



data protection - legal changes published in September 2021

I. European Union

1 REGULATIONS

1.1 EDPB establishes cookie banner taskforce

The EDPB decided during its latest plenary to set up a taskforce to coordinate the response to complaints concerning cookie banners filed with several EEA SAs by NOYB.

This taskforce was established in accordance with Art. 70 (1) (u) GDPR and aims to promote cooperation, information sharing and best practices between the SAs.

In particular, the taskforce will:

- exchange views on legal analysis and possible infringements;
- provide support to activities on the national level;
- streamline communication.

1.2 Starting September 27, 2021, the new Standard Contractual Clauses, available for the transfer of personal data to third countries under the GDPR, have entered into force

Following the judgment of July 16, 2020 in the Data Protection Commissioner v. Facebook Ireland Limited and Maximilian Schrems, C-311/18 (known as 'Schrems II'), the Court of Justice of the European Union (CJEU) declared the Privacy Shield between the European Union and the United States of America invalid, considering the level of protection of personal data transferred from the EU to the United States to be insufficiently adequate.

The old Standard Contractual Clauses (SCC), adopted in 2004 (controller to controller relationship) and 2010 (controller to processor), will, in principle, lose their validity starting with September 27, 2021. According to the transitional provisions established by the Decision of the European Commission (the so-called "sunset clauses") by which the new SCC model was adopted:

- Companies that conclude new contracts after September 27, 2021, will use the new SCC;
- The companies having established SCC through the previous contracts will be able to use the old SCC for another 15 months after the date of entry into force of the new clauses, respectively until December 27, 2022, if there are no new processing operations within these contracts.

The new SCC contain a more modern and modular approach (in line with the GDPR provisions) of the obligations to protect personal data when transferred to third countries, compared to the previous version. More onerous obligations for data importers are established (e.g. regarding transparency and the right of access to data of the data subject). Moreover, SCC are a form of "appropriate safeguards" that can be used when there is no adequacy decision in the country of data import under Article 45 of the GDPR.

Following the decision of 04.06.2021 of the European Commission, even if the model clauses remain, in principle, a valid mechanism for the export of data outside the EU, in order to be able to rely on them, the exporters and importers of the data will have the obligation to carry out a serious analysis to demonstrate that



the receiving country guarantees the same level of protection as the EU and to take additional protection measures/ guarantees, if there is no equivalent protection.

Binding Corporate Rules (BCRs) are affected in the same way by the Schrems II ruling as the Model Clauses, as even in the case of this transfer tool, U.S. laws take precedence.

More information about SCC is available at: <https://www.vf.ro/hotararea-schrems-ii-cum-mai-transferam-datele-personale-catre-tari-terte-cateva-recomandari-practice/>

1.3 Plenary session of the European Data Protection Board

At the plenary of the European Data Protection Board, held online on September 24, 2021, the Opinion no. 32/2021 on the draft regarding the European Commission Decision on the recognition, in accordance with Regulation (EU) 2016/679, of an adequate level of protection of personal data in South Korea came into force. More information is available at: https://edpb.europa.eu/news/news/2021/edpb-adopts-opinion-draft-south-korea-adequacy-decision_ro

2 EUROPEAN UNION – SANCTIONS GRANTED IN THE EU.

2.1 The Norwegian Data Protection Authority ("Datatilsynet") imposed a fine of €496,000 for alleged breaches of the GDPR

The Norwegian Data Protection Authority ("Datatilsynet") imposed, on 28 September 2021, a fine of NOK 5 million (approximately EUR 496,000) on Ferde AS for the illegal transfer of drivers' personal data to a processor in China.

Datatilsynet found that Ferde AS violated, for a period of between one and two years, a series of basic obligations that the company has under the General Data Protection Regulation, namely Art. 5 (1) f), Art. 5 (2), Art. 28 (3), Art. 32 (2) and Art. 44 GDPR.

In addition, Datatilsynet pointed out that, among other things, the company did not have a valid basis for the transfer of personal data to China and that a large number of people were affected.

Datatilsynet stated that they will maintain the decision to impose the fine in question after sending the company a notice to impose the fine in the amount indicated above, earlier this year.

2.2 Hamburg's Commissioner for Data Protection and Freedom of Information (HmbBfDI) imposed a GDPR fine of €900,000 to Vattenfall Europe Sales GmbH

On September 24, 2021, the Hamburg Commissioner for Data Protection and Freedom of Information (HmbBfDI) imposed a GDPR fine of EUR 900,000 on Vattenfall Europe Sales GmbH.

The fine was imposed due to a breach of GDPR's transparency obligations under Articles 12 and 13.

HmbBfDI took into account both the rights to protect customer data and the economic interests of the company when defining the final amount of the fine.

HmbBfDI stated that Vattenfall demonstrated cooperation in the process and immediately ceased comparing non-transparent data, which contributed to a significant reduction in the fine.



2.3 The Danish Data Protection Authority fines the Danish Cancer Association with an amount of €107,000

The Danish Data Protection Authority imposed a fine of EUR 107,000 on the Danish Cancer Association for breaching Art. 32 GDPR. The association did not comply with the GDPR requirements for appropriate security measures. At least 1,448 citizens' information - including sensitive personal health information - has been compromised.

However, the Danish Data Protection Authority is aware that the Danish Cancer Association is an organization where the majority of the association's revenue comes from donations and private funds. In calculating and evaluating the amount of the fine, the Danish Data Protection Agency took, as a starting point only the income of the Danish Cancer Society from recycling, events, sales of goods and other products, which corresponds to approximately 10% of the total income of the Association.