Other regulation affecting the advice process

LEARNING OBJECTIVES

In this topic we are going to look at other important legislation and regulations that affect the advice process. Some, such as the UK General Data Protection Regulation (UK GDPR), are relevant to everyone working in the sector, while others, such as the Directives on life and general insurance, relate to specific areas of business. Many laws and regulations that originated from the EU were maintained on the UK statute books (ie 'onshored') as part of Brexit, but some were amended (and will be further amended in the future following the introduction of the Financial Services and Markets Act 2023).

By the end of this topic, you should have an understanding of:

- the provisions of the UK General Data Protection Regulation (UK GDPR), including the data protection principles;
- how the UK GDPR is enforced;
- the role of the Pensions Regulator and the Pension Protection Fund;
- the Markets in Financial Instruments Directives (MiFID I and II);
- Undertakings for Collective Investment in Transferable Securities (UCITS) Directive and Alternative Investment Fund Managers Directive (AIFMD);
- directives relating to life and general insurance;
- the role of oversight groups.

This topic covers the Unit 2 syllabus learning outcomes U5.6, U6.1–U6.3, part of K2.1, K2.4, K3.1 and 3.2.

THINK . . .

The aspect of this topic that is likely to be most familiar to you is data protection. Occasionally there are reports in the media about serious breaches of data protection legislation by companies and government departments. The fact that such breaches make the news indicates how serious they are considered to be.

Before you start working through this topic, think about:

- the kind of personal data you have to provide every time you buy a product online, apply for a job or take out any kind of contract, such as a mobile phone contract;
- what assurances you recall from the other party about how they will keep your personal data secure;
- what the implications for you might be if that data became available to fraudsters.

24.1 What are the rules relating to data protection?

Interacting with a financial services institution inevitably involves the customer providing personal information; in Topic 23, for example, we looked at the process of customer due diligence, which requires the customer to prove their identity in order to complete a transaction. If such information is not handled appropriately and stored securely, then not only does the firm breach the customer's right to privacy, it also exposes the customer to the risk of becoming a victim of crime as a result of identity theft.

IDENTITY THEFT

Personal data is valuable to fraudsters. Details such as an individual's name, address and date of birth – sometimes pieced together and supplemented from a number of sources – can be used to open bank accounts, take out credit cards, order goods, take over the victim's original accounts or apply for key documents such as a passport or driving licence. The latter items can then be used to facilitate further criminal activity.

The prevention of fraud arising from identity theft falls within the remit of the FCA, as part of its objectives to reduce financial crime and enhance consumer protection.

FACTFIND

If you are interested in finding out more about how the FCA seeks to combat fraud, go to:

www.fca.org.uk/firms/financial-crime/fraud

Until May 2018, the EU data protection legislation was the Data Protection Directive of 1995. The primary UK legislation in relation to data protection was the Data Protection Act 1998.

To update the EU legislation, particularly in relation to online activity and the rise of social media, a General Data Protection Regulation came into force in May 2016 and each EU member state was required to adopt its provisions by 25 May 2018. The primary UK legislation became the Data Protection Act 2018.

CHECK YOUR UNDERSTANDING 1

Think back to your previous work on EU Directives and regulations. What impact does the fact that the EU data protection legislation is in the form of a regulation rather than a Directive have upon the way it is implemented by member states?

24.1.1 The General Data Protection Regulation

On 25 May 2018, the General Data Protection Regulation (GDPR) came into effect in the UK. It applies to 'personal data', which is information relating to an individual who can be identified (for example, by name, identification number, location data or online identifier). This reflects changes in technology and the way information is collected.

The GDPR applies to both automated personal data and to manual records containing personal data. The provisions of the GDPR were retained in UK Law as 'UK GDPR' at the end of the Brexit transition period.

24.1.2 What are the data protection principles?

The basis of the UK GDPR is a set of six data protection principles, which all relate to the processing of personal data. The data must be:

1) Processed lawfully, fairly and in a transparent manner in relation to individuals.

2) Collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall not be considered to be incompatible with the initial purposes.

3) Adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed.

4) Kept accurate and up to date. Every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay.

5) Kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed, although archiving is allowed in certain circumstances.

6) Processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures.

24.1.3 UK GDPR requirements

Some of the relevant definitions are as follows:

- **Data subject** – an individual (a natural person) whose personal data is processed.
- **Personal data** – information that can directly or indirectly identify a natural person. This information can be in any format.
- **Special categories of personal data** – this data is more sensitive and so needs more protection. Generally (although there are exceptions) such data can only be processed if the individual has given explicit consent. Sensitive data includes information about an individual's:
  - race;
  - religious beliefs;
  - political persuasion;
  - trade union membership;
  - sexual orientation;
  - health;
  - biometric data;
  - genetic data.
- **Processing** – this has a very broad meaning, covering all aspects of owning data, including:
  - obtaining the data in the first place;
  - recording of the data;
  - organisation or alteration of the data;
  - disclosure of the data, by whatever means;
  - erasure or destruction of the data.
- **Data controller** – this is the 'legal' person who determines the purposes for which data are processed and the way in which this is done. The data

controller is normally an organisation/employer, such as a company, partnership or sole trader. They have prime responsibility for ensuring the data protection requirements are adhered to.

- **Data processor** – this is a person who processes personal data on behalf of the data controller.

An organisation must have a lawful basis for processing data. At least one of the following must apply when processing personal data.

1) Consent – clear consent has been given by the individual to process their personal data for a specific purpose.
2) Contract – the processing is necessary for a contract between the organisation and the individual, or because the individual has asked for certain steps to be taken before entering into a contract.
3) Legal obligation – the processing is necessary for the organisation to comply with the law.
4) Vital interests – the processing is necessary to protect someone's life.
5) Public task – the processing is necessary for the organisation to act in the public interest.
6) Legitimate interests – the processing is necessary for the organisation's legitimate interests or the legitimate interests of a third party, unless there is a good reason to protect the individual's personal data which overrides those legitimate interests.

A data subject has a number of rights, including the right to:

- access personal data through subject access requests (under UK GDPR, no charge can generally be made for this);
- correct inaccurate personal data;
- have personal data erased, in certain cases;
- object;
- move personal data from one service provider to another.

In order to demonstrate compliance with the UK GDPR, an organisation must:

- establish a governance structure with roles and responsibilities;
- keep a detailed record of all data processing operations;
- document data protection policies and procedures;
- carry out data protection impact assessments for high-risk processing operations.

The UK GDPR contains rules on the transfer of personal data to receivers located outside the UK that are separate controllers or processors. These rules apply to all transfers, no matter the size of transfer or how often they are carried out. Only the controller or processor who initiates and agrees to the transfer is responsible for complying with the UK GDPR rules on restricted transfers. A restricted transfer can be made if the receiver is located in a third country or territory, is an international organisation, or is in a particular sector in a country or territory covered by UK 'adequacy regulations'.

FACTFIND

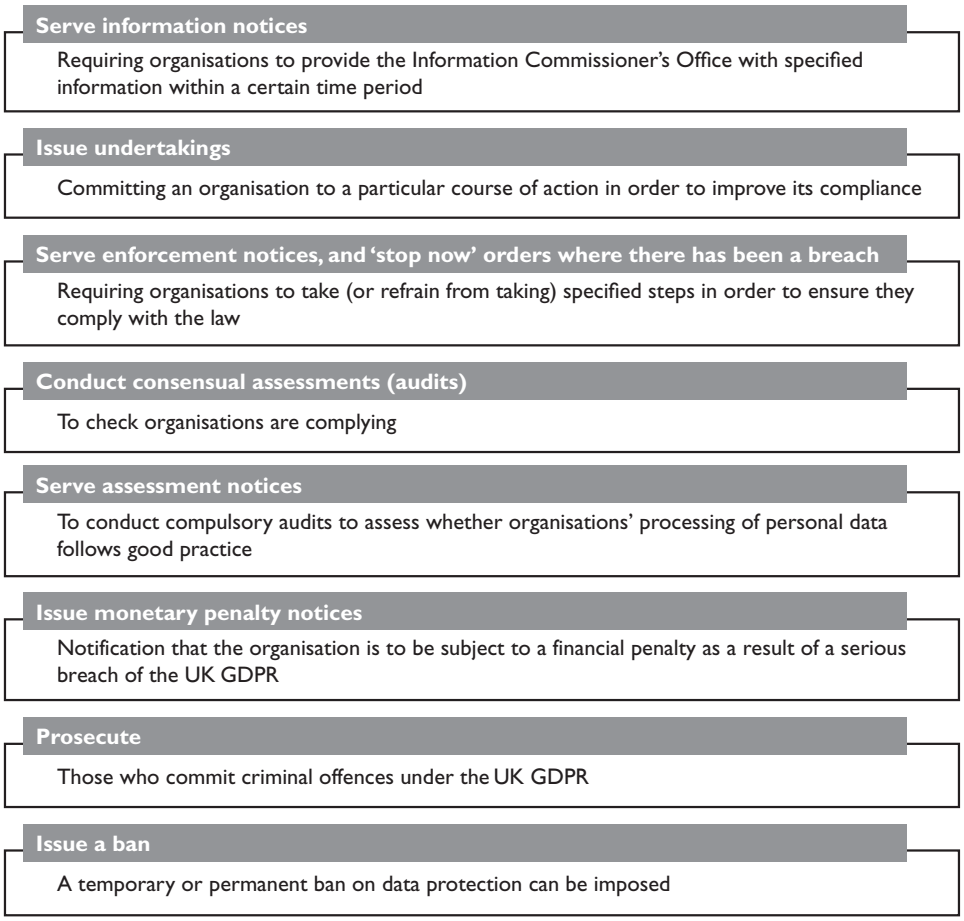
To find out more details about the UK General Data Protection Regulation go to:

ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/

24.1.4 How is the UK GDPR enforced?

The Information Commissioner is responsible for overseeing the application of the UK GDPR. Firms should report significant personal data breaches to the Information Commissioner. There are several courses of action the Commissioner can take if there has potentially been an infringement of the terms of the Regulation (see Figure 24.1).

FIGURE 24.1 INFORMATION COMMISSIONER'S POWERS TO ENFORCE UK GDPR



CRIMINAL OFFENCES UNDER THE UK GDPR

The following are criminal offences.

- For a data controller to fail to comply with an information or enforcement notice.
- Failure to make a proper notification to the Information Commissioner. 'Notification' is the way in which a data controller effectively registers with the Information Commissioner's Office by acknowledging that personal data are being held and by specifying the purpose(s) for which the data are being held.
- Processing of data without authorisation from the Commissioner.

- Intentionally or recklessly re-identifying individuals from data that is pseudonymised – it can no longer be attributed to a specific person without the use of additional information, which is kept separately – or anonymised – it does not relate to a natural person or has been processed so the data subject cannot be identified (ICO, no date).

The maximum penalty is the higher of £17.5m or 4 per cent of an organisation's total annual worldwide turnover in the previous financial year.

24.2 What is the role of the Pensions Regulator?

The regulation of work-based (ie occupational) pension schemes remains separate from the regulation of other financial services – separate even from the regulation of private pension arrangements such as personal pensions and stakeholder pensions. Nevertheless, financial advisers should have a good knowledge of matters relating to work-based schemes, in order, for instance, to be able to advise individuals who are members of such schemes or employers who may be considering establishing a scheme.

The Pensions Regulator (TPR) is responsible for the regulation of work-based pension schemes (as well as some personal pension schemes), and it aims to:

- ensure employers enrol their staff onto a work-based pension scheme (known as 'automatic enrolment');
- protect the benefits of a work-based pension scheme, as well as people's savings;
- protect the benefits of personal pension schemes where there is a direct pay arrangement;
- promote good administration of work-based schemes, as well as people's savings;
- reduce the risk of situations arising that might lead to claims for compensation from the Pension Protection Fund (see section 24.3);
- maximise employer compliance with duties and safeguards under the Pensions Act 2008;
- minimise any adverse impact on the sustainable growth of an employer (TPR, 2024).

The Pensions Regulator aims to identify and prevent potential problems rather than to deal with problems that have arisen, and takes a risk-based approach

to its work. It assesses the risks that might prevent it from meeting its statutory and operational objectives, such as inadequate funding, inaccurate record-keeping, lack of knowledge or understanding on the part of the trustees, or even dishonesty or fraud. The regulator considers the combined effect of:

DIRECT PAY ARRANGEMENT

A direct pay arrangement is one where the employer collects an employee's pension contributions from their gross salary and pays them over to the pension provider.

- the likelihood of the event occurring; and
- the impact of the event on the scheme and its members.

Schemes that are judged to have a higher risk profile will be more closely monitored than those that represent a lower risk.

To protect the security of members' benefits, the TPR has a range of powers, and these fall broadly into the three categories shown in Figure 24.2.

The Pensions Act 2004 requires the Pensions Regulator to issue voluntary codes of practice on a range of subjects. The codes provide practical guidelines for trustees, employers, administrators and others on complying with pensions legislation, and set out the expected standards of conduct.

The TPR supervises pension schemes through engagement with trustees, managers and sponsoring employers of pension schemes. The TPR has worked with the FCA to develop a joint strategy for regulating the pensions and retirement income sector and works with other bodies including the Department for Work and Pensions, Pension Protection Fund and the Money and Pensions Service.

FIGURE 24.2 POWERS OF THE PENSIONS REGULATOR

Investigating schemes	Putting things right	Acting against avoidance
• Identifying and investigating risks • Requiring all schemes to make regular returns to the regulator • Requiring trustees or scheme managers to give notification of any changes to important information, such as the types of benefit being provided by the scheme • Requiring that the regulator be informed quickly if the scheme discovers that it cannot meet the funding requirements, so that remedial action can be taken at an early stage	• Requiring specific action to be taken to improve matters within a certain time • Recovering unpaid contributions from an employer who does not pay them to the scheme within the required period (by the 19th day of the month following that in which they were deducted from the member's salary) • Disqualifying trustees who are not considered fit and proper persons • Imposing fines or prosecuting offences in the criminal courts	• Preventing employers from deliberately avoiding their pensions obligations and so leaving the Pension Protection Fund to cover their pension liabilities • Issuing: – *contribution notices*, requiring the employer to make good the amount of the debt either to the scheme or to the Pension Protection Fund; or – *financial support directions*, which require financial support to be put in place for an underfunded scheme

The Act also introduced requirements for trustees to have a sufficient knowledge and understanding of pension and trust law, and of scheme funding and investment. Trustees must also be familiar with the trust deed and other important documents such as the scheme rules and the statement of investment principles.

24.3 What is the Pension Protection Fund?

The Pensions Act 2004 established the Pension Protection Fund (PPF) to protect members of private sector defined-benefit pension schemes in the event that a firm becomes insolvent with insufficient funds to maintain full benefits for all its scheme members. The PPF is also responsible for the Fraud Compensation Fund, which provides compensation to occupational pension schemes that suffer a loss as a result of dishonesty.

The role of the PPF has been brought into focus as a growing number of occupational pension schemes have encountered financial problems.

The PPF provides varying levels of compensation, depending on the circumstances of the member. There are only limited circumstances where the compensation paid is 100 per cent of the benefits being drawn or to which the member would have been entitled had the scheme remained solvent.

The PPF funds the compensation payments it makes in several ways:

- It imposes a levy on defined-benefit schemes (there are exceptions for some schemes in certain circumstances).
- It takes on the assets of schemes that are transferred to the fund.
- It seeks recovery of assets from insolvent employers.
- It seeks to grow its funds through investment.

FACTFIND

To find out more information on the Pension Protection Fund, including arrangements for dependants on the death of the scheme member and sharing compensation with a former spouse or civil partner, go to:

www.ppf.co.uk

24.4 EU Directives affecting regulation of the financial services sector

In Topic 2 we explored the role of the EU in financial services and the differences between directives and regulations. In Topic 19 we looked at the provisions of the Capital Requirements Directive and Solvency II. In this section we are going to look at some other examples of how EU legislation affects the provision of financial services and advice.

24.4.1 Electronic Money Regulations 2011

The second Electronic Money Directive (2EMD) was implemented in the UK on 30 April 2011, in the form of the Electronic Money Regulations 2011.

ELECTRONIC MONEY (E-MONEY)

Electronically stored monetary value issued on receipt of funds for the purpose of making payment transactions, including prepaid cards and electronic prepaid accounts for use online.

The issuance of e-money has been regulated since 2002; the Electronic Money Regulations 2011 introduced new requirements for all electronic money issuers (EMIs), and new authorisation/registration and prudential standards for electronic money institutions.

The UK government initially retained the Payment Services Regulations 2017 and the Electronic Money Regulations 2011 on UK statute books post-Brexit. This was achieved through the Electronic Money, Payment Services and Payment Systems (Amendment and Transitional Provisions) (EU Exit) Regulations 2018.

As part of HM Treasury's programme of secondary legislation to replace retained law, the Electronic Money, Payment Card Interchange Fee and Payment Services (Amendment) Regulations 2023 are now in effect. These regulations remove a limitation on the FCA's powers to make rules in relation to authorised electronic money institutions, small electronic money institutions, authorised payment institutions, small payment institutions and registered account information service providers.

24.4.2 Markets in Financial Instruments Directive (MiFID)

The Markets in Financial Instruments Directive (MiFID) applies to firms that provide services to clients in relation to tradeable financial instruments, which include shares, bonds, units in a collective investment, and derivatives. Life assurance, pensions and mortgages are outside the scope of MiFID.

In the UK, MiFID became effective from November 2007. It is a key element of the EU Financial Services Action Plan and aims to harmonise the regulation of investment services across the EU. MiFID has the main objectives of increasing both competition and consumer protection by setting requirements in three main areas:

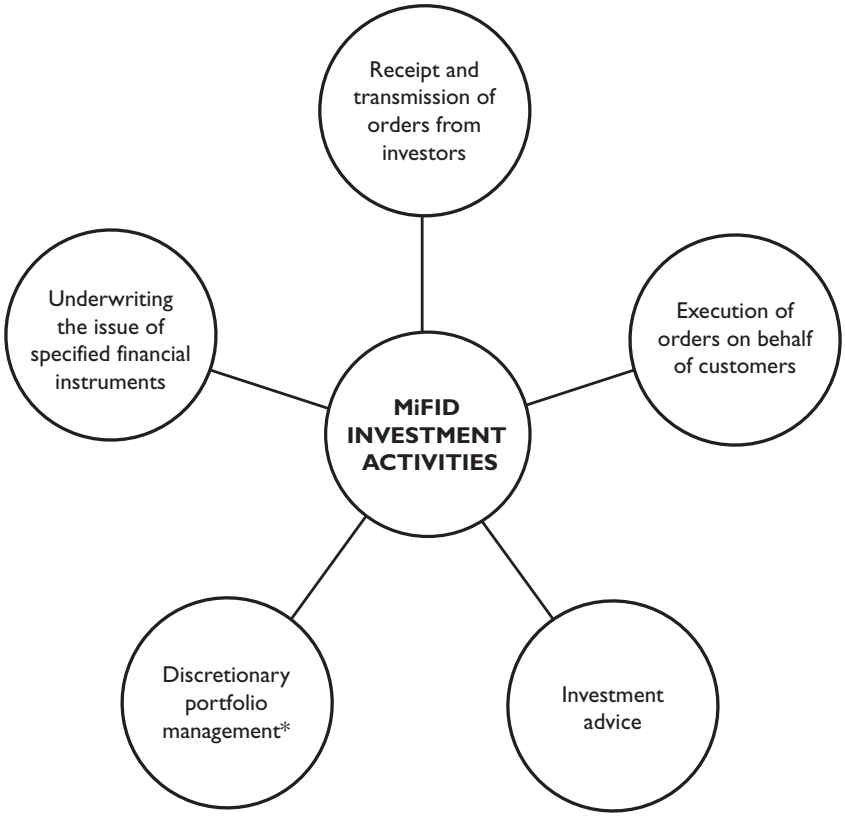
- conduct of business;
- organisation;
- market transparency.

MiFID distinguishes between core and non-core activities: core activities are "investment services and activities" and non-core activities are "ancillary services". Where a firm performs both core and non-core activities, MiFID applies to both aspects of its activities. A firm that only performs non-core activities is not subject to MiFID.

MiFID includes the principle of an EU 'passport', meaning that a firm subject to MiFID has the right to operate throughout the EEA on the basis of a single authorisation in its home state. The aim of the directive is to make cross-border activity easier to conduct by imposing a single set of rules across the EEA.

The FCA, as the body responsible for the securities industry in the UK, has written MiFID into its Handbook. Firms affected include securities and futures firms, banks conducting securities business, recognised investment exchanges and alternative trading systems. The types of investment activity covered by MiFID are summarised in Figure 24.3.

FIGURE 24.3 INVESTMENT ACTIVITY SUBJECT TO MIFID



*on a client-by-client basis, in accordance with mandates given by investors

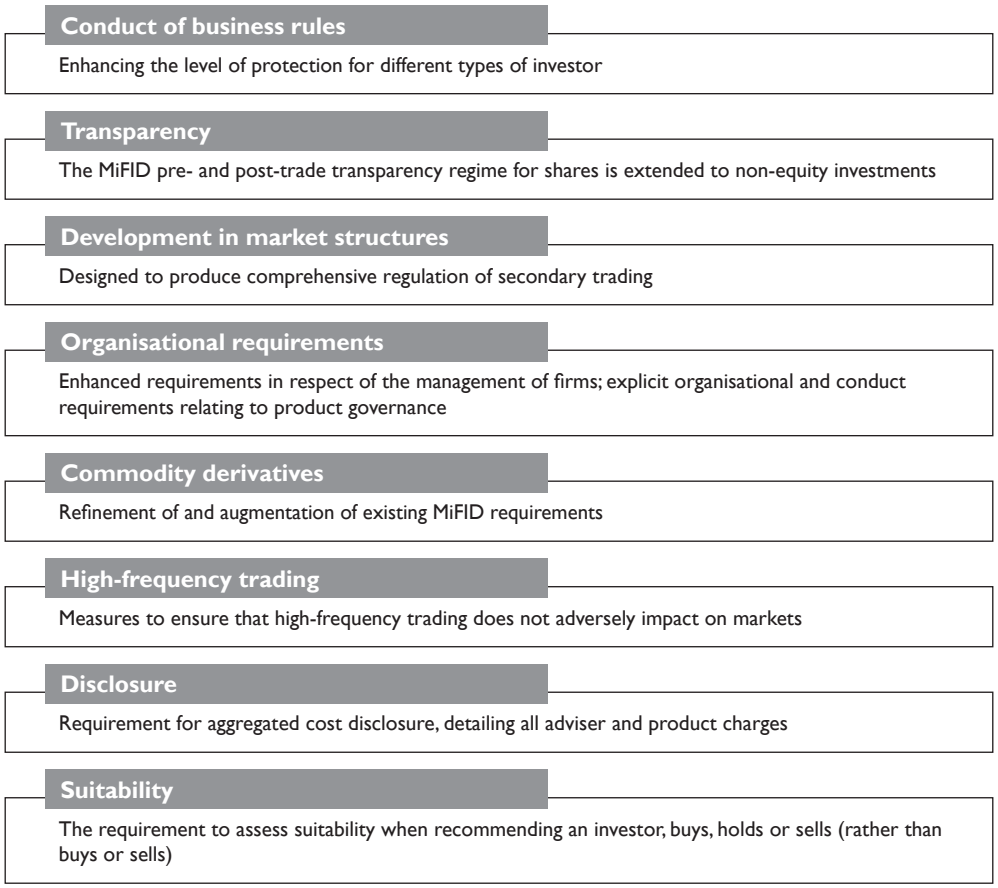
Given that MiFID does not apply where a business only carries out 'non-core activities', UK firms are exempt from MiFID if they do not hold client money and do not advise on or arrange complex investments such as derivatives. However, any firm making use of the exemption in respect of 'non-core' activities will not be able to engage in cross-border business on the basis of home state authorisation.

MiFID II

The European Commission launched proposals for reform in 2010. These were intended to improve the functioning of financial markets in light of what was learned from the financial crisis, improve investor protection and tackle some of the issues that were missed in the original MiFID.

MiFID II represents a comprehensive set of reforms covering eight main areas (see Figure 24.4). The legislation was published in June 2014 and has applied within EU member states since 3 January 2018. The onshore UK MiFID framework commenced at the end of the Brexit transition period on 31 December 2020.

FIGURE 24.4 REFORMS UNDER MIFID II



24.4.3 Undertakings for Collective Investment in Transferable Securities and the Alternative Investment Fund Managers Directive.

Two EU directives regulate investment funds and their managers – the Undertakings for Collective Investment in Transferable Securities (UCITS) Directive (2009) and the Alternative Investment Fund Managers Directive (AIFMD). The UK government retained both directives in UK law after Brexit.

The UCITS Directive applies to regulated investment funds that can be sold to the general public throughout the EU. It aims to provide a common framework of investor protection and product control.

The Directive lays down the principle of mutual recognition of authorisation that facilitates free circulation within the EU of the units of funds it covers. The funds must comply with various requirements, which include having an adequate spread of risk among their underlying investments and a high degree of liquidity to enable investors to redeem their units on demand. Since July 2011, management companies established in any EU state have been able to operate UCITS funds established in another state.

The UCITS V Directive was implemented in the UK from March 2016 and aims to increase standards of investor protection and customer confidence.

Since Brexit, UCITS authorised by the FCA are referred to as 'UK UCITS' but have lost their passporting right to market under a streamlined process in EU member states. UK UCITS wishing to market into the EU will be designated as Alternative Investment Funds (AIF) and therefore must comply with the marketing rules in the member state where the investor is located. Some member states do not permit the marketing of non-EU funds to retail investors.

The AIFMD applies to the managers of AIFs that are typically sold to professional investors (eg hedge funds and private equity funds) and those funds that invest in assets which are ineligible for UCITS (eg real estate). The AIFMD provides a passporting framework for managing and marketing funds across the EU, enabling cross-border activities to be carried out. Some AIFs are sold to retail investors but cannot be marketed cross-border to a retail investor using the marketing passport. Instead, the local marketing rules in the member state where the investor is located apply.

The AIFMD entered into force on 22 July 2011. The UK government retained the AIFMD in UK law after Brexit. As is the case with UCITS, AIF that are domiciled in the UK lost their passporting right to market under a streamlined process in EU member states.

FACTFIND

The FCA are reviewing the AIFMD alongside UCITS. 'DP23/2: Updating and improving the UK regime for asset management' was issued in 2023 with an FCA Consultation Paper expected in 2024.

You can read the discussion paper here:

www.fca.org.uk/publication/discussion/dp23-2.pdf

24.4.4 Life assurance

The two main objectives of a European single market for insurance are to:

- provide all EU citizens with access to the widest possible range of insurance products, while ensuring the highest standards of legal and financial protection; and
- enable an insurance company authorised in any of the member states to pursue its activities throughout the EU.

In setting out to achieve these objectives, the EU has always dealt with life assurance and non-life insurance separately, in order to take account of their

different characteristics and also in acknowledgment of the close ties that life assurance has with the long-term savings industry.

EU legislation on life assurance evolved over a number of years and the Consolidated Life Directive (2002) sets the framework for the regulation of life assurance in the EU. The Consolidated Life Directive brought together the provisions of three previous EU Life Directives and includes the following:

- Definitions of what constitutes life assurance – in addition to life insurance, the definition also includes annuities and income protection insurance.
- The rules applying to an insurer that wishes to provide life assurance services on a 'cross-border' basis.
- Requirements that must be adhered to for a life assurance company to be authorised.
- Requirements in respect of the ongoing supervision of a life assurance company, with specific rules with regard to financial supervision. The responsibility for the financial supervision of an assurance company is that of the regulator in its home state.
- A requirement for policyholders to be provided with clear and accurate information about the essential features of products offered to them. As a consequence, the FCA requires that life assurance customers are provided with a key features document.
- Cancellation rights – in the UK, FCA rules require that those applying for life assurance are granted a statutory 'cooling-off period'.

As with other EU legislation, the aim is to harmonise laws throughout the EU with the objective of promoting competition.

The UK government retained the Consolidated Life Directive in UK law after Brexit.

CHECK YOUR UNDERSTANDING 2

From your studies in Topic 21, can you recall where in the FCA Handbook:

a) the requirement to provide insurance policyholders with clear and accurate information about the essential features of the products offered to them is found; and

b) the rules relating to cancellation rights are addressed?

24.4.5 General insurance

In 1988, the Second Non-Life Council Directive laid down rules for cross-frontier non-life insurance that balance the needs of freedom of service and consumer protection. This allowed companies to supply insurance in another member state without having to establish a branch or subsidiary in the other state.

The Third Non-Life Council Directive, issued in 1992, completed the process and now any insurance company whose head office is in one of the member states can establish branches, and carry on non-life insurance business, in any other state. That activity will be under the supervision of the competent authorities of the member state in which the insurance company's head office is situated.

Authorisation to carry out insurance business under the terms of this directive is granted for a particular class of insurance (or even, sometimes, for some of the risks relating to a particular class). General insurance risks are classified into a large number of categories or classes; companies can, of course, be authorised for more than one class.

Directive on Insurance Mediation

As well as ensuring that insurance companies can operate throughout the EU, the EU also wants to ensure that retail markets in insurance are accessible and secure. To this end, a Directive on Insurance Mediation (IMD) came into force in January 2003, the purpose of which is to establish the freedom for insurance intermediaries to provide services in all states throughout the EU.

A key aim of the IMD has been to regulate the sales standards of insurance brokers and intermediaries.

Insurance mediation is defined in the Directive as "the activities of introducing, proposing or carrying out other work preparatory to the conclusion of contracts of insurance, or of concluding such contracts, or of assisting in the administration and performance of such contracts, in particular in the event of a claim". When an employee of the insurance company, or someone acting under the responsibility of the insurance company (a tied agent), carries out such activities, they are not included in the definition of insurance mediation.

The Directive has established a system of registration for all independent insurance (and reinsurance) intermediaries. They must be registered with a competent authority in their home state: independent financial advisers based in the UK who are selling life assurance or general insurance must be registered with the FCA.

Registration is subject to strict requirements regarding professionalism and competence: intermediaries must have the necessary general, commercial and professional knowledge and skills. Exactly what this means depends on the relevant national authority.

CHECK YOUR UNDERSTANDING 3

Which section of the FCA Handbook do you think addresses the requirements for intermediaries to have the necessary general, commercial and professional knowledge and skills?

Insurance intermediaries are also required to be "of good repute". Again, local interpretations of this may vary, but minimum requirements are that an intermediary must not have been:

- convicted of a serious criminal offence relating to crimes against property or other financial crimes;
- declared bankrupt.

The latest Directive requires that insurance intermediaries should hold professional indemnity insurance of at least a minimum threshold per case and a minimum in total per annum, or an amount equivalent to a percentage of annual income to a maximum limit – whichever is higher.

Rules are also included to protect clients' funds, including the requirement to keep client money in strictly segregated accounts. This is backed up by a requirement for intermediaries to have financial capacity of an amount equal to a percentage of premiums received per annum, subject to a minimum amount.

The regulations specify in some detail what information an intermediary must give to a customer. In relation to the intermediary, the following information must be supplied:

- name and address;
- details of registration and means of verifying the registration;
- whether the intermediary has any holding of more than 10 per cent of the voting rights or capital of an insurance company;
- conversely, whether any insurance company has a holding of more than 10 per cent of the voting rights or capital of the intermediary;
- details of internal complaints procedures and of external arbitrators (eg ombudsman bureaux) to which the customer could complain;
- whether the intermediary is independent or tied to one or more insurance companies.

In relation to the advice offered and products recommended:

- independent intermediaries must base their advice on analysis of a sufficiently large number of contracts available on the market to enable

them to recommend, in accordance with professional criteria, a product that is adequate to meet the customer's needs;

- the intermediary must give the customer (based on the information supplied by the customer) an assessment of their needs and a summary of the underlying reasons for the recommendation of a particular product. This requirement is satisfied in the UK by the use of a confidential client questionnaire, or factfind, to obtain the necessary information, and by the issue of a suitability letter to justify the specific recommendation.

All information provided by an intermediary to a customer must be set out in a clear and accurate manner, and must be comprehensible to the customer.

CHECK YOUR UNDERSTANDING 4

Where does the FCA Handbook address the requirements relating to:

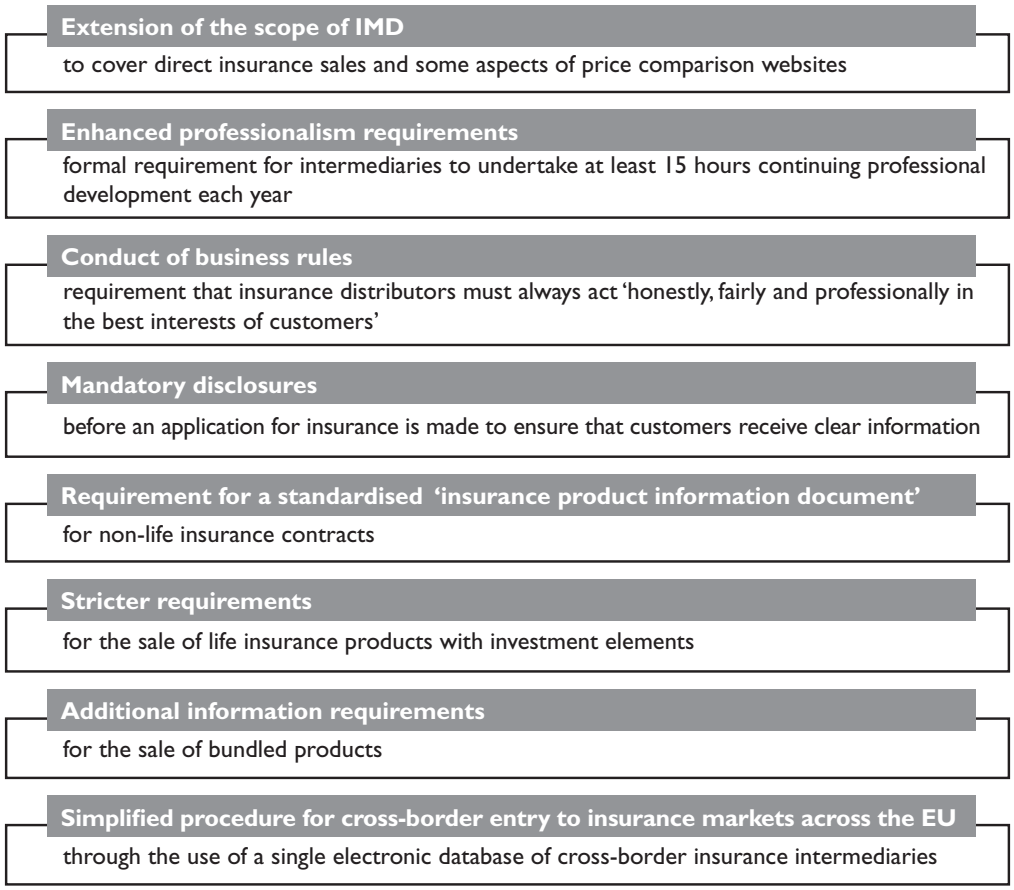
a) the information the intermediary must provide to the customer regarding how to complain, and whether the intermediary is independent or restricted?

b) the assessment of the customer's needs and the summary of reasons for recommending a particular product?

Insurance Distribution Directive

The existing IMD was replaced with effect from 1 October 2018 under the terms of the Insurance Distribution Directive (IDD). The aim is to address issues of inconsistency with regard to the way the IMD was adopted across member states and provide better consumer protection and greater legal clarity and certainty. The FCA has consulted on transferring the retained IDD Regulations into their rules and will do so with effect from April 2024.

FIGURE 24.5 REFORMS UNDER THE IDD



24.5 What is the role of oversight groups?

In addition to the regulation of the financial services sector set out in EU Directives and carried out by bodies such as the FCA, there are also a number of other ways in which the activities of financial services institutions are kept under review. It is important to ensure that the investments of both shareholders and customers are being handled safely and honestly and that the institution is abiding by all the applicable laws and regulations, in the best interests of all its stakeholders. This oversight of an institution's business can be carried out by different individuals and groups, such as auditors, trustees or compliance officers.

24.5.1 Auditors

External auditors

External auditors are concerned particularly with published financial statements and accounts. They are independent of the business whose accounts are being audited; they are normally firms of accountants, and it is their responsibility to provide reasonable assurance that published financial

reports are free from material misstatement and are compiled in accordance with legislation and with appropriate accounting standards. They must conform to the professional standards of the Auditing Practices Board and the Accounting Standards Committee.

External auditors may also be members of professional bodies, such as the Institute of Chartered Accountants in England and Wales (ICAEW) or the Association of Chartered Certified Accountants. Both bodies publish ethical codes that their members are expected to adhere to.

Internal auditors

Internal auditors may be in-house members of staff, or the process may be outsourced. Their basic task is to:

- review how an organisation is managing its risks;
- ascertain whether appropriate controls have been established; and
- evaluate and suggest improvements to control and governance processes.

They check that operations are being conducted effectively and economically in line with the organisation's policies, and that records and reports are accurate and reliable. It is not the responsibility of internal auditors to put controls and systems in place; that remains the responsibility of management. The role of the internal audit is to inform management decisions by identifying problems and recommending possible solutions.

Internal auditors may be members of a professional body, such as the Chartered Institute of Internal Auditors.

24.5.2 Trustees

A trustee is a person (or in some cases an organisation) whose responsibility is to ensure that any property held in trust is dealt with in accordance with the trust deed for the benefit of the trust's beneficiaries. Examples of trusts can be found throughout the financial services industry. For instance, unit trusts are investment schemes set up under a trust deed and the trustees are the legal owners of the trust's assets on behalf of the unit-holders. Similarly, most occupational pension schemes are set up under trust: this is important for the security of members' benefits because it enables the pension assets to be kept separate from the employer's business assets. The rights and duties of pension scheme trustees are set out in the Pensions Acts of 1995 and 2004.

Trustees are subject to statutory requirements in respect of the way they carry out their duties. The key legislation is the Trustee Act 1925 and the Trustee Investment Act 2000. The former is concerned with the general duties of trustees, the latter with the way in which trustees deal with the investment of trust assets.

24.5.3 Compliance officers

Firms that are authorised by the Financial Conduct Authority (FCA) or the Prudential Regulation Authority (PRA) are required to appoint a compliance officer to have oversight of the firm's compliance function, in other words to ensure compliance with all relevant legislation and regulations. Firms are also required to appoint a money laundering reporting officer (MLRO). Both roles are senior management functions under the Senior Managers and Certification Regime (SM&CR). Responsibilities of a compliance officer will include:

- production and publication of a compliance manual;
- maintenance of compliance records such as complaints register and promotions records;
- responding to and corresponding with the FCA on compliance matters;
- ensuring that staff meet FCA requirements as regards recruitment, training, supervision and selling practices.

Compliance officers may be members of a professional body, such as the Association of Professional Compliance Consultants.

CODES OF CONDUCT

Many professional bodies and trade associations have codes of conduct to which their members must adhere. For example, we saw in 18.6.4 that in order to receive a Statement of Professional Standing (SPS), an adviser must meet the professional standards of their professional body and declare that they adhere to its code of ethics.

Other examples of codes of conduct include:

- The Advertising Standards Authority (described in 20.5);
- The Standards of Lending Practice (described in 21.7).

THINK AGAIN ...

Now that you have completed this topic, how has your knowledge and understanding improved? For instance, can you:

- explain what is meant by the terms 'data subject', 'personal data', 'sensitive personal data' and 'data controller'?
- describe the role of the Pensions Regulator?
- outline the areas of financial services that are covered by, respectively, the Investment Services Directive, MiFID, the Insurance Mediation Directive and the Insurance Distribution Directive?
- describe the different types of oversight group that play a role in the financial services industry?

Go back over any points you don't understand and make notes to help you revise.

Test your knowledge before moving on to the next topic.

References

ICO (no date) *What is personal data?* [online]. Available at: ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/what-is-personal-data/what-is-personal-data/

TPR (2024) *What we do and who we are* [online]. Available at: www.thepensionsregulator.gov.uk/en/about-us/what-tpr-does-and-who-we-are

Test your knowledge

Use these questions to assess your learning for Topic 24. Review the text if necessary.

Answers can be found at the end of this book.

1) What is the difference between a data controller and a data processor?

2) What does UK GDPR define as 'sensitive data'?

3) Which of the following is **not** one of the UK GDPR principles?

   a) Data must be adequate (but not excessive) and relevant to the purpose for which it is processed.

   b) Data controllers must take appropriate technical and organisational measures to keep data secure from accidental or deliberate misuse, damage or destruction.

   c) Data must not be kept for longer than five years from the point at which it is gathered.

   d) Data must be kept accurate and up to date.

4) What is the penalty for committing a criminal offence in relation to UK GDPR?

5) The Pensions Regulator is responsible for the regulation of occupational pension schemes only. True or false?

6) What is the role of the Pension Protection Fund?

7) Which of the following products is UK **not** subject to MiFID?

   a) Units in a collective investment.

   b) Shares.

   c) Life assurance.

   d) Bonds.

8) What investment activities are subject to MiFID?

9) A general insurer with a head office in one of the member states may set up branches in other member states; these branches will be regulated by the national regulator of the state in which the head office is situated. True or false?

10) With which regulator must UK-based IFAs who sell life assurance or general insurance be registered?

a) The FCA.

b) The PRA.

c) The CMA.

d) The IDD.