LMA GENERAL DATA PROTECTION REGULATION (GDPR) GUIDE

PREPARED BY THE LMA WITH DAC BEACHCROFT

Issued May 2018

INSIGHT CONSENSUS INFLUENCE

DAC beachcroft

IMPORTANT NOTE: This guide is based on the version of the Data Protection Bill as amended in Public Bill Committee (Bill 190 2017-19) and guidance issued as at the date of publication. This guide is not exhaustive. It is provided solely for general information purposes and should not be relied upon as legal advice. No liability is accepted for errors of fact or opinion this guide may contain.

Table of contents

Where terms in this Guide appear in ***bold italics*** they have a specific meaning which is set out in Appendix 1.

1. WHAT IS THE GDPR?

Regulation (EU) 2016/679 (known as the General Data Protection Regulation or the ***GDPR***) will replace the UK Data Protection Act 1998 and other national (data protection) legislation across Europe on 25 May 2018.

The ***GDPR*** is an attempt to harmonise data protection laws across Europe. However, it leaves key areas (such as which breaches will constitute a criminal offence) to Member States to legislate. The UK has done this through the Data Protection Act 2018 which we anticipate will come into force on 25 May 2018. This means that there will still be differences in data protection laws across Europe.

The ***GDPR*** will be applicable in the UK despite Brexit. It will apply before Brexit occurs and the Government has confirmed that the ***GDPR*** will remain applicable in the UK post-Brexit.

The ***GDPR*** places greater and more prescriptive obligations on organisations when ***processing personal data***.

It also provides ***data subjects*** with more rights which are easier to enforce.

A key aspect of the ***GDPR*** is the change in risk profile of data protection compliance. Under the ***GDPR***, data protection regulators (known as "***supervisory authorities***") across Europe have greater power than they have previously had, including the right to audit and impose fines of up to €20,000,000 or 4% of annual worldwide turnover of an undertaking, whichever is the higher. The Information Commissioner's Office or "**ICO**" is the UK ***supervisory authority***.

2. KEY DEFINITIONS

There are a number of key definitions which you will need to be aware of in order to understand your data protection responsibilities. You can find a full list of defined terms in Appendix 1.

The ***GDPR*** regulates the "***processing***" of "***personal data***".

"***Processing***" is defined as any operation or set of operations which is performed on ***personal data***, whether or not by automated means, such as collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. Essentially, it is any use that can be made of ***personal data***, even merely storing it.

"***Personal data***" is defined as any information relating to an 'identified' or an 'identifiable' natural living person. An 'identified' or 'identifiable' individual (known as a ***"data subject***") is one who can be identified directly or indirectly, in particular by reference to an 'identifier', an online 'identifier' or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.

In the Lloyd's Market, you are likely to come across three broad categories of ***data subjects***:

- employment - ***personal data*** of employees, potential employees and contractors;
- insurance - ***personal data*** of policyholders, beneficiaries, claimants and witnesses; and
- service providers and business partners - ***personal data*** of business contacts and service providers such as individual underwriters, brokers, claims handlers, experts, lawyers and accountants.

Identifiers such as names, email addresses, identification numbers such as policy numbers and identification documents such as driving licenses and passports will clearly be ***personal data***. ***Personal data*** also includes information which, if combined with other information (for example, a policy number which is allocated to a specific individual), allows you to identify an individual.

 A postcode may or may not be ***personal data*** depending on the circumstances. For example, a postcode for an address in Central London is unlikely to enable you to identify a sole ***data subject*** without further information. In contrast, a postcode for an address in a remote part of England may enable you to identify a sole occupier.

The definition of ***personal data*** also extends to any information specific to an individual such as their physical appearance, economic situation (such as bank details), employment status or information about their property ownership status e.g. homeowner or living with parents.

"**Anonymous data**" is defined as “information which does not relate to an identified or identifiable natural person or to ***personal data*** rendered anonymous in such a manner that the ***data subject*** is not or no longer identifiable”. Anonymous data is not subject to the requirements of the ***GDPR***.

"***Pseudonymisation***" is defined as the ***processing*** of ***personal data*** in such a manner that the ***personal data*** can no longer be attributed to a specific individual without the use of additional information, provided that such additional information is kept separately. The use of

pseudonymisation as a data security method is supported by the ***GDPR*** because it is recognised as being able to reduce security risks to ***data subjects***.

 The LMA is currently preparing Data Security Guidance which will include more guidance on ***pseudonymisation***.

"**Pseudonymous data**" is ***personal data*** which has been ***pseudonymised***.

Pseudonymised or encrypted information is still ***personal data*** and subject to the ***GDPR*** because:

- encrypted data can be accessed using passwords; and
- a ***data subject*** can be identified from ***pseudonymised*** data when you re-match the data. For example, whilst claimant names might be replaced with a unique number and kept in a spreadsheet, if the code revealing the corresponding names of the claimants is also kept, when the two datasets are combined, a ***data subject*** can be identified.

"***Special categories of personal data***" (previously known as "sensitive personal data" under the Data Protection Act 1998) is a specific list of ***personal data*** relating to:

- health;
- genetic or biometric data;
- sex life or sexual orientation;
- racial or ethnic origin;
- political opinions;
- religious or philosophical beliefs; or
- trade union membership.

By their nature, ***special categories of personal data*** are highly sensitive and merit specific protection. Therefore, additional safeguards may be needed, such as stronger security measures. The ***ICO*** can impose a fine for any infringement of the ***GDPR*** and it is likely that a higher fine will be imposed where large amounts of ***special categories of personal data*** are involved.

Examples

Personal Data	***Special Categories of Personal Data***
Names and addresses	Medical reports or underlying medical data such as X-rays or blood tests of a policyholder or third party claimant
An opinion about an individual	An employee's trade union membership

Consumer lines insurance policy number	Fingerprints or facial recognition
Location data obtained from a telematics box	Details of the sight problem of a named driver
IP addresses	Details about an individual's civil partnership

Personal data relating to criminal convictions and offences are afforded similar protections to ***special categories of personal data*** under the UK Data Protection Bill.

3. *DATA CONTROLLERS AND DATA PROCESSORS*

When ***processing personal data***, an organisation is either: (i) a ***data controller***; (ii) a ***data processor***; or (iii) a ***joint data controller*** with a third party. The distinction between these is important because the obligations which arise under the ***GDPR*** are different for each.

The "***data controller***" is the natural or legal person who, alone or jointly with others, determines the purposes and means of the ***processing*** of ***personal data***.

The "***data processor***" is the natural or legal person which ***processes personal data*** on behalf of a ***data controller***. A ***data processor*** has some obligations under the ***GDPR***, predominantly in relation to data security. Employees of a ***data controller*** are not ***data processors***.

A "***joint data controller***" arrangement arises where two or more ***data controllers*** jointly determine the purposes and means of ***processing*** of ***personal data***. Under the ***GDPR***, ***joint data controllers*** have joint and several liability to ***data subjects*** and a ***data subject*** may exercise his or her rights against each of the ***data controllers***. ***Joint data controllers*** are also required, by way of an arrangement, to determine their respective responsibilities for compliance with the ***GDPR***. This arrangement should set out how the rights of ***data subjects*** should be exercised, who should respond to ***data subject*** requests and set out how the parties will deal with the provision of a ***fair processing notice***.

When entering into a new arrangement, it is important to consider both your own status and the status of the party you are contracting or dealing with.

- The ***GDPR*** prescribes certain obligations which must be set out in a contract between a ***data controller*** and a ***data processor***.
- ***Joint data controllers*** must have an "arrangement" in place which determined their respective responsibilities for compliance with the ***GDPR***. This could be done by putting in place a contract or another form of agreement.

IMPORTANT NOTE: The status of the parties is a matter of fact, rather than a matter for the parties to determine by way of contract. If the issue were to be considered by the *ICO* or the courts, an assessment would be made on the basis of the factual circumstances of *processing*. It is therefore important to ensure that you are confident that the right analysis has been carried out.

How to determine whether you are engaging a separate *data controller* or a *data processor*

In order to determine if you are engaging a separate ***data controller*** or a ***data processor*** who will act on your behalf, you need to understand who determines the "purposes and means" of ***processing***.

The ***ICO*** has produced useful guidance which sets out the decisions which can only be made by a ***data controller***. If you are dealing with a third party

who has discretion to make any of the following decisions, they will be a separate ***data controller*** (rather than your ***data processor***):

- to collect the ***personal data*** in the first place and the legal basis for doing so;
- which items of ***personal data*** to collect, i.e. the content of the data;
- the purpose or purposes the data is to be used for;
- which individuals to collect data about;
- whether to disclose the data, and if so, who to;
- whether subject access and other individuals' rights apply; or
- how long to retain the data or whether to make non-routine amendments to the data.

In the Lloyd's Market, it will often be the case that each party in a distribution chain or providing services will be required to make one or more of the decisions above, either because they are being engaged for a professional opinion or because they are bound by their own legal or regulatory obligations, in which case they will each be ***data controllers***.

The ***ICO*** Guidance specifically calls out "professional services providers". Using the example of "accountants and similar providers of professional services", the ***ICO*** highlights that these professions work under a range of professional obligations which oblige them to take responsibility for the ***personal data*** they ***process***. In addition, professional service providers (such as medical experts and lawyers) are engaged specifically for their professional opinion, and cannot be instructed to change that opinion or the content of the advice that they provide. This makes them a ***data controller***.

A similar argument can be applied to regulated companies. Regulated companies will have a number of obligations of their own to meet. For example, firms regulated by the Financial Conduct Authority are obliged to consider conflicts of interest and act with integrity, have adequate risk management systems and retain data for certain data periods; all of which mean that such firms must have a certain degree of discretion regarding their ***personal data processing*** activities. As a rule of thumb, parties providing regulated services will be ***data controllers***.


You can find the full ***ICO*** Guidance "Data Controllers and Data Processors: what the difference is and what the governance implications are" here.

It is important to remember that "***data controller***" and "***data processor***" are data protection concepts. Even if you are engaging a separate ***data controller***, you can still put contractual restrictions in place relating to the third party's use of ***personal data***. A common restriction is to prohibit the third party from carrying out marketing activities.

Typical situations where you are likely to be engaging or dealing with a separate *data controller*:

Coverholder or Managing General Agent ("**MGA**")	A Coverholder or MGA is likely to make at least one of the decisions set out in the ***ICO*** Guidance above. A ***data subject*** is likely to exercise his or her rights against the Coverholder or MGA, and the Coverholder or MGA would likely decide whether such rights apply. In addition, it has its own professional and regulatory responsibilities.
Broker	A broker is likely to make at least one of the decisions set out in the ***ICO*** Guidance above. In addition, it has its own professional and regulatory responsibilities.
Reinsurer	A reinsurer will ***process personal data*** for its own purposes. In addition, it has its own professional and regulatory responsibilities.
Law firm/Accountant	Whilst a law firm or accountant will be engaged to provide specific advice, it will exercise control over the content of the final advice. In addition, it has its own professional and regulatory responsibilities.

Typical situations where you are likely to be engaging a *data processor*:

IT provider	Whilst an IT provider may be engaged for its technical IT expertise, it is unlikely to have authority to use data for its own purposes.
Print production provider	A print provider is likely to be given very specific instructions regarding its ***processing*** activities and to be prohibited from acting outside of those instructions.

Determining whether or not you are engaging a ***data controller*** or ***data processor*** can be challenging. Within the Lloyd's Market, you may engage the same third party for some services for which they are acting as a ***data controller*** and for other services for which they are acting as a ***data processor***. This could even be done under the same contract.

 A good example of this is will be a third party administrator or "TPA":

- In some cases a TPA may be operating under very strict instructions and will have no discretion as to how ***personal data*** is ***processed*** (e.g. providing First Notification of Loss services only). They would likely be ***data processors***.
- In other cases a TPA may have a wide scope of claims settlement authority. They may be given authority to instruct experts, approach witnesses and collect any and all ***personal data*** considered necessary to investigate and settle the claim appropriately. They would only revert to the insurer for instructions in limited circumstances. They would likely be ***data controllers***.

How to determine whether you are engaging a *joint data controller*

There is little guidance on the concept of ***joint data controllers***. Currently the only guidance has been issued by the Article 29 Working Party or "***WP29***" (a group of European data protection regulators).

You can find the ***WP29*** guidance on ***joint data controllers*** here and ***ICO*** draft ***GDPR*** guidance on contracts and liabilities between controllers and processors can be accessed here.

This guidance states that ***data controllers*** who share a "macro" purpose are likely to be considered ***joint data controllers*** even if, at a "micro-level", they have different ***processing*** operations. When acting as ***joint data controllers***, as long as there is a shared purpose, the joint determination of the purposes and means of ***processing*** can take different forms and does not need to be equally shared between the parties.

An example of a ***joint data controller*** relationship in the insurance market would be a data sharing initiative where a number of insurance bodies are pooling data to combat fraud.

Review all arrangements with third parties to determine whether you are engaging with a ***data controller***, a ***data processor*** or a ***joint data controller***.

Depending on the data protection status of the other party, ensure that there are appropriate data protection provisions in all agreements.

Consider prioritising remediation of higher risk contracts, for example all ***data processor*** contracts involving significant amounts of ***personal data*** and contracts involving an extra ***EEA***-transfer.

4. WHO DOES THE GDPR APPLY TO?

The ***GDPR*** expands the geographical scope of European data protection legislation.

In addition, whereas the Data Protection Act 1998 "***DPA***" only applied to ***data controllers***, the ***GDPR*** will now impose certain obligations on ***data processors*** as well as ***data controllers***.

Territorial application of the *GDPR*

The Data Protective Directive 95/46/EC (on which the ***DPA*** was based) only applied to ***data controllers*** established in the ***EU***.

The ***GDPR*** applies to ***data controllers*** and ***data processors*** that are:

(1) established in the ***EU***, regardless of whether the ***processing*** takes place in the ***EU*** or not;

(2) not established in the ***EU*** but whose ***processing*** activities are related to the offering of goods or services to ***data subjects*** in the ***EU*** (irrespective of whether a payment by the ***data subject*** is required); or

(3) not established in the ***EU*** but whose ***processing*** activities are related to the monitoring of behaviour of ***data subjects*** in the ***EU*** as far as that behaviour occurs in the ***EU***.

"Monitoring" the behaviour of ***data subjects*** in the ***EU*** includes tracking ***data subjects*** in the ***EU*** on the Internet for profiling purposes or analysing or predicting preferences, behaviours and attitudes (if the behaviour takes place in the ***EU***).

The meaning of "establishment"

An "establishment" means an effective and real exercise of management activities determining the main decisions as to the purposes and means of ***processing*** through stable arrangements e.g. a branch of an insurer.

If your organisation is established in the ***EU***, you will need to comply with the ***GDPR*** for **all** of your ***processing*** activities even in relation to ***data subjects*** located outside of the ***EU***.

This is currently (subject to Brexit arrangements) the position of all Lloyd's Managing Agents.

A Lloyd's Managing Agent will need to comply with the ***GDPR*** in relation to US insureds (even where the ***personal data*** is provided by a Coverholder based in the US) because it (the Lloyd's Managing Agent) is established in the UK. This may lead to practical challenges (e.g. where a US Coverholder is asked to provide the Lloyd's Managing Agent's ***fair processing notice*** which meets the requirements of the ***GDPR***

even though that Coverholder is not itself caught by the ***GDPR***).

Non-*EU* established organisations

When assessing if a non-***EU*** established organisation is offering goods or services to ***data subjects*** in the ***EU***, consideration needs to be given to whether the organisation is:

- offering goods or services in a language or currency of a ***Member State***; and/or
- enabling ***EU*** residents to place orders in such other language; and/or
- referencing ***EU*** customers in its publications.

If the ***processing*** involves these activities, it will likely be “apparent that the organisation envisages offering goods or services” to ***data subjects*** in the ***EU***, and therefore the organisation will be subject to the ***GDPR*** for those ***processing*** activities.

Merely having a website which is accessible by ***data subjects*** in the ***EU*** will not, on its own, be sufficient to indicate that the organisation intends to offer goods or services to ***data subjects*** in the ***EU***.

The position post-Brexit remains unclear. Technically, the UK will become a "third country" outside of the ***EU***. This may mean that specific steps need to be taken when receiving ***personal data*** from Member States. We expect this position to be negotiated as part of the ***EU*** withdrawal package.

EU Representative

A ***data controller*** or ***data processor*** established outside the ***EU*** but caught by the ***GDPR*** should appoint a representative established in the ***EU*** unless its ***processing*** activities are:

- occasional;
- do not include large scale ***processing*** of ***special categories of personal data***; and
- unlikely to result in a risk to the rights and freedoms of ***data subjects***.

There is currently no definitive guidance as to the interpretations of what "occasional" or "large scale ***processing***" mean.

A representative should be explicitly designated by a written mandate of the ***data controller*** or ***data processor*** to act on the organisation's behalf and will act as the point of contact for the relevant ***supervisory authority***. In reality this role is likely to be taken by a group company within the ***EU*** where such a company exists.

The designation of a representative does not affect the responsibility or liability of the ***data controller*** or ***data processor*** under the ***GDPR***. However, the designated representative will be subject to enforcement proceedings in the event of non-compliance by the ***data controller*** or ***data processor***

organisation it represents. Therefore Lloyd's Managing Agents should think very carefully before taking on this role for Coverholders because the Lloyd's Managing Agent could become responsible for its Coverholder's failings.

Examples

Insurer based in the ***EU processing personal data*** about policyholders inside the ***EU***.	***GDPR*** will apply.
Lloyd's Managing Agent based in the ***EU processing personal data*** received on bordereau from its US Coverholder.	***GDPR*** will apply.
Coverholder based outside the ***EU*** servicing ***EU*** based policyholders.	***GDPR*** will apply. ***EU*** representative is likely to be required.
US Coverholder ***processing personal data*** of US policyholders.	***GDPR*** will not apply to the Coverholder. However, the ***GDPR*** will apply to the Lloyd's Managing Agent. The Lloyd's Managing Agent may need the Coverholder's assistance to meet its own obligations. For example, the Lloyd's Managing Agent may need the Coverholder to pass on its ***GDPR*** compliant ***fair processing notice***.

5. DATA SUBJECT RIGHTS

The ***GDPR*** provides ***data subjects*** with rights over and above those already provided under the existing data protection regime. These include the right to restrict ***personal data processing*** and the right to data portability.

The ***ICO*** has confirmed that requests from ***data subjects*** can be made either in writing or verbally.

 For more information on ***data subject*** rights click here.

How long do you have to comply?

Data controllers must comply with requests from ***data subjects*** without delay and at the latest within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of requests. However, the ***data controller*** must inform the ***data subject*** of any such extension within one month of receipt of the request, together with the reasons for the delay.

 Implement an internal policy and procedure to set out how requests from ***data subjects*** exercising their rights under the ***GDPR*** will be recognised and dealt with.

 Ensure that you comply with all ***data subject*** requests in accordance with the prescribed time frames.

 Ensure that your ***fair processing notice*** provides information on all ***data subject*** rights set out below.

The following table provides an outline of each right:

Right	Description
The right to access *personal data*	**What is a *data subject* entitled to?** Under the ***GDPR***, a ***data subject*** has the right to access a copy of his or her ***personal data*** and obtain the following information: • confirmation as to whether or not ***personal data*** concerning him or her are being ***processed***; • the purpose of ***processing***; • the categories of ***personal data processed***;

- the recipients or categories of recipients to whom ***personal data*** has been disclosed (including details of any extra-***EEA*** transfers);
- the retention period or, if not possible, the criteria used to determine the retention period;
- the existence of the rights of rectification, erasure, restriction and objection and the right to lodge a complaint with the relevant ***supervisory authority***;
- the source of ***personal data****;*
- the existence of automated decision making, the logic involved and envisaged consequences; and
- details of the safeguards used to protect ***personal data*** transferred outside of the ***EEA***.

This is known as the right of "***data subject access***" and a request is commonly referred to as a "***DSAR***".

Data controllers must respond to a ***DSAR*** in an intelligible format. This means that where a ***data subject*** has made their request electronically, the ***data controller*** should provide the information in a commonly used electronic format, unless otherwise requested by the ***data subject***.

Note that this right applies to all ***personal data*** held by a ***data controller***, not just the ***personal data*** provided directly by the ***data subject****.*

An employee making a ***DSAR*** would be entitled to much more than just the ***personal data*** contained within his or her personnel file. Subject to any applicable exemptions, he or she would be entitled to information such as board minutes and the contents of emails where such documents contain his or her ***personal data***.

Can you charge a fee?

No. Under the ***GDPR***, unlike under the existing law, ***data controllers*** cannot charge a fee for complying with a ***DSAR***, unless the request is manifestly unfounded or excessive, in particular because of its repetitive character.

Ensure that those responsible for dealing with ***DSARs*** understand the extent of the right.

	 Do not charge the £10 fee or refuse to comply with a request unless you can demonstrate that the ***DSAR*** is manifestly unfounded or excessive. Treat every request on a case by case basis.
The right to erasure	The ***GDPR*** provides ***data subjects*** with a new enhanced right to request erasure of their ***personal data***. ***Data controllers*** must erase ***personal data*** on request where specified grounds apply. Such grounds include where the: • ***personal data*** is no longer necessary in relation to the purposes for which it was collected or otherwise ***processed***; and • ***data subject*** withdraws his or her consent and no other legal ground for ***processing*** applies. **Remember (!) :** The right to erasure is not an unlimited right, and there are a number of grounds on which ***data controllers*** can rely in order to deny a request and continue to retain the ***personal data***.  In the insurance industry, ***data controllers*** are likely to have legal and/or regulatory obligations to keep records for reasonable periods of time. In such circumstances, a request for erasure can be denied.  Implement a data retention policy that defines the legal and regulatory reasons for retaining different categories of ***personal data*** for specified periods of time.  Where requests for erasure are denied, the reasons for any such denial should be recorded. This will be helpful if the decision is challenged by the ***data subject***, ***ICO*** or courts.
The right to data portability	The ***GDPR*** introduces a new right of data portability for ***data subjects***. On request, a ***data controller*** must:

- provide the ***data subject*** with a copy of the ***personal data*** which was provided by him or her to the ***data controller*** (not additional data which has been generated by the ***data controller*** itself) in a structured, commonly used and machine readable format; and

- where technically feasible, transmit that ***personal data*** to a new ***data controller***.

However, the right to data portability is not an unlimited right, and only applies where the:

- ***processing*** of ***personal data*** is carried out by automated means; and

- ***data subject*** has provided consent to the ***processing***; or

- ***processing*** is necessary to enter into or perform a contract with the ***data subject***.

The insurance industry needs to be prepared for this new right as it allows customers to transfer their entire profile from one broker or insurer to another broker or insurer in a structured, commonly used and machine-readable format. The format for portability will depend on the format of the original data. For example, a XML or CSV file.

ICO Guidance confirms that ***personal data*** which has been subjected to ***pseudonymisation*** will be within scope for data portability requests.

Review the ***personal data*** that you currently hold and the IT systems on which it is stored and establish how it can be provided to the ***data subject*** and to third parties on request. If you expect to receive a high volume of requests, consider the use of secure messaging, an SFTP server, a secured WebAPI or WebPortal.

When transmitting ***personal data*** to ***data subjects*** or another ***data controller***, assess the specific security risks and take appropriate risk mitigation measures and ensure that appropriate security measures are adopted.

For more information, read the ***WP29*** "Guidelines on the right to data portability" which can be accessed here.

The right to rectification	***Data subjects*** can require a ***data controller*** to rectify any inaccurate ***personal data*** concerning him or her and to have incomplete ***personal data*** completed.
The right to restriction of processing	In certain circumstances, ***data subjects*** are entitled to ask ***data controllers*** to restrict the ***processing*** of their ***personal data***. This right will apply if the: • ***data subject*** disputes the accuracy of the ***personal data*** (and only for the length of time it takes the ***data controller*** to verify that accuracy); • ***processing*** is unlawful and the ***data subject*** opposes the erasure of the ***personal data*** and requests the restriction of ***processing*** of their ***personal data*** instead; • ***data controller*** no longer needs the ***personal data*** for its original purpose, but the data is needed by the ***data subject*** to establish, exercise or defend his or her legal rights (so erasure is not appropriate); or • ***data subject*** has objected to ***processing*** based on the legitimate interests legal ground and the verification is pending as to whether the legitimate interests of the ***data controller*** override those of the individual. There is no current guidance as to who is responsible for verifying whether the legitimate interests of the ***data controller*** override the ***data subjects'*** rights and freedoms.  ***Data controllers*** should maintain records of any verification process they undertake and the outcome. This will be helpful if the decision is challenged by the ***data subject***, ***ICO*** or courts.
The right to object to processing	In certain circumstances, a ***data subject*** will have the right to object to the ***processing*** of their ***personal data***. This right arises when the legal ground relied upon (as discussed in section 7) is either that the ***processing*** is necessary for: • the purposes of legitimate interests pursued by the ***data controller***; or • the performance of a public task. This right is most likely to apply in an insurance context where "legitimate interests" is relied upon. If the right applies then the ***data controller*** can no longer ***process*** the relevant ***personal data*** except if:

	• the ***data controller*** can demonstrate compelling legitimate grounds for the ***processing*** which override the interests, rights and freedoms of the ***data subject***; or • it is for the establishment, exercise or defence of legal claims.  Ensure that robust "legitimate interests assessments" have been undertaken and documented to support any argument for "compelling legitimate grounds".  Keep a record of objections received and where the objection is denied, the reasons for any such denial should be recorded. This will be helpful if the decision is challenged by the ***data subject***, ***ICO*** or courts.  Stop ***processing*** the relevant ***personal data*** where any objection is successful.
The right to object to marketing	A ***data subject*** has the right to object to marketing sent by a ***data controller*** at any time. When such an objection is received, the ***data controller*** must stop ***processing*** the ***personal data*** for direct marketing purposes. ***Data controllers*** must inform ***data subjects*** of their right to object "at the point of first communication" (i.e. at the point that the ***data subject's personal data*** is collected for marketing purposes) and in its ***fair processing notice***. **ACTION:**  Maintain a suppression list of any ***data subjects*** who have objected to marketing to ensure their preferences are respected in the future.  Do not contact a ***data subject*** who is on the suppression list at a later date asking them to update their marketing preferences or asking them whether they want to receive marketing.  For more information read the ***ICO*** Direct Marketing guidance which can be accessed here.
The right not to be subject to automated decision-making (including profiling)	Automated decision making refers to a situation where a decision is taken using ***personal data*** that is ***processed*** solely by automated means (i.e. using an algorithm or computer software) rather than a decision that is made with some form of human involvement.

"Profiling" is defined as any form of automated ***processing*** of ***personal data*** evaluating the personal aspects relating to a person, in particular to analyse or predict performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

A ***data subject*** has the right not to be subject to a decision which is based solely on automated ***processing***, including profiling, and which produces legal effects concerning him or her or significantly affects him or her (such as where underwriting risk is assessed or a claim is rejected), unless:

- the decision is based only on ***personal data***; and
  - is necessary to enter into or perform a contract with the ***data subject***; or
  - the ***data subject*** has provided his or her consent.
- the decision is based on ***special categories of personal data***; and
  - is necessary for an insurance purpose (see page 24); or
  - the ***data subject*** has provided his or her consent.

In addition, ***data subjects*** have the right to:

- be informed about when such automated decision making has taken place; the logic used and likely consequences; and
- ask the ***data controller*** to reconsider the decision or to take a new decision on a different basis (e.g. by introducing some form of human involvement).

Review decision making in your organisation and determine where such decision making is automated.

Ensure that your ***fair processing notices*** provides information about any automated decision making you carry out, the logic involved and likely consequences.

Use appropriate mathematical or statistical procedures for profiling, implement technical and organisational measures to ensure, in particular, that factors which result in inaccuracies in ***personal data*** are corrected and the risk of errors is minimised.

	 For more information, read the ***WP29*** "Guidelines on automated individual decision-making and profiling" which can be accessed here.
The right to withdraw consent	Where a ***data controller*** relies on the legal ground of "explicit consent" to ***process personal data*** the ***data subject*** has a specific right to withdraw their consent at any time. ***Data controllers*** must inform ***data subjects*** of this right. Historically, insurance market participants have relied on consent to ***process special categories of personal data***. However, the UK Data Protection Bill creates a new legal ground for the ***processing*** of ***special categories of personal data*** (e.g. health data) and information on criminal convictions where such ***processing*** is necessary for "insurance purposes" such as administering an insurance policy or handling claims. Where it applies, there will be no need for insurance market participants to obtain advance consent of ***data subjects*** for core insurance purposes such as underwriting and administering a policy and handling claims.  Identify what legal ***processing*** grounds you will be relying on for all ***processing*** activities and in particular identify in what circumstances you will be relying on consent.  Ensure your ***fair processing notice*** sets out when you will be relying on consent.  Implement a procedure to deal with withdrawal of ***data subject*** consent.
The right to lodge a complaint with the ICO	***Data subjects*** have a right to complain to the ***ICO*** if they believe that a ***data controller's*** use of ***personal data*** is in breach of applicable data protection laws and regulations.

6. FAIR PROCESSING NOTICES

A ***data controller*** must provide detailed information to ***data subjects*** regarding how it ***processes personal data***. This information is given in a ***fair processing notice*** (sometimes known as a "privacy notice" or "privacy policy" or "information notice"). The information given must be transparent, concise, intelligible and easily accessible and drafted using clear and plain language.

In light of the volume of the information that is required to be provided, the ***ICO*** endorses a "layered" approach to providing ***fair processing notices***. This means that the ***data subject*** is provided with a short form "top layer" (***Layer 1***) which provides the ***data subject*** with the most important information. This top layer then links through to a long form notice (***Layer 2***).

In the insurance market, the short form (Layer 1) will usually be included in proposal forms, incorporated in MRC slips and/or policy documentation and claims notifications forms. This will link through to the long form (Layer 2), which will usually be hosted on the ***data controller's*** website.

 The LMA has produced a model Short Form Notice (Layer 1) which is published on the Lloyd's Wordings Repository.

The Long Form Notice (Layer 2) is firm-specific. Each ***data controller*** needs to prepare its own long form notice according to its own structure and data ***processing*** activities. Appendix 3 contains a checklist that firms can use when preparing their own long form notice.

The LMA has produced a third layer of information designed to help ***data subjects*** understand how the various insurance market participants ***process personal data***. This is known as the "London Market Core Uses Information Notice" and can be used as an additional layer - Layer 3. Firms may link to this from their own long form notice.

 The London Market Core Uses Information Notice can be found here and guidance on its use found here . The ***ICO*** Guidance can be accessed here.

 For more information on the approach to ***fair processing notices***, please see the ***WP29*** "transparency guidelines" which can be accessed here.

Ensure your ***fair processing notice*** is ***GDPR*** compliant and in line with the ***WP29*** transparency guidelines.

7. LEGAL GROUNDS FOR PROCESSING UNDER THE GDPR

A ***data controller*** must be able to rely on a "legal ground" when ***processing personal data***. This forms the valid legal basis for ***processing***.

Legal grounds for *processing personal data*

There are six legal grounds under the ***GDPR*** for the ***processing*** of ***personal data***. These are (in summary):

- the ***data subject*** has given consent;
- ***processing*** is necessary for the performance of a contract with the ***data subject*** or in order to take steps at the requests of the ***data subject*** prior to entering into a contract;
- ***processing*** is necessary for compliance with a legal obligation which the ***data controller*** is subject to;
- ***processing*** is necessary to protect the vital interests of the ***data subject;***
- ***processing*** is necessary for the performance of a public task; and
- ***processing*** is necessary for the purposes of the legitimate interests pursued by the ***data controller*** or by a third party, except where such interests are overridden by the rights or freedoms of the ***data subject***.

The ***ICO*** has published detailed Guidance on the use of the legitimate interests ground and the use of a "legitimate interests assessment" to balance the rights of the ***data subject***. You can find the Guidance here.

For insurance market participants, ***personal data*** will generally be ***processed***:

- where it is necessary for the performance of the insurance contract (e.g. to price the risk or manage the claim). Note that this ground only applies to the contract between the ***data controller*** and the ***data subject***. When ***processing personal data*** of other third parties (e.g. family members or other beneficiaries or witnesses) a different legal ground will be required;
- to comply with the ***data controller's*** legal obligations, e.g. to meet FCA requirements; and/or
- for legitimate business interests (e.g. internal business management and reporting) or handling third party claims. When relying on this ground, the ***data controller*** must consider the balance between its legitimate interests and the rights and freedoms of ***data subjects***. If the ***data subject's*** rights outweigh the business interests, this ground will not apply.

Legal grounds for *processing special categories of personal data*

When a ***data controller*** is ***processing special categories of personal data***, it must be able to identify a legal ground for general ***processing*** and an additional legal ground for ***processing special categories of personal data***.

There will generally be limited legal grounds that can be relied upon for the ***processing*** of ***special categories of personal data***. Historically, the only relevant legal ground available for most ***processing*** activities of ***special categories of personal data*** by the insurance industry has been consent. However, consent poses multiple challenges in the insurance industry with the key issues being that:

- in some instances, consent is inoperable due to the complexity of the insurance distribution chain, particularly in the Lloyd's or subscription market;
- for certain policies (e.g. health insurance) the provision of the policy and payment of claims must be conditional on the provision of ***special categories of personal data***. This goes against the requirement for consent to be freely given; and
- there could either be no right to withdraw consent where such ***special categories of personal data*** were necessary for the provision of the insurance policy or payment of claim; or the policy or claim may not be able to be honoured.

For further detail regarding consent please see Section 8.

Under the ***GDPR***, EU Member States are permitted to add additional legal grounds for ***processing*** of ***special categories of personal data*** where necessary in the substantial public interest. The LMA and other industry bodies worked with Government to implement such a new legal ground. The result is the "insurance purposes" ground.

Insurance market participants can rely on this ground where the ***processing*** of certain ***special categories of personal data*** is:

(1) necessary for an insurance purpose. “Insurance purpose” is defined to include advising, arranging, underwriting, administering, administering a claim under, exercising a right or complying with an obligation in connection with an insurance contract. The government has confirmed that “insurance” includes “reinsurance”;

(2) is of ***personal data*** revealing racial or ethnic origin, religious or philosophical beliefs or trade union membership, genetic data or data concerning health; and

(3) is necessary for reasons of substantial public interest. Risk basing pricing, detecting and investigating fraudulent claims and the efficient administration and payment of insurance claims have been given as examples of activities that are in the substantial public interest.

A similar condition has been implemented in relation to the ***processing*** of criminal convictions data, although with no requirement to demonstrate that the ***processing*** is in the substantial public interest.

There are, however, exceptions to the use of this ground, including where the ***data subject*** does not have a tangible link to the policy or claim (for example, a witness). Insurance market participants must consider and document how the insurance purposes ground is used and implement a "Part IV Policy" which sets out:

- where the ground is relied upon;
- how the data protection principles are complied with; and
- the policies in place to deal with retention and erasure.

Assess where your organisation can rely on the insurance purposes ground and implement a Part IV Policy.

8. CONSENT UNDER THE *GDPR*

The bar for consent is extremely high under the ***GDPR***. Consent must be:

- **Freely given** - the ***data subject*** must have a genuine choice whether to provide his or her consent. Consent must be clearly distinguishable from other matters (i.e. not bundled up with other non-negotiable terms and conditions or buried in an agreement).

- **Specific** – a ***data subject*** should be free to choose which purpose of ***processing*** he or she consents to. When the ***processing*** has multiple purposes, consent should be given for all of them specifically. ***Data controllers*** should provide specific information with each separate consent request about the data that will be ***processed*** for each purpose, in order to make ***data subjects*** aware of the impact of the different choices they have.

  

  For example, Lloyd's Market participants cannot ask a ***data subject*** to tick a box consenting to its use of health data for marketing purposes and to disclosure of health data to his or her employer. Two separate consent requests should be made (e.g. via two consent boxes).

- **Informed** – a ***data subject*** should know what he or she is consenting to and should be told about the right to withdraw consent. The process for withdrawing consent should be as easy as it was to give consent and withdrawal of consent should be without detriment or disadvantage i.e. should not result in any costs for the ***data subject***. Where consent is withdrawn, ***processing*** of ***personal data*** must stop unless the ***data controller*** can rely on an alternative legal ground. Additionally, for consent to be informed, it is necessary to inform the ***data subject*** of certain elements that are crucial to make a choice. The ***WP29*** Guidelines (see below) sets out the information that is required, including the ***data controller's*** identity, the purpose of each of the ***processing*** operations for which consent is sought and what type of data will be collected and used.

- **An unambiguous indication of the *data subject*'s wishes** must take clear, affirmative action to consent such as ticking a box or writing an email. Silence and pre-ticked boxes will no longer constitute consent.

- **Demonstrable** – consent must be evidenced.

Current guidance indicates where a product or service (e.g. an insurance policy) is conditional on consent being provided, such consent is unlikely to meet the freely given requirement. The ***ICO*** Guidance (see below) states that where the ***processing*** of ***special categories of personal data*** is genuinely necessary to provide a service, organisations may be able to rely on explicit consent, provided that no other legal ground applies. However the ***processing*** of ***special categories of personal data*** must be necessary to provide the product or service and it is arguable whether this will meet the 'freely given' requirement. In an insurance context, organisations were left with no other option but to rely on conditional consent. This was the driving force behind the lobbying for an insurance specific ***processing*** ground. The insurance purposes ***processing*** ground appears to have now remedied the situation for core insurance ***processing*** activities in respect of UK activities.

Identify the ***processing*** activities for which you will be relying on consent only.

Review consent wording and ensure it is ***GDPR*** compliant.

Keep records of all consent which can be provided if it is later challenged.

Implement a procedure for when a ***data subject*** exercises their right of withdrawal of consent.


For further information, please see the ***WP29*** "Guidelines on consent" which can be accessed here and the ***ICO*** "Guidance on consent" which can be accessed here.

9. DATA RETENTION, DESTRUCTION AND TRANSFER

Data Retention and Destruction

The ***GDPR*** contains a requirement that ***personal data*** is retained for no longer than is necessary. This is the same position as under the current data protection regime. However the ***GDPR*** introduces a new right to erasure for ***data subjects***, which makes it easier for ***data subjects*** to compel a ***data controller*** to delete their ***personal data***, if it is no longer required.

To ensure compliance, a data retention policy should be implemented that specifies the legal and regulatory reasons for retaining categories of ***personal data*** for specified periods of time. This policy needs to be implemented in respect of new and existing records. Likewise, policies and procedures should be put in place that document how destruction of records is handled.

Data controllers should review all ***personal data*** and delete any unnecessary ***personal data*** or consider anonymising any ***personal data*** which is not needed. This will take the data outside of the scope of ***GDPR***.

Implement a data retention policy which covers all ***personal data processed*** by your organisation.

International Transfers

The ***GDPR*** prohibits the transfer of ***personal data*** outside of the ***European Economic Area*** ("**EEA**") unless "adequate data protection" is ensured. This is the same position as under the current data protection regime.

A transfer is permitted if:

- the jurisdiction has been deemed adequate by the European Commission. An updated list of jurisdictions deemed adequate can be found here;
- an approved mechanism is used. The most commonly used approved mechanism is the "Standard Contractual Clauses" (sometimes referred to as the "model clauses"). These are a specific set of contractual wordings approved by the European Commission which can be found here. They should be appended to data transfer agreements or agreements under which ***personal data*** is transferred outside the ***EEA***. The clauses themselves should not be amended as they will lose validity as an approved transfer mechanism; or
- a derogation applies such as:
    - the ***data subject*** has provided consent;
    - the transfer is necessary for the performance of a contract between the ***data subject*** and the controller;

- it is necessary to protect the vital interests of the ***data subject*** (for example a travel policy whereby a ***data subject*** needs assistance when ill on holiday and medical experts need to be instructed); or

- the transfer is necessary for the establishment, exercise or defence of legal claims.

Review all extra-***EEA*** transfers of ***personal data***.

Ensure that all extra-***EEA*** transfers are covered by an "adequacy" mechanism.

Implement a data sharing policy which covers extra-***EEA*** transfers.

10. DATA SECURITY

Personal data must be ***processed*** in a way that ensures appropriate security, including protection against unauthorised or unlawful ***processing*** and against accidental loss, destruction or damage, using technical or organisational measures. This obligation applies to both ***data controllers*** and ***data processors***.

The ***GDPR*** requires ***data controllers*** and ***data processors*** to balance the changing state of technology, the costs of implementation, the risks presented by the ***data processing*** and consequences of breach for ***data subjects***, and implement a level of security appropriate to that risk. This may include:

- ***pseudonymisation*** and/or encryption;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of ***processing*** systems and services;
- the ability to quickly restore the availability and access to ***personal*** data in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of security measures.

The LMA is currently preparing Data Security Guidance which will be published shortly.

ICO guidance on data security can be accessed here and other information contained will be updated in due course to reflect ***GDPR*** requirements.

Review your internal security policy and carry out a review of all physical, organisational and technical security measures. Amend your security policy as appropriate and ensure that a regular review is timetabled.

Consider your approach to encryption, ***pseudonymisation*** and anonymisation.

11. BREACH NOTIFICATION REQUIREMENTS

In the event of a ***personal data breach***, the ***data processor*** must notify the relevant ***data controller*** without undue delay.

The ***data controller*** must notify both the ***supervisory authority*** (the ***ICO*** in the UK) and the affected ***data subjects*** if certain thresholds are met.

Notification to the ICO:

The ***data controller*** must notify the ***ICO*** without undue delay and, where feasible, not later than 72 hours after becoming aware of a ***personal data breach***, unless the breach is "unlikely to result in a high risk to the rights and freedoms" of ***data subjects***.

If the notification is made after 72 hours, the notification should be accompanied by reasons for the delay.

Notification to affected data subjects

The ***data controller*** must notify the affected ***data subjects*** where the ***personal data breach*** "is likely to result in a high risk" to their rights and freedoms.

A notification is not required if:

- the ***data controller*** has implemented appropriate security measures that render the ***personal data*** unintelligible to any unauthorised person, such as encryption;
- the ***data controller*** has taken subsequent measures to ensure the high risk to ***data subjects*** does not materialise; or
- it would involve disproportionate effort, in which case a public communication will suffice.

Firms should also remember that a notification to the Financial Conduct Authority and/or Lloyd's may be necessary in accordance with their requirements.

Organisations should implement a data breach response plan (which may be part of a wider policy/procedure) which sets out key roles and responsibilities within the organisation, saving time and confusion if a ***personal data breach*** occurs. This will enable a quick reaction to identifying and containing a ***personal data breach*** and notifying the ***ICO*** within the 72 hour period.

Once implemented, the data breach response plan should be regularly reviewed and tested, with training given to employees.

Contracts with third parties should be reviewed to ensure that there are appropriate requirements in place requiring such third parties to notify ***data controllers*** of a ***personal data breach*** relating to its ***personal data*** within an appropriate period. The LMA Market Model Agreements, which can be accessed here, require notification of a ***personal data breach*** within 24 hours.

For further information, please see the ***WP29*** "Guidelines on ***personal data breach*** notification" which can be accessed here.

12. ACCOUNTABILITY

The ***GDPR*** introduces a new principle of accountability. ***Data controllers*** are responsible for, and must be able to demonstrate compliance with, the data protection principles.

There are many obligations throughout the ***GDPR*** which require documentation to be kept, which will need to be produced to a ***supervisory authority*** on request.

Data controllers must have appropriate policies and procedures in place to demonstrate compliance with the principle of accountability. Please see Appendix 3 for a sample list of policies and procedures.

Record of Processing

The ***GDPR*** obliges both ***data controllers*** and ***data processors*** to maintain records of ***processing*** activities. Such records need to include details such as:

- data retention periods;
- recipients of ***personal data***; and
- extra-***EEA*** transfers of ***personal data.***

Organisations must maintain a record of ***processing*** for all ***processing*** activities it carries out. There should also be a process for updating the record of ***processing*** and this should be undertaken by those employees who will be best placed to recognise changes in ***processing*** on a regular basis.

An appointed individual should conduct annual reviews to ensure consistency.

The ***ICO*** has published a template record of ***processing*** for both ***data controllers*** and ***data processors*** which can be found here.

Data Protection Impact Assessments

The ***GDPR*** also introduces a requirement to carry out a Data Protection Impact Assessment (known as a "**DPIA**") where ***processing*** activities present a “high risk” to ***data subjects***.

The ***GDPR*** sets out a particular list of activities which are likely to result in "high risk" to ***data subjects*** and which will trigger the need to carry out a ***DPIA*** prior to the ***processing*** of that ***personal data***. The list is non-exhaustive and includes:

- activities which are systematic and extensive and which use automated ***processing*** of ***personal data*** in order to evaluate, analyse or predict behaviour; and
- large scale ***processing*** of ***special categories*** of ***personal data***.

A ***DPIA*** should contain:

- a description of the ***processing***, including the legitimate interest pursued by the ***data controller***;
- an assessment of the necessity and proportionality of the ***processing***;
- an assessment of the risks to ***data subjects***; and
- the safeguards and measures implemented to protect against those risks.

The ***GDPR*** states that the ***data controller*** should seek the advice of the ***DPO*** when carrying out a ***DPIA***. The ***DPIA*** should be reviewed whenever there is a change to the risks presented by the ***processing*** operations.

If a ***DPIA*** indicates that the ***processing*** would result in a high risk to ***data subjects***, in the absence of steps taken by the ***data controller*** to mitigate the risk, prior consultation with its ***supervisory authority*** is required.

Implement a ***DPIA*** policy and procedure clearly setting out how to identify when a ***DPIA*** should be carried out.

Create a ***DPIA*** template.

In addition to the circumstances set out in the ***GDPR*** and the ***WP29*** Guidance, ***data controllers*** should consider whether a ***DPIA*** is needed when carrying out a new ***processing*** activity, undertaking a new project or implementing a new system.


For further information, please see the ***WP29*** "Guidelines on ***DPIAs***" which can be accessed here.


For further information, please also see the ***ICO*** draft guidance for consultation which can be accessed here. It sets out a list of types of ***processing*** it considers likely to be high risk and which will require a ***DPIA***.

Appointment of a Data Protection Officer

The ***GDPR*** obliges both ***data controllers*** and ***data processors*** to appoint a ***DPO*** in three situations:

- where they are a public body;
- where core activities require regular and systematic monitoring of ***personal data*** on a large scale; or
- where core activities involve large scale ***processing*** of ***special categories of personal data.***

  For the insurance industry, this means that ***processing*** of ***personal data*** must be carried out on a 'large scale' before the requirement to appoint a ***DPO*** is triggered.

  WP29 Guidance states that, in assessing whether or not ***processing*** is large scale, organisations should consider the:

  - number of ***data subjects*** concerned;
  - volume of ***personal data*** being ***processed***;
  - duration, or permanence, of the ***personal data processing****;* and
  - geographical extent of the ***processing*** activity.

If you conclude that you do not meet the threshold for appointing a ***DPO***, this analysis should be documented. It is still advisable to have an individual responsible for data protection compliance.

The ***DPO*** must be selected on the basis of professional qualities and expert knowledge of data protection law but do not need to be legally qualified. The ***DPO*** can either be an employee or contractor. Group companies can appoint a single ***DPO***, provided that the ***DPO*** is easily accessible from each establishment.

The ***DPO*** must be informed of all data protection issues within the organisation in a proper and timely manner, be provided with the necessary resources to carry out his/her tasks and have access to all ***personal data*** and ***processing*** operations.

The ***DPO*** must be independent from the ***data controller*** or ***data processor*** that appoints him or her, must report directly to the highest level of management and shall not be dismissed or penalised for performing his or her tasks. This effectively provides the ***DPO*** with a special "protected status" within an organisation, and may create challenges for employers if there is a need to take legitimate performance management or other action against a ***DPO*** in the context of the employment relationship.

In practice, many organisations within the insurance industry already have a ***DPO*** in place. Nevertheless, the current job specification of the ***DPO*** should be considered in light of the new requirements within the ***GDPR***.

Where a ***DPO*** is not already in place, and prior to such an appointment, consideration should be given to practical issues surrounding the ***DPO's*** appointment, such as the need for independence and appropriate support.

Consider whether your organisation needs to appoint a ***DPO***.

On an ongoing basis, monitor the volume of work assigned to the ***DPO***. Consider additional support as required.

Ensure that the ***DPO*** reports directly to the highest level of management.


For further information, please see the ***WP29*** "Guidelines on ***DPOs"*** which can be accessed here.

Appendix 1

GLOSSARY

Data controller	The natural or legal person which, alone or jointly with others, determines the purposes and means of the ***processing*** of ***personal data***.
Data processor	A natural or legal person which ***processes personal data*** on behalf of the ***data controller***.
Data subject	The living individual about whom ***personal data*** relates.
DPA	Data Protection Act 1998
DPIA	A data protection impact assessment. These assessments, often conducted by a ***DPO***, are used to assess compliance with the ***GDPR*** and any associated data privacy risks.
DPO	Data protection officer.
DSAR	A ***data subject*** access request – a request from a ***data subject*** for access to his or her ***personal data*** and certain information regarding how it is ***processed.***
EEA	European Economic Area.
EU	European Union
Fair processing notice	The notice in which a ***data controller*** must provide detailed information to ***data subjects*** regarding any intended ***processing*** of ***personal data*** (sometimes referred to as a Privacy Statement, Privacy Policy or Information Notice)**.**
GDPR	Regulation (Europe) 2016/679 on the protection of natural persons with regard to the ***processing*** of ***personal data*** and on the free movement of such data (General Data Protection Regulation).

ICO	Information Commissioner's Office.
Joint data controllers	Two or more ***data controllers*** who jointly determine the purposes and means of ***processing*** of ***personal data***
Personal data	Any information relating to an identified or identifiable living person. This information must be held electronically or digitally or in highly structured manual files.
Personal data breach	A breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, ***personal data*** transmitted, stored or otherwise ***processed***.
Process, processing, processed	All possible handling of ***personal data***, including collection, analysis, updating, storing, archiving and deleting
Pseudonymise, pseudonymisation	The process by which ***personal data*** is changed so that it can no longer be attributed to a specific individual without the use of a key (which must be kept securely and separately). At its most simple, it could be removing names and contact details from records and replacing with a reference number.
Special categories of personal data	***Personal data*** revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data or biometric data, data concerning health or data concerning a natural person's sex life or sexual orientation.
Supervisory authority	The data protection regulator in the applicable Member State. In the UK, this is the ***ICO.***
WP29	The Article 29 Working Party, which is the Committee made up of the ***ICO*** and equivalent data privacy regulators across Europe. It is responsible for issuing Europe-wide guidance on the ***GDPR***. Post 25 May 2018, the ***WP29*** will become the European Data Protection Board.

Appendix 2

USEFUL REFERENCES

GDPR text	The text of the ***GDPR*** can be accessed here.
UK Data Protection Bill	The version as amended in Public Bill Committee (Bill 190 2017-19) can be accessed here (the LMA will update this link once the Bill is enacted). Please note that this is unlikely to be the final version of the Bill.
ICO website	The ***ICO*** website can be accessed here. In particular, the ***ICO***'s Guide to the ***GDPR*** is regularly updated and can be accessed here.
WP29 website	The Article 29 Working Party website can be accessed here.
London Market Core Uses Information Notice and guidance	The London Market Core Uses Information Notice can be accessed here and the guidance can be accessed here.
LMA Market Model Agreements and Wordings	The LMA model agreements (***GDPR*** and criminal finance act 2017 amendments) can be accessed here.

Appendix 3

FAIR PROCESSING NOTICE (LONG FORM – LAYER 2) CHECKLIST

Identity and contact details of ***data controller*** and ***DPO***	It should be clear who the relevant ***data controller*** is.
About the Insurance Market	Insert the wording below which provides information about the insurance market and links to the London Insurance Market Core Uses Notice: "*Insurance involves the use and disclosure of your personal data by various insurance market participants such as intermediaries, insurers and reinsurers. The London Insurance Market Core Uses Information Notice sets out those core necessary personal data uses and disclosures. Our core uses and disclosures are consistent with the London Market Core Uses Information Notice. We recommend you review this notice by clicking here [insert link].* "
Categories of ***personal data*** you ***process***	• Include information about the ***personal data*** and ***special categories of personal data*** which is ***processed*** for each type of ***data subject***.
Set out each use you make of ***personal data*** and the legal ground you rely on	• Set out each use you make of ***personal data*** and ***special categories of personal data*** and the respective legal grounds you rely on. • If relying on "legitimate interests" for ***processing personal data***, explain what that interest is.
Source of ***personal data***	• Set out all sources of ***personal data*** including publically available sources.
Recipients /categories of recipients to whom you disclose ***personal data***	• Where possible, name recipients. This will often be hard to do in an insurance context as there will be various third parties and complex insurance chains. As a minimum you should provide information about the categories of recipients (e.g. brokers, reinsurers). • Reference disclosure with group companies.
Details of international transfers	• This should include the mechanisms you rely on to make such transfers "adequate" such as the Standard Contractual Clauses.

Data retention periods	• It is not sufficient to state generically that ***personal data*** will be kept as long as necessary. • Where possible, different retention periods should be stipulated for different categories of ***personal data*** (e.g. if you take out a policy with us but do not make a claim, we will keep your information for 7 years from the date of policy expiry). • Alternatively, provide information about the criteria that is used to determine retention periods, (e.g. the Limitation Act 1980 means that claims under contract cannot be brought after 6 years and therefore we delete your ***personal data*** after that period has elapsed)F.
Data subject rights including the right to complain to the ***ICO***	• Summarise each right and how it can be exercised. • Where you rely on consent, tell ***data subjects*** they have the right to withdraw their consent. • Where you carry out automated decision-making (such as using credit scoring to assess a premium credit application or assess insurance applications) or profiling, provide information about the automated decision making including the logic behind it and consequences.
Whether the provision of ***personal data*** is legally or contractually required and possible consequences of failure to provide such data	For example: • where you need ***personal data*** to administer an insurance policy; or • where a policyholder exercises their right to erasure but then makes a claim under a travel policy and medical experts need to be instructed - it would be impossible to do so without receiving information about the medical problem.

Appendix 4

SAMPLE LIST OF POLICIES AND PROCEDURES

Data controllers are required to implement appropriate data protection policies to demonstrate compliance with the data protection principles. This essentially means that there will be an obligation to have in place all data protection policies which are applicable to an organisation's processing activities. These can be stand-alone or combined.
External Fair Processing Notice (governing the use of non-employee data)

Employee policies:

- Employee data privacy notice (governing the use of employee data)
- HR handling of employee personal data policy
- Data protection compliance policy
- Data protection training
- Bring your own device
- Appointment of a DPO
- Data protection governance structure
- Data protection training materials

General:

- Personal data inventory/processing record
- Personal data access policy
- Data retention
- Data sharing
- Procurement policy
- Procedures for outsourcing
- Data accuracy policy and guidelines
- Engagement of third party data processors
- Data Subject Rights policy (to cover handling of all data subject rights)
- Procedure for producing and maintaining records of processing activities
- Privacy impact assessment template and procedure
- Design of new systems policy
- Use of CCTV
- Transfer of data outside of the EEA

Security policies:

- Data security policy
- Policy and procedure on pseudonymisation or anonymisation and aggregation
- Acceptable use policy
- Disaster recovery / Business continuity
- Breach response – operational management; relevant supervisory authority notification and data subject notification

Online/Marketing:

- Social media
- Cookies policy
- Direct marketing

Data Protection Bill - Part IV Policy


INSIGHT CONSENSUS INFLUENCE


DAC beachcroft