General Data Protection Regulation (GDPR)

The General Data Protection EU Regulation (the "GDPR") has applied in all EU Member States since 25 May 2018. The national Data Protection Authorities (DPAs) are in charge of enforcing the rules and are coordinating their actions through new cooperation mechanisms and the European Data Protection Board (EDPB).
processing of health data by insurance intermediaries

> The GDPR only covers the **processing of personal data:** this is information that relates to a living identified or identifiable person (a data subject). Special categories of data, such as health data, are subject to additional protection and such data will only be processed with express consent from the data subject. Derogations are possible. **Data processing** covers most activities involving personal data: collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure and destruction.

The GDPR is a cross-sectoral legislation. **It applies to the insurance distribution sector** but is not specific to it.

The GDPR and insurance intermediaries

Controllers or Processors or Joint Controllers?
In most cases, insurance intermediaries will process personal data on their own account and will act as data controllers. In some others, intermediaries will act under clear processing instructions from a data controller (example: an insurer) and will be data processors. Intermediaries could also be joint controllers. The GDPR requires joint controllers to reach an arrangement to determine their respective responsibilities for compliance with the obligations under the GDPR.

Legal basis for processing sensitive data
A significant GDPR challenge for insurance intermediaries is the processing of sensitive and mainly health data. Under the GDPR, as a matter of principle, it is prohibited to process sensitive data. Derogations are provided to this general prohibition in the circumstances exhaustively described in Article 9§2. However, the processing of health data by insurance intermediaries does not readily fall in one of the exceptions to the general prohibition of the processing of personal data. It should consequently be verified whether the can be covered under one of the derogations.

The May 2022 Commission's proposed Regulation on the European Health Data Space (EHDS) builds on the GDPR and aims to "provide a trustworthy setting for secure access to and processing of a wide range of health data". BIPAR will study the impact of the proposal on the sector and will monitor the EP and Council readings on it.

EDPB Guidelines

The GDPR is supplemented by guidance issued by the EDPB. Over the last years, the EDPB has published different guidelines on key GDPR issues, and in particular, in July 2021, its **guidelines on the concepts of controller and processor in the GDPR.** The application of these concepts to insurance intermediaries has been challenging and continues to be in some markets. Other guidelines of interest to insurance/financial intermediaries have also been published over the last 12 months, such as EDPB draft **guidelines on "data subject rights - Right of access".**

The transfer of personal data from the European Economic Area (EEA) to third countries

UK adequacy decisions
Several solutions are provided by the GDPR regarding the transfer of data to third countries (outside the EEA). The adoption of an adequacy decision by the European Commission under GDPR Article 45 is one solution. In June 2021 the European Commission adopted two adequacy decisions for the UK - one under the GDPR and the other for the Law Enforcement Directive (see texts here).

The effect of such a decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to the UK without any further safeguards being necessary. In other words, transfers to the UK will be assimilated to intra-EU transmissions of data. This is an important decision for EEA insurance intermediaries who are transferring personal data of their clients to the UK, and for UK intermediaries.

The decisions will automatically expire four years after their entry into force. After that period, the adequacy finings might be renewed.

Review of the Standard Contractual Clauses (SCCs)

In June 2021 the Commission adopted two sets of Standard Contractual Clauses (SCCs), one for the transfer of personal data to third countries and one for data processing between controllers and processors in the EEA.

European Commission's revised SCCs for the transfer of personal data to third countries

SCCs are the most frequently used mechanism by firms - including insurance intermediaries - in the EEA when transferring data to countries outside the EEA (third countries) that the Commission identifies as providing an "inadequate "level of data protection.

Under the GDPR, and in the absence of a Commission adequacy decision with those third countries, a controller or processor may transfer personal data to third countries only if they have provided appropriate safeguards. Such safeguards may be provided for by Commission standard data protection clauses. However, on July 16, 2020, in the Schrems II decision, the Court of Justice of the EU brought substantial doubt about whether the current SCCs remain effective, especially regarding transfers to the United States. *Schrems II* requires parties relying on the standard clauses to implement additional appropriate safeguards ensuring that transferred personal data is adequately protected when personal data is transferred to countries outside of the EEA.

Following its November 2020 consultation in which BIPAR participated, on 4th June 2021 the Commission published **its revised SCCs for the transfer of personal data to third countries** (*available in all EU languages here*). According to the Commission, the revised SCCs reflect the requirements of the GDPR and take into account the Schrems II decision. The Commission considers that they provide appropriate safeguards, subject to the parties' identification of sufficient technical and organisational measures for protecting personal data.

EDPB recommendations

In June 2021, following public consultation on its draft recommendations in which BIPAR participated, the EDPB adopted its final recommendations on measures that supplement transfer tools (like SCCs) to ensure compliance with the level of protection required under EU law of personal data transferred to third countries. The recommendations aim to assist controllers and processors acting as data exporters with their duty to identify and implement appropriate supplementary measures where they are needed to ensure an essentially equivalent level of protection to the data they transfer to third countries. Regarding the revised SCCs for the transfer of personal data to third countries, the Recommendations are helpful to check "*Local laws and practices affecting compliance with the Clauses*" (Clause 14 of the revised SCCs) and the possible need to implement supplementary measures.

European Commission's new SCCs between controllers and processors in the EEA

Article 28 (3) of the GDPR **require**s data controllers, when entrusting a processor with processing activities, to put in place a contract or other legal act that stipulates the strict terms and conditions of the processing (duration of the processing, the nature and purpose of the processing, the types of personal data being processed, the categories of data subjects, and the obligations and rights of the controller).

Insurance intermediaries, agents or brokers, use data processing contracts in their daily activities:

- in their relations with data controllers (e.g. insurers) when agents/brokers are data processors processing data on behalf of the data controllers or
- in their relations with data processors who are processing data on behalf of agents/brokers when those are data controllers.

In June 2021, following a consultation on its draft Controllers-Processors SCCs in which BIPAR participated, the Commission published **its SCCs between controllers and processors** (*see document available in all EU languages here*). The use of new EEA Controller-Processor SCCs is not mandatory. However, the use of the EEA Controller-Processor SCCs is important as they give a clear signal on the level of information that the Commission expects to see in these binding data processing contracts. In effect, the Controller-Processors SCCs will benefit from a presumption that they meet the requirements of GDPR Art. 28.

In June 2022, the Commission developed Questions and Answers (Q&As) to provide practical guidance on the use of the two sets of SCCs and assist stakeholders in their compliance efforts under the GDPR. The Q&As are intended to be "a dynamic source of information and will be updated as new questions arise".