



The Impact of 2018 Regulatory Changes on HR

Nicky Archibald, Kenneth Underhill and Jason Jones



Agenda

1

Introduction

2

**The Insurance Distribution
Directive**

3

**Senior Managers Certification
Regime**

4

**General Data Protection
Regulation**

5

Questions

Introduction

1

- ICSR is an advisory and consulting firm
- ICSR has a team experienced at assisting regulated entities
- ICSR cover Governance, Control Frameworks and Company Secretarial, Compliance and Risk
- They respond quickly with the appropriate level of resources:
 - Outsourced
 - Co-Sourced
 - Resourced
- They are able to quickly and effectively apply our resources to the needs of the client to achieve the best possible result
- They thereby add value in a cost efficient manner

The Insurance Distribution Directive

2

- The IDD will be the basis for all regulation for distribution of insurance in the EEA (including the UK). It replaces the IMD. It sets out the basis for what activities relating to the distribution of insurance are regulated and then regulates who may and how they may be carried out. It is a minimum harmonisation regulation and EU Member States must enact enabling legislation
- The IDD is due to 'go live' on 23rd February 2018. But:
 - Only the FA and BaFin (German regulator) look to be ready
 - ECON and most market associations have called for a delay in the 'go live' date
 - Options are February or October 2018 or February 2019
- Much of what is in the IDD was already in the IMD and has already been implemented in the UK and can be seen in things like SIMR but there will be changes in areas such as SMCR

The IDD Changes – T & C

Training and Competence - IDD

- Employees must have appropriate level of knowledge and skills to complete their tasks and perform their duties adequately
- Employers must be able to assess their knowledge and competence:
 - at least 15 hours of professional training per annum taking into account:
 - the nature of the products
 - The type of distributor
 - The role they perform, and
 - their activities
 - which shall be evidenced by a certificate
- applicable to those (a) directly involved in distribution; (b) within the management structure responsible for distribution; and (c) those responsible for oversight of those directly involved in distribution

2

The IDD Changes – T & C

Training and Competence - FCA

- Covers:

- Knowledge of terms and conditions of policies and ancillary risks covered by policy
- Rules governing distribution including consumer protection, tax & social and labour laws
- Claims handling
- Complaints handling
- Assessment of customer needs
- Insurance market
- Business ethical standards
- Financial competence

- Not just applicable to employees but also:

- Contractors
- Third party distributors acting for you
- Appointed Representatives

Note: Where the FCA T & C rules apply (IBIPs) the 35 hour minimum will continue to apply

2

The IDD Changes - Misc

2

Good Repute

- Employees are required to be of good repute and as a minimum shall:
 - have a clean criminal record free of serious criminal offences linked to crimes against property or related to financial activities
 - not be a declared bankrupt unless “rehabilitated” in accordance with national law

But these requirements again need only be applicable to management responsible for and those involved directly in distribution or their supervisors

Record Keeping

- The FCA/PRA is introducing new requirements that all training and competence records are maintained for a minimum of 5 years (Note: The IDD only requires the record keeping to be applicable to insurers and reinsurers but the FA is introducing the record keeping requirements for brokers, MGAs and others who act as an intermediary)

Product Governance

- The IDD is introducing new rules of Product Governance and Oversight. These already exist in practise in the UK. The training element of new product development needs to not be overlooked.

The IDD - Remuneration

2

FCA

- **Non-Life**
- A Firm must manage conflicts of interest fairly. This extends to soliciting or accepting inducements where it would conflict with the firm's duties to its customers. Inducements include cash, cash equivalents, commissions, goods, hospitality and training.
- **Life**
- A firm must not accept a fee or commission which would impair compliance with the firm's duty to act in the best interests of the client or have a detrimental impact on the service being provided.

IDD

- Distributors must not be remunerated and must not remunerate or assess the performance of their employees in a way that conflicts with their duty to act in accordance with the best interests of the customer
- In particular utilising sales targets or otherwise to incentivise them to recommend a product to a customer when the distributor could offer a different product which would better suit the needs of the customer

What is required:

- A Board approved Remuneration Policy which covers remuneration arrangements for brokers, third party providers and employees.

Note: Other conflicts rules will remain

The Senior Managers Certification Regime

3

Introduction

- The Senior Managers Regime was came into force in March 2016
- The PRA/FCA have been required by the Treasury to introduce to the insurance sector a new module broadly in line with that already applicable in the banking industry regarding certification.
- Consultation closed in November 2017 and the proposed Policy Statement and draft rules are expected in summer of 2018 becoming effective in 2018
- It applies to almost all reinsurers, insurers, Lloyd's Managing Agents, ISPVs and branches of overseas insurers operating in the UK
- It will impact almost all existing SIMF persons and many others but not approved persons of Appointed Representatives
- It represents an increase in the focus on those in control and oversight roles and is a further raising of the bar on governance and culture within firms
- It does not change the roles firms need to hire for nor the shape of the organisations
- It is for firms to organise themselves having regard to their size and complexity, best practise and law and regulations
- It does however focus on management taking personal responsibility and accountability for their decisions and exercising rigorous oversight of the business areas they lead

SMCR - The Key Proposals

3

Documentation

- A number of SIMR documents are being replaced by SMCR documents. They are the same but have different names to match the new nomenclature in the legislation e.g. “Scope of Responsibilities” is being replaced with a “Statement of Responsibilities” and the “Governance Map” will be replaced by a “Responsibilities Map”.

New SIMF Approvals

- The FCA and PRA are proposing new SIMF roles for the following:
 - Chief Operating Officer (COA and/or Head O & T) (PRA)
 - Head of Key Business Area Function (£10bn or 20%) (PRA)
 - Chair & CEO roles to be Split (£1bn API or £10bn assets) (PRA)
 - Overall Responsibility of Key Function (FCA)
 - Compliance Oversight for Non-Life (FCA)
 - Conduct Risk Oversight (Lloyd’s only) (FCA)
 - Other Overall responsibility (FCA)
 - Chair Nominations Committee (FCA)
 - Chair With-Profits Committee (Life) (FCA)

SMCR - The Key Proposals

3

Certification

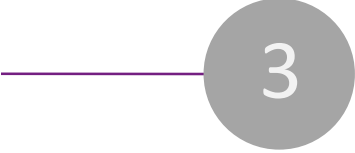
- Applies to individuals who are not Senior Managers but whose role means it is possible for them to cause significant harm to the firm or its customers
- Certification Functions include:
 - Significant Management
 - Proprietary traders
 - CASS Oversight Function
 - Functions subject to qualification requirements
 - Client Dealing Function
 - Algorithmic Traders
 - Material Risk Takers
 - Anyone supervising any of the above
- Not approved but firm must check and confirm (certify) at least once a year, that they are fit and proper to perform their role

SMCR - The Key Proposals

Senior Manager Conduct Rules	Senior Managers Regime <ul style="list-style-type: none">• Senior Management Functions• Overall Responsibility• Prescribed Responsibilities• Statements of responsibility• Responsibilities Maps• Duty of Responsibility• Criminal Records Checks• Handover Procedures	Fit and Proper Requirements Including Regulatory References
Individual Conduct Rules	Certification Regime	Fit and Proper Requirements including Regulatory References

SMCR - Impact

Senior Management Function Holders

- 
- On hiring:
 - Obtain Regulatory Reference
 - Evidence assessment of fit and proper compliance
 - Undertake criminal records check and bankruptcy check
 - Have to have formal induction/handover
 - Update Responsibilities Map
 - Contract should record:
 - What business activities they are responsible for
 - Which prescribed responsibilities apply
 - Compliance with Senior Manager Conduct Rules and Individual Conduct Rules
 - Must be annually assessed
 - Must have training

Certified Individuals

- On hiring:
 - Obtain Regulatory Reference
 - Evidence of Fit and Proper compliance
 - Fit and proper requirements
 - Contract should record:
 - What business activities they are responsible for
 - Compliance with Individual Conduct Rules
- Must be annually assessed
- Must have training

General Data Protection Regulation

The headlines...

4

- **EU regulation**, must be incorporated into local law in each EU member state (despite Brexit, the UK will follow by replacing the Data Protection Act 1998)
- Concerns **personal data** (broader definition than Data Protection Act, now including online and biometric identifiers)
- **Extra-territorial effect** applies to organisations in the EU (or UK), and those who are addressing EU (or UK) residents
- Compliance required from **25 May 2018**
- Fines for the most serious breaches of up to **4% of worldwide turnover or €20M**
- **Enhanced data subject rights** - subject access (now 1 month and no fee), portability, erasure, objection to profiling (automated decision making)
- Comprehensive requirements for **privacy notices** including specifying processing conditions and retention periods
- **Consent may only be relied upon in limited circumstances**, increased focus on legal basis for processing
- New systems must adhere to **privacy by design and by default**. In certain circumstances **data privacy impact assessments** and **data protection officers** may be required.
- **72 hour security breach notification** - to authorities, and potentially to data subjects
- **Compensation for data breaches** - damages for pure distress, burden of proof on the party responsible for the breach (check your insurance)

General Data Protection Regulation

Employees' consent to processing...

4

- Employers have historically relied on **consent** to legitimise the processing of employees' personal data (and sensitive personal data e.g. health, criminal)
- Arguably blanket consent provisions in **standard employment contracts** don't meet the test that consent should be freely given (employees effectively have no choice)
- The UK regulator, the Information Commissioner's Office, continues to encourage employers to **move away from relying on consent** and instead ensure they satisfy other conditions for processing personal data
- GDPR reinforces this principle and introduces even more **stringent conditions for securing consent** (e.g. ease of withdrawal)
- Employers should **consider dropping standard consent clauses** from employment contracts and instead review their data processing to ensure it satisfies other processing conditions - e.g. necessary for performance of contract, compliance with EU/member state legal obligations (how will this apply to UK laws post-Brexit?)
- Whether or not employers choose to continue to rely on consent, they will have to update their **employee privacy notices** to include the information prescribed by GDPR, including legal basis for processing, data retention periods, rights of erasure and portability, existence and nature of any profiling and right to object to profiling, right to complain to the regulator, and information on international transfers
- HR functions should prepare by auditing their processing of employee data (including retention periods), considering their approach to consent and updating their employee privacy notices

General Data Protection Regulation

Employees' data subject access rights...

4

- **GDPR makes exercising data subject access rights easier** - data processors must respond within 1 month (previously 40 days) and cannot charge a fee (previously up to £10)
- Subject access requests can require extensive retrieval of archived emails and other files, and can be **costly and time-consuming** to address
- Awareness of GDPR may lead to an **increase in current and former employees choosing to exercise their subject access rights**, whether in pursuit of specific goals (e.g. disputes, litigation) or idle curiosity
- Under GDPR data subjects will be entitled to **more extensive information** about their personal data being processed, including the legal basis of processing, the period of data storage, details of any transfers outside the EEA and the safeguards applied
- GDPR gives data subjects **enhanced rights of rectification** (of incorrect data) **and restriction of processing**, no longer needing a court order
- HR functions should prepare by reviewing their protocols for employee data subject access requests, including those linked to litigation, to ensure procedures are in place to cope with tighter timescales, greater information requirements and a potential increase in frequency; as well as protocols for requests for prompt rectification or restriction of processing

General Data Protection Regulation

Employees' rights to be forgotten...

4

- Under the current UK Data Protection Act, data subjects, including employees, have a right to have their personal data erased only if they can prove **substantial unwarranted damage or distress**, or by **court order if it is inaccurate**
- Otherwise, under DPA, data controllers, including employers, are obliged to ensure they **keep personal data no longer than necessary**, although many find this challenging
- **GDPR substantially enhances subjects' right to erasure** where the data are no longer necessary for the original purpose, or where the subject withdraws their consent and no other legal ground for processing remains
- However, **the data controller may retain the data if** there are compelling legitimate grounds, for compliance with a legal obligation, or for the establishment, exercise or defence of legal claims
- Regulated financial services businesses will have **obligations to retain** certain categories of personal information (e.g. for regulatory references, or to demonstrate compliance with certification, training and competence requirements)
- HR functions should prepare by reviewing their data retention policy to ensure it specifies the reasons and timeframes for retaining certain categories of employee personal data, ensuring the retention policy is implemented in all relevant systems (or data is migrated to capable systems), and putting in place protocols to handle (former) employee requests for erasure

General Data Protection Regulation

Employees' rights on data portability and profiling...

4

- GDPR gives data subjects a **new right to personal data portability** which does not exist under the UK's Data Protection Act
 - This is the right to a copy of the personal data provided by the subject, and must be supplied in a structured, commonly-used machine readable form
 - This only applies to data processed by automated means, where the subject has provided consent or the processing is necessary to fulfil a contract
 - The GDPR introduces this new right to help protect customers against lock-in effects and to facilitate switching - it's **unlikely to be used by employees** who would be better off making a data subject access request
- GDPR gives data subjects an enhanced **right to not be subject to a decision based solely on profiling** unless necessary for performance of a contract, authorised by law or with the explicit consent of the data subject
 - Profiling is automated processing to analyse, evaluate or predict aspects concerning a person (including e.g. their performance at work)
 - Data controllers using profiling techniques must incorporate measures to safeguard against inaccuracies and discrimination
 - In practice **employers rarely subject employees to decisions based solely on profiling**
- HR functions should prepare by reviewing their protocols for employee requests to exercise their rights to data portability and objection to profiling, and ensure their employee privacy notices are accurate regarding both

General Data Protection Regulation

Recruitment candidates, contractors and temps...

4

- HR functions should prepare by:
 - considering their approach and wording for securing **consent** for processing recruitment candidates' personal data
 - ensuring their **privacy notices** for candidates, contractors and temps include the information prescribed by GDPR, including data retention periods
 - review their **data retention policy** for candidates, contractors and temps
 - ensure their **contracts with recruitment agencies, contractor providers and temp agencies** that provide candidates' or workers' personal data are reviewed in light of GDPR and that their data handling processes will enable compliance with the obligations therein
 - review their use of **profiling** in recruitment processes (if any)
 - review their protocols for handling requests for **data subject access, rectification, restriction of processing, erasure or objection to profiling** from candidates, contractors and temps

QUESTIONS ?

Yes, we'll email you the slides !





Thanks
Keep in touch

kenneth.underhill@icsr.co.uk

07715 655745

Jason.Jones@icsr.co.uk

07920 199331

[linkedin.com/company-beta/16227843/](https://www.linkedin.com/company-beta/16227843/)

www.icsr.co.uk

Appendix: SMCR – List of Existing SIMF Roles

- Chairman
- Chair Remuneration Committee
- Chair Risk Committee (PRA)
- Chair Audit Committee (PRA)
- Senior Independent Director
- CEO
- CFO
- Chief Actuary
- With-Profits Actuary
- CRO
- CUO
- Executive Directors
- Compliance Oversight
- SIMF - overall Responsibility for a Key Business Area (investment, claims, underwriting, pricing, reinsurance, capital management, liquidity management, operational systems and controls and IT)
- Money Laundering Reporting Officer

Appendix: Prescribed Responsibilities

- Senior Management Regime
- Employee Certification Regime
- Responsibilities Map
- Induction Training and PD of governing body
- Induction Training and PD of designated SIMFs and key function holders
- Oversight of Internal Audit where outsourced
- Whistleblowing
- Code of Conduct
- Financial Crime
- CASS
- Oversight of Adoption of Culture
- Developmental Lead for Culture by governing body
- Remuneration Policies and Practices
- Maintenance and Allocation of Capital and liquidity
- Production and integrity of financials and regulatory reporting
- Development and maintenance of firm's business model by governing body
- Performance of ORSA

Appendix: Conduct Rules

Individual Conduct Rules

- Must act with integrity
- Must act with due care, skill and diligence
- Must be open and cooperative with all regulators
- Must pay due regard to the interests of customers and treat them fairly
- Must observe proper standards of market conduct

Senior Manager Conduct Rules

- Must take reasonable steps to ensure that the business of the firm for which you are responsible is controlled effectively
- 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
- 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
- Must disclose appropriately any information of which the regulators would reasonable expect notice

Appendix: Duty of Responsibility

- Enshrined in the Financial Services and Markets Act s.66A
- Provides that if a Firm breaches an PRA or FCA requirement the senior manager responsible for that area of business could be held accountable if they did not take “reasonable steps” to prevent or stop the breach