THE DATA PROTECTION IMPLICATIONS OF BREXIT

After more than four years of negotiations following the UK's referendum on Brexit, a Trade and Cooperation Agreement (hereinafter referred as "TCA") was finally agreed on 24 December 2020. The TCA sets out arrangements in various areas including the processing of personal data.

I. IMPACTS ON DATA TRANSFERS

Under the TCA which is applicable from the 1 January 2021, the EU has agreed to delay restrictions on data transfer from the EEA to the UK for an additional period maximum until June 30, 2021 (the so called bridge). This enables the transfer of personal data to the UK to flow in accordance with the GDPR without any further restrictions. Without this bridge the UK would be considered as a third country. However, if the bridge ends and by then no adequacy decision will be adopted by the EU Commission, data transfers can only take place if the requirements of the GDPR on data transfer to third countries are met.

II. APPLICABLE LAWS

The GDPR is an EU Regulation and as of 1 January it no longer applies to the UK. However, the GDPR may also still apply to UK controllers/processors who operate in the EEA, offer goods or services to individuals in the EEA, or monitor the behaviour of individuals in the EEA. The provisions of the GDPR were incorporated directly into UK law (UK GDPR) at the end of the transition period (31.12.2020). So the core data protection principles, rights and obligations of the GDPR practically remained the same. Alongside the UK GDPR the UK Data Protection Act 2018 (DPA 2018) continues to apply in the UK and also for controllers/processors based outside the UK if their processing activities relate to the offering goods or services to individuals in the UK or monitoring the behaviour of individuals taking place in the UK.

III. COMPETENT AUTHORITY FOR CROSS-BORDER ISSUES

For any EU-UK cross-border disputes UK controllers/processors, in order to benefit from the one-stop shop mechanism of the EU, from 1 January 2021, will need to have a principal establishment in the EU.

IV. EU REPRESENTATIVE

As of 1 January 2021, UK controllers/processors, who are subject to the GDPR, are required to appoint a "representative" in the EU.

V. ADEQUACY DECISION

Also, the UK is covered by the requirement of adequacy where to third countries must provide of an adequate level of data protection if personal data from the EEA will be transmitted. Hence, the data protection safeguards in place in a third country must provide the same levels of safeguards that apply in the EU for the protection of personal data. You need to consider what alternative safeguards you can put in place to ensure that data can continue to flow into the UK for being prepared if no adequacy decision will be rendered by the European Commission.

DATA TRANSFER INTO THIRD COUNTRIES

According to the requirements of the GDPR any transfer of personal data to a third country (country outside the EU) is only permissible if this third country ensures an adequate level of protection and the level of protection for natural persons guaranteed by the GDPR is not undermined. The rules on the permissibility of a data transfer to third countries are incorporated into Art 44-49 GDPR. Since the UK is no longer an EU member state, it qualifies as a third country, although this qualification has been delayed during the bridge period, until 30 June 2021 at the latest.

I. ADEQUACY DECISION

As mentioned previously, the question whether an adequate level of protection is ensured for the data transfer to a third country is determined, i.e. by an adequacy decision. In case an adequacy decision was taken by the EU Commission, data controllers from an EU member states may transfer personal data to this third country without additional guarantees being required.

II. ALTERNATIVE LAWFUL BASIS

In addition to an adequacy decision, the following may - among others - also serve as lawful basis for data transfers to the UK or to any third country:

- standard data protection clauses adopted by the EU Commission;
- ad hoc contracts authorised by the competent data protection authority;
- binding corporate rules (BCR) authorised by the competent data protection authority;
- explicit consent of data subjects after having been informed of the possible risks of the absence of adequacy decision and appropriate safeguards; or
- in the absence of an adequacy decision or appropriate safeguards: performance or conclusion of a contract, vital interests or establishment, exercise or defence of legal claims etc.

It needs to be carefully evaluated which of the alternative lawful basis provided for by the GDPR will be suitable for the data transfer in question. This requires a case-by-case examination including risk evaluation (frequency of data transfer, types of data, other processing criteria, etc).

In the light of the recent 'Schrems' decision of the ECJ, in case you would like to rely on standard data protection clauses adopted by the EU Commission, you must also conduct a risk assessment as to whether the legal framework of the target country offers an appropriate level of protection. What this exactly in the practice means, still needs to be seen.

III. SANCTIONS FOR BREACH OF ARTICLE 44 PP GDPR

The absence of the lawful basis for the data transfer qualifies as a breach of the GDPR, in which case a fine up to EUR 20 million or 4 % of the worldwide annual turnover may be imposed. Companies need therefore to be prepared for the event that the EU Commission will not have adopted an adequacy decision on the UK by the end of the bridge period.

THE EU-UK AGREEMENT ON DATA TRANSFER

I. THE TRADE AND COOPERATION AGREEMENT

The most important provision of the TCA regarding data protection sets out that personal data may be transferred from the EU to the UK with no further guarantees for a period of four months (the bridge) from the end of the transitional period, that is from 1 January 2021. It was also agreed that this temporary period will be automatically extended by a further period of two months unless either the EU or the UK declares otherwise.

II. ADEQUACY DECISION

An adequacy decision is a formal decision made by the EU Commission, in accordance with Article 45 of the GDPR, which recognises that another country provides an equivalent level of protection for personal data as laid down in the GDPR. The UK is currently seeking an adequacy decision under GDPR. The effect of an adequacy decision is that personal data can flow from the EU (and Norway, Liechtenstein and Iceland) to the third country without any further safeguard being necessary. The abovementioned bridge period will end earlier if, in the meantime, the EU Commission adopts an adequacy decision.

III. ALTERNATIVE SOLUTIONS

The UK data protection authority, the Information Commissioner's Office, pointed out

that during this bridge period businesses need to be prepared to develop alternative data transfer mechanisms for the event that no adequacy decision will be made until the end of the bridge period. Other data transfer mechanisms which offer alternative solutions to comply with the GDPR are set out in Articles 46-50 of the GDPR. These rules govern any data transfers into third countries (countries outside the EEA) from the EEA. From 1 January 2021, the UK qualifies as a third country, though the application of the relevant rules is delayed during the bridge period.

IV. FURTHER COOPERATION

The EU and the UK also agreed to cooperate on data protection matters both at bilateral and multilateral levels through the exchange of experience and fight against crime. Regarding the location of data storage, the parties agreed that none of them will require that personal data is stored or processed in their territory.

NEW DATA PROTECTION LAW IN THE UK: THE UK REPRESENTATIVE

Obviously, the British people have not been satisfied with the EU. However, the GDPR was probably no ground to complaint, as now a "UK -GDPR" was put into effect on 1 January 2021 containing very similar rules comparing to its predecessor.

I. THE UK REPRESENTATIVE

Among others, the UK GDPR includes the requirement of a 'representative', the one introduced under Article 27 GDPR that applies to companies not established in the EU.

Companies that do not have a place of business in the UK but offer goods or services to individuals in the UK or monitor the behaviour of individuals within the UK shall appoint a representative under Article 27 of the UK GDPR. This obligation applies to but is not limited to online providers and IT companies that process personal data for their customers. It applies even if the IT company is carrying out the processing solely by order, which means that the data will be processed on behalf of a third party only.

Similarly to the European model, the UK representative shall act as a local contact person and, if necessary, shall communicate with the British Information Commissioner's Office as the responsible data protection authority. He/she is also the delivery agent for all communications relating to data protection in the UK. This is to avoid losing too much time in cross-border communication.

II. QUALIFICATION OF THE REPRESENTATIVE

The representative may be a company or an individual established or resident in the UK and it need to be notified to British Information Commissioner's Office in writing. He/she shall have access to the company's records of processing activities (Article 30 GDPR) and be fully authorised to act on the company's behalf. Hence, he/she shall be an expert in the field of data protection law. He/she shall also be listed in the company's data privacy policies with his/her contact details.

III. POSSIBLE SANCTIONS

The penalties for a breach of the UK GDPR are likewise draconian as those under the GDPR: Fines up to GBP 8,700,000 or 2% of a company's annual worldwide turnover may be imposed. Thus, personal data of persons from the United Kingdom should enjoy the same level of protection and the same principles should be applied as under the GDPR.

YOUR BREXIT-CHECKLIST REGARDING DATA PROTECTION

The following list is intended to help you identifying the measures your enterprise needs to take for complying with the new legal requirements after Brexit:

- What personal data of your company are processed in the UK?
- What data of UK citizens are processed by you?
- Is there a legal basis for each processing?
- Is the UK listed as a new third country in your records of processing activities?
- As to consents: Are those sufficiently recorded or does additional information on the new legal situation have to be submitted?
- Do measures need to be taken to ensure an adequate level of data protection? Do you have sufficient information from your cooperation partners?
- Do your data privacy policies (employees, website, customers) need to be adapted? Has the UK representative been listed?
- Will affected persons be informed on the data being processed in the UK? Did you ensure that affected parties will be informed on the processing of data in the UK when initiating a request according to Art. 15 GDPR (right of access)?
- Are data protection impact assessments to be updated or repeated with respect to the new legal situation?

CONTACT

Austria:
Michael Pachinger
M.Pachinger@scwp.com

Bulgaria:
Cornelia Draganova
Cornelia.Draganova@schindhelm.com

Czech Republic/Slovakia:
Monika Wetzlerova
Wetzlerova@scwp.cz

France:
Maurice Hartmann
Maurice.Hartmann@schindhelm.com

Germany:
Karolin Nelles
Karolin.Nelles@schindhelm.com

Sarah Schlösser
Sarah.Schloesser@schindhelm.com

Hungary:
Beatrix Fakó
B.Fako@scwp.hu

Italy:
Tommaso Olivieri
Tommaso.Olivieri@schindhelm.com

Poland:
Anna Materla
Anna.Materla@sdzlegal.pl

Romania:
Helge Schirkonyer
Helge.Schirkonyer@schindhelm.com

Spain:
José Tornero
J.Tornero@schindhelm.com

Turkey:
Müge Şengönül
Muge.Sengonul@schindhelm.com

Publisher, media owner, editorial office: Saxinger, Chalupsky & Partner v.o.s., advokátní kancelá | 301 00 Plze , B. Smetany 2, Tel.: +420 377 330 163, plzen@scwp.com | 110 00 Praha 1 Tel.: +420 221 803 350, praha@scwp.com | Saxinger, Chalupsky & Partner v.o.s., advokátní kancelá is a member of SCWP Schindhelm Services SE, Alliance of European Commercial Law Firms | All information is subject to correction in spite of careful processing and cannot replace individual advice in individual cases. The liability of the authors or the publisher is excluded.