- **Impacts**:
  - Expanded data governance obligations for businesses
  - New rights for data subjects
  - Expanded territorial application
  - New obligations for processors
- ***Threshold Question***: Is your fund structure subject to the GDPR?
- **Fines**, big ones: **up to €20m or 4%** of global annual revenues

Territorial Scope of the GDPR

- Two ways to be caught by the GDPR:
  - Processing of personal data in the context of activities of an **establishment** of a **controller or processor in the EU**.
  - Controllers and processors **not established in the EU** but where that organisation:
    - **Offers goods or services** to data subjects in the EU; and/or
    - **Monitors** data subject's EU behaviour.

- Coverage by the GDPR generally depends more on who the organization is, what it does, and where, than on who the data subject is.

Controller or Processor?

- **Data Controller**
  - Fund entity, GP, Manager?; employer
  - Makes decisions about how data is to be used/processed
  - Instructs Data Processor via Data Processing Agreement
  - Liable for compliance, including Processor compliance
- **Data Processor**
  - Service Provider – Manager, Administrator, Depository…
  - Acts pursuant to Controller's instructions in Data Processing Agreement
  - Less onerous liability under GDPR but Controllers flow down their obligations contractually
- **Joint Controllers?**
  - "acting together"

Compliance Snapshot

Controller's Obligations

1. Transparency (Privacy Policy)
2. Comply with Individuals' Rights
3. Legal Basis For "Processing"
4. Core Privacy Principles
5. Privacy Impact Assessments
6. Consultation with DPAs

Controller's & Processor's Obligations

1. Data Processing Contract
2. Record Keeping
3. Lead DPA
4. Security measures
5. DPO & EU Representative
6. Cross-border transfers
7. Cooperation with DPAs
8. Data Breach Notification

Lawful Basis for Processing

- In order to process data, an organisation must have a valid and prescribed legal basis, including:
  - Necessary for the **performance of a contract** to which the data subject is a party, e.g. a Subscription Agreement.
  - Necessary for compliance with a **legal obligation**, e.g. AML checks.
  - Necessary for the **legitimate interests** pursued by the data controller or a third party except if overridden by the interests/rights of the data subject.
  - **Consent**.

- Generally, processing activities for one specific purpose cannot be based on multiple bases.

Privacy Notices

- Data subjects have a **right to be informed** about how their data is being processed.
- Notice should contain certain information including:
  - Controller or Representative Information
  - Purposes of Processing and Legal Basis
  - Transfers to Third Countries
  - Retention Periods
  - Data Subject Rights
- Notice to be in clear, intelligible and plain language. Easily accessible form.

- ***TO DO:***
  - Check Privacy Notice/Policy for compliance with GDPR.
  - Associated internal policies (e.g., data retention, data security, etc.) will also need to be reviewed for GDPR compliance.

Data Security, Data Breach

- *Implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk*
- **Controllers**
  - Notify DPAs **within 72 hours** of awareness if breach is likely to result in "**risk**" to individuals
    - Who? DPA of the EU establishment or "main establishment"
  - Notify data subjects if the breach may result in "**high risk**"
- **Processors**
  - Must notify Controllers "**without undue delay**"
- ***TO DO:***
  - Review incident management & response plans; vendor agreements; cyber risk insurance policies, employee training
  - Consider impact of global mandatory notification laws (e.g., US, Mexico, Australia)

International Transfers

- GDPR has not greatly changed the obligations with respect to international transfers. Transfers are still prohibited unless they fall under an exception.
- Options to transfer personal data from the EU to US transfers include:
  - Binding Corporate Rules
  - Standard Contractual Clauses
  - Privacy Shield
- US organisations will also find that EU organisations seek to include certain processing clauses into agreements which are required by the GDPR when personal data is shared.
- ***TO DO:***
  - Check method of international transfer. If none in place, consider best approach given type of data, who it is being sent to, whether it is a one off transfer etc.

Data Processing Agreements

- Data Processing Agreements
  - Mandatory minimum requirements
    - Process on instructions of Controller
    - Restrictions on sub-processing
    - Delete or return data
    - Appropriate security measures
    - Confidentiality obligations
    - Assist with appropriate technical and organisational measures
    - Assist with data breach, DPIA and regulatory consultation obligations
    - Information provision and audit rights
  - Super-processors
  - Liability risk

Joint Controller Arrangements

- “Arrangement” to determine respective responsibilities for compliance
- Transparent
- Available to data subjects
- Data Subject can exercise rights against either Controller

Data Subject Rights

- Data subjects have a number of rights but these only apply in certain cases:
  - Right of access (Data Subject Access Requests)
  - Right to rectification
  - Right to erasure
  - Right to data portability
  - Right to restrict processing
  - Right to object
  - Right related to automated decision-making including profiling
- Rights will be exploited in litigious circumstances.
- ***TO DO:***
  - Review and updated protocols for addressing data subject complaints, objections, and requests.

Data Protection Officers: Controller and Processors

- Mandatory if “core activities” involve:
  - “Large-scale” “regular and systematic **monitoring**
  - “Large-scale” processing of **sensitive data** or **criminal offence data**
- Role: counsel and monitor GDPR compliance, cooperate with DPAs
- Staff member or external service provider (“expert” knowledge)
- “Independent”
  - No instructions, no dismissal for performing DPO tasks
  - No conflict of interest (e.g., CFO, head of HR or IT)

- ***TO DO*:**
  - Document the internal analysis for decision whether to appoint a DPO
  - Develop policies that set out when the DPO must be consulted

EU Representative: Controller and Processors

- Mandatory if not established in the EU
- Limited exceptions
- Located where data subjects are based
- Mandated “to be addressed” by supervisory authorities and data subjects
- Subject to enforcement proceedings for Controller/Processor breach

Data Governance

- Data Protection Impact Assessment (DPIA):
  - Assessment to consider the nature, scope, context, purpose, type and use of new types of processing of personal data.
  - Mandatory where processing is “likely to result in a high risk to the rights and freedoms of natural persons”.
- Privacy by Design
  - Consider privacy at the initial design stages and throughout the complete development process of new products, processes or services.
- Privacy by Default
  - Default setting should be the most privacy friendly ones.

- ***TO DO:***
  - Consider business areas where DPIAs are relevant.
  - Consider putting in place template DPIA.
  - Put in place training to cover privacy by design and privacy by default principles

Accountability

- Controller responsible for compliance with core processing principles:
  - Lawfulness of processing
  - Transparency; choice
  - Purpose limitation
  - Data minimization
  - Accuracy
  - Data integrity
  - Storage limitation
  - Confidentiality
- Demonstrate compliance
  - Implement technical and organisational measures (training, policies and audits)
  - Document everything
  - DPO?
  - data minimisation, pseudonymisation, transparency, “state of the art” security
  - Consider data protection impact assessments

Enforcement – Who?

- **Data Subjects:**
  - May complain to a Data Supervisory Authority or seek judicial redress; and
  - Have the right to compensation for material or non-material damage.
- **Civil liberties organizations:**
  - Could bring claims on behalf of individuals.
  - Dawn of class action suits in the EU?
- **Data Supervisory Authorities**:
  - Can act on tip offs (e.g. hotlines); and
  - Can carry out audits on organisations.

Enforcement – What?

- Factors when Data Supervisory Authorities consider fines include:
  - Nature, gravity, duration of infringement
  - Intention or negligent
  - Actions taken to mitigate damage
  - Degree of responsibility
  - Previous infringements
  - Degree of cooperation
  - Categories of data
  - Manner in which infringement known
  - Other aggregating or mitigating factors

- Reprimands and enforcement orders may be ordered instead of fines.