NIPH
Norwegian Institute of Public Health

UiO : University of Oslo

Comments: Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data

What constitutes a transfer of personal data?

In *Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data* (the recommendations), the principle of accountability in data transfers is emphasized. A "first step" in applying this principle is to ensure that you - as a data exporter - are fully aware of your transfers[1]. In order to obtain the necessary awareness and control, data exporters must therefore understand what is classified as a transfer of personal data.

As the term "transfer of personal data" is not defined in the General Data Protection Regulation (GDPR/the Regulation), we encourage The European Data protection Board (EDPB) to address this critical issue by supplementing the text paragraph 13[2] so that there is no doubt with respect to the subject or applicability of these recommendations.

The European Data Protection Supervisor (EDPS) called on the Union legislature to include a definition of transfer of personal data in the Privacy Regulation[3]. The European Parliament`s Committee on Civil Liberties, Justice and Home Affairs did the same[4]. This was not followed up by the legislature.

European supervisory authorities interpret "transfer of personal data" differently. The EPPB, the EDPS, and several other supervisory authorities, assume that remote access from a third country to data stored in the EEA also constitutes such a transfer. In the recommendations on measures that supplement transfer tools, we urge EDPB to clarify whether this should also apply to remote access without the possibility of exporting or downloading any data. Where data in the EEA are made available for remote access from a third country, but all export and download of data are blocked for the data viewer, should this be considered a transfer according to the GDPR? And if so, is this interpretation consistent with the purpose behind the principles and regulations of data transfer in

[1] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 8.
[2] Paragraph 13 only gives reference to EDPB Frequently Asked Questions on the judgement Schrems II, 23 July 2020 nr. 11; *"it should be borne in mind that even providing access to data from a third country, for instance for administration purposes, also amounts to a transfer".*
[3] EDPS, 'Opinion on the data protection reform package' (2012), p. 17.
[4] Albrecht, J. P., Committee on Civil Liberties, Justice and Home Affairs, 'Draft report on the proposal for a regulation of the European Parliament and of the Council on the protection of individual with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation) (COM(2012)0011 – C7-0025/2012 – 2012/0011(COD))' (2013), amendment 86, p. 65.

the GDPR – especially as these appear from Article 44, Recital 101, and judgements of the Court of Justice of the European Union[5]?

We find that there is little consistency between European supervisory authorities regarding what constitutes a transfer of personal data, particularly under conditions that vary in the manner in which data may be accessed, and when such data access is considered a transfer according to the GDPR.

Is technology that allows remote access without the possibility of exporting data a sufficient supplementary technical measure?

The EDPB emphasizes that in some situations only technical measures might impede or render ineffective access by public authorities for surveillance purposes[6]. This means that adequate technical measures are essential for the transfer of personal data to most third countries.

The possibility of exporting or downloading data is not mentioned in connection with the brief reference to remote access in the recommendations[7]. Neither is it mentioned as a technical measure under the guidance for adopting supplementary measures[8]. Even though the technical measures listed in Annex 2; «Examples of supplementary measures», are not exhaustive and any supplementary measures may only be deemed effective based on a case-by-case assessment, the need for further recommendations concerning technical measures is crucial. More attention should be given throughout the recommendations to technical measures that provide access to data for analysis only and circumvent the physical transfer of personal data to a third country.

The EDPB describes how pseudonymisation of personal data[9] can provide an effective supplementary measure e.g. in transfers of data to a third country for analysis for purposes of research in Annex 2. In research projects, pseudonymisation is often a key measure undertaken to safeguard the privacy of the research participants. Nevertheless, given the prerequisite for accepting this as an effective supplementary measure[10], pseudonymisation is not possible in all cases or projects where research collaboration across borders is critical and important to public interest.

If remote access from a third country to data localized in the EEA without the possibility to export or download any data should be considered a transfer of personal data, the EDPB should address whether EEA based platforms utilizing technologies such as file lock and data diode to restrict all data export, constitute effective technical measures. EEA based platforms are used for purposes of research and in international research collaboration.

Platforms utilizing this technology will:

---

[5] The judgment of the Court of Justice of the European Union I; Case C-101/01 Criminal Proceedings against Bodil Lindqvist (Lindqvist), Case:C-362/14 Maximillian Schrems v Data Protection Commissioner (Schrems I), and case C-311/18 Data Protection Commissioner v Facebook Ireland Ltd and Maximillian Schrems (Schrems II).
[6] Recommendations 01/2020 on measures that supplement transfer tools to ensure compliance with the EU level of protection of personal data, paragraph 48.
[7] Paragraph 13.
[8] 2.4. Step 4: Adopt supplementary measures.
[9] Definition of pseudonymisation in GDPR Article 4 (5); *'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.*
[10] Paragraph 80 and 81.

- be based solely in the EEA,
- be limited to remote access,
- block export of all files and data to a recipient in a third country,
- use encryption during transit, and
- only store data in the EEA.

Such technology is able to remedy the consequences of legislation in the third country that may affect the level of protection.

Any supplementary measure may only be deemed effective in the meaning of the CJEU judgment "Schrems II" if and to the extent that it address the specific deficiencies identified in the assessment of the legal situation in the third country [11]. As a technical measure, remote access from a third country to data localized in the EEA without the possibility to export or download any data, will effectively protect the data from public authorities' surveillance with encryption in transit, and ensure that the platform is subject to third country surveillance laws.

Public authorities in third countries may access transferred data in transit by accessing the lines of communication. Platforms allowing remote access encrypt data from the service which is "pulled" from the user's browser on request, thus enabling the user to read content from the database. Decryption takes place on the client, in the browser or in the computer memory. This means that all data are encrypted during transit and cannot be monitored by unauthorized persons. Data cannot be transferred to a local hard disk or forwarded and thus be subject to monitoring.

Platforms will utilize 2FA login solutions through a browser or a dedicated client. In practice, the user will only see screenshots, as well as sending keystrokes and mouse movements into the service. Since data export for users in third countries is deactivated, all data storage, apart from temporary storage in the recipient's computer memory, takes place in the EEA.

Public authorities in third countries may also access data while data are in custody by either accessing the processing facilities, or by requiring a recipient of the data to turn it over to the authorities.

By using platforms that allow remote access from third countries, but where all export and download of data is blocked, data will not be transferred to another jurisdiction. The information pulled to the user's browser is temporarily stored in the computer's memory. The memory is cleared when the computer is turned off or restarted. No files are transferred from the service and data is not stored on the user's hard drive.

In order for unauthorized persons to access data or to download data from the memory, they would have to take a memory dump before the memory is cleared. This is very unlikely. For the authorities to carry out monitoring of the memory, it would have to be done on the bases of dedicated targeting while accessing specific computers and by using large resources.

Furthermore, EEA based platforms offering such technical solutions will not be subject to third country legislation. There is no indication that US authorities, or other third country authorities, can exercise extraterritorial jurisdiction over European service providers.

[11] Paragraph 70.

Further recommendations have a general interest, beyond research

As research institutions, we urge the importance of further recommendations concerning remote access and effective technical measures as a prerequisite for processing of personal data for research purposes, where international collaboration and data sharing constitute a major component in research. However, we also believe that technical solutions that allow remote access from third countries, but where all export and download of data are blocked, are suitable for scientific research, and also more generally to protect data transfers to EEA countries.

Lars Oftedal
Director of Information Technology
Center for Information Technology Services
University of Oslo

Gun Peggy Strømstad Knudsen
Deputy Director General
National Institute of Public Health