afme/ Finance for Europe

Association for Financial Markets in Europe

AFME Member Briefing

GDPR Compliance in Financial Services

28 February 2018

Richard Middleton, Co-Head Policy Division, AFME
Richard Jones, Director of Data Policy, Clifford Chance
Nathan Coffey, EMEA Head of Data Privacy and Technology Compliance, JPMorgan
Nicola Kerr-Shaw, Head of IP, Technology and Procurement, CIB Legal, BNP Paribas

afme/ Finance for Europe

Association for Financial Markets in Europe

Introduction

Richard Middleton, Co-Head Policy Division, AFME

CLIFFORD

CHANCE

GDPR COMPLIANCE

AFME MEMBERS' BRIEFING CALL – 28 February 2018

INTRODUCING THE GDPR
WHAT IS THE GDPR?

- An EU Regulation – takes direct effect in each EU member state from 25 May 2018
  - the GDPR does not need to be implemented by national laws
  - however national laws will be passed to make additional rules, exceptions, etc.
  - the legal position will be much more closely harmonised across the EU than under the current law, but there will still be variations
- Preserves all the key features of the existing regime
- Severe sanctions
- Tightening of existing rules
- New requirements for “accountability”
- Changes in geographical application (“extra-territorial effect”)
- Local variations

KEY FEATURES OF THE EXISTING REGIME
… PRESERVED BY THE GDPR

- Regulates “processing” of “personal data” by “controllers” (or “processors” on their behalf)
- All processing must be justified by meeting one of a series of specified conditions
- All processing must comply with various data protection principles
  - fairness, proportionality, time limitation, security, etc.
- Individuals must be given information about the processing of their personal data
- Individuals have rights which they can exercise against controllers
  - access, correction, objection, etc.
- Transfer of personal data to countries outside the EEA, with lower data protection standards, is restricted

THE GDPR
SANCTIONS

- Preserves and enhances a range of sanctions available under the current regime:
  - audit by data protection authorities
  - orders requiring remediation
  - compensation through the courts, with a new right for non-profit organisations to bring “class actions”
- Very severe fines for non-compliance
  - Maximum fines set at:
    - higher of EUR 20 million and ***4% of global group turnover*** for infringement of some requirements (e.g. unjustified processing)
    - higher of EUR 10 million and ***2% of global group turnover*** for infringement of other requirements (e.g. failure to meet required security standards)

THE GDPR
TIGHTENING THE EXISTING RULES

1. Legitimacy and Consent

- As in the current regime, all processing of personal data must meet one of the conditions specified in the law. The available conditions are largely unchanged.
- However it is much harder to rely on ***consent***:
  - as under current law, consent must be "freely given" – the GDPR spells out that:
    - consent can be withdrawn at any time, and this must be pointed out when the consent is obtained
    - consent will not be effective where there is an imbalance of power – so an employer can rarely rely on consent to justify processing of employee data
      - *consent will only be appropriate for **genuinely optional** processing*
  - as under current law, consent must be "informed" – the GDPR stresses the need for full and detailed supporting information and effective choices
  - records must be kept of all consents
- In practice, firms will rarely be able (or need) to rely on consent and will instead need to look to "legitimate interests" and the other conditions. This requires careful consideration of the need for processing and how the interests of the data subject are protected.

2. Transparency

- As in the current law, firms must proactively provide information to employees and other data subjects about its processing of their personal data.
- The GDPR is much more specific as to the information to be provided – a long list of items of information must be provided, even where relatively trivial personal data are collected
  - *e.g. explanation of legal basis for processing; information on international transfers and safeguards protecting transferred data; right to complain to data protection authority…*

  Specific issues:
  - **How granular does the information really need to be?**
  - **New privacy notices to data subjects whose personal data are already held?**
  - **What about individual contacts at corporate suppliers and customers?**

3. Security

The basic security standard is essentially unchanged, however:

- new and strict **security breach notification** requirements (reporting to data protection authority and sometimes also to data subjects)
- complex and prescriptive requirements as to the terms on which firms contract with their processors (service providers)

Specific issues:

- **Re-papering existing service providers**
- **Breach response plans**

4. Automated decision-taking

Very tight restrictions on use of automated decision-taking techniques:

- Use without consent must be authorised by law or necessary for entering into or performing a contract
- Very tight restrictions on application to sensitive data

5. Data Subject Rights

Data subjects have enhanced rights which they can exercise against firms:

- subject access – broadly similar to the current regime
- withdrawal of consent at any time (*so firms should avoid reliance on consent*)
- objection – the onus will be on a firm to demonstrate its compelling, legitimate interests
- erasure / to be forgotten / restriction – very limited rights in practice
- "portability"
  - the right to take away copies of certain data in machine-readable format
  - of limited application outside the retail context: only applies to personal data provided by the data subject and processed based on consent or necessity for performance of a contract

THE GDPR
NEW REQUIREMENTS

“Accountability”

The spirit of the GDPR is that controllers and processors should not only comply with specific rules, they should also be able to demonstrate the efforts that they have made to comply – that they are taking responsibility for compliance.

Mandatory requirements include:

- implement appropriate measures to ensure compliance
- build data protection principles into the design and procurement of systems
- conduct data protection impact assessments before implementing “high-risk” processing arrangements
  - but in practice, at least a basic “legitimate interests” assessment will generally be necessary even where the risks are not high
  - in extreme cases it may be necessary to consult data protection authorities
- in some circumstances, appoint data protection officers
- keep a record of processing of personal data (and records of consents obtained)

THE GDPR
EXTRA-TERRITORIAL EFFECT

When does the GDPR apply?

- Processing in the context of the activities of an EU establishment
  - as in current regime
  - applies some requirements to processors as well as controllers
- Processing related to:
  - offering goods or services to data subjects in the EU
    - ***offering*** not ***providing***
    - only if ***targeted*** at the EU or a member state
  - monitoring behaviour of data subjects in the EU

    e.g. cookies – potentially very broad

Note: does not apply merely because processing is carried out on equipment in the EU – in this respect the GDPR is narrower in scope than the current regime.

THE GDPR
LOCAL VARIATIONS

Key areas in which the GDPR anticipates variations between EU member states:

- **HR processing** – *the GDPR allows member states to impose additional rules*
- **Data protection officers** – *the GDPR requires appointment of a DPO only in relatively narrow circumstances, but allows the EU member states to require appointment of a DPO in wider circumstances*
- **Sensitive personal data** – *the member states are essentially left to set the rules on processing of personal data in particularly sensitive categories (e.g. health, criminal record)*

In most member states, the national laws are not yet in final form (one exception: Germany), but drafts have been published.

THE GDPR
KEY COMPLIANCE STEPS THAT FIRMS ARE TAKING (1)

- Consider when and where the GDPR applies to the firm's business
  - processing audit and gap analysis
  - identify high risk processing
  - prepare record of processing
  - provide for regular refresh
- Justification strategy
  - review and document legal basis for all processing
  - is a formal impact assessment required?
  - particular focus on consent: move to another legal basis or re-visit / re-draft consent forms
  - document results

THE GDPR
KEY COMPLIANCE STEPS (2)

- Accountability
  - review security and “IT readiness”, including breach readiness
  - update data protection policies
  - communications and training
  - assess need for DPO / appoint
- Transparency
  - address transparency in internal policies
  - develop / update notices for key constituencies (clients / employees / web visitors / etc.)
  - consider “re-papering” issues
- Outsourcing management
  - develop standard forms and supporting checklists / playbooks
  - identify key relationships
  - approach and negotiate

THE GDPR
KEY COMPLIANCE STEPS (3)

- International data transfers
  - review and adjust current strategy
  - intra-group (framework agreement / binding corporate rules?)
  - extra-group (service providers – model clauses / privacy shield)
  - extra-group (other – case-by-case consideration)
- Data subject rights
  - strategy for responding to new exercise of data subject rights
  - where is the firm dependent on consent that might be withdrawn?
  - IT readiness for production / deletion / correction / etc.
- “Local” issues
  - strategy for taking account of local variations

THE GDPR
SOME DIFFICULT ISSUES FOR FIRMS

- Record of processing – how granular?
- IT issues – pro-active deletion / archiving, response to data subject rights, privacy by design, security
- Potential tension between GDPR and need to process for regulatory, crime prevention and similar purposes
- Specific issues with processing of criminal record and other sensitive data and use of automated decision-taking techniques
- Re-papering of large numbers of service providers
- Transparency requirements / re-papering of corporate customers?

ANNEX: BASIC DATA PROTECTION CONCEPTS IN THE CURRENT EU REGIME

THIS ANNEX SUMMARISES BASIC REQUIREMENTS OF EU DATA PROTECTION LAW THAT ARE KEPT IN PLACE BY THE GDPR

1. Scope and Definitions

- EU data protection laws protect the privacy of individuals where their personal data are processed
  - current EU data protection laws are based on the EU Data Protection Directive of 1995 – there is already a degree of consistency across the EU
- They regulate the "processing" of "personal data" by "controllers" and "processors"
  - "personal data" – information relating to identifiable individuals ("**data subjects**")

    e.g.: individual clients, employees, individual representatives of corporate customers / suppliers / regulators / etc., website visitors, visitors to premises
  - "processing" – collection, storage, use, disclosure, deletion – anything at all
  - "controller" – the responsible entity, usually a company – determines purposes and means of processing

    e.g. a firm providing financial services and/or employing people
  - "processor" – an entity processing personal data on behalf of the controller

    e.g. a third party or "captive" service provider providing support services to a firm

2. Legitimacy

All processing of personal data must be justified by meeting a condition set out in the law, e.g.:

- consent
- necessity for performance of a contract with the data subject (*e.g. to pay interest to an individual client*)
- necessity for performance of a legal obligation (*e.g. AML record-keeping, or tax reporting*)
- the firm's legitimate interests, balanced against those of the data subject

Processing of data in certain sensitive categories (e.g. health data) must meet an additional, narrower, condition (e.g. explicit consent, necessity for employment law reasons)

3. Data Protection Principles

- Transparency: data subjects to be informed about the processing of their personal data
- Processing must be proportionate and time-limited
- Personal data must be secure
  - requirement for “appropriate” technical and organisational measures to protect personal data
  - appointment of a processor
    - security due diligence to be performed
    - relationship to be governed by a written agreement imposing basic data security obligations
    - compliance to be checked over time

4. Data Transfer Restrictions

- Free movement of personal data within the EU
- Free transfer to countries ensuring “adequate” protection for personal data
  - *e.g. Switzerland, U.S. “privacy shield” scheme*
- Otherwise, transfers restricted except in limited circumstances, e.g.:
  - consent
  - approval by data protection authority
    - *European Commission’s standard contractual clauses*
    - *intra-group “binding corporate rules” (but CLNS does not have an approved BCR scheme)*
    - *public interest justifications*

5. Data Subject Rights

Data subjects can exercise rights against the controller

- "subject access" – right to a copy of their data
- correction of inaccurate personal data
- objection
  - an absolute right to object to direct marketing

    (note that there is a separate EU regime on direct marketing by electronic means)
  - otherwise, objection on "compelling, legitimate grounds"
- the courts also acknowledge a "right to be forgotten", based on the right to object and the time-limitation principle

CLIFFORD

CHANCE

ANY QUESTIONS?

afme/ Offices

Finance for Europe

The Association for Financial Markets in Europe (AFME) is the voice of all Europe's wholesale financial markets, providing expertise across a broad range of regulatory and capital markets issues.

We advocate for deep and integrated European capital markets which serve the needs of companies and investors, supporting economic growth and benefiting society.

London
39th Floor
25 Canada Square
London, E14 5LQ
United Kingdom

Tel: +44 (0)20 3828 2700

Brussels
Rue de la Loi 82
1040 Brussels
Belgium

Tel: +32 (0)2 788 3971

Frankfurt
Skyper Villa
Taunusanlage 1
60329
Frankfurt am Main
Germany

Tel: +49 (0)69 5050 60 590

www.afme.eu