BIPAR's comments on the Article 29 Working Party guidelines, aspects requiring further clarification and sector-specific examples of data processing

1. Data portability

The GDPR creates **a new right to data portability**: it allows data subjects to receive the personal data, which they have provided to a controller (such as an insurance intermediary), in a structured, commonly used and machine-readable format, and to store it for further personal use on a private device or to transmit to another data controller "without hindrance". This is a duty **only on data controllers** and **only in set circumstances** (where data processing is based either (i) on the data subject's consent or (ii) on performance of a contract and (iii) the processing is carried out by automated means).

- The WP29 guidance states that the right to data portability only covers data provided by data subjects, not data inferred and derived by the controller or processor in the course of executing the insurance contract. BIPAR understands this to mean that claims histories for instance do not fall within the scope of the right to data portability. Is that a correct understanding?

- BIPAR wonders **how this new right of data portability will impact the insurance industry as a result of other existing rights which enable clients to receive more extensive information than that to which they would be entitled pursuant to Article 20 of GDPR.**
  For example under the laws of some EU countries, insurance intermediaries' clients are entitled to receive copies of documents held on their policy files or request that they are provided to another intermediary in the event that they want to change intermediary. Whilst clients are not entitled to everything held on the files, they are entitled to the following (regardless of whether it contains personal data):
  - Policy documents including slips, endorsements and the policy wording
  - Correspondence between intermediaries and the client
  - Correspondence between intermediaries and the insurer where they are acting on the client's behalf
  - Correspondence between intermediaries and a third party where they are acting on the client's behalf
  - Meeting and/or telephone notes recording discussions with the client or with the insurer where intermediaries are acting on the client's behalf.

- There is no reference to **proportionality** in the guidelines. BIPAR believes that SME data controllers may face disproportionate costs in setting up the systems required to fulfil portability requests. BIPAR believes that further guidance is needed, in particular to interpret the term "technically feasible".

- Often, individuals arrange insurance for themselves as well as other members of their household or family (see section 5 below). Insurance intermediaries therefore process personal data about several data subjects. The WP29 states that in such cases, data controllers **must not take an overly restrictive interpretation** of the GDPR provisions which would limit data portability rights to **"personal data concerning the data subject"**. BIPAR understands this to mean that when answering a data portability request, it would not be unlawful to provide to the requesting data subject the personal data on all family or household members covered by the insurance policy. BIPAR welcomes such a pragmatic approach, which is in the interest of consumers and beneficial for insurance intermediaries. That said, page 9 of the guide states: 'Where personal data of third parties are included in the data set, another ground for lawfulness of processing must be identified' which in itself could hamper the activities of the receiving controller in supplying the requested service to the data subject.

- The **impact of data portability on relations between joint controllers and between controllers and processors** remains unclear. There are many circumstances in which intermediaries are likely to be considered either joint controllers with a (re)insurer or a processor to a (re)insurer, such as where business is written under a binding authority agreement. BIPAR regrets that no guidance was given on this critical aspect and calls for greater clarification.

Av. Albert-Elisabeth, 40- B-1200 Bruxelles - Tel: 0032-2-735.60.48 - Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu

- BIPAR would welcome guidance clarifying whether the controller's duty to comply with a portability request is limited to its interaction with the data subject or **whether there is a duty on a controller to share portability requests with other controllers with whom they have shared personal data.**

- BIPAR believes that development of common standards by national professional associations would enable sectors to deal effectively with the requirement to provide information in a "structured, commonly used and machine-readable format", mindful of legal frameworks and national preferences. Further guidance from the WP29 would be useful.

- Additionally, as the guidance stipulates that the data subject must be able to 'store it for further use on a private device' this limits the 'commonly used and machine readable' formats to those used by software that might typically be found on a home laptop (such as a Microsoft Office application), or widely downloaded app for a smartphone (if such can be identified). There is a high risk that such formats may not be compatible with the programmes that commercial firms operate for processing customer data. This then in turn, creates a situation where firms need to develop programmes that permit downloads in many different formats – with obvious significant cost implications.

- It should be noted that the insurance intermediation market is made up of many small businesses and so have neither the resources to create APIs, nor to develop secure areas of their websites (if they even have one) to permit a data subject to perform a direct download of their data.

2. Data Protection Officers (DPO)

The WP29 guidelines are intended to help controllers and processors fulfil their duties to appoint a DPO and assist DPOs in their role.

The examples given in the WP29 Guidelines, suggest that the **larger insurance intermediaries** should appoint a DPO. **However, it remains to be seen whether micro and small insurance intermediaries should appoint a DPO as it is still not entirely clear what "core activity" and "large scale" processing means.** BIPAR recalls its concerns that the special consideration expressly provided for micro enterprises and SMEs in Recital 13 of the GDPR may not be applied in practice. BIPAR expects further guidance on the issue.

The **DPO** must be provided with **necessary resources to fulfil the role** (e.g. active support from senior management; continuous training; appropriate financial resources; etc.) and must **be autonomous and independent** (i.e., to avoid any conflict of interests). BIPAR questions how a micro enterprise or SME will be able to comply with these requirements. One possible solution, set out in Article 37.4 of the GDPR, is to share a DPO between groups of firms, however there are concerns around confidentiality of commercially sensitive data (rather than personal data) and the logistical impracticality where firms trying to share a DPO are in different towns or different regions of a country. BIPAR would appreciate clarity on the ability of professional associations to provide a shared DPO as a service to members and what guidance it might give to such a DPO to manage the issues above.

3. Lead supervisory authority

The WP29 has interpreted **how a controller or processor carrying out cross-border processing should determine its main establishment for the purposes of choosing the lead supervisory authority.**

- BIPAR has questions regarding the possible interaction between provisions in the Insurance Distribution Directive on cross-border activities and the WP 29 guidelines.
- BIPAR believes that the guidance remains unclear for joint controllers. One possible way forward would be to have a single authority monitor the joint data processing activities.
- BIPAR would welcome clarity on both aspects.

Av. Albert-Elisabeth, 40- B-1200 Bruxelles - Tel: 0032-2-735.60.48 - Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu

4. Aspects for further WP29 guidance: processing personal data where there is no direct relationship with the data subject prior to processing

The GDPR provides a number of legal bases which need to established before personal data may be processed. BIPAR believes that insurance intermediaries are likely, in many circumstances, to have to rely on explicit consent. At first sight, it does not appear that other bases, such as processing "for the establishment, exercise or defence of legal claims..." or legitimate interest would be appropriate.
The difficulty with consent is firstly that it should be given prior to processing and secondly it should be a freely given, specific, informed and unambiguous indication of the data subject's wishes. By a statement or a clear affirmative action, data subjects should agree to the personal data processing on the basis of a given purpose and legal basis. The controller should be able to demonstrate that the data subject has given consent.

Consent is particularly problematic where intermediaries do not have a direct relationship with the data subject prior to processing. Examples illustrate: an intermediary may not have a direct relationship with an employee insured under a group contract concluded between a corporate policyholder and an insurer until it is instructed to pay-out a claim to that individual directly. An intermediary will certainly not have a direct relationship with an injured third party before that data subject is involved in a motor accident and becomes eligible for compensation. However, in both cases, the intermediary should process this personal data, both in the interest of fulfilling the insurance contract – between the policy holder and the insurer, not the data subject, and in the interest of the data subject. Further details are provided below at point 5.

Clarity is therefore needed regarding:

- The extent to which intermediaries can rely on consent obtained by, for example, an individual's employer where the intermediary arranges the employer's compulsory employers' liability insurance that inures to the benefit of the individual employee but where the intermediary does not have a direct relationship

- What is required to satisfy the obligation for "clear affirmative action" (could it be satisfied by continuing to transact with the relevant insurer and/or intermediary?)

- What GDPR-compliant steps would need to be taken by the intermediary to "demonstrate" that the data subject's rights have been safeguarded? Does he need to give consent or is it sufficient to inform the data subject of his rights (to object etc.) at the first contact with the intermediary?

The GDPR provides a margin of manœuvre for Member States to adopt rules, including for the processing of sensitive personal data (Article 9.5) and it may be helpful to explore this further in situations where the processing remains objectively in the data subject's interest (for example to receive compensation under their employers' liability insurance policy). We consider it unlikely that we will overcome this challenge without further clarification on the interpretation of certain grounds for processing. For example, would it be possible to argue that in the examples outlined above the processing is permitted on the grounds of "for the establishment, exercise or defence of legal claims..."?

As consent is problematic, for the reasons outlined above, an alternative basis for processing could be **the legitimate interests' basis.** However, the GDPR potentially restricts intermediaries from relying on this basis as it requires the controller to explicitly notify the data subject of the legitimate interests (as part of a full fair processing notice) in advance of any data processing. The GDPR provides two exceptions to this requirement: in cases where notification proves impossible or would involve disproportionate effort.

Is the WP29 intending to clarify the impossibility /disproportionate effort exceptions?

5. Practical examples of insurance intermediaries' data processing activities

Motor insurance:

Av. Albert-Elisabeth, 40- B-1200 Bruxelles - Tel: 0032-2-735.60.48 - Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu

(a) a road traffic accident where the policyholder of a motor insurance contract is responsible for an accident which causes serious injury to a third party. The third party is entitled to receive compensation from the insurance company of the policyholder, but to process the compensation claim, both the insurer and intermediary need to process sensitive personal data. There is no contractual relationship between the third party, the insurance company or the insurance intermediary of the policyholder. Additionally, neither the insurance company nor the insurance intermediary have had prior contact with the third party and so have not had the opportunity to request the third party's consent to process their sensitive personal data or inform him of the purpose and legal grounds for processing as well as the data subject's rights. Nevertheless, it is clearly in the third party's interest to have the compensation claim rapidly processed. BIPAR seeks clarity on how to do this within the boundaries of the GDPR and WP29 guidance;

(b) **a road traffic accident where the policyholder is the innocent victim of an accident** which causes damage to their vehicle and possibly injury to the policyholder. The policyholder's insurer will need to process personal details - obtained from the policyholder rather than the third party causing the accident - on that third party, in order to pursue recovery of claims costs from 'them'. In turn, the third party's insurer will instruct their client not to respond to requests from the victim's insurer, but to pass correspondence unanswered to them, so as not to prejudice any legal proceedings that might result. How might an intermediary obtain consent to process the third party's personal data in this instance?

(c) temporary additional drivers. Some motor insurance contracts allow the policyholder to add temporary additional drivers. Would the intermediary / insurer have to obtain unambiguous/explicit consent from the temporary additional driver before they were able to process the policyholder's request?

Private medical insurance. Some policies allow a policyholder to extend cover to household and family members. Intermediaries are concerned about how this personal data can be disclosed to the insurer and intermediary and, as mentioned on page 1, how such data can be rendered "portable".

Additionally, **life insurance contracts with death benefits**, require policyholders to appoint a beneficiary. Not all policyholders wish to disclose to their beneficiary in advance that they will receive death benefits. Therefore, insurers need to be able to process this information without notifying the data subject.

In cases of **short-term non-investment insurance contracts**, the question of frequency of consent arises. How often would the firm need to obtain evidence of consent from the policyholder- at every renewal or at every mid-term adjustment?

Av. Albert-Elisabeth, 40- B-1200 Bruxelles - Tel: 0032-2-735.60.48 - Fax: 0032-2-732.14.18 - bipar@bipar.eu - www.bipar.eu