EuroCloud DEUTSCHLAND | eco

Verband der Cloud-Computing-Wirtschaft

Legal Guidelines

Brexit is Coming – What You Still Need To Do

The EU General Data Protection Regulation (GDPR) applies also to the use of cloud services within the European Union (EU). As such, providers are typically regarded as processors as defined in the GDPR, depending on the type of use in individual cases. Under the GDPR, cross-border processing of personal data within the EU is permissible without any further requirements (Article 1 (1), Articles 44 et seq. GDPR).

While the United Kingdom (UK) leaving the EU does not change the overall legal situation, it does change the data protection treatment of a data transfer to the UK. The legal requirements of Articles 44 et seq. of the GDPR must be then complied with to make a legal data transfer to the UK – as well as for transfers to, for example, Switzerland or the USA. The final details of the withdrawal negotiations between the EU and the UK – "deal or no deal" – is irrelevant: In any case, the UK – whether from 30 March 2019 or at a later date – will be a third country for the purposes of the GDPR.

An independent (additional) legal basis will be required for data transfers to the UK after its departure from the EU. The European Commission has promised an adequacy decision pursuant to Article 45 GDPR. However, this has not yet been delivered and, as things stand at present, will probably not have been by the time the UK withdraws.

Do note that there is no formal legal grace period. As soon as the withdrawal becomes effective, a data transfer is illegal and subject to a fine, unless the requirements of Articles 44 et seq. of the GDPR are observed or a transitional agreement has been agreed upon as part of a withdrawal deal. In order to ensure the continuation of cloud services, the prerequisites for the alternative adequacy regulations must be created!

Personal data may also be transferred to third countries if "suitable safeguards" exist which guarantee an adequate level of protection (Article 46 (1) GDPR). Apart from the strict exceptions under Article 49 GDPR, such safeguards may consist of the following measures under Article 46 (2) GDPR:

- Binding Corporate Rules (BCR) pursuant to Article 47 GDPR
- Standard Data Protection Clauses adopted by the European Commission (typically the 'standard contract clauses (processors)' in the case of contract processing)
- Standard Data Protection Clauses of the supervisory authority of a Member State (such clauses are not yet available)
- Codes of Conduct (Article 40 GDPR) or Certification Mechanisms (Article 42 GDPR) approved for this purpose by the competent supervisory authority in conjunction with the obligation to

apply the safeguards suitable for the third country
- Contractual clauses approved in individual cases by the competent supervisory authority and agreed with the processor in the third country (Article 46 (3)(a) GDPR)

The so-called standard contractual clauses[1] are the first option for implementation in the short-term. For cloud services which are typically classified as order processing, the Standard Contractual Clauses (Processors)[2] should be used. These are ready-to-use templates. However, it is imperative to note that these standard contractual clauses must be only filled in – and not varied or modified – in order to be valid.

Cloud services can also face challenges on another level: Cloud services that, from a data protection point of view, are offered from the UK by the cloud provider often use other subcontractors in third countries. The UK company acts as a kind of "bridgehead". The data protection border is only crossed at the contractor-subcontractor level. After leaving the EU, however, this will be considered a further transfer to third countries. Additional requirements may then arise under the GDPR and other EU standard agreements.

As a consequence, the data protection re-evaluation must not be limited to the first level of outsourcing, but must cover the entire subsequent chain of subcontractors!

Recently, the European Data Protection Board (EDPB), an association of the national data protection supervisory authorities of the EU Member States, also pointed out the urgent need for action. In its information paper[3] of 12 February 2019, the EDPB expressly confirmed the use of the Standard Contractual Clauses as a "ready-to-use instrument".

In short: the withdrawal of the United Kingdom from the EU does not give rise to any fundamental legal issues with regard to the use of cloud services. However, there is still an urgent need for action: the specifications for data transfers to third countries must be created in time for the departure. The Commission's existing Standard Contractual Clauses for the transfer of data to processors in third countries constitute a quick and simple solution.

Authors

Dr. Jens Eckhardt,
Lawyer

dmp Derra, Meyer & Partner Attorneys-at-Law PartGmbB, Dusseldorf, Ulm, Berlin

Specialist Lawyer in IT Law, Privacy Auditor (TÜV), Compliance Officer (TÜV), ECSA Auditor

Board member, EuroCloud Deutschland_eco e.V.

Johanna Mäkert,
LL.M. (Bucharest), Lawyer

dmp Derra, Meyer & Partner Attorneys-at-Law PartGmbB, Berlin

EuroCloud Deutschland_eco e.V.
Lichtstraße 43h
50825 Cologne, Germany

Email: info@eurocloud.de
Web: www.eurocloud.de

[1] https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en
[2] https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX%3A32010D0087
[3] https://edpb.europa.eu/our-work-tools/our-documents/other/information-note-data-transfers-under-gdpr-event-no-deal-brexit_en