GERMAN SUPERVISORY AUTHORITY INITIATES POST-*SCHREMS II* ENFORCEMENT AGAINST EU COMPANIES USING U.S. SERVICE PROVIDERS

Date: 1 April 2021

EU Data Protection, Privacy, and Security Alert

By: Claude-Étienne Armingaud, Dr. Thomas Nietsch, Martin Fokken

The Bavarian Data Protection Authority recently prohibited a European company from using U.S. newsletter provider Mailchimp in a first-of-its-kind decision.

Since the *Schrems II* decision of the Court of Justice of the European Union (CJEU) last year (see our alert here), companies in the European Union found themselves between a rock and a hard place, as many still rely on U.S.-based online service providers in one capacity or another, and the CJEU, in addition to totally invalidating the Privacy Shield framework, mandated additional requirements over the Standard Contractual Clauses (SCCs), the most widely used lawful transfer mechanisms.

Following this CJEU decision, the Bavarian Data Protection Authority (Bayerisches Landesamt für Datenschutzaufsicht) has now effectively barred a European online magazine from using the popular U.S.-based newsletter delivery service, Mailchimp.

Companies using Mailchimp to route their newsletters must generally transfer personal data (e.g., the recipients' email addresses) to Mailchimp's servers in the United States. Previously certified under the late EU-U.S. Privacy Shield framework, Mailchimp had to pivot to offer its European customers an alternative transfer mechanism, i.e. the SCCs. While their general validity was left untouched by the *Schrems II* decision, the CJEU argued that it may be required for companies relying on the SCCs to assess whether additional safeguards should be implemented on top of the SCCs in order to effectively protect personal data.

As expressly mentioned in the *Schrems II* decision, transfers to cloud service providers in the United States would require such additional safeguards, due to the broad investigative powers of U.S. authorities, e.g., under Section 702 (50 U.S.C. § 1881a) of the Foreign Intelligence Surveillance Act (Cloud Services Act).

Until now, it had seemed that the EU supervisory authorities had granted companies an unofficial grace period to adjust to the amended legal situation, especially as new templates for SCCs taking into consideration the *Schrems II* decision are expected to be finalized in the coming weeks.

The action of the Bavarian Data Protection Authority shows that this restraint might have come to an end. In a recent press release concerning this investigation, the authority commented that the case was exemplary for their enforcement of the requirements of the *Schrems II* decision, which had already been taken up with a high degree of intensity even without publicly perceived investigations or sanctions.

The Bavarian Data Protection Authority based its action expressly on the fact that the European company has not assessed whether additional safeguards for transferring personal data to Mailchimp were required, in particular as

Mailchimp may be subject to the Cloud Services Act. While no fine was imposed in this case and the Bavarian Data Protection Authority did not issue a formal decision, the authority still informed the company that their use of Mailchimp was (in their view) not in line with General Data Protection Regulation (GDPR) requirements. The company also promised to cease using Mailchimp in the future.

However, it should be noted that the official reason for not imposing a fine was on the one hand, the low sensitivity of the data transferred (email addresses only) and, on the other hand, the limited scope of the transmission (only two newsletters were sent). The details of the case being leaked and officially commented on by the supervisory authority could be considered as a warning to other EU companies transferring data to U.S. cloud service providers, which should probably expect less leniency from the supervisory authorities from now on.

The current case was rather clear, as the European company in question has apparently taken no steps at all to establish and document whether additional safeguards were required and were already (because of this omission) in breach of their statutory obligations under GDPR. Future cases will probably not be as easy to decide, in particular when an EU company has documented a respective assessment or even implemented additional safeguards, and supervisory authorities and ultimately courts will have to assess what is really required to ensure adequate security of personal data in countries outside the European Union.

Following the decision of the Bavarian Data Protection Authority, EU companies using U.S. online service providers, especially cloud services, are therefore encouraged to check the basis of their data transfers to the United States and, if necessary, adapt them to the new legal situation in order to avoid facing potentially high fines.

K&L Gates' global data protection team (including in each of our European offices) remains available to assist you in achieving the compliance of your data transfers at global levels.

KEY CONTACTS

CLAUDE-ÉTIENNE ARMINGAUD
PARTNER

PARIS
+33.1.58.44.15.16
CLAUDE.ARMINGAUD@KLGATES.COM

DR. THOMAS NIETSCH
PARTNER

BERLIN
+49.30.220.029.408
THOMAS.NIETSCH@KLGATES.COM