GENERAL DATA PROTECTION REGULATIONS (GDPR)

OVERVIEW FOR UNDERWRITERS

Issued July 2017

INSIGHT CONSENSUS INFLUENCE

Introduction

- GDPR becomes effective on 25 May 2018, replacing the current Data Protection Act 1998 (it will take direct effect in UK law before Brexit).
- GDPR is relevant to those dealing with policies relating to individuals, either singly or part of a group scheme.

Definitions

- **Personal data:** Any information relating to a living person by which they can be identified ("data subject").
- **Special Categories of personal data:** Any data relating to racial or ethnic origin, political opinions, religious beliefs, membership of a trade union, physical or mental health or condition, sexual life and (subject to UK government decision) commission, or alleged commission, of any offence.
- **Data Controller:** A firm which decides which data to collect and how it is processed (e.g. a broker, coverholder, insurer and reinsurer).
- **Data Processor:** A firm which processes the data on the instruction of a Data Controller (e.g. a TPA).
- **Processing:** Processing means any operation or set of operations performed upon personal data or sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Legal Position

- GDPR prohibits the processing of personal data unless there are legal grounds to do so. Below are potentially relevant legal grounds you can rely upon under GDPR in order to process personal data and special categories of data:

Personal data	**Special categories of personal data**
• Consent (processing permitted if the data subject has consented to the processing)	• Explicit Consent of the data subject (significantly harder to obtain and requires an affirmative action – see ICO draft guidance)
• Performance of a contract with the data subject (processing necessary for the performance of a contract to which the data subject is a party; or for the taking of steps at the request of the data subject with a view to entering into a contract)	• Legal claims (processing necessary for establishment, exercise or defence of legal claims)
• Vital interests (processing necessary to protect the vital interests of the data subject or other individual)	• Vital interests (processing necessary to protect the vital interests of the data subject or other individual)

• Legitimate interests (processing necessary for the purposes of legitimate interests pursued by the controller (or by a third party), except where the controller's interests are overridden by the interests, fundamental rights or freedoms of the affected data subjects which require protection, particularly where the data subject is a child)	
• In substantial public interest & set out in UK law	• In substantial public interest & set out in UK law (processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject)

Consent and structure of the Lloyd's/London market

- The structure of the Lloyd's and London market presents a potential issue. There could be several different firms which are all Data Controllers (i.e. they collect and process data for their own purposes). As such, where consent is relied upon as the ground for processing, this is required for each of these entities. This makes a Fair Processing Notice complicated as it is required to cover all such entities.
- Those entities not in direct contact with the data subject rely on the entity which is in direct contact to provide a Fair Processing Notice suitable for the entire market.

NOTE: this is the subject of representations by the LMA to government and the ICO.

Fair Processing Notice

- Fair processing notices to be provided to data subjects/policyholders, which must;
  - contain details on purposes and legal grounds for processing
  - set out 'legitimate interest' (where relied upon as a ground)
  - set out right to withdraw consent (where relied upon as a ground)
  - identify recipients / categories of recipients of the personal data
  - provide details of international transfers
  - contain data retention periods or the criteria used
  - confirm existence of data subject rights to: access data, rectification, erasure, restriction, object
  - confirm existence of automated decision making/profiling and the right to complain to the Information Commissioner.

NOTE: The LMA has been working with the other market associations and law firms to produce a draft model Fair Processing Notice. This follows a layered approach with a short form notice being provided to consumers which directs them to a long form notice to be hosted on firms' websites. The draft model notice will be published on the LMA website.

Profiling

- Profiling is the assessment of risk through an examination of data which enables aspects of an individual's personality or behaviour, interests and habits to be determined, analysed and predicted. This is accomplished using various data sources, e.g.:
    - internet and browsing history
    - education and professional data
    - data derived from existing customer relationships
    - driving/location data
    - buying habits
    - social network information.
- Under GDPR, insurers will have to request consent routinely for profiling of individuals as part of underwriting and claims processing. When processing personal data for profiling purposes, firms must ensure that appropriate safeguards are in place, including:
    - ensuring processing is fair and transparent by providing meaningful information about the logic involved, as well as the significance and the envisaged consequences
    - using appropriate mathematical or statistical procedures for the profiling
    - implementing appropriate technical and organisational measures to enable inaccuracies to be corrected and minimise the risk of errors
    - securing personal data in a way that is proportionate to the risk to the interests and rights of the individual and prevents discriminatory effects.

Subject access rights

- Subject access rights entitle an individual to be told:
    - whether any personal data is being processed
    - the reasons for processing, a description of the data and whether it will be given to any other organisations or people, as well as a copy of the data.

Data security breach notification

- A Data Controller is required to notify any data security breach that leads to unauthorised disclosure, access to, or destruction of, personal data to the Information Commissioner's Office ("ICO") within 72 hours.
- The data subject should also be notified if the breach is likely to affect adversely the protection of the personal data or privacy of the data subject.

Right of erasure – the right to be forgotten

- The GDPR provides data subjects with a new enhanced right to request erasure of their personal data.
- Data controllers must delete personal data on request where specified grounds apply. Such grounds include:
    - where the personal data is no longer necessary for the original purpose for which the personal data was collected/processed
    - if the data subject withdraws their consent and no other legal ground for processing applies.

Fines

- The ICO is the regulator of GDPR in the UK and has a range of powers available, including fines for serious breaches up to EUR 20 million or 4% of total worldwide annual turnover, whichever is higher in the preceding financial year.

Materials

This is a high-level overview only of the GDPR. The GDPR can be found here.

The website of the Information Commissioner's Office (ICO).

The LMA GDPR webpage.