DIGITALEUROPE

17 MAY 2021

Data transfers and effectiveness of supplementary measures

Introduction

The need to implement supplementary measures for transfers of personal data to third countries has become a key consideration following the *Schrems II* ruling.[1] This paper describes companies' best practice in the use of measures to complement the adoption of standard contractual clauses (SCCs) for data transfers, and sets out how such safeguards can reduce the impact of possible access requests, in particular excessive and disproportionate ones.

Internal company processes, along with contractual provisions with third-party service providers, provide for a structured, documented and controllable set of safeguards reflecting the nature, scope, context and purposes of the transfer concerned, as required by the *Schrems II* ruling and in light of the GDPR rules pertaining to technical and organisational measures.

This paper complements DIGITALEUROPE's initial analysis of the *Schrems II* ruling[2] as well as our response to the European Data Protection Board's (EDPB) initial Recommendations.[3]

We call on the EDPB to duly consider all these elements in the upcoming revision of its Recommendations.

[1] Case C-311/18.

[2] DIGITALEUROPE, *An early analysis of Schrems II – key questions and possible ways forward*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/08/DIGITALEUROPE_An-early-analysis-of-Schrems-II_Key-questions-and-possible-ways-forward.pdf.

[3] DIGITALEUROPE, *Response to draft EDPB Recommendations on supplementary measures for personal data transfers*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2021/01/DIGITALEUROPE-Response-to-draft-EDPB-recommendations-on-supplementary-measures-for-personal-data-transfers.pdf.

DIGITALEUROPE
Rue de la Science, 14A, B-1040 Brussels
T.+32 (0) 2 609 53 10 / www.digitaleurope.org / @DIGITALEUROPE
EU Transparency Register: 64270747023-20

Table of contents

Supplementary measures in light of the GDPR

The EDPB's current interpretation provides that all transfers must make access to the transferred data impossible or ineffective, simply based on a theoretical possibility of interference by third-country public authorities. Crucially, the current EDPB Recommendations appear to require such impossibility to apply to access not only by public authorities but also, in most cases, *by the data importer itself*.

There are urgent reasons to reconsider this approach, which goes against not only the *Schrems II* ruling, which always refers to the need to consider each specific transfer 'in the light of all the circumstances of that transfer,'[4] but most importantly the General Data Protection Regulation's (GDPR) very rules pertaining to technical and organisational measures, which should be the logical blueprint for any additional measures supplementing the use of SCCs.

The GDPR requires due consideration for 'the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons' when it comes to determining the appropriate technical and organisational measures for processing, including security.[5]

The likelihood and severity of risk are therefore central aspects to be taken into account along with the other circumstances surrounding the transfer. While such factors may not be relevant to the theoretical assessment of the third-country law and practice that companies must assess when adopting SCCs, they should be considered as part of the assessment of the appropriate supplementary measures.

In other words, if the data is of limited real-world interest to public authorities – for example business contact information or other personal data unlikely to be relevant for surveillance or intelligence purposes – this should have a bearing on the type of supplementary measures that are required. Experience companies have had with these types of requests in the past should also be factored in.

Real-world transfers and economic impact

As evidenced by our recent survey, scenarios with a low likelihood or severity of risk represent a predominant part of all data transfers outside the EU.[6]

---

[4] See notably paras 112, 113 and 121, C-311/18.

[5] Arts 25(1) and 32(1) GDPR.

[6] DIGITALEUROPE, *Schrems II impact survey report*, available at https://www.digitaleurope.org/wp/wp-content/uploads/2020/11/DIGITALEUROPE_Schrems-II-Impact-Survey_November-2020.pdf.

We estimate that 85 per cent of companies operating in Europe use SCCs, the vast majority (75 per cent) headquartered in the EU, and that 90 per cent of them are business-to-business (B2B) entities. Over 57 per cent transfer data to non-EU subsidiaries or close business partners using controller-to-controller SCCs. Such controllers in the destination country *must* be able to access the transferred data lest the transfer be made completely pointless.

In our response to the initial EDPB Recommendations we illustrate three scenarios, modelled after real-world use cases, showing the disproportionate economic impact that the EDPB's interpretation would have if enforced.[7]

To remedy such impact and stay true to the GDPR's approach, the EDPB's Recommendations should be amended to better reflect the role of both technical and organisational measures in safeguarding personal data when transferred.

Existing best practice

Most European companies have already developed a solid and controlled set of policies and processes providing protection to data subjects' personal data and rights, in particular in relation to transfers.

In order to ensure effective and secure data transfers, companies have implemented structured and controlled processes adapted to their business and operational methods (including security measures), the nature of the data concerned, the available IT solutions, and past experience surrounding the frequency and seriousness of potential requests for access to data by non-EU authorities.

In most cases, these processes and measures report to the highest company level, i.e. top management and Board of Directors, operationally similar to companies' commitment under binding corporate rules (BCRs) approved by data protection authorities (DPAs) for a group to designate a data protection officer (DPO) or another privacy professional reporting directly to the highest management level.

Resorting to such context-specific and tailored measures, or as need be reinforcing them, offers solid and proportionate protection for transfers, in particular in relation to less sensitive data, without having to implement extremely constraining technical protection such as systematic encryption.

[7] See pp. 6-9, *Response to draft EDPB Recommendations on supplementary measures for personal data transfers*.

Analysis of the processing and transfer

The starting point lies in an analysis of the organisation's processing activities, including data transfers. Such analysis records what data will be transferred, the purposes of such transfers, the role and characteristics of the recipient, its 'need to know' and the country of destination. The nature and type of data concerned, as well as the context of the envisaged processing or transfer, constitute particularly important elements of this analysis.

This analysis ensures that an assessment of the impact of the transfer is performed in a structured, objective and documented basis. It includes whether the data to be transferred is likely to be covered by relevant third-country legislation, and can encompass the company's past experience about such transfers, providing a realistic assessment of the degree of risk exposure presented by the transfer at hand.

If processing is identified as presenting a particular level of sensitivity or risk, for example due to the high volume or the special categories of personal data involved, a data protection impact assessment (DPIA) is performed in accordance with Art. 35 GDPR and relevant DPA and EDPB guidance.[8] DPIAs provide a well-known and defined framework to evaluate the proposed processing, including the possible transfer.

Irrespective of whether a DPIA is performed, if required following the analysis of the organisation's processing activities and transfers, a specific remediation plan is defined and implemented under the accountability principle. Such remediation plan can for instance include the following measures:

- A limitation of the functionalities allowed for the specific IT solution considered;
- Further data minimisation and safeguards relating to the need to know and access modalities to the data;
- The conclusion of specific reinforced confidentiality or non-disclosure agreements, even on a person-by-person basis; and
- Reinforced, more specific IT security measures.

[8] See, for example, Section 42, 'Transfers: compliance with the obligations bearing on transfer of data outside the European Union,' of CNIL's *Privacy Impact Assessment (PIA) 3: knowledge bases* guidelines, available at https://www.cnil.fr/sites/default/files/atoms/files/cnil-pia-3-en-knowledgebases.pdf.

Strict assessment of third-party provider solutions

In addition to the above, a number of additional safeguards can be implemented in the relationship with IT providers, some of which complement measures already identified under the GDPR.

During the negotiating phase, an EU data exporter will typically carry out an assessment of the data importer's ability to comply with the terms of the SCCs and to implement and maintain the appropriate technical and organisational security measures to safeguard the personal data they are processing.

From this perspective, data exporters can complete security and data protection assessment questionnaires during the selection process of a potential service provider, based on the documentation made available by the importer, in order to precisely assess the level of security measures taken and made available by the latter for the services requiring data transfers.

The data exporter can also use such questionnaires to assess the technical, organisational and contractual supplementary measures the provider/data importer takes and makes available to further protect personal data. These measures may include: encryption (e.g. at rest, in transit, with robust key management systems); data minimisation policies and controls to limit the data importer's access to data; processes that the data importer implements to review and assess the validity of law enforcement orders; measures to allow the data exporter to control where data is stored and transferred; reports detailing the number and types of law enforcement requests the data importer has received; and contractual commitments to challenge law enforcement requests. Following this analysis, the data exporter can perform an assessment of the proposed processing and transfers to assess whether to use the IT solution.

Contractual measures

The conclusion of a data processing agreement between the data controller (the company) and the processor (IT provider) provides binding contractual force to the defined modalities and safeguards. The agreement, which the SCCs are annexed to, specifically defines the modalities of implementation of the obligations imposed on the data processor (including Art. 28 GDPR) and provides the legal basis for the implementation of the necessary safeguards.

As encouraged by Recital 109 GDPR, additional contractual measures are in most cases already taken by the data exporter in order to detect, trace and keep as much as possible control in case of compelled disclosure by the public authority against the data importer/supplier. This also facilitates the data controller's prompt response, such as transfer interruption, to further mitigate the risk.

Companies seek to include a 'compelled disclosure' clause as a contractual best practice in any organisation data processing agreement template. Under this clause, a specific process is defined between the data exporter and data importer, the latter being committed to:

- Notifying the data exporter;
- Informing the authority of an order's conflict with EU law and resorting to any available legal means to question such order;
- Redirecting the request to the data exporter and avoid disclosing associated personal data, unless legally forced to do so pursuant to an enforceable legal decision; and
- In any event, minimising the disclosure to what is strictly necessary.

The new draft SCCs proposed by the European Commission include such compelled disclosure provisions by default.[9] They would further harmonise such approach and significantly mitigate the risk triggered by compelled disclosures in third countries through obligations of the data importer both to report disclosure orders to the data exporter and to legally oppose and challenge the disclosure whenever permitted by law.

In cases where the data importer's domestic law would prohibit disclosure, including to the exporter, companies include provisions committing the importer to challenge the request, disclose only data which is absolutely necessary and with respect to which it has received a legally binding request.

Further clauses are being implemented to reinforce this mechanism, such as:

- Public records made available by importers providing aggregate statistical data about past requests for access; and
- Increasingly, the inclusion in the data processing agreement of a commitment from the importer to produce reports specific to the exporter concerned and setting out information on past data requests that could concern it. This last type of provision will benefit from further harmonisation with the adoption of the new SCCs.

Related guarantees involve cooperation, transparency and dedicated legal resources made available by the data importer to challenge orders, as well as to limit access to personal data that is strictly necessary to the request, thus ensuring effectiveness of the legal safeguards in place and a right balance

[9] https://ec.europa.eu/info/law/better-regulation/have-your-say/initiatives/12741-Cothefmmission-Implementing-Decision-on-standard-contractual-clauses-for-the-transfer-of-personal-data-to-third-countries

between the national security risk of the third country and the data subject's rights.

It is important to note that requests involving business data remain extremely rare and depend on the nature of the services and the type of data. Cloud providers receive relatively few demands regarding enterprise customers, which are in any event handled according to the process highlighted above.

Certification and unauthorised access

Verification mechanisms such as data protection and data security certifications can help demonstrate data minimisation and organisational security measures that protect against unauthorised access.[10]

In addition, remote access from a third country for maintenance/support purposes can be governed by very strict rules, which can include ad hoc authorisations that are limited in time and scope by the data exporter and under strict tracking and logging.

Concluding remarks

The above elements show that internal company governance and processes, along with provisions included in contracts with third-party service providers, provide for a structured, documented and controllable framework to register and assess proposed processing and transfers, and implement a wide set of safeguards, internally and externally.

These processes allow companies to adapt the degree of protection to the nature of the data concerned and the sensitivity of the context, as required by the *Schrems II* ruling and in light of the GDPR rules pertaining to technical and organisational measures.

We call on the EDPB to duly consider all these elements in the upcoming revision of its Recommendations.

[10] For example, ISO 27701, providing a globally recognised tool for international data transfers.

FOR MORE INFORMATION, PLEASE CONTACT:

Alberto Di Felice

Director for Infrastructure, Privacy and Security

alberto.difelice@digitaleurope.org / +32 471 99 34 25

Martin Bell

Policy Manager for Privacy and Cybersecurity

martin.bell@digitaleurope.org / +32 492 58 12 80

About DIGITALEUROPE

DIGITALEUROPE represents the digital technology industry in Europe. Our members include some of the world's largest IT, telecoms and consumer electronics companies and national associations from every part of Europe. DIGITALEUROPE wants European businesses and citizens to benefit fully from digital technologies and for Europe to grow, attract and sustain the world's best digital technology companies. DIGITALEUROPE ensures industry participation in the development and implementation of EU policies.

DIGITALEUROPE Membership

Corporate Members

Accenture, Airbus, Amazon, AMD, Apple, Arçelik, Atos, Autodesk, Bayer, Bidao, Bosch, Bose, Bristol-Myers Squibb, Brother, Canon, Cisco, DATEV, Dell, Dropbox, Eli Lilly and Company, Epson, Ericsson, Facebook, Fujitsu, GlaxoSmithKline, Global Knowledge, Google, Graphcore, Hewlett Packard Enterprise, Hitachi, HP Inc., HSBC, Huawei, Intel, Johnson & Johnson, JVC Kenwood Group, Konica Minolta, Kyocera, Lenovo, Lexmark, LG Electronics, Mastercard, Microsoft, Mitsubishi Electric Europe, Motorola Solutions, MSD Europe Inc., NEC, NetApp, Nokia, Nvidia Ltd., Oki, OPPO, Oracle, Palo Alto Networks, Panasonic Europe, Philips, Pioneer, Qualcomm, Red Hat, Ricoh, Roche, Rockwell Automation, Samsung, SAP, SAS, Schneider Electric, Sharp Electronics, Siemens, Siemens Healthineers, Sky CP, Sony, Swatch Group, Technicolor, Texas Instruments, Toshiba, TP Vision, UnitedHealth Group, Visa, VMware, Workday, Xerox, Zoom.

National Trade Associations

Austria: IOÖ
Belarus: INFOPARK
Belgium: AGORIA
Croatia: Croatian Chamber of Economy
Cyprus: CITEA
Denmark: DI Digital, IT BRANCHEN, Dansk Erhverv
Estonia: ITL
Finland: TIF
France: AFNUM, SECIMAVI, Syntec Numérique, TECH IN France
Germany: Bitkom, ZVEI
Greece: SEPE
Hungary: IVSZ
Ireland: Technology Ireland
Italy: Anitec-Assinform
Lithuania: INFOBALT
Luxembourg: APSI
Netherlands: NLdigital, FIAR
Norway: Abelia
Poland: KIGEIT, PIIT, ZIPSEE
Portugal: AGEFE
Romania: ANIS
Slovakia: ITAS
Slovenia: ICT Association of Slovenia at CCIS
Spain: AMETIC
Sweden: Teknikföretagen, IT&Telekomföretagen
Switzerland: SWICO
Turkey: Digital Turkey Platform, ECID
United Kingdom: techUK