Group Risk Development (GRiD)

Statement of Best Practice

Supplier Agreements and Non-Disclosure Agreements

Contents

September 2023

1.0 Statement of Best Practice

1.1 Background

When companies purchase products or services, they quite reasonably wish to ensure that the company they are purchasing the products or services from acts in an appropriate manner and that they are protected if problems arise.

However, companies are often unfamiliar with the way that group risk insurance operates in the UK, or the protection automatically provided through financial services laws and regulation. This can lead to several areas of misunderstanding:

- Insurers provide insurance, which is a product, not a service.
- Firms (insurers, intermediaries, and reinsurers) must comply with UK laws and regulations relating to the way in which insurance products are designed, sold, and administered. The services provided to customers by advisers and insurers are also subject to Financial Services regulations. Advisers and Insurers cannot operate in a way which conflicts with these obligations.
- Firms who operate in the UK are not required to comply with legislation and regulation in other countries.
- Agreements which may be necessary between a company and their suppliers in a 'non-regulated' environment are not appropriate in the context of insurance in the UK, which is highly regulated.

The 'service' which a firm provides in managing the insurance provided is a high priority for all firms who will need to meet regulatory standards. However, making this a contractual obligation for group risk cover is not appropriate.

1.2 Purpose

This Statement is intended to provide guidance and positioning to assist insurers and advisers with clients proposing agreements in addition to, or instead of, the insurance policy.

This Statement of Best Practice has been formulated to explain:

- the approach recommended by GRiD that firms should take in relation to supplier agreements, non-disclosure agreements and service agreements;
- how group insurance operates; and
- the safeguards in place for purchasers of this insurance cover.

In addition to this statement of best practice, firms may provide additional information on their own policies and protocols outlining how they operate.

1.3 Principles of Group Protection

Insurance operates on the principle that the premiums paid by many customers are used to help fund the insured losses of a few. Firms offering insurance within the UK must meet stringent laws and regulation designed to ensure they have sufficient

capital to meet their liabilities, as well as offer fair value products that meet genuine customer needs.

- Insurers operating within the UK will have robust governance policies in place to meet their legal and regulatory responsibilities. The FCA and PRA conduct audits to help ensure compliance.
- Insurance is neither goods nor a service. The insurer is required to confirm the contract of insurance within a policy document, that it writes and provides.
- Data security is of paramount importance to any firm operating within financial services. Group risk insurers determine the personal data they need to assess insurance risks and manage the insurance cover; they are independent data controller and need to register with the ICO.
- The FCA expects insurers to regularly review their products and the way they are distributed. An insurer must document its product lifecycle management processes, reviews and outcomes which may be audited by the FCA.

Many insurers will support new customers to complete due diligence exercises so they can be confident they've chosen a reputable firm.

However, an insurer is highly unlikely to adapt the way it operates its business to meet a specific customer's needs or extend audit rights.

- An insurer's internal governance will be designed to meet the complex laws and regulation financial services firms must follow. Their internal governance will cover the typical concerns of purchasing companies such as bribery, conflicts of interest and modern slavery.
- An insurer will find it very difficult to support an IT Security audit because many customer audits increase security risks, it may be inappropriate to meet an audit action, and they need to follow relevant regulations.
- The scale of a typical insurer's customer base makes it impractical.

1.4 Supplier Agreements

Insurers should not enter into supplier agreements as these are not appropriate to Group Risk business.

Group Risk insurers are authorised by the Prudential Regulatory Authority (PRA) and regulated by the Financial Conduct Authority (FCA) and the PRA to provide insurance. An insurer may also include value-added services alongside the insurance; however, these are generally provided by third parties as they are not authorised to provide these services directly.

The FCA requires insurers to provide a formal contract of insurance called a policy document. The policy document is usually formed of a standard set of terms and conditions accompanied by a schedule confirming who is insured, the benefits and cover options provided, and any agreed special terms. It must meet the FCA's regulatory standard clearly documenting when a claim is paid and premium expectations. The policy document doesn't need to be signed by both parties; acceptance of the quoted terms and payment of premiums is sufficient to confirm contract is in place.

Supplier agreements, for example those typically used for the supply of goods or services, are unsuitable for documenting insurance. They often conflict and could potentially override:

- The quotation terms.
- The policy terms.
- The insurer's responsibilities under relevant UK legislation and regulation including the Data Protection Act and FCA rules.
- The insurer's governance policies in areas like security and disaster recovery. The insurer is required to have 'suitable systems and controls in place so it's resilient, and any residual risks monitored and minimised.

Business models and scale means that it is often not possible to make specific changes for specific customers. Governance policy details may also be subject to commercial confidentiality, and therefore cannot be shared.

1.5 Non-Disclosure Agreements

It is recommended that insurers do not enter into generic non-disclosure agreements that are not specifically drawn up for use with group insurance products.

Protection for clients is already provided by FCA regulations and the Data Protection Act 2018 (DPA), and these agreements can conflict with an insurer's responsibilities under this UK legislation and regulations.

Insurers will need personal data to provide a Group Risk policy and will have registered with the Information Commissioner's Office (ICO) as a data controller.

Insurers will also require high level details about their commercial clients, much of which is usually in the public domain. They are unlikely to ask for commercially sensitive information about a client's products and operations.

Generic non-disclosure agreements often include clauses that are incompatible with insurance law. For example, they may not warrant the accuracy or completeness of the information a client provides. Insurers need complete and accurate information to assess insurance risks, and insurance law may permit them to reduce or not pay claims if it isn't provided.

Non-disclosure agreements aren't always written with UK law and regulation in mind. For example, they may require an insurer to delete confidential information before the insurer's legal, regulatory, and contractual needs for it have expired. They may also conflict with the insurer's responsibilities for helping prevent financial crime.

1.6 Data processing agreements

It is recommended that insurers do not enter into Data Processing agreements, as under the DPA they and their clients are Data Controllers.

Insurers determine the purpose and manner any personal data is, or will be, processed, which means they are independent Data Controllers.

Joint data controller agreements, or unnecessary processing agreements where the customer mistakenly believes an insurer may process personal data on their behalf, could cloud the responsibilities and create unnecessary risks for customers.

1.7 Service level agreements

It is recommended that insurers do not enter into contractual service level agreements, although these may be agreed as a statement of principle.

When a firm is supplied a service on which it depends to operate its business, if that service is not supplied to a suitable standard, the firms' business could suffer, financially. It is therefore common practice to agree service standards as part of the contract to provide services. If the standards are not met, the agreement will stipulate the financial penalties that might apply and what remedial action can or will be taken if the service standards are not met, to the extent that the firm can cancel the contract early without incurring a penalty to enable it to find an alternative supplier.

Most group risk insurers have a set of minimum service standards. Financial Services regulation is based on a mixture of Principles and Outcomes. Regulatory expectations that service meets reasonable customer expectations and how any complaints are handled. An independent complaints mechanism, the Financial Ombudsman Service (FOS) may consider the complaints of smaller businesses and insured persons if not resolved.

In addition, regulations require insurers to only provide products that represent fair value to customers and that the features and construction minimise the risk of foreseeable harm to customers. This means that a good proportion of the premium is set aside to meet claims and firms run the risk of regulatory sanctions if service levels are deemed unacceptable. It is therefore not appropriate for them to form part of a legally binding agreement and they are not outlined in the insurance policy. The provision of group risk cover is a product, not a service.

Under a group risk policy, the insurer can only cancel the cover if the client fails to meet its commitments under the policy, for example, paying the premium on time. The client can cancel the cover at any time, for any reason, and without any penalty. They can obtain cover from another insurer if they are unhappy with their current insurer.

2.0 Group Risk and UK legislation and regulation

2.1 How group insurance works

Group insurers provide insurance for employers or trustees. The process operates as follows:

i) The insurer is provided with appropriate information about the employer and its employees, usually via an intermediary, in order that it can provide a quotation for the group risk cover required. It is the responsibility of the employer or trustees to provide accurate information and answer all underwriting questions accurately and completely.

If the client is aware of circumstances that may influence a prudent insurer's assessment of the risk, premium and terms; they need to volunteer this information even if it's unasked for. For example, if a new client ticks a box to confirm they offer waste disposal services they will need to volunteer additional information if they handle nuclear waste.

ii) The insurer issues a quotation for the cover. This includes the insurer's terms and conditions. The basis of the quotation may be subject to negotiation, and any changes must be agreed by the insurer.

iii) The client does not have to accept the quotation, but if they do, once the insurer has agreed risk, the client will complete a proposal form confirming their requirement for cover and agreeing to pay the premium for the cover. This is the basis of the contract.

iv) The insurer then issues the insurance policy document, which is the formal contract between the insurer and the client.

The Policy describes the responsibilities of both the insurer and the client, and gives the client clear details of:

- who must be included for cover, from when and for what benefits,
- any exclusions in respect of the cover,
- what premiums are payable by the employer / trustees and when,
- how and when the basis of the Policy can be changed,
- when and how the employer / trustees can make a claim.

It is a requirement of the Financial Conduct Authority (FCA), under the Insurance Conduct of Business Sourcebook (ICOBS), that the insurer issues a policy document.

v) Insurers will only share information about the client or individual employees with third parties that are directly concerned with the provision of the requested insurance. Further information would be contained in the relevant Privacy Policies.

Insurers authorised by the PRA and regulated by the FCA are authorised to provide insurance cover. They are not authorised to provide professional or any other services.

For the reasons listed above, it is our view supplier agreements and confidentiality agreements which are designed for use with companies that provide services to clients in connection with their business are not appropriate for insurance. These could conflict with the insurance policy that outlines the cover, make it difficult for the insurer to carry out its normal activities in connection with the insurance, and conflict with the insurer’s regulatory and legal responsibilities.

2.2 Regulation of firms by the Financial Conduct Authority (FCA)

There is a high degree of protection in the UK through legislation and regulation that applies to the insurance sector.

The FCA regulates all financial services firms in the UK and sets out 12 principles of business that are a general statement of the fundamental obligations of all authorised firms:

1. **Integrity**. A firm must conduct its business with integrity.
2. **Skill, care, and diligence**. A firm must conduct its business with due skill, care, and diligence.
3. **Management and control**. A firm must take reasonable care to organise and control its affairs responsibly and effectively, with adequate risk management systems.
4. **Financial prudence**. A firm must maintain adequate financial resources.
5. **Market conduct**. A firm must observe proper standards of market conduct.
6. **Customers' interests**. A firm must pay due regard to the interests of its customers and treat them fairly.
7. **Communications with clients**. A firm must pay due regard to the information needs of its clients and communicate information to them in a way which is clear, fair, and not misleading.
8. **Conflicts of interest**. A firm must manage conflicts of interest fairly, both between itself and its customers and between a customer and another client.
9. **Customers: relationship of trust**. A firm must take reasonable care to ensure the suitability of its advice and discretionary decisions for any customer who is entitled to rely on its judgment.
10. **Clients' assets**. A firm must arrange adequate protection for clients' assets when it is responsible for them.
11. **Relations with regulators**. A firm must deal with its regulators in an open and co-operative way and must disclose to the FCA anything relating to the firm of which the FCA would reasonably expect notice.
12. **Consumer Duty**. A firm must assess and evidence how it delivers good outcomes for its retail customers.

The FCA requirements for Systems and Controls covers some of the main issues which a firm is expected to consider in establishing and maintaining the systems and controls appropriate to its business. These include:

1. **Organisation.** A firm should have clear and appropriate reporting lines.
2. **Compliance, financial crime, and money laundering.** A firm must establish and maintain effective systems and controls for compliance with applicable requirements and standards, including having a Money Laundering Reporting Officer and a Compliance Function.
3. **Employees and agents.** A firm should be able to satisfy itself of the suitability of anyone who acts for it.
4. **Business strategy**. A firm should plan its business appropriately so that it is able to identify, measure, manage and control risks of regulatory concern.
5. **Business continuity**. A firm should have in place appropriate arrangements, to ensure that it can continue to function and meet its regulatory obligations in the event of an unforeseen interruption.
6. **Records**. A firm must make and retain adequate records of matters and dealings (including accounting records) which are the subject of requirements and standards under the regulatory system.
7. **Senior Managers have individual responsibility and accountability** for ensuring regulatory requirements are met and that good customer outcomes are provided.

The FCA does not set down specific rules on how firms must meet these principles, systems, and controls. Firms will have their own policies and procedures in place to meet these principles, that they are satisfied meet the FCA requirements.

The FCA requires firms to report compliance with the above principles and controls and firms will be audited by the FCA to confirm their compliance.

From July 2023, firms are required to provide to their Boards, an annual report detailing the firm’s compliance with the Consumer Duty requirements. Consumer Duty enhances existing regulation setting higher and clearer standards across financial services and expects firms to consumer’s needs first.

2.3 Information handling by the insurer

The insurer requires information to be able to:

- Assess the insurance risk
- Calculate the premiums to charge for the cover
- Issue any necessary documentation.
- Assess and pay claims.

This will include:

- Membership data, which, where an individual can be identified, will be classed as personal information, and is protected by the Data Protection Act 2018 (DPA)

  An insurer will operate as an independent data controller under DPA and share its privacy policy that explains how personal data is used and the personal data rights. An insurer is unlikely to hold contact details of the people their clients insure; they may ask their clients to share the privacy policy with those insured.

- General information about their client. For example, the location of the workforce, the nature of their occupations, and details of their employee benefits. This is usually in the public domain.

  Insurers do not seek confidential information that might involve, for example, commercially sensitive information about a client's products and operations.

Protection is provided for the information required by the insurer through the DPA and FCA regulations, and it should not be necessary to enter into any non-disclosure agreements which could conflict with the insurer's legal and regulatory responsibilities.

The following outlines how the DPA applies to both the insurer and the employer / trustees:

- The insurer and the employer are separate and independent controllers. They hold and use personal data for different reasons.
- Privacy policies must provide clear summaries of how personal data is processed, shared, and retained. An insurer will not normally hold the contact details of the people an employer insures and cannot directly share its privacy policy with them. They may ask the employer to pass on this information.
- DPA 2018 Schedule 1 Part 2 Section 20 includes a relaxation relating to insurance of third parties where substantial public interest can be demonstrated.
- The explicit consent of an insured person is needed for medical underwriting and the assessment of claims for illnesses or injuries.
- The consent of an insured person is needed before an insurer can obtain medical reports and information. The insurer must explain the rights given to individuals under the Access to Medical Reports Act.

- If a person chooses to restrict how an insurer uses their personal data, it may mean cover is withdrawn or a claim cannot be assessed and paid.
- Insurers and advisers must apply the data minimisation requirements set out in the DPA

2.4 The contractual nature of group risk arrangements

The contractual nature of the relationships between the parties involved in a group risk contract is not the same as other types of insurance.

The employee
Any group risk benefits are promised to the employee by their employer via their contract of employment. The employee has no direct relationship with the insurer and generally any Third-Party rights that an employee could have under the Contracts (Rights of Third Parties) Act 1999 are excluded from the insurance contract.

The employer
The employer initially establishes a scheme and funds it. For group income protection and group critical illness schemes, the employer is responsible for managing the scheme and can insure part or all the benefits if required and if they do, they will be the policyholder of the group contract and have a direct contractual relationship with the insurer.

For group death in service cover, the employer will need to distribute claim payments through a 'scheme' established using a discretionary trust. An employer may choose to set up its own scheme or participate within a 'master trust scheme' set up by a third party. The employer has no direct responsibility for managing the scheme, this rests with the trustees.

- If the employer sets up its own death in service scheme, it will often appoint itself as the sole corporate trustee, although some choose to appoint others as trustees. In addition to describing the trustees' responsibilities, the scheme will also describe the employer's rights and responsibilities such as a right to appoint trustees and usually a responsibility to fund expenses such as insurance premiums. The trustees will be the beneficial owners of the insurance policy.
- If the employer chooses to participate within a third-party master trust, it will be either the employer or the trustees of the master trust who will own the insurance policy. The employer will need to assign claim payments to the trustees of their chosen master trust, if they are the policyholder, and this will be made possible by deed or within the master trust application.

The trustees (group death in service cover)
The trustees are responsible for the management of the scheme and providing the death in service benefits promised for the beneficiaries of a deceased employee.

The insurer
The insurer provides group risk cover for the employer or trustees, who are the policyholder. The insurer can only deal with the employer / trustees or persons appointed to act on their behalf.

2.5 How a ‘scheme’ providing group risk benefits works

Group income protection and group critical illness

For group income protection and group critical illness, the employer will usually set out some rules for employees outlining the benefits they are entitled to and when they are eligible for these benefits. The employer can insure all or part of these benefit promises.

Group death in service

Death in service benefits can be provided for employees as part of a pension scheme, which also provides retirement pensions, or via a ‘stand alone’ group life scheme. Both these arrangements are set up using a discretionary trust. This is referred to as the scheme. There are greater regulatory controls on pension schemes.

Most schemes are registered with HM Revenue & Customs (HMRC), but it is also possible to have schemes that are not registered. Both types will be established via a discretionary trust.

Historically employers have set up their own schemes to provide death in service benefits, however in recent years insurers and other third parties have set up ready made master trust schemes that their clients can choose to participate in instead. Master trusts are often available at minimal, or no extra, cost, and run by experienced trustees.

A scheme is established by ‘executing’ a trust deed. The trust deed:

- Appoints the first trustees of the scheme.
- Explains how trustees can be appointed and removed, and how they can resign.
- Sets out the key trustee responsibilities including:
    - setting out any discretionary powers they have and how / when these can be used;
    - accountability for any tax due to HMRC;
    - any reporting responsibilities.
- Identifying any time limits within which the trustees must act.
- For schemes registered with HM Revenue and Customs (HMRC) the trust will clarify the scheme administrator’s role and responsibilities and will also adopt the scheme rules. The rules themselves will set out:
    - the benefit structure
    - who is eligible to join the scheme
    - the range of beneficiaries and dependants the trustees can take into consideration in exercising their discretion to pay out benefits.
- For schemes not registered with HMRC, the trust will also explain the trustees’ administrative powers, i.e. what they can/can’t do under the terms of the trust.

The trustees must act in accordance with the trust (and rules if applicable) in making all decisions about the scheme. They also have a fiduciary duty to act in the best interest of all the beneficiaries of the scheme.

Although the trustees will take account of any wishes a scheme member notified them of before their death, the final decisions as to how the scheme benefits are distributed rests with the trustees. This makes sure that the scheme benefits do not form part of the deceased's estate for inheritance tax purposes.

The rationale for using this approach is that it provides protection for employees and provides the most beneficial tax treatment for benefits and premiums. Most UK insurers only offer group death in service cover in association with schemes that are established under a discretionary trust.

There can be individually appointed trustees and / or corporate trustees. Often an employer setting up its own scheme will appoint itself as a sole trustee and act through its authorised officials.

If any work is required in connection with the scheme, the trustees or the scheme administrator must formally request a person or organisation to undertake work on their behalf. For example, a purchasing department of the employer who set up a scheme would not be able to act on the scheme's behalf, unless they had been formally requested to do so by the trustees or the scheme administrator.