



## FINAL REPORT 2020

### Taskforce for Data Protection

Taskforce Chair: Ms Eva Jacino (Swedish Transport Agency)

Author: Ms Liza Abrahamse (EReg Secretariat)

Date: June 2020

# INTRODUCTION

The EReg Taskforce Data Protection in International Data Exchange is set up to help EReg members in living up to the optional guidelines of EReg TG XX on the General Data Protection in International Data Exchange.

The purpose of these EReg guidelines is to ensure an adequate level of protection of personal data in international data exchange. These EReg guidelines provide specific guidance on how the GDPR should and can be applied in international exchange of personal data in the transport sector. The guidelines help to overcome or address differences in interpretations and implementations of the GDPR by specifying the measures that RAs and/or NCPs have already taken or are committed to take in international data exchange. These EReg guidelines do not address data protection requirements arising within the context of the registration and national exchange of data of vehicles, driving licences and accompanying personal data, organised in national law.

In February 2020, the Taskforce sent out a questionnaire with the aim of monitoring the state of affairs regarding data protection in international data exchange and of living up to the guidelines. The Taskforce analysed the outcomes of the questionnaire and discussed this during two virtual meetings. In addition to the answers of the questionnaire, participants shared issues and questions from their organisations in the group. The outcomes of these discussions have also been incorporated in this report.

This report provides an overview of the outcomes of the questionnaire. It follows the structure of the guidelines and provides insight in the conclusions that can be drawn from the outcomes.

<b>Respondents</b>		
Spain	Hungary	Slovakia
Isle of Man	United Kingdom	Finland
Luxembourg	Iceland	Sweden
Switzerland	The Netherlands	Lithuania
Portugal	Norway	Gibraltar
Latvia	Ireland	

<b>Taskforce Members</b>	<b>Reading Members</b>
United Kingdom	Switzerland
Norway	Lithuania
Finland	Greece
EUCARIS	
the Netherlands	
Latvia	
Sweden	

# OUTCOMES QUESTIONNAIRE

## Personal data definition

In international data exchange, differences in national interpretation of the definition of personal data exist. The EReg guidelines proposes to deal with these differences mainly by being transparent about these differences and how these are approached. The questionnaire tried to find out if problems occurred due to differences in interpretation of personal data.

Most members indicated that they experienced no major problems, but a few examples were provided. Latvia faced some problems with the exchange of odometer data with other member states, for example on mileage data. Other examples are VIN number and vehicle registration number, which are considered personal data in some countries and not in others. This doesn't raise a lot of problems, but as Finland explained, can cause extra work because a lot of clarification e-mails/messages are necessary to determine if the existing legal basis is enough.

Conclusion: the outcomes of the questionnaire show that few real problems arise, but transparency and clarification on different national approaches would be helpful. Therefore, the EReg Taskforce would like to request the registration authorities to fill in the data overview and furthermore to draw attention to the personal data definition in their (English) privacy notice.

## Lawfulness of processing

The international exchange of personal data between RAs and/or NCPs shall be lawful. Personal data shall only be processed by RAs and/or NCPs if one or more of the legitimate grounds of Article 6 of the GDPR apply.

The questionnaire showed that organisations have procedures in place to exchange personal data lawfully. However, there are still cases where personal data is exchanged through e-mail and then it is more time consuming to check if an exchange is lawful, because extra work needs to be done to check the lawfulness of the request. Different policies are in place and e-mail requests need to be checked manually, case-by-case. On the question of if there is an audit-mechanism in place to verify the legitimacy of requests of national authorities via EUCARIS/Tachonet, almost all of the respondents indicated that this is not the case.

The Netherlands provided insight in another issue. RDW carried out a pre-audit for its role as NCP. The outcomes of the pre-audit show that there are several topics that are still unclear. These are for example: how do you label your responsibility as a NCP, when you are the only the technical intermediary for information provisioning between a foreign RA and a national competent authority that needs the data for its legal tasks? First of all it is clear that there is a difference between the two roles. The RA is providing data from its registers, where the NCP is responsible for the transfer of data between different parties in the information chain. The exact tasks and responsibilities belonging to the role of NCP, however, have not been described yet in the EU legislation or in Dutch legislation. Regarding the bi-directional data exchange that we have organized with EUCARIS or TACHOnet, the EReg Authorities have two roles: they act as RA and provide Vehicle or Driving Licence Registration Data, but they also act as NCP. Here we have two questions:

is the NCP to be regarded as a processor or as a controller and is it arranged within national law that the NCP is allowed to send, receive and process information received under different EU directives and regulations? These questions are currently reviewed in the Netherlands. It was also discussed in the Taskforce and the conclusion was that clarification is needed.

Conclusion: Lawfulness of processing personal data is very important. The outcomes show that e-mail exchanges of personal data still exist which costs more work to verify the legitimacy of the request. The Taskforce continue to promote the use of information systems such as EUCARIS so that lawfulness of processing personal data is better identified and easier to control.

The Netherlands brought forward a new topic that needs attention. The Taskforce will monitor the developments on the pre-audit of the role as NCP in the Netherlands and if necessary, will discuss this topic and bring forward proposals on how best to deal with this in international data exchange. This specific topic is not included in the guidelines of EReg on the GDPR in international data exchange.

### **Data minimization**

The international exchange of personal data shall be adequate, relevant and limited to what is necessary. On the question of if personal data is exchanged via other means than EUCARIS or EU systems and how to guarantee data minimization, respondents answered that data minimization is mainly relevant in the case of exchanges via e-mail. In the case of exchanging data via one of the information systems, data minimization is more easily ensured because the message is predefined and thus extra data is not easily requested. However, in the case of e-mail, respondents agree that is more difficult. The Netherlands mentions that e-mail or letter requests occurs on verification regarding exchange on foreign driving licences. These e-mails are necessary to clarify the request in more detail. Employees involved in this process follow the written procedures to ensure data minimization. In Finland, the request is assessed regarding the intended use and shall be rejected if the request is too extensive for its intended purpose.

Conclusion: These investigations of e-mail requests are manual processes and are therefore time consuming. The Taskforce would like to stress again to use the information systems for international personal data exchange, because it could help ensure data minimization because the message is pre-defined and therefore no extra data is requested. It should however be mentioned that the definition of the message needs to be minimized as well. The standardised exchange will at least contribute to minimize the risk of a data breach.

## Quality of data

Data quality is one of the more important topics. Almost all of the respondents have a system of rectification, erasure or restriction in place. The question on the existence of a mechanism to flag a data element that has been contested is answered very differently. Some respondents have such a mechanism in place, but only in a few cases it is possible to share this flag internationally. The intended use of this flag would be to inform others of data elements that might be contested but are still under investigation. Only Portugal, Latvia and Sweden (only in certain cases) indicated that it is possible to share this flag in international data exchange. The Netherlands answered that there is a flagging mechanism in place, but the usage of this instrument is minimal and it will only be possible to share this internationally after necessary changes within procedures and IT. EUCARIS has explained the possibilities that exist within the system to share flags internationally. The basic idea is to create a table with flags on or connected to the EUCARIS platform. The flags indicate that a certain key, e.g. the licence number of a vehicle, has to be processed in a specific way. Depending on the type of flag, the data exchange may be blocked completely, or a warning or remark is included in the EUCARIS message. The Taskforce is currently researching this possibility. The EUCARIS TWG showed that there are still a lot of questions on the use of such a flag and the added value it would bring us.

On the question of reuse of personal data (to guarantee the actuality of the data) almost all of the respondents answered that they don't reuse the data. Only 2 countries (Spain and Isle of Man) indicated that this is done. Isle of Man reuses current details if a person has a vehicle/driver licence record. There is clear wording to explain that their personal data may be used for specific reasons.

Conclusion: In most organisations, the adequate procedures are in place. However, improvements can still be made. One of the elements that was discussed in the EReg Topic Group XX was the flagging instrument and exchanging this flag internationally. There are still many questions to look into and in the coming period the Taskforce will examine the flagging instrument and evaluate the added value. The Taskforce will connect with the work of EReg Topic Group XXI on harmonisation of registration procedures and data quality, because this group will also discuss data quality.

## Data retention

All respondents have national legislation on data retention. 60% of the respondents have automated procedures in place (outside of EUCARIS) for purging of the data after the retention period. Also, only 40% of the respondents indicated that they have a reference to the data retention policy in their privacy notice.

Conclusion: Data retention is based on national legislation. There is little transparency on the different policies in place between countries. The Taskforce would like to stress to include a reference to the retention period in the English privacy notices. The Taskforce will also look into how data retention is ensured in the case of e-mail exchanges, because this should be archived only for a limited period. This could be included in next year's questionnaire.

## Security and confidentiality

The different questions in the questionnaire show that e-mail is still used in international data exchange. On the question of if personal data is exchanged via e-mail, many respondents

indicated that this is still done, mainly for requests on driving license verification, re-registration exchange / imported vehicles and diplomatic permits. Often, encryption of these e-mails is done, but in a few countries this is not the case.

There is no personal data originating from other MS stored in data centres outside the EU/EEA. And apart from the EUCARIS DPIA, respondents explained that there were no Data Protection Impact Assessment (DPIA) carried out for international personal data exchange, which means that these cannot be shared. The Netherlands publishes information on the ISO certificate on their website and Lithuania shared recommendations on a recent security audit in the EUCARIS system.

Conclusion: the Taskforce recommends limiting the use of e-mail in the personal data exchanges as much as possible. The Taskforce will look into the possibilities of alternative ways to exchange the abovementioned information through one of the information systems.

### **Personal data breaches**

Only 2 respondents indicated that they have faced a personal data breach in international data exchange. In the case of Latvia, this concerned a data breach of Latvian citizens data in CBE services. Fourteen countries were informed. These lessons learned will be analysed by the Taskforce and shared with the EReg members. In the Netherlands, in 3 separate occasions an answer was sent to the wrong canton (district) in Switzerland. On 1 occasion they received multiple owner/holder records for 1 vehicle and forwarded the wrong one to the collecting agency. In 1 occasion the Netherlands delivered an incorrect file with personal data to Hungary. This personal data was requested with regard to offences regarding driving without a tollvignet (toll sticker). The lesson learned here is that it is important to assemble and share as little as possible manually.

During one of the Taskforce meetings, lessons, experiences and questions on personal data breaches in general were shared. The added value of the Taskforce is to provide a platform to share this information and to invite your colleagues to reflect on it.

Conclusion: Up until now there are only few cases where a data breach crosses borders. The Taskforce recommends sharing as much as possible on lessons learned from personal data breaches. It can be of added value to discuss practices and lessons in general. The Taskforce will collect the lessons learned that will be applicable in general and publish this on the EReg website. In the coming period, the lessons learned from the Latvian case will be shared.

### **Transparency and information requests**

RAs and/or NCPs are transparent to citizens (data subjects) that personal data concerning them may be or actually have been processed and exchanged internationally. Some of the respondents indicated that they have track and trace facilities in place for international data exchange, to provide the data if requested by the citizen. Hungary and Gibraltar responded that they had to provide assistance to another MS regarding a data subject request. Many countries have a privacy notice in English in place, but not all of them made a reference to international exchange of personal data.

Conclusion: providing assistance to each other can be very helpful to speed up to the process of data subject requests and will help the citizen as best as possible. The Taskforce recommends reviewing the English privacy notices and include a reference to international personal data exchange, so that citizens are aware of the fact that their data might cross borders. The Taskforce will make a reference to the different English privacy notices on the private part of the EReg website.

### **Transfer of personal data to non-EU countries**

On the question if personal data is provided to third countries (non-EU), respondents indicated that in the case of driving licence exchange, a lot of EU countries have data agreements with non-EU countries and thus share personal data with them. For TACHO, personal data is shared via the HUB with non-EU countries. Next to that, personal data is shared with Jersey and Gibraltar via EUCOP for re-registration and driving licences.

Conclusion: These exchanges should be part of the different national privacy notices and the Taskforce recommends that organisations include a reference to the transfer of personal data to non-EU countries in their English privacy notice as well.

### **General conclusions and next steps Taskforce**

This is the first report of the EReg Taskforce on Data Protection in international data exchange. It provides a first insight in the state of affairs on data protection of the different EReg members. The Taskforce mission is to promote, support and share best-practices on data protection in international data exchange to improve the protection of personal data of the EU citizens as much as possible, gain mutual trust and to facilitate the EReg members to deal with the GDPR in a similar and adequate way.

Based on the outcomes of the questionnaire the Taskforce will take action on:

1. E-mail exchanges. An important part of the guidelines is to minimize the exchange of e-mail as much as possible because it causes problems because of errors during manual processing, level of security, and manual checks on lawfulness and information requests. Although it will always remain an option, the Taskforce will look into e-mail exchanges and possible improvements that can be done such as agreement on the use of secure e-mail according to a standard protocol and using a generic version of the 'secure message' of the European Commission (RESPER);
2. The Taskforce will set up a page on the EReg website that includes information on data protection in international data exchange. Different findings, studies and references to privacy notices will be included here;
3. The Taskforce will suggest improvements for an English privacy notice taking into account international personal data exchange that can be used by the different EReg members. This will be published on the EReg website;
4. The Taskforce will examine the flagging instrument on the added value for improving data quality;
5. The Taskforce will monitor the study that the Netherlands is currently conducting on the role of the NCP and will share the outcomes with the EReg members.