Elborne Mitchell LLP

SOLICITORS

A Birds Eye View of Regulatory Pitfalls

A lecture by Alexandra Booth and Mark Estafanous

26 January 2018

These notes are derived from a talk by Alexandra Booth and Mark Estafanous of Elborne Mitchell LLP, given at Lloyd's Old Library on 26 January 2018.

Where specific reference is made to the law it is to English law as at 26 January 2018.

For specific advice, you should please contact Alexandra Booth and Mark Estafanous at Elborne Mitchell LLP.

Introduction

As we are giving this lecture at the beginning of 2018 we thought we would take the opportunity to go through some of the major changes that will be happening this year affecting the insurance market. The lecture will cover three topics:

1) General Data Protection regulation (GDPR)
2) Insurance Distribution Directive (IDD)
3) Senior Managers & Certification Regime (SM & CR)

Perhaps the overall theme of these three topics can be summed up by noting that the regulatory approach increasingly focuses on:

- Strengthening consumer protection
- Accountability – of firms and of individuals
- Being able to demonstrate compliance

1. GDPR

It is vital that all firms know what GDPR means for their business because the penalties for getting it wrong can be expensive both financially in fines and remedial action, and in terms of reputational damage. A recent survey conducted in November 2017 by the accountants RSM suggested that 92% of 400 European businesses surveyed were not ready and a quarter doubted they would be ready in time.

Overview

GDPR applies both to businesses with an establishment in the EU and those who process personal data of EU data subjects in relation to offering them goods or services or monitoring their behaviour. It will come into force in the UK on 25th May 2018 and is being enacted via the Data Protection Bill which has just cleared the House of Lords, and will be debated in the House of Commons.

Like the current UK Data Protection Act 1998 (DPA), GDPR applies to personal data, but the definition has been broadened to make it clear that an IP address can be personal data. It therefore encompasses any information relating to an identified or identifiable living individual who can be identified, directly or indirectly, in particular by reference to:

- An identifier such as name, identification number, location data or online identifier; or
- One or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of the individual.

GDPR also applies to what was previously known as sensitive personal data but will now be known as **special categories of personal data** (referred to in this note as special category data). Special category data is broadly the same as under DPA but now specifically includes genetic and biometric data where it can uniquely identify an individual. The categories are:

- Racial or ethnic origin

- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic or biometric data processed for the purpose of uniquely identifying an individual
- Health data
- Data concerning an individual's sex life or sexual orientation

Criminal convictions are not strictly special category data but are also treated in a similar way.

Like under the DPA, firms will need a lawful basis for processing data. The potential bases for processing "ordinary" data (rather than special category data) are:

- The data subject has given consent to the processing for one or more specific purposes.
- Processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing is necessary for compliance with a legal obligation to which the controller is subject.
- Processing is necessary in order to protect the vital interests of the data subject or another individual.
- Processing is necessary for the performance of a task carried out in the public interest or exercise of official authority.
- Processing is necessary for the purposes of the legitimate interests pursued by the controller or a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject.

There is little change there from the DPA.

So what are the main GDPR changes? Perhaps some of the most significant changes under the new regime are:

- Consent will be both more difficult to obtain and easier to withdraw.
- But explicit consent will in many cases be the only acceptable basis for lawful processing of special category data and criminal convictions. There is now however a new carve-out for the insurance industry which is explained below.
- Where firms receive personal data indirectly i.e. not from the data subjects themselves, they still have obligations to provide privacy information to the data subjects.
- There are new rights for individuals including erasure of data, data portability, withdrawal of consent and rights in relation to automated decision making – and some of these may have practical consequences for the insurance industry.
- Accountability – there is a new requirement to be able to demonstrate compliance via accurate record keeping which is going to place a greater compliance burden on firms

because if they cannot demonstrate compliance to the regulator, that in itself will be a breach of the rules.

- Reporting data breaches. Unless they are unlikely to result in a risk to individuals' rights (which is probably difficult to argue in many cases), firms must self-report to the ICO as soon as possible, and generally within 72 hours. And the data subject themselves may have to be notified if the breach is likely to result in a high risk to them.

- And financial penalties are going to be significantly more severe than they have been – up to the higher of €20m or 4% of annual worldwide turnover, plus there will be potential claims from individuals for financial loss or distress. Failures in record keeping or to notify breaches will themselves carry fines up to €10m or 2% of turnover.

Consent

Under the GDPR, consent has to be freely given so the individual has genuine choice and control. It must be specific and informed so it covers all purposes of processing – so if one of the purposes is for example marketing, the customer must have understood and consented to that in particular. It must be unambiguous so the ICO considers that statements such as "if you don't object you will be taken to consent" or pre-ticked boxes are not going to be acceptable. There must be an active opt-in such as a signed paper statement, email response or clicking of an opt-in button. Consent must be unbundled –so it can't be hidden in the middle of a long set of Ts & Cs to which the customer clicks their agreement. Requests for consent will have to be separately drawn to the attention of a customer. Consents should be documented – who gave them, when did they give them and how were they given. Firms should consider whether existing consents meet GDPR standards and also look at their processes for revisiting and potentially refreshing consents – how often this is necessary will depend on the particular context including whether the firm is in regular contact with the individual – if in doubt the ICO is recommending every two years.

In many instances, rather than consent, firms can instead rely on the ground that processing is necessary for performing the contract or for pursuing legitimate interests, provided that the Privacy Notice sets out clearly that this is the lawful basis for processing.

Special Categories of Data

However, as mentioned earlier, the only basis for processing most special category data under the GDPR is explicit consent and that caused serious concern in the insurance market about how that would work in practice, particularly for insurers engaged in life/health businesses – not least the practicalities of obtaining all of those consents and how to deal with claims if consent was withdrawn.

The good news is that these concerns should be largely resolved by an amendment to the Data Protection Bill, which was approved by the House of Lords (although has yet to clear the House of Commons).

The amendment allows processing by the insurance industry in the following circumstances:

- It is necessary for an insurance purpose, namely:

  - Advising on, arranging, underwriting or administering an insurance contract
  - Administering a claim under an insurance contract
  - Exercising a right or complying with an obligation arising in connection with an insurance contract

- It is processing of personal data revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health or criminal convictions
- It is necessary for reasons of substantial public interest
- Where the processing is not for the purpose of measures or decisions with respect to the data subject themselves (i.e. they won't actually benefit under the policy or in relation to the claim), then other requirements apply including that the data controller cannot reasonably be expected to obtain the data subject's consent

To be within the amendment, the processing must be necessary in the substantial public interest. During House of Lords debate on the amendment, it was recognised that the availability of insurance at a reasonable cost to members of the public through risk-based pricing, detection of fraud and efficient administration of payment of claims are matters in the substantial public interest. The controller must still be able demonstrate that all of the processing they do under this provision is actually 'necessary' i.e. that it is a reasonable way to achieve the insurance purpose, and there is no other reasonable and less intrusive way to achieve the same end. Controllers must also have in place an appropriate policy document which meets the requirements of the Data Protection Bill. This must be kept up to date and be available to the ICO on request.

Article 14 – Indirect Provision of Data

Another area that has sparked debate is Article 14 of GDPR regarding the indirect provision of data. Where personal data has not been obtained from the data subject themselves (i.e. it has been supplied by someone else, such as by an insurer to a reinsurer) the controller still has to provide the data subject with information including:

- Identity and contact details of the controller.
- The legal basis on which, and the purposes for which, the controller processes personal data.
- The categories of personal data being processed.
- The recipients or categories of recipients of personal data.
- The right to lodge a complaint with the ICO and ICO contact details.
- How to exercise the data subject's rights - automated processing, rectification and erasure.
- Any other information needed to secure that personal data is processed fairly and transparently.

Where for example a reinsurer is being given personal data by an insurer, on the face of it they have an obligation to provide this information to the insured whose data has been shared. That clearly raises a number of practical questions:

- What is the Privacy Notice going to say? How do you clearly explain to an insured what a reinsurer's role is?
- Who will provide the reinsurer's Privacy Notice to the insured? Will reinsurers seek agreement from their cedants that they will do so? This may be workable where there is a simple insurer/reinsurer relationship.
- If there are a number of reinsurers, an insured could end up receiving multiple Privacy Notices which will be confusing and seems an unintended consequence which goes against the stated purpose of GDPR of making things easier to understand for insureds.
- How far up the chain will this need to go? Retrocessionares?

It may be that for some contracts, the problem can be solved by anonymising data such that it ceases actually to be personal data (from which an individual can be identified) but in many cases that may not be easy to achieve, given the breadth of what constitutes personal data.

What are the other considerations? The Data Protection Bill states expressly that the data controller may make the information generally available to the public where they consider it appropriate to do so. So an appropriate Privacy Notice could be on a reinsurer's website. The Bill also provides that the controller is not required to give information if the data subject already has it – so if an insurer's Privacy Notice adequately covers the data processing throughout the insurance market chain there should be no obligation on a reinsurer or someone further up the chain to provide that information again.

To help address this need to explain the processing throughout the London market, the LMA (in conjunction with the IUA, LIIBA and BIBA) has produced a working draft "Core Uses Information Notice". The Notice explains the insurance life cycle including who are the various market participants; how they collect, share and process personal data; and the purposes for which data may be used. It also covers issues such as automated processing and other data subject rights that are referred to below, and also transfers of data including outside the EEA (which is outside the scope of this lecture). It does not cover marketing activities, only activities which are core to the provision of insurance. The goal is that market participants might link to the Notice from their own (probably shorter) Privacy Notices. The LMA is though keen to stress that firms should not simply rely on it as a template and should always individually consider their own processing activities and Privacy Notice requirements.

It also still leaves open the question whether a data subject is being given adequate information about, say, the identity of the controller – they will not be able to look at a reinsurer's Privacy Notice unless they know which reinsurers have been given their data. However, there is a carve-out if giving the information to the data subject would be impossible or would involve disproportionate effort. Also, the LMA Notice envisages data subjects being invited to ask their insurer or broker for details of the market participants to whom their data has been passed. It is to be hoped that common sense will prevail and this layered approach e.g. a combination of (i) an insurer's well drafted Privacy Notice (ii) the LMA Notice covering London market processing generally and then (iii) reinsurers themselves making their Privacy Notices available on their websites, will satisfy the ICO (at

least where there are complex relationships). This is though an area where further industry specific guidance from the ICO will certainly be welcome.

Rights of the Individual

Data subjects now have the following rights:

- Right of access, including confirmation whether or not personal data is being processed and access to that data and prescribed information without undue delay and generally within one month
- Right to rectification of data
- Right to erasure or restriction of processing
- Right to data portability
- Right not to be subject to automated decision-making save in prescribed circumstances

Rights to erasure may present practical difficulties for firms but there are rights to refuse in certain circumstances. Although the burden of proof is generally on the data controller to show refusal was acceptable.

Rights in relation to automated decision making and profiling is an interesting area for the insurance market. It is permissible to carry out decision making based solely on automated processing, either with consent or where it is necessary for entering into or performing a contract – so insurers may be able to rely on that ground, e.g. 'it is part of our underwriting process in determining whether to insure you'. However, there are still requirements to tell a data subject that a firm engages in this type of decision making and to enable the individual to understand the underlying reasoning the processing and potentially to challenge a decision. These issues should all be covered in firms' Privacy Notices as appropriate.

Third Party Contracts

Insurers, reinsurers and brokers should consider the data protection provisions in their reinsurance treaties and Terms of Business Agreements. Also, however, it is vital that contracts with third parties such as data processors, outsource providers, consultants and suppliers are not overlooked. Firms need to ensure data protection obligations are adequately covered and all parties know who will be responsible for what. Under GDPR any contracts with a data processor must be in writing and include various prescribed terms including:

- Subject matter, duration, nature and purpose of processing
- Types of personal data and categories of data subjects involved
- Obligations and rights of the controller and processor
- Confidentiality duties
- Obligations to assist the data controller to ensure compliance with data subject rights
- Deletion or return of data at the end of provision of the services

There are also requirements to keep detailed records of processing activities. All outsourcing agreements should as a bare minimum include obligations on counterparties to comply with the legislation and confidentiality, data retention and deletion. Consider also terms such as (i)

data security obligations (ii) obligations to report data breaches and rights to audit the counterparty (iii) responsibility for training obligations and (iv) contractual indemnities.

What You Should Do Now

To sum up key practical points on steps to take now:

- Consider your lawful basis of processing – do you need to rely on consent and if so, how has this been obtained to date and how will it be obtained in the future? Alternatively, identify other lawful bases.
- Consider data minimisation – do you actually need to receive that personal data at all? Can data be anonymised?
- Draft/update your Privacy Notice and consider how it will be provided to Data Subjects.
- Assess record keeping procedures – registers of data processing activities/consents. Remember the requirement to demonstrate compliance.
- Look at the role of your Data Protection Officer (DPO). There are express requirements for firms to provide DPOs with necessary resources and access, and to avoid conflicts.
- Review training – DPOs will be responsible for this.
- Update third party agreements to ensure compliance and impose both necessary and preferred terms on third parties.
- Review data retention/deletion policies.
- Review incident response procedures.

2. IDD

The IDD was even more imminent than GDPR as it was due to come into force on 23rd February 2018. However, because that timescale became increasingly unrealistic current indications are that D-day will be 1st October 2018. There are various areas in which the IDD will not change anything in the UK as the UK already has those requirements (or indeed in some cases even more stringent ones which will not be watered down). For example the IDD covers all insurance distributors including insurers selling directly to customers, who are already covered by FCA regulation.

The areas this lecture note covers include:

- Customer Best Interests Rule
- Pre-Contract Disclosure – Conflicts/transparency
- Pre-Contract Disclosure – Remuneration
- Demands and needs/personal recommendations
- IPID

- Cross-selling
- Knowledge and ability/good repute
- Reinsurance client money

The IDD beefs up a number of conduct rules, mainly reflected in the FCA Insurance Conduct of Business Sourcebook (ICOBS), with the stated aim of improving consumer protection and transparency. One important point to note at the outset is the scope of the conduct of business changes, which vary depending on the type of business. So generally they do not apply to reinsurance or 'large risks' (as defined)[1] situated outside the EEA as these are not within ICOBS. Changes do apply to some 'large risks' within the EEA in certain instances – so always consider the scope of the rules when determining the changes you need to make.

Customer Best Interests Rule

A new customer best interests rule is being introduced which will put the concept of treating customers fairly even more centre stage. It encompasses obligations:

- To act honestly, fairly and professionally in the best interests of customers ("the customer best interests rule") (to be a new rule in ICOBS 2)
- To communicate in a way which is clear, fair and not misleading, and to ensure that marketing materials are clearly identifiable as such (amendment to ICOBS 2)
- Remuneration of a distributor or its employees, and performance management of employees, must not conflict with the duty to act in the customer's best interests (a new rule in SYSC)

Although these concepts feature to some extent already in FCA guidance, they will now be rules - and 'paying due regard to customers' becomes 'acting in their best interests'. These rules apply to all firms carrying out insurance distribution activities where they have a direct impact on the policyholder, wherever they are in the distribution chain – so a wholesale intermediary who concludes a policy for a retail intermediary will still be caught by the best interests rule.

The new rule about remuneration conflicts means that Boards and Remuneration Committees will need to consider carefully how employees are being remunerated, for example in relation to calculation of bonuses and whether they could be incentivised to act against customer interests in order to boost profits and maximise their own remuneration, particularly in the short term.

---

[1] a) Railway rolling stock, aircraft, ships, goods in transit, aircraft liability and liability of ships
b) Credit and suretyship where the policyholder is engaged professionally in an industrial or commercial activity or in one of the liberal professions, and the risks relate to such activity
c) Land vehicles (other than railway rolling stock), fire and natural forces, other damage to property, motor vehicle liability, general liability, and miscellaneous financial loss, insofar as the policyholder exceeds the limits of at least two of the following three criteria:
i) Balance sheet total: €6.2m
ii) Net turnover: €12.8m
iii) Average number of employees during the financial year: 250

Pre-contract disclosure - Conflicts/Demands and Needs

The new provisions build on the existing requirements in ICOBS and require intermediaries to disclose various matters including whether they have 10% or more voting rights or capital in an insurer or vice versa.

Intermediaries must disclose whether they act for the customer or the insurer and, if they are giving advice, whether they do so based on a 'fair and personal analysis of the market'. Where an intermediary is contractually bound to place business with specific insurers, or does not provide advice on a fair and personal analysis of the market, there will be a positive obligation to name the insurers with whom it will or may place business rather than waiting to be asked.

There are also some beefed up rules regarding offering only contracts that meet customer demands and needs. It will not be acceptable simply to offer all the firm's available products with generic statements about the type of needs each product will meet. Where a personal recommendation is given, there is a requirement to explain why the proposed product best meets the customer's demands and needs.

Remuneration Disclosure

There are also new requirements (in ICOBS 4) for pre-contract disclosure to customers about remuneration, which in this case refers to remuneration that is not guaranteed or which is contingent on meeting certain targets. Intermediaries must disclose the nature **and** basis of the remuneration they **receive**. Insurers must disclose the nature of remuneration they **pay** to employees.

The FCA explains the distinction as follows. "Nature" of remuneration requires firms to disclose the type of remuneration they will receive or pay - whether basic commission, bonus, profit share or other financial incentive. "Basis" of remuneration means disclosure of the source of the remuneration received by firms, e.g. from an insurer or broker.

The requirement is to disclose remuneration only **in relation to the contracts proposed** so firms will need to consider whether remuneration relates to an actual contract or not. The FCA has given as an example that bonuses to an individual for hitting a sales target where the specific contract sold will count directly towards that target are likely to be disclosable, but measures such as rewards for adherence to quality standards may not. It is easy to see that there are going to be some very grey areas as to what does and does not need to be disclosed.

The current position that the actual amount of commission needs to be disclosed only on request is presently unaffected by IDD. If remuneration is in the form of a fee, there is a requirement to disclose the exact amount of the fee unless it cannot be calculated at the time, in which case the method of calculation will be permissible. The FCA has indicated that merely providing a range such as "up to £50" without more information is unlikely to be sufficient. All post-contract fees must also be disclosed including e.g. administrative fees for mid-term adjustments.

The FCA has given some examples of the types of remuneration disclosure that may be necessary. Some are set out below and there are others in the FCA's consultation and policy statements.

"We arrange the policy with the insurer on your behalf. You do not pay us a fee for doing this. We receive commission from the insurer which is a percentage of the total annual premium".

"When we sell you a policy the insurer pays us a percentage commission from the total premium. If the type of policy we sell reaches specific profit targets, the insurer also pays us an additional bonus."

"The insurer pays us a flat fee per policy to deal with claims on their behalf. Every month the insurer calculates the profit made on policies we administer and if this is above a certain amount, they also pay us a share of this."

However, none of the FCA examples so far address what they expect to see by way of disclosure of employee remuneration, so there is still a level of uncertainty about what is necessary to comply with this aspect.

IPID

There are also new provisions requiring a standardised Insurance Product Information Document (IPID).

The information to be provided in the IPID is prescribed directly by European regulation including not only the content but also that it be in a certain layout and font size and on only two sides of A4 paper (exceptionally up to three sides but then the ICO is entitled to require an explanation of why more space was needed!). The information to be provided includes the following:

(a) What is the type of insurance?
(b) What is insured?
(c) What is not insured?
(d) Are there any restrictions on cover?
(e) Where am I covered?
(f) What are my obligations?
(g) When and how do I pay?
(h) When does the cover start and end?
(i) How do I cancel the contract?

Much of this information will be standard across any given product allowing for a standardised template. One area of concern was how the requirement to detail things such as start and end dates of cover would be dealt with, and whether this would require each IPID to be bespoke. The FCA has accepted that this can be done by referring to other documents e.g. "the start and end dates of your cover are as shown in your policy schedule".

One issue for the FCA is whether or not to apply IPID to commercial as well as retail customers as under the IDD this has seemingly been left to the discretion of member states. The FCA's present view is that the IPID information should be provided to commercial customers but not necessarily in the prescribed IPID format (as this could lead to over simplification) – another type of appropriate policy summary can suffice.

Cross-selling

Cross-selling, i.e. where an insurance policy is sold in connection with or alongside other goods or services, will be the subject of new requirements in ICOBS 6A(3). If it is the insurance which is the primary product, then the customer must be given information on whether they can buy the different components of the package separately and they must have an adequate description of each of the component products. On the other hand, if it is the insurance that is ancillary to the other goods or services the customer must be able to buy the primary product or service without the insurance.

These provisions do not apply where the package consists only of insurance contracts or where the insurance is ancillary to certain other financial products, such as some bank accounts or mortgages. Also, they do not affect the sales of multi-risk policies.

Knowledge and Ability/Good Repute

The IDD requires that individuals within the management structure responsible for, and any staff directly involved in, insurance or reinsurance distribution must be of good repute. This is similar to the present rules. The IDD also stipulates rules for knowledge and ability of staff and continuing professional development (CPD) requirements. Records of training and CPD are required to be kept for a minimum period of not less than three years and there will be a new rule making clear that a firm must not prevent an employee from obtaining a copy of their CPD records.

Although for the most part there is little change to FCA rules in this area, we can anticipate a rather different focus on these requirements given the increased accountability of individuals to the regulators under the SM & CR regime and new requirements for regulatory references, which are explained below.

Reinsurance Client Money

One big change which will affect the reinsurance sector is that client money provisions will now apply to reinsurance. Currently, the rules (which are in the FCA's Client Assets Handbook (CASS 5)) are optional for reinsurance intermediaries. The FCA will now extend the CASS 5 rules to become compulsory for reinsurance contracts. It was also considering narrowing the scope of available options for reinsurance by allowing only risk transfer rather than segregated accounts, i.e. reinsurers would be obliged to agree that monies were being held by intermediaries on their behalf and at their risk. However, this prompted a great deal of concern from the industry about the lack of choice, what it would mean for reinsurance business already opted into the rules and using segregated accounts, and the potential need for wholesale amendments to many existing TOBAs. The FCA has accepted this is not the way forward. The same options will be open for reinsurance as for insurance.

Other Issues

There are other areas addressed by IDD, some of which (along with more detail on some of the issues in this lecture note) are in a briefing note which is on our website

www.elbornes.com. There are also more stringent requirements applying only to insurance based investment products (or IBIPs) which these notes do not cover.

3. SM & CR

The final topic of this lecture is the change to the present regime for approval of individuals within insurers and brokers and its replacement with the new Senior Managers & Certification Regime (SM & CR). This is going to impact many individuals within insurers and brokers in terms of who bears personal responsibility as far as the regulator is concerned, and will require some careful thought by boards and HR departments as to which individuals are fulfilling which roles, reporting lines, employment contracts and also what happens when staff move between firms, particularly in relation to references. The regulators believe that the new rules will reduce harm to consumers and strengthen market integrity by making individuals more accountable for their conduct and competence. It is notable that during 2017, more FCA fines were levied against individuals than companies – and this trend has generally seen a year on year increase.

At present, the full SM & CR regime applies to banks and PRA investment firms. Insurers are presently subject to a narrower regime, the Senior Insurance Managers Regime (SIMR).

Scope

The SM & CR regime has three limbs:

1) The Senior Managers Regime – this applies to individuals that perform Senior Management Functions (SMF) – such individuals must be approved by the firm's regulator;

2) The Certification Regime which applies to individuals who are not Senior Managers but whose role means that they could expose the firm or customers to significant harm. It is firms themselves that have to assess whether individuals fall into this category and the fitness and propriety of such employees;

3) Conduct Rules which will apply to all other staff apart from some very limited ancillary roles.

The SM & CR regime will mean wider duties and obligations for firms. The full regime will apply to insurers. However, the extent to which it applies to a firm which is only subject to FCA regulation (e.g. a broker) will vary because the FCA has created three new classifications of firms:

- Core firms (who will be the majority of FCA regulated firms and therefore the majority of brokers) who will be subject to the key parts of SMCR – i.e. key aspects of the Senior Managers Regime plus the Certification Regime and Conduct Rules;

- Enhanced firms - this will include CASS large firms and firms with total intermediary regulated business revenue of £35m per annum. Such enhanced firms will be subject largely to the whole of the SM & CR requirements;

- Limited scope firms who will include sole traders, service companies, and authorised professional firms whose only regulated activities are non-mainstream. Such firms will be subject to a significantly lighter approach.

Senior Managers Regime

Below is a list of all of the senior management functions. These will be largely familiar to insurers.

- SMF1 – Chief Executive*
- SMF2 – Chief Finance Office*
- SMF3 – Executive Director
- SMF4 – Chief Risk Officer*
- SMF5 – Head of Internal Audit*
- SMF6 – Head of Key Business Area*
- SMF7 – Group Entity Senior Manager*
- SMF8 – Credit Union Senior Manager*
- SMF9 – Chair of the Governing Body*
- SMF10 – Chair of the Risk Committee*
- SMF11 – Chair of the Audit Committee*
- SMF12 – Chair of the Remuneration Committee*
- SMF13 – Chair of the Nomination Committee
- SMF14 – Senior Independent Director*
- SMF15 – Chair of With Profits Committee
- SMF16 – Compliance Oversight
- SMF17 – Money Laundering Reporting Office (MLRO)
- SMF18 – Other overall responsibility
- SMF19 – Head of Overseas/Third Country Branch*
- SMF20 – Chief Actuary*
- SMF20a – With Profits Actuary*
- SMF21 – EEA Branch Senior Manager
- SMF22 – Other Local Responsibility
- SMF23 – Chief Underwriting Officer*
- SMF23a – Underwriting Risk Oversight (Lloyd's) *
- SMF23b – Conduct Risk Oversight (Lloyd's)
- SMF24 – Chief of Operations*
- SMF25 – Small Insurer Senior Management Function*
- SMF26 – Head of Small Run Off Firm*
- SMF27 – Partner

Firms will need to consider which prescribed responsibilities apply to them and therefore need to be allocated to Senior Managers. Senior Managers will be personally responsible and may be held accountable by the regulator in the event of a regulatory breach.

There will be a new form – a Statement of Responsibilities – which a firm will need to submit when applying for approval of a Senior Manager. Firms will need to keep these statements of responsibilities up to date and re-submit them to the regulator if there is a significant change in the Senior Manager's responsibility.

A more limited set of Senior Managers will apply to the FCA core regime – i.e. the majority of insurance brokers other than those who are large enough to be in the Enhanced Regime or small enough to be Limited Scope. A list of those functions is below:

- SMF1 – Chief Executive
- SMF3 – Executive Director
- SMF27 – Partner
- SMF9 – Non-executive Chairman
- SMF16 – Compliance Oversight
- SMF17 – Money Laundering Reporting Officer (MLRO)

Most of these will be already familiar to firms falling within the FCA approved persons regime.

For those within the Enhanced FCA regime (which the FCA anticipates being less than 1% of all FCA firms), they will need to consider whether additional roles apply.

These additional roles are:

- SMF2 – Chief Finance Function
- SMF4 – Chief Risk Function
- SMF5 – Head of Internal Audit
- SMF7 – Group Entity Senior Manager
- SMF10 – Chair of the Risk Committee
- SMF11 – Chair of the Audit Committee
- SMF12 – Chair of Remuneration Committee
- SMF13 – Chair of the Nominations Committee
- SMF14 – Senior Independent Director
- SMF24 – Chief Operations Function
- SMF18 – Other overall responsibility

SMF 18 is worth noting – it is something of a catchall but is designed by the regulators to ensure that there are no gaps in accountability. The guidance given by the FCA is that firms should consider what activities, business areas and management functions they have, who is responsible at the most senior level for each of these and, if they have not been covered elsewhere, they should be allocated SMF 18.

Insurers and large brokers subject to the enhanced regime will need to create and maintain a management responsibilities map setting out each of the relevant roles, who performs them, and how the roles interact. This is going to be an important document for firms and one which they can expect to have to produce to a regulator on request.

For limited scope firms, they will only be subject to a lighter approach and have fewer SMF functions than core firms.

Certification Regime

This is one of the biggest changes as all of those appearing on the list below will fall within this regime (including anyone in the management reporting line above them up to the senior managers).

- Significant management function
- Proprietary traders
- CASS oversight function
- Functions that are subject to qualification requirements (such as mortgage advisors, financial advisors)
- Client dealing function
- Algorithmic traders
- Material risk takers
- Anyone who supervises or manages a certified function but is not a senior manager

None of these people will be approved individually by the regulator (even though some of these roles may have been subject to approval previously) as the regulators want to see a shift in responsibility to firms for assessing the fitness and propriety of these types of staff member. Instead, firms themselves will have to check and confirm to the regulator at least once a year that these individuals are fit and proper for their roles.

Obviously not all of these roles are going to apply generally to insurance and some will apply only to firms in certain market sectors or above a certain size. One which will be of general application is the significant management function (akin to the current CF29) which is someone with "significant responsibility for a significant business unit". Firms will need to consider what is significant by reference to the size and nature of their business. The CASS oversight function will be relevant for those that hold client money or assets, if CASS oversight is carried out by someone who is not under the Senior Managers regime.

Conduct Rules

This is another important change and one which will have ramifications for people throughout regulated firms. Although they will not be subject to regulatory approval, almost all staff in regulated firms will be subject to the conduct rules that appear below:

1. You must act with integrity;
2. You must act with due care, skill and diligence;
3. You must be open and co-operative with the FCA, PRA and other regulators;
4. You must pay due regard to the interest of customers and treat them fairly;
5. You must observe proper standards of market conduct.

There are four further rules which apply only to Senior Managers:

1. You must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively.
2. You must take reasonable steps to ensure that the business of the firm for which you are responsible complies with the relevant requirements and standards of the regulatory system.

3. You must take reasonable steps to ensure that any delegation of your responsibilities is to an appropriate person and that you oversee the discharge of the delegated responsibility effectively.

4. You must disclose appropriately any information of which the FCA or PRA would reasonably expect notice.

Those who are excluded staff who are not subject to the first five rules are very limited indeed. There is an exhaustive list of excluded staff set out by the FCA which is set out below (although there will no doubt be many areas for argument as to whether staff do or do not fall within these):

- Receptionists
- Switchboard operators
- Post room staff
- Reprographic/print room staff
- Property/facilities management
- Events management
- Security guards
- Invoice processing
- Audio visual technicians
- Vending machine staff
- Medical staff
- Archive records management
- Drivers
- Corporate social responsibility staff
- Data controllers and processors under the DPA
- Cleaners
- Catering staff
- Personal assistants/secretaries
- Information technology support (i.e. help desk)
- Human resources / administrators / processors

Everyone else is covered and subject to conduct rules 1-5, which is a significant change from the current position where the focus was only on those who are individually approved by the regulator, so staff training is going be of increased importance.

Firms must be aware that they are required to notify the FCA when any disciplinary action has been taken against someone for breach of the conduct rules – for senior managers notification must be within seven business days and for anyone else, there is an annual notification requirement.

Timescales for Transitioning to SM & CR

The new requirements on firms to certify employees as fit and proper are intended to come into effect twelve months after the commencement date of SM & CR which will be set by HM Treasury – at present it is expected to be some time later this year. The conduct rules will apply to employees from the commencement date so firms should know from day one which of their staff fall within the new regime. However, they will have twelve months to complete their fitness and propriety assessments and make their initial certifications to the regulator.

The regulators have released some forms to deal with the transitioning of staff. For core and limited scope FCA firms, the FCA proposes automatically to convert most approved persons into their corresponding new SMFs. Insurers and enhanced firms however will need to submit

a conversion notification (Form K) and accompanying documents. Failure to do so could lead to a firm's approvals lapsing at the date SM & CR comes into force and the firm being automatically in breach so it is important that firms get to grips now with what requirements will apply to them.

Where firms are presently in the process of considering new appointments or reshuffles of staff, it may be worth thinking about doing those now, such that people are in post before the new regime commences.

Regulatory References

The final point that we want to touch on is what the new regime means when staff move on. Under the enhanced requirements for references, firms must request a reference from the previous employers of any Senior Manager, Non-Executive Director or person falling within the Certification Regime going back six years, so potentially across a number of previous employers. Each of those employers is required to give a reference and a standard template has been prescribed by the FCA.

Information required to be provided will include details of any disciplinary action for breaches of conduct rules, any finding that a person was not fit and proper and also any other information relevant to assessing whether a candidate is fit and proper over the previous six years. If the issues relate to serious misconduct however, there is no time limit. It will be important therefore for firms to retain records for a lengthy enough period to comply with their obligations.

There are two other important points to remember.

The first is that firms also have an obligation to update regulatory references where new, significant information comes to light.

The second is that firms are not permitted to enter into arrangements that conflict with their regulatory reference obligations – this is absolutely crucial for firms when considering entering into settlement agreements with employees in the event of an employment dispute as the requirement to give a regulatory reference will often tie a firm's hands in terms of what they can agree, for example in the way of an agreed reference.

Employment Issues

There are a number of further employment issues to consider, including those set out below.

When recruiting employees firms should consider:

- Making offers conditional on the firm's assessment of the individual's fitness and propriety, and in the case of candidates for senior management roles, approval by the regulator.
- Requesting a statement from new recruits or writing into their contracts that they have not been disciplined for any conduct that would amount to a breach of the conduct rules or that would give rise to concerns about that individual's fitness and propriety.

- In the case of senior managers – potentially drafting their contracts to refer specifically to their senior manager status and relevant regulatory obligations.

Firms should consider amending policies and procedures to include references to the consequences of failing to meet the standards for fitness and propriety.

Firms should also carefully consider the level of training required to assist employees in understanding their obligations. If proper training is not given employees could use this to argue that dismissal for any conduct breach constitutes an unfair dismissal. And finally firms should be aware that when they discipline employees on conduct issues, this will likely need to be reported to the regulator. Firms should keep this in mind when drafting letters, carrying out interviews and throughout the disciplinary process.