General Data Protection Regulation

In this briefing we take a closer look at the General Data Protection Regulation (GDPR) and highlight some of the areas that are likely to be of greatest interest to the insurance industry

Executive Summary

At a time of fast paced change and innovation within the insurance sector the combination of data and technology is increasingly intertwined with every area of business. It is against this backdrop that GDPR enters the stage and revamps the law in relation to how data can be lawfully processed i.e. how it is collected, analysed, shared and stored. Compliance with existing legislation such as the Data Protection Act 1998 will tick many of GDPR's boxes; however GDPR also imposes new obligations, enhances existing rights and creates new ones.

In this briefing we focus on several areas of GDPR of particular interest and importance to the UK insurance sector, providing an overview and hopefully some illumination of some key areas and requirements. GDPR runs to over 100 pages and includes 99 Articles (the law) and 173 Recitals (the reasons) so this document is intended to provide a useful highlight of some of the key points, covering the requirements for lawful processing and the implications for areas such as fraud and data security.

Although it is true that GDPR introduces a tougher enforcement regime, with significant penalties for non compliance, it also provides new opportunities. The ability to demonstrate compliance, to offer transparent processing of personal data and systems that keep data secure will be a business enabler that is likely to generate increased customer confidence and may influence purchases.

Introduction and scope

GDPR comes into force on 25 May 2018 and represents the most significant overhaul of data protection and privacy laws in over 20 years, replacing the 1995 EC Directive from which the Data Protection Act 1998 flowed.

The law was well overdue an update to reflect the advances in technology and the fundamental shift in how data is collected, stored and shared. There was also a desire for a stronger enforcement and sanctions regime and a need for consistency across the 28 Member States, each with their own data protection laws, requiring alignment.

Published in May 2016 GDPR provides the supervisory authority with increased powers, enhances and strengthens the provisions of the Data Protection Act 1998 and creates several new important obligations and rights. The scope of GDPR extends not only to organisations established within the EU, but also to organisations outside of the EU who offer goods or services to EU citizens, or monitor their behaviour.

In addition to the broadening of territorial scope, the definition of personal data has also been broadened or at least better defined and under GDPR can include locational data (such as GPS co-ordinates) ‘online identifiers’ such as IP addresses, device ID's and Cookies.

GDPR does not apply to purely personal or household activities or to law enforcement.

Brexit and the Data Protection Bill

With the UK set to leave the EU in 2019 and GDPR taking effect from 25 May 2018 the ICO has confirmed that organisations will be expected to comply with the Regulation from the date of implementation. Post Brexit, organisations who process the personal data of EU Citizens relating to the offering of goods or services or the monitoring of their behaviour will continue to be bound by the Regulation regardless of any new domestic legislation. Furthermore, in June 2017 the Queen’s Speech heralded a new Data Protection Bill for the UK to implement the provisions of GDPR into UK law. This announcement was amplified by the Government's Statement of Intent on 7 August 2017 when it was confirmed that the Data Protection Bill would, in addition to implementing GDPR, exercise the available derogations under GDPR, repeal the Data Protection Act 1998 and implement the EU Data Protection Law Enforcement Directive.

A snapshot of some of the new provisions under GDPR

– Explicit consent required	– Right to erasure
– Enhanced right to object	– Data portability
– Reduced SARS response time	– Removal of SARS fee
– Privacy by Design & Default	– Reduced Exemptions
– Enhanced privacy notices	– Enhanced data security
– Mandatory breach reporting	– Mandatory record keeping
– Robust enforcement regime	– Broader territorial scope
– Accountability	– Mandated DPIA
– Enhanced profiling rights	– Direct processor liability

The principles

Six general principles relating to the processing of personal data form the cornerstone of the GDPR. These are very similar to the principles within the Data Protection Act 1998 and are as follows:

– Lawfulness, fairness and transparency	– Purpose limitation
– Data minimisation	– Accuracy
– Storage limitation	– Integrity and confidentiality

– **Lawfulness, fairness and transparency -** Data Controllers must show that their processing is lawful, fair and transparent in relation to data subject rights.

– **Purpose limitation -** Data processing must relate to a specific, explicit and legitimate purpose. Data must not be processed in a manner that is incompatible with the stated purpose/s. Generic purpose statements will not be compatible with GDPR.

– **Data minimisation -** Data collected must be limited to what is necessary. It must be adequate, relevant and not excessive, having regard to the stated purpose for which data is being processed.

– **Accuracy -** Data must be kept accurate and up to date. Controllers must be able to correct personal data 'without undue delay'.

– **Storage limitation -** Data should not be kept for any longer than is necessary. Data retention policies should establish time limits for erasure, although it is permissible to retain data for longer periods for archive or statistical purposes only.

– **Integrity and confidentiality -** Personal data must be processed in a manner that ensures appropriate security including protection against unauthorised or unlawful processing, loss, destruction or damage, using appropriate technical or organisational measures.

What constitutes lawful processing?

In addition to complying with the six data processing principles above, data processing will not be lawful unless it also satisfies at least one of the following processing conditions:

– **Consent –** The data subject has provided consent for the processing. Valid consent is much harder to gain under GDPR and implied consent or default 'opt ins' will not comply. Consent needs to be explicit and involve a clear affirmative act by the data subject.

– **Contract –** The processing is necessary for the performance of a contract.

– **Legal obligation –** The processing is necessary for compliance with a legal obligation to which the controller is subject.

– **Legitimate interest –** The processing is necessary for the purposes of the legitimate interests pursued by the controller, or by a third party, except where such interests are overridden by the interests or fundamental rights of the data subject. Fraud prevention, cybersecurity and direct marketing are examples of the type of activities that might constitute legitimate interests.

– **Vital interest -** The processing is necessary to protect the data subject's vital interests, such as in a medical emergency.

– **Public interest** – Processing is necessary for a task carried out in the public interest.

Practice Point:

- Be clear about the purposes for which you are going to be processing personal data and for each purpose know which of the above grounds for lawful processing that you are going to rely upon.
- If you are relying upon consent as a ground for lawful processing then ensure that you are aware of the more stringent requirements under GDPR for valid consent

Data Subject rights

Individuals' rights are enhanced under GDPR and controllers need to have adequate policies, systems and modalities in place to facilitate those rights. It is likely to take some time to implement these new requirements and the preparation time involved should not be underestimated.

– **Information Notices** - If personal data is collected there is an obligation to inform individuals at the time of collection. This has been the case under the Data Protection Act 1998 but under GDPR there are additional requirements. Information Notices must use clear and plain language, be intelligible, transparent and easily accessible. Additional information must be supplied to individuals under GDPR as the table below illustrates:

Contents of information notices	DPA 1998	GDPR
– Identity of controller and any representatives	✓	✓
– The purpose of processing	✓	✓
– Identity of any recipients of the data	✓	✓
– An explanation of the rights of access and rectification	✓	✓
– Any additional reasonably necessary information to guarantee fair processing	✓	✓
– An explanation of the controller's legitimate interests (if relied on as a processing condition)		✓
– The data retention period		✓
– Contact details of the DPO		✓
– An explanation of the rights to erasure, portability, restriction of processing, object and withdraw consent		✓
– That the individual has a right to complain to the Supervisory Authority		✓

– **Right to object** - GDPR enhances an individual's right to object to processing. Whereas under the DPA 1998 this right was limited to a right to object to processing that caused damage or distress, GDPR contains no such limitation.

– **Right to object to automated decision making** – Although this right existed previously it is enhanced by GDPR to include a right to request human intervention.

– **Subject access requests** – Individuals have the right to request confirmation of whether their personal data is being processed and if so access to that data and the following information:

Subject Access Requests – responses to include

– Purpose of the processing
– Categories of personal data concerned
– Recipients or categories of recipient of the data
– Existence of the rights to request erasure; rectification; restriction of processing; to object
– Data retention period
– Right to lodge a complaint with the Supervisor Authority
– Existence of any automated decision making, including profiling
– Source of data collected, if not from the data subject

GDPR makes significant changes to the Subject Access Request procedure. In particular, the time limit for compliance is reduced from 40 days (under the DPA 1998) to one month. In addition, the £10 fee that was previously chargeable by controllers for responding to such requests has now been abolished and controllers are required to respond free of charge. It is important for all processors to note that subject access requests they receive need to be passed to and dealt with by the controller.

– **Right to rectification** - Individuals have the right to request that controllers rectify any inaccuracies in their personal data, without undue delay.

– **Right to data portability** – This is a completely new right and gives individuals the right to request that their personal data be transferred from one controller to another, free of charge, in a structured, commonly used and machine readable format. This does not apply to paper records. This right only relates to data that was provided to a controller.

– **Right to erasure** – Commonly referred to as the 'right to be forgotten' this right empowers individuals to request that a controller erase their personal data, without undue delay. The right only applies in certain situations including when the individual withdraws their consent for processing or objects; where the processing is unlawful or where the data is no longer required for the stated purpose of processing.

– **Right to restrict processing** – Individuals have the right to request that the controller restricts the processing of their personal data where one of the following applies:
  – The accuracy of the data is contested
  – The processing is unlawful
  – The controller no longer needs the data for the stated processing purpose
  – The individual has objected to the use of processing based on the controller's legitimate interests

Where processing has been restricted under this right, it should only be stored and not further processed until either the data

subject has provided consent or the processing is necessary in connection with legal claims, protection of rights or for reasons of important public interest. It may be appropriate to move data that is subject to restricted processing to a suppression list to prevent further processing.

Practice Point:

- Review your processes and systems for dealing with customers and third parties and ensure that they are sufficient to facilitate the revised and expanded data subject rights.
- Review template letters and documents to ensure that the additional required information under GDPR is included.

Exemptions

The rights of data subjects are qualified rights and not absolute. Article 23 of the GDPR enables Member States to introduce their own derogations to GDPR in specified areas including the selection below. The UK Government has already confirmed that it intends to utilise these exemptions within the Data Protection Bill and the ICO has indicated its view that these should be similar to exemptions contained in existing legislation.

Selection of exemptions

- National Security
- Public Security
- The Enforcement of Civil Law Claims
- Defence
- Prevention, Investigation, Detection or Prosecution of Criminal Offences
- Matters of General Public Interest including Monetary, Taxation, Budgetary and Public Health objectives

Controllers and processors

Controllers

Controllers are responsible for implementing appropriate technical and organisational measures to ensure that any processing of personal data is compliant with the Regulation. Controllers must only use processors who can provide sufficient guarantees that they will comply with GDPR.

Controllers must ensure that processing by a processor is governed by a contract and this contract needs to stipulate that the processor:

- Processes personal data only on documented instructions from the controller
- Ensures that persons involved in the processing are committed to confidentiality
- Ensures processing meets the security requirements laid out in Article 32
- Shall not engage another processor without the written approval of the controller
- Where another processor is engaged, the contractual obligations between the controller and processor shall be imposed on that other processor
- Assists the controller in facilitating data subjects rights
- Assists the controller in ensuring compliance with Articles 32-36 (security, breach notifications and impact assessments)
- At the choice of the controller, deletes or returns all personal data to the controller

Processors

In a significant change to the Data Protection Act 1998, GDPR will apply directly to processors whose legal obligations will include maintaining written records of processing carried out for each controller, implementing adequate security measures, designating a data protection officer where required, ensuring contracts with controllers contain specific provisions in accordance with Article 28(3) and notifying the controller of any personal data breach.

Sensitive Personal Data

The default position under GDPR as regards to sensitive personal data (referred to as 'special category data') such as data concerning racial or ethnic origin, political views or religious beliefs is that processing of it is prohibited unless one of the following conditions applies:

Sensitive Personal Data	
– The data subject has given explicit consent	– Processing is necessary for the purposes of carrying out specific rights of the controller or data subject
– Processing is necessary to protect the vital interests of the data subject	– Processing is carried out in the course of legitimate business activities with appropriate safeguards in place
– Processing relates to personal data that has been made public by the data subject	– Processing is necessary for the establishment or defence of legal claims

– Processing is necessary for reasons of substantial public interest	– Processing is necessary for public interest in the area of public health
– Processing is necessary for the purposes of preventative or occupational medicine	– Processing is necessary for archiving purposes in the public interest such as scientific research
– The data subject has given explicit consent	– Processing is necessary for the purposes of carrying out specific rights of the controller or data subject

GDPR expands the categories of sensitive personal data to include genetic data and biometric data.

Security

GDPR places greater emphasis on ensuring that personal data is properly protected. Article 32 mandates a risk based approach requiring the ongoing confidentiality, integrity, availability and resilience of data and processing systems. A multi layered, defence-in-depth approach is required to avoid single points of failure.

Techniques such as encryption and pseudonymisation of data are encouraged and explicitly referred to within GDPR. Pseudonymisation involves the splitting of data, to separate the data from which a person cannot be identified which can be held on one database, and data from which a person can be identified will be held on another database and subject to additional security measures.

In addition to the implementation of robust security measures, controllers and processors are required to be able to demonstrate effective monitoring of those measures, including regular testing as part of a wider Business Continuity Plan and to have the ability to restore systems in a timely manner. The security controls in place should enable an organisation to reduce dwell time.

Breach Notification

Controllers and processors are now subject to a mandatory personal data breach requirement. The Supervisory Authority must be notified of any personal data breach without undue delay and no later than 72 hours after becoming aware of it.

The breach notification should include the following information:

- The nature of the breach including the approximate number of data subjects, personal data records and the categories of data concerned
- The name and contact details of the DPO
- The likely consequences of the breach
- The measures taken by the controller to address the breach and mitigate its effect

Fraud

Concern has been expressed that GDPR does not contain an equivalent of section 29(3) of the Data Protection Act 1998 which organisations regularly rely upon when processing personal data during the course of fraud investigations. That section created an exemption from the requirement to process data fairly and lawfully where the purpose of processing was to prevent or detect crime.

Article 2 stipulates that GDPR does not apply to data processing by 'competent authorities' for the purposes of prevention, investigation, detection or prosecution of criminal offences. This category of processing is instead covered by the EU Data Protection Law Enforcement Directive. This does not assist the private sector in terms of their ability to lawfully process personal data in connection with fraud investigations. It is hoped that the Data Protection Bill will be worded to facilitate such processing. It is encouraging that the Government has confirmed that the Bill will exercise the available exemptions in GDPR and it is also noteworthy that the ICO has indicated its view that those exemptions should mirror the exemptions that apply in existing legislation i.e. the Data Protection Act 1998.

In the absence of an exemption to the requirement to process personal data fairly and lawfully it is necessary to consider whether it is possible to process data for the purposes of fraud prevention/detection in a lawful manner. This means satisfying one of the six processing conditions that we have set out above. Processing for the purposes of legitimate interests is one such condition and Recital 47 does expressly stipulate that the processing of personal data for the purposes of preventing fraud can constitute a legitimate interest. In addition, insofar as automated processing is concerned Recital 71 states that processing, including profiling, should be allowed where authorised by law including for fraud, tax evasion monitoring and prevention.

Article 23 contains several possible exemptions to data subject rights. We have listed those exemptions above and one such exemption is the processing of personal data that is necessary for the 'prevention, investigation, detection or prosecution of criminal offences'. It is anticipated that this exemption will be included within the Data Protection Bill which would potentially permit restricting data subject rights during fraud investigations.

Practice Point:

- Consider whether you need to conduct a DPIA in respect of your fraud prevention activities including the handling of intelligence alerts, disclosure requests and responses and counter fraud systems.

- Remember that the Data Protection Bill will clarify permitted exemptions and this is likely to be highly relevant to counter fraud activities

Governance

Accountability

GDPR introduces a new principle of accountability. This places obligations on controllers around data governance, to not only comply with the Regulation, but to be able to demonstrate compliance. This includes requirements to maintain certain documentation, implement data protection by default and design and to conduct data protection impact assessments for any processing activities that create a high risk to data subjects. The accountability principle can be satisfied in part by having appropriate policies, records and systems in place.

Record keeping

The record keeping requirements are set out in Article 30. Whilst there is an exemption for companies with under 250 employees, most of the information required to be recorded is likely needed in order to comply with other Articles such as the requirements to provide information notices. Controllers and processors are obligated to maintain records in respect of the following:

Records to be kept

– Name and contact details of the controller	– The purpose of processing
– A description of the categories of data subjects and personal data	– The categories of recipients to whom the personal data will be disclosed
– Envisaged time limits for erasure of different categories of data	– Transfers of personal data outside of the EU
– A general description of the technical and organisational security measures	

In addition, processors are also required to maintain a record of all processing activities carried out on behalf of a controller containing:

– The name and contact details of the processors and of each controller on behalf of which the processor is acting	– The categories of processing carried out for each controller

Data protection by design and default

Controllers are obligated to implement appropriate technical and organisational measures to ensure that at the outset of any service, product, system or process design, data minimisation is applied so as to ensure that only data that is necessary is collected, stored and processed.

Data Protection Impact Assessments

Article 35 mandates the use of Data Protection Impact Assessments for any processing activity that is likely to result in a high risk to data subjects. Even when a DPIA is not mandated, organisations should consider using them as best practice. Privacy Impact Assessments have been recommended by the ICO since 2006 and are renamed as Data Protection Impact Assessments by GDPR.

A DPIA should include the following:

– A systematic description of the envisaged processing operations and purposes of processing
– An assessment of the necessity and proportionality of the processing
– An assessment of the risks to the rights of data subjects
– The measures envisaged to address the risks, including safeguards, security and mechanisms to ensure protection of the personal data

Data Protection Officers

GDPR stipulates that a DPO must be appointed when any of the following apply:

– Processing is carried out by a public authority
– The core activities of the controller or the processor involve systematic monitoring of data subjects on a large scale
– The core activities of the controller or processor consist of processing sensitive data on a large scale

The Article 29 Working Party have provided some guidance on the appointment of a DPO and within that they cite an example of ‘systematic monitoring of data subjects on a large scale’ as an insurance company processing customer data.

Even where the appointment of a DPO is not mandated, it might be considered best practice.

A DPO must have an independent function from the business and have access to senior management and be empowered to address issues. They may be either internal or external and should have an expert knowledge of data protection law.

Expected tasks of a DPO

– To inform & advise the controller or the processor and the employees who carry out the processing of their obligations under GDPR

- To monitor compliance with GDPR including awareness raising, training, audits and assignment of responsibilities
- To provide advice in relation to data protection impact assessments
- To cooperate with the supervisory authority
- To act as the point of contact for the supervisory authority

Practice Point:

- Consider whether you need to appoint a DPO
- Ensure that you are keeping records for all of the required data fields
- Supplier contracts and arrangements will need to be audited and updated to reflect the obligations of data processors under GDPR

Penalties

As the ICO have recently pointed out, there has been a good deal of scaremongering in respect of the consequences of non-compliance and the level of fines that may be imposed, underlining its commitment to advising and educating organisations and using its powers judiciously and proportionately.

However, the new enforcement regime certainly warrants highlighting. Where a breach infringes a data protection principle or a data subject right, fines of up to 4% of global turnover or €20 million, whichever is higher can be imposed. Where the breach infringes a controller or processor obligation, a fine of up to 2% of global turnover or €10 million, whichever is higher, is possible.

Recital 148 states that when considering the level of fine the nature, gravity and duration of any breach will be taken into account and in the case of a minor infringement a reprimand may be more appropriate.

Fines are not the only element of the enforcement regime. In addition, Article 82 provides a right to claim compensation for any person who has suffered material or non-material damage as a result of an infringement of GDPR. Supervisory authorities also have powers to conduct investigations, audits, access premises and equipment and to issue warnings, reprimands and corrective orders.

Achieving compliance

The appropriate next steps in achieving GDPR compliance will vary considerably between organisations. Here are some suggested starting points: checking your level of compliance with existing data protection and privacy legislation should help identify any immediate gaps that require addressing. It is also important to understand what personal data you hold, where it is located, what the data entry, exit points and transfer methods are within your business. A data mapping exercise can help achieve this. Start to think about and plan how you are going to facilitate the enhanced data subject rights such as the new requirements for information notices, the right to erasure and the more onerous subject access request procedure. Don't forget that any areas of processing that might be regarded as high risk must be subject to a data protection impact assessment. Policies, contracts and all data protection wording/clauses should be reviewed and revised to ensure they are GDPR compliant. Consider whether you are obligated to appoint a DPO and even if not, whether you ought to do so anyway as best practice.

This briefing not does not constitute and is not a substitute for legal advice and is limited to certain aspects of GDPR only.

Contacts

If you would like to discuss in more detail how DWF can help your organisation, please do not hesitate to contact us

Jamie Taylor
Director
T +44 161 604 1606
M +44 7712 799 712
E Jamie.Taylor@dwf.law