EU Personal Data Transfers 2021: Planning for a Year of Increased Scrutiny

By Dan Goldstein, Co-Founder, Tueoris, LLC and Daniela Fábián Masoch, Founder FABIAN PRIVACY LEGAL
www.tueoris.com / www.privacylegal.ch
dan.goldstein@tueoris.com / daniela.fabian@privacylegal.ch

As 2021 begins, ex-EU transfers of personal data continue to pose a challenge for data privacy professionals. While new Standard Contractual Clauses ("SCCs") appear promising, the lingering impact of the *Schrems II* decision along with the European Data Protection Board's Draft *Recommendations on Measures that Supplement Transfer Tools*[1] (the "EDPB Recommendations") are likely to leave exporters and importers of European resident personal data spending valuable time focused on data transfer risk mitigation strategies.

Across Europe, Data Protection Authorities maintain a consistent view that countries with laws or practices that allow government "generalized" access to the content of electronic communications do not provide privacy safeguards essentially equal to those in EU member states. Such laws or practices are viewed as impinging on the effectiveness of safeguards contained in the EU General Data Protection Regulation ("GDPR"). Parties relying on SCCs or Binding Corporate Rules ("BCRs") for transfers to such countries must identify and implement, on a case-by-case basis, supplementary measures that elevate protections to a level equal to EU law.

Prior to determining whether such measures will be adequate, parties to a transfer should – in line with the EDPB Recommendations – undertake to ascertain a complete view of the data transfers taking place within the lifecycle of defined processing activities. Upon gaining a holistic view of these data flows, the parties should then conduct Transfer Impact Assessments ("TIAs") to determine risks the transfers to data importers and sub-processors pose to the data subjects, as well as compliance risks faced by the parties to the transfers. Where those TIAs uncover risks of government access to personal data, supplementary controls will be necessary. However, controls considered adequate by EU authorities may be limited.

Know Your Data Flows

The logical starting point for compliant ex-EU personal data transfers is to fully understand where EU personal data is flowing within and outside of your organization. The EDPB acknowledges in its Recommendations that "recording and mapping all transfers can be a complex exercise", but also stresses that awareness of personal data flows is "necessary to ensure that it is afforded an essentially equivalent level of protection wherever it is processed".

Since the GDPR came into effect in 2018, most organizations processing EU resident personal data have spent time and effort to understand the flow of such data, typically by recording the characteristics of processing activities in accordance with GDPR Article 30. However, Article 30 records often fall short in

[1] European Data Protection Board's Draft *Recommendations on Measures that Supplement Transfer Tools to Ensure Compliance with the EU Level of Protection of Personal Data,* adopted on 10 November 2020. https://edpb.europa.eu/our-work-tools/public-consultations-art-704/2020/recommendations-012020-measures-supplement-transfer_en

capturing a holistic view of personal data flows across an organization's third-party ecosystem and the countries in which those parties are located.

Conducting a thorough and detailed exercise to create visual depictions of data flows (i.e., data mapping) enables the identification of transfers not only to ex-EU importers, but also subsequent third-party transfers throughout the personal data lifecycle .

To design and implement reasonable security controls, the organization must first understand the nature of the data that must be secured. A successful data mapping initiative will not only map the flow of personal data, but also identify and depict the specific personal data elements involved in the process, facilitating the development of tailored safeguards necessary for each transfer throughout the data lifecycle. These detailed data maps become a highly valuable tool, not only to determine security controls commensurate to the risks to the data subjects, but also to demonstrate appropriate diligence to regulatory authorities should transfers come under scrutiny.

Transfer Impact Assessments

Overview

In line with the EDPB Recommendations, it has become imperative to conduct a TIA prior to transferring EU resident personal data to parties in non-adequate countries[2]. TIAs must be conducted for prospective transfers of EU data to recipients in non-adequate countries, as well as current, ongoing transfers (and should assess any onward transfers). As such, in addition to conducting TIAs for transfers identified in the data mapping exercise, a TIA should be triggered prior entering into contracts with service providers that will require ex-EU transfers of EU personal data.

A thorough TIA will consider numerous risk factors, however whether the laws or practices of the country where the importer is located impinge on the effectiveness of the safeguards of the transfer tool being used (e.g., SCCs) is of primary importance to EU authorities. For transfers of EU personal data to the US, the prevailing EU view is that Section 702 of the U.S. Foreign Intelligence Surveillance Act does not adequately safeguard privacy rights under EU law. Thus, transfers being made to US recipient using transfer mechanisms such as SCCs or BCRs *must* be supplemented with additional measures to limit government access. Notably, even considering what may be viewed as a rather black or white view of Section 702, the EDPB Recommendations do recognize that an organization's TIAs should consider the context of the specific transfer – an important point, as different activities will carry widely different risks of government access.

Conducting the TIA

TIAs must be conducted diligently and be thoroughly documented, as Data Protection Authorities will expect a TIA to be available if a transfer comes under their scrutiny. Developing and implementing a standard and repeatable TIA methodology supports outcomes that meet EU authorities' expectations.

A TIA which includes a series of questions with "scored" answers allows the organization to consistently quantify results and create requirements for completed TIAs that fall within various score ranges. For example, a score within a defined low-risk range might allow a transfer to go ahead without further action. A score within a defined medium-risk range might require implementation of supplementary measures to bring the level of protection to an EU level, and review and approval by the Chief Privacy

[2] The EDPB Recommendations state that, "you must assess. . . if there is anything in the law or practice of the third country that may impinge on the effectiveness of the appropriate safeguards of the Article 46 GDPR transfer tool you are relying on, in the context of your specific transfer."

Officer. A score within a defined high-risk range might require review by the Chief Privacy Officer and may lead to a decision to suspend or stop the transfer.

The EDPB emphasizes that the TIA should primarily focus on the laws of the country to which the transfer will be made, and, specifically, on factors indicating whether government authorities in that country will seek access to the data. In addition to these objective factors, it is useful – in order to obtain an overall risk score indicating appropriate technical, contractual and organizational measures – to consider other aspects of the data and transfer as well ("context"). This context helps to establish relative likelihood of government requests for EU personal data for transfers made for widely disparate purposes. For example, a transfer initiated by a data subject to manage their customer preferences will pose different risks of government access than a transfer of a large volume of personal data of EU resident social media users to a US importer.

In establishing the TIA risk criteria, consideration should be given to additional factors such as:

- Purpose of the transfer;
- Exporting party (category);
- Data subject type;
- Types of data transferred;
- Volume of data transferred;
- Manner in which access is provided to the importer (e.g., limited push or unlimited pull);
- Frequency of transfers;
- Onward transfers (including category of sub-processor and purpose); and
- Security controls in transit;
- Importer security controls;
- History of government access requests to the importer; and
- History of government access requests to similarly situated importers.

While the EDPB does not place much value in evaluation of historical government requests to the importing organization or other similarly situated organizations, these factors should be considered so that the parties conducting the TIA can gain an internal understanding of the actual risks of government requests and develop an appropriate response strategy.

Remediating Identified Risks

Upon completing the TIA and ascertaining the risk score, along with defined requirements aligned to the scores, it may be necessary to take steps to remediate risks and, as the EDPB Recommendations state, "bring the level of protection of the data transferred up to the EU standard of essential equivalence".

Technical Controls

Significant attention has been focused on encryption of personal data in transit to, and at rest in, the recipient in the ex-EU country. The EDPB Recommendations specify that *in those circumstances where encryption may be appropriate*, it will only be considered an effective control if the encryption keys are maintained by the EU-based exporter, other entities in the EEA, or an ex-EU country with an adequacy designation. In other words, if a US-based importer holds the encryption key, the control will likely not be considered effective by EU authorities.

The Recommendations call out the common scenario[3] in which a data importer – in a country in which the government may access the personal data (e.g., the US) – uses EU personal data to provide services to the EU controller (e.g., payroll or other HR-focused services). The EDPB takes the position that if the importer in such a scenario is able to use the data in the clear, even encryption in transit and at rest will not provide an adequate level of protection of the rights of the data subjects, as the government could compel production of the data.

The logical outcome of strict adherence to this position appears to be a new level of EU data localization. In such instances, exporters and importers may need to evaluate alternatives (e.g., storage and processing of data in the EEA or in an adequate country). If data localization is not an option, the parties may consider a risk-based decision to move forward with the transfer, implementing supplemental organizational and contractual controls[4] in order to continue business operations in a manner beneficial to shareholders, employees and other interested parties. Where the risks are deemed to be too high, the parties may need to either suspend or stop further transfers.

Where appropriate, depending on the context of the transfer, pseudonymization may also present an adequate control. However, in accordance with the EDPB Recommendations, any additional information that would allow the identification of individuals whose personal data is transferred, must be held by the exporter either in the EU or other adequate country (this is a common scenario, for example, in the conduct of clinical trials). In addition, the parties should establish in the TIA that the individuals cannot be identified by public authorities by cross-referencing the pseudonymized personal data with additional information that the authorities may possess.

Contractual Limitations

Based on the context of the transfers taking place, contractual provisions may comprise additional controls supporting the compliant transfer of EU personal data. Contractual provisions may include:

- Limitations on the data being transferred, for example, only specified data subjects or data elements;
- Requirements for technical measures which must be implemented for the transfers to take place;
- A commitment to inform the EU data controller of government requests for personal data and – where commercially feasible and permitted by applicable law – to inform data subjects of such requests; and/or
- A binding commitment by the importer to challenge government requests, including efforts to delay response to requests pending resolution of the challenge.

Contractual limitations should be drafted considering other contractual obligations that may already be in place, for example in SCCs or in an organization's BCRs.

Administrative Controls

Administrative controls represent a further means for organizations importing personal data of EU residents to a non-adequate country to safeguard such personal data – where appropriate – from government access. Controls may include updating internal privacy policies and procedures to include detailed actions in the event of government requests. Such provisions may detail, for example, the

[3] See *Use Case 7* in the EDPB Recommendations

[4] Such supplemental controls may include, for example, a documented commitment to challenge compelled government disclosure of personal data.

process for the intake and response to requests, including review by appropriate internal stakeholders in the EU and in the country from which the government request is made. They may also document the organization's commitments to inform data subjects of such requests and, where appropriate, to challenge government requests.

In addition, personnel who may be tasked with the intake, review and disposition of requests should receive training on internal procedures for managing government requests for access to personal data.

Final Thoughts

As we enter a new year, the state of ex-EU data transfers remains a moving target. While anticipated new SCCs are promising – particularly the processor-to-processor and processor-to-controller SCCs – they do not mitigate the risk of access to EU personal data by governments in non-EU countries. The EDPB Recommendations provide highly valuable guidance, but ultimately include some conclusions that point to EU data localization. In order to minimize risks associated with data transfers, organizations should (in line with EDPB Recommendations) undertake detailed data mapping exercises for processing activities which include transfers of EU resident personal data and conduct detailed TIAs to identify risks related to the transfers. A consistent approach to mapping and TIAs will not only provide information necessary to implement appropriate data protection controls, but will also demonstrate to EU regulatory authorities that your organization takes compliance with transfer rules seriously, and has taken appropriate measures to safeguard the privacy rights of EU residents.

About the Authors

Dan Goldstein, CIPP/E, CIPP/US
Partner and Co-Founder, Tueoris, LLC, www.tueoris.com
dan.goldstein@tueoris.com

Dan advises clients operating in complex business and regulatory environments on privacy and data risk mitigation strategies and solutions. Dan's career has centered on guiding U.S. and multinational clients through international data protection requirements in order to provide business solutions that can be implemented across large organizations. Dan is the former Director of International Data Privacy for Amgen (Europe) GmbH in Zug, Switzerland, is a graduate of the University of California, Los Angeles and the Golden Gate University School of Law and is a member of the State Bar of California.

Daniela Fábián Masoch,
Founder, FABIAN PRIVACY LEGAL GmbH, Switzerland, www.privacylegal.ch
daniela.fabian@privacylegal.ch

Daniela is the founder and executive director of FABIAN PRIVACY LEGAL, a law firm specialized in international, European and Swiss data protection laws, governance, risk management and program implementation. Daniela is a Swiss attorney at law, certified Privacy Professional CIPP E, CIPPM, FIP and a certified ISMS 27001 Lead Auditor, with 30 years of experience in data protection, labor law, risk and program management, security and related matters. Daniela supports her clients in the EU, Switzerland and the US in evaluating, developing, implementing and monitoring data protection strategies, governance models and global privacy programs as well as data transfer mechanisms with a pragmatic approach. Daniela is the former Global Head Data Privacy for Novartis, and member of various associations and networks.