Annex 6: Data transfers between an EEA insurer and non-EEA National Bureau

DISCLAIMER.

This paper originates from the Council of Bureaux (CoB). It was prepared by the CoB Working Group on Data Protection. More information can be found at **https://www.cobx.org/.**

This paper is intended to assist the National Bureaux and their stakeholders involved in the claims handling process (i.e. insurers and their intermediaries, where applicable) in assessing the necessary steps to consider when data exchange between EEA entities and non-EEA entities occur and compliance with Chapter V of the General Data Protection Regulation (GDPR) **prevails.**

This paper does not tackle the situation describing a data transfer between an EEA insurer and an EEA National Bureau. It is clear from the beginning that data transfers between an EEA insurer and an EEA National Bureau is a purely EEA scenario, therefore it does not fall under the rules provided under Chapter V of the General Data Protection Regulation (GDPR) regarding the transfer of data to" third" countries.

This paper describes that an exchange of data between an EEA insurer and a non-EEA National Bureau might occur and makes an attempt in finding legally justified reasons allowing the exchange.

This paper does not provide tailor made solutions as each data transfer between EEA entities and non-EEA entities should be considered individually, on an ad-hoc basis, by the responsible involved parties.

All opinions published in this document are, regardless of source, given in good faith. No representation or warranty, express or implied, is given and no responsibility or liability is or will be accepted by or on behalf of the CoB or the members of the CoB Working Group on Data Protection as to the accuracy, completeness or correctness of this document and any such liability is expressly disclaimed.

Situation of a data transfer from an EEA insurer to a non-EEA National Insurance Bureau

An EEA vehicle causes an accident in a non-EEA country and the claim must be handled by the GCB (handling bureau) based on the Green Card issued by the EEA insurer. Probably the insurer (data controller) will transfer data (accident statement) to the National Bureau of the non-EEA country of accident for further processing (i.e. assessing the circumstances of the accident and liability of drivers, understanding the scope of damages and in case of need defending the claim in court). In practice, apart from the communication between two National Bureaux, National Bureaux when dealing with claims under the Internal Regulations have to communicate (and exchange personal data) with insurers: eg. a Handling Bureau has to communicate with the foreign MTPL insurer directly under Article 3 IR as well as Article 5 IR.

The discussion carried out during the meeting of the WG on Data Protection showed that the data exchange between an EEA insurer and a non-EEA National Bureau is not covered by the CoB Personal Data Processing Agreement, as the latter is only binding for the National Bureaux and the CoB.

There are approximately 2000 insurers in the EEA system. For this reason, the idea of adopting a similar solution to the one between the National Bureau (e.g. concluding multilateral agreements) would not be realistic due to the immense number of stakeholders involved.

It is important to realise however, that the exchange of personal data directly between insurers and Bureaux is inevitable, therefore the discussion during the previous meeting of the Working Group on Data Protection showed that there is a need to have a systematic solution to avoid that individual National Bureaux would be confronted with requests of hundreds or thousands different MTPL insurers in Europe trying to find each a solution by individual agreement.

The insurers are not part of any of the CoB's data protections agreements. Consequently, the idea is to analyse whether there is any lawful legal basis for such transfer to be made from an EEA insurer to the non-EEA National Bureau.

1. Article 44

The European Data Protection Board (Guidelines 2/2018 on derogations of Article 49 under Regulation 2016/679) reminds us that when applying Article 49, one must bear in mind that according to Article 44, the data exporter transferring personal data to third countries or international organisations must also meet the conditions of the other provisions of the GDPR. Each processing activity must comply with the relevant data protection provisions, in particular with Articles 5 and 6. Hence, a two-step test must be applied: first, a legal basis must apply to the data processing as such together with all relevant provisions of the GDPR; and as a second step, the provisions of Chapter V must be complied with.

2. Article 49 (1) § 1

According to the GDPR, a transfer or a set of transfers of personal data to a third country, in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, shall only take place on one of the following conditions:

a) *The data subject has explicitly **consented** to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;*

b) *the transfer is necessary for the **performance of a contract** between the data subject and the controller or the implementation of pre-contractual measures taken at the data subject's request;*

c) *the transfer is necessary for the conclusion or **performance of a contract** concluded in the interest of the data subject between the controller and another natural or legal person;*

d) *the transfer is necessary for important reasons of **public interest**;*

e) *the transfer is necessary for the **establishment, exercise or defence of legal claims**;*

f) *the transfer is necessary in order **to protect the vital interests of the data subject** or of other persons, where the data subject is physically or legally incapable of giving consent;*

g) *the transfer is made from a **register** which according to Union or Member State law is intended to provide information to the **public** and which is open to consultation either by the public in general or by any person who can demonstrate a legitimate interest, but only to the extent that the conditions laid down by Union or Member State law for consultation are fulfilled in the particular case.*

The CoB had also consulted the expert view of Mr Jos DUMORTIER, who showed preference for point c) above.

The EDPB states that Recital 111 differentiates among the derogations by expressly stating that the "contract" and the "legal claims" derogations (Article 49(1) subpar. 1 (b), (c) and (e) shall be limited to "occasional" transfers.

a. The transfer is occasional and not repetitive;

The question is whether data transfers between an EEA insurer and a non-EEA National Bureau, of personal data concerning individuals can be considered as being occasional or not repetitive.

The EDPB notes that the terms "occasional" (recital 111) and "not repetitive" indicate that such transfers may happen more than once, but not regularly, and would occur outside the regular course of actions, for example, under random, unknown circumstances and within arbitrary time intervals. For example, a data transfer that occurs regularly within a stable relationship between the data exporter and a certain data importer can basically be deemed as systematic and repeated and can therefore not be considered occasional or not-repetitive.

Based on the interpretation of the EDPB, it can be argued that the circumstances in which road traffic accidents take place are random, and within arbitrary time intervals. The transfer of data to the non EEA Bureau by the EEA insurer is not regular but contingent.

b. Necessity test

One overarching condition for the use of several derogations is that the data transfer has to be "necessary" for a certain purpose. The necessity test should be applied to assess the possible use of the derogations of Articles 49 (1) (b), (c), (d), (e) and (f). This test requires an evaluation by the data exporter in the EU of whether a transfer of personal data can be considered necessary for the specific purpose of the derogation to be used.

It is necessary for the transfers between an EEA insurer and a non-EEA National Bureau in the context of an accident in order to handle properly a claim in performance of an MTPL insurance contract. If the EEA insurer intends to perform for the best the insurance cover, the transfer of a version, an accident statement etc..is necessary because it allows the non EEA Bureau to make use of arguments resulting from the reliable data and this in the same way as the insurer or even the insured would have done.

In light of the analysis above and the guidelines provided by the EDPB on derogations of Article 49 under Regulation 2016/679, we may therefore, in the absence of an adequacy decision pursuant to Article 45(3), or of appropriate safeguards pursuant to Article 46, consider appropriate to rely on the following legal grounds under Article 49:

*(a) the data subject has explicitly **consented** to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards;*

The general conditions for consent to be considered as valid are defined in Articles 4 (11), 10 and 7 of the GDPR. The WP29 provides guidance on these general conditions for consent in a separate document, which is endorsed by the EDPB. These conditions also apply to consent in the context of Article 49 (1) (a). However, there are **specific**, additional elements required for consent to be considered a valid legal ground for international data transfers to third countries and international organisations as provided for in Article 49 (1) (a), and this document has to focus on them.

Important to note that public authorities are not able to rely on this derogation in the exercise of their public powers according to Article 49(3).

To rely on this consent however may be risky if one considers the possibility that the insured still could refuse to give consent, while the insurer sees a necessity to transfer data.

*b) the transfer is necessary for the **performance of a contract** between the data subject and the controller (...)*

The insurer has to perform the MTPL contract. The driver of the vehicle however is not necessarily the data subject that concluded the contract.

*(c) the transfer is necessary for the conclusion or performance of a **contract concluded in the interest of the data subject** between the controller and another natural or legal person; or*

The occasional and necessity tests in relation to a contract concluded in the interest of the data subject are a prerequisite for the controller to perform before deciding whether it can be relied upon or not.

… The insurer has to perform the MTPL contract. The driver of the vehicle however is not necessarily the data subject that concluded the contract.

*(e) the transfer is necessary for the establishment, exercise or defence of **legal claims**;*

A non-EEA National Bureau will handle a claim based on its national legal obligation as it is responsible for the handling and settling of claims arising from accidents caused by visiting motorists. Further in the guidelines, the EDPB brings the necessity test of the data transfer, explaining that it requires a close and substantial connection between the data in question and the specific establishment, exercise or defense of the legal position. It is defendable to consider this legal obligation of the National Bureaux to fall under the above-mentioned paragraph. Moreover, by its mere existence the non EEA Bureau creates a guarantee for domestic victims who otherwise would have to sue the visiting motorists. Further, any non-EEA Bureau in its capacity of a Handling Bureau is obliged by the IR to act in the best interest of the insurer and its client. The fulfilment of this obligation is intensively conditioned by the availability of the personal data of the client of the insurer.

3. Article 49 (1) § 2 GDPR

When a transfer could not be based on a provision in Article 45 or 46, and none of the derogations for a specific situation is applicable under Article 49 (1) § 1 of the GDPR, the GDPR allows for **another derogation as last resort** the derogation available under Article 49 (1) § 2 GDPR.

This can only be used in residual cases according to Recital 113 and is dependent on a significant number of conditions expressly laid down by law. In line with the principle of accountability enshrined in the GDPR the data exporter must be therefore able to demonstrate that it was neither possible to frame the data transfer by appropriate safeguards pursuant to Article 46 nor to apply one of the derogations as contained in Article 49 (1) § 1. This implies that the data exporter can demonstrate serious attempts in this regard, taking into account the circumstances of the data transfer. This may for example and depending on the case, include demonstrating verification of whether the data transfer can be performed on the basis of the data subjects' explicit consent to the transfer under Article 49 (1) (a).

Such transfers can only be performed under certain conditions:

a. The transfer is not repetitive;

According to its express wording, Article 49 (1) § 2 can only apply to a transfer that is not repetitive. This test is identical with the one mentioned above under Chapter 1 of this paper.

b. Concerns only a limited number of data subjects;

No absolute threshold has been set as this will depend on the context but the number must be appropriately small taking into consideration the type of transfer in question. The number of data subjects involved in such a data transfer exchange between an EEA insurer and non-EEA National Bureau is limited when compared to the data pool of most of the EEA insurers or non-EEA National Bureaux.

c. Necessary for the purposes of compelling legitimate interests pursued by the controller which are not overridden by the interests of rights and freedoms of the data subject;

d. The compelling legitimate interest could here be the goal to avoid unjustified financial burden when it becomes impossible to dispute because data transfer is blocked. Any non-EEA Bureau in its capacity of a Handling Bureau is obliged by the IR to act in the best interest of the insurer and its client. The fulfilment of this obligation is intensively conditioned by the availability of the personal data of the client of the insurer.

e. The controller has assessed all the circumstances surrounding the data transfers and has on the basis of that assessment provided suitable safeguards with regard to the protection of personal data.

As to the nature of such safeguards, it is not possible to set up general requirements applicable to all cases in this regard, but these will rather very much depend on the specific data transfer in question. Safeguards might include, depending on the case, for example measures aimed at ensuring deletion of the data as soon as possible after the transfer, or limiting the purposes for which the data may be processed following the transfer. Particular attention should be paid to whether it may be sufficient to transfer pseudonymized or encrypted data.

What is more, the controller shall:

f. inform the supervisory authority of the transfer;

The duty to inform the supervisory authority does not mean that the transfer needs to be authorised by the supervisory authority, but rather it serves as an additional safeguard by enabling the supervisory authority to assess the data transfer (if it considers it appropriate) as to its possible impact on the rights and freedoms of the data subjects affected. As part of its compliance with the accountability principle, it is recommended that the data exporter records all relevant aspects of the data transfer e.g. the compelling legitimate interest pursued, the "competing" interests of the individual, the nature of the data transferred and the purpose of the transfer.

g. in addition to providing the information referred to in Articles 13 and 14, inform the data subject of the transfer and on the compelling legitimate interests pursued.

The data controller must inform the data subject of the transfer and of the compelling legitimate interests pursued. This information must be provided in addition to that required to be provided under to Articles 13 and 14 of the GDPR.

4. Assessment

EEA Insurers should be able to assess if they prefer to apply either article 49(1) §1, or 49(1)§2 GDPR.

EEA Insurers, normally, should keep record of their processing activities, which implies that the record contains the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries (article 30, 1.c), d) and e) GDPR.