Insights: Alerts

Cross-Border Data Transfers: Spain's Data Protection Authority Imposes Its Largest Fine

March 23, 2021

Written by

On March 11, 2021, the Spanish Data Protection Authority ("AEPD"), imposed the regulator's largest ever fine, totaling €8.15 million ($9.378 million), upon Vodafone España, S.A.U ("Vodafone"), a telephone operator, for violating multiple data protection laws while Vodafone carried out marketing campaigns. Most notably, it penalized Vodafone for non-compliant data transfers. Below is a summary of the four fines imposed by the AEPD and recommendations for organizations hoping to minimize the risk of similar scrutiny from the Spanish regulator.

A. Summary of Fines

Fine #1: The AEPD imposed a €4 million fine against Vodafone for violating Article 28 of the General Data Protection Regulation ("GDPR"), which requires data controllers to use processors that provide sufficient guarantees and protections when processing personal data on their behalf, as well as Article 24 of GDPR, which requires controllers to "implement appropriate technical and organizational measures" and policies that are compliant with the GDPR. The AEPD concluded that Vodafone did not comply with GDPR when Vodafone and its distributors, collaborators, and agents contacted individuals via e-mail, phone, and text who opted-out of its marketing campaigns.

The AEPD came to this conclusion for multiple reasons:

- First, Vodafone alleged that it implemented a new routing system to verify the legality of its data and filter out users who had opted out of marketing communications. The AEPD concluded, however, that the system was not effective as consumers complaints of improper marketing messages continued even after Vodafone implemented this system. The AEPD also noted that a filtering system should have been required of all parties that carried out marketing on Vodafone's behalf.

- Second, the AEPD concluded that Vodafone should have required its processors, e.g., distributors, collaborators, or agents who carried out its marketing campaigns on Vodafone's behalf, to enter into contracts with guarantees to assure that the processors had implemented effective technical and organizational measures, as Vodafone had no such guarantees in place.

- Third, the AEPD held that Vodafone's procedures, including allowing individuals contacted to opt out of its marketing campaigns (rather than only contacting those that had opted in to receive marketing) and having managers review lists with those who opted-out, were insufficient. Article 21.1 of the Law No. 34/2002, of July 11, 2002, on Information Society Services and Electronic Commerce ("LSSICE") requires a data subject's "request or express authorization" to carry out marketing activities.

- Fourth, the AEPD noted there was no evidence that Vodafone carried out continuous data-monitoring through the entire data lifecycle, despite numerous known claims and investigations carried out by the AEPD.

Fine #2: The AEPD imposed a €2 million fine based on Vodafone's violation of Article 44 of the GDPR, which governs transfers of personal data to countries that are not within the European Economic Area or otherwise deemed adequate in accordance with the GDPR. The AEPD imposed this fine due to a contract between Vodafone and Casmar Telecom, SL, which stated that the "current treatment location" for data is Peru. The AEPD stated that the contract did not contain certain mandatory contractual clauses required by the European Commission's Decision of February 5, 2010, regarding Standard Contractual Clauses for the transfer of personal data to processors established in third countries (the "SCCs").

Fine #3: The AEPD imposed a €2 million fine for Vodafone's violation of Article 48(1)(b) of the General Law 9/2014, of May 9, 2014, on Telecommunications ("LGT"), in relation to Article 21 of GDPR and Article 23 of the Organic Law 3/2018, of December 5, 2018, on the Protection of Personal Data and Guarantee of Digital Rights ("LOPDGDD"), which governs the data subject's right to object to certain processing. The AEPD concluded that Vodafone violated LGT as the claimants did not consent to receive marketing communications and Vodafone did not stop contacting those who had elected to opt-out of receiving such communications.

Fine #4: The AEPD imposed €150,000 fine for violation of Article 21 of LSSICE, which prohibits marketing communications that have not previously been requested or expressly authorized. The AEPD stated that Vodafone's marketing communications did not have the express authorization of the recipients as Vodafone contacted recipients by generating random numbers and addresses, which prevented Vodafone from verifying that the recipients authorized the communications.

B. Compliance Recommendations

The *Vodafone* decision by the AEPD provides valuable lessons with respect to both establishing technical and organizational measures for ensuring compliance with data protection laws and contractual requirements for transferring personal data to countries outside of the EEA.

A critical lesson learned from the *Vodafone* decision in terms of technical and organizational measures is that processors and subcontractors can be a significant source of risk to organizations. As demonstrated by the AEPD's actions in this enforcement action, data protection authorities can hold your organization accountable for the actions of your distributors, collaborators, and agents. This means that it is not only important for your organization to have measures in place that are compliant with relevant data privacy laws, but it is also important to contractually require any third parties with access to personal data to implement and maintain the same protections. As the *Vodafone* decision suggests, one way in which to accomplish this task is to have contracts in place that require such third parties to have implemented effective technical and organizational measures. Contracts should also include transparency obligations, which should require processors to promptly disclose any inability to comply with data privacy commitments. If your organization is a party to any contracts with third parties that handle personal data without such guarantees and transparency obligations in place, these contracts should either be amended or terminated if necessary. Finally, before entering into contracts with third parties with access to personal data, it is important to conduct adequate due diligence and inquire into how these third parties are handling personal data in order to assess their ability to guarantee that proper technical and organizational measures are in place.

In terms of data transfers to countries outside of the EEA, the *Vodafone* decision makes it clear that organizations should have a process in place for identifying international data transfers from EEA countries to non-EEA countries that are not considered adequate by the EU. Once contracts with such international data transfers are identified, your company should sign SCCs or rely on another GDPR-compliant data transfer mechanism to effectuate such data transfers. SCCs can be utilized in new third party relationships as well. Notably, this decision represents the most significant enforcement action following last summer's *Schrems II* decision.

Even companies that have executed SCCs must still consult relevant data privacy laws in the relevant transferee non-EEA countries to determine if such clauses are enforceable with counterparties in such countries. Finally, companies should consult the European Data Protection Board's recommendations adopted on November 10, 2020, to adopt appropriate supplemental and procedural measures for data transfers from the EEA to other countries. These include technical measures, such as

encryption, pseudonymization, and split processing, and organizational measures, such as internal policies for governance of data transfers, involvement of a data protection officer on all international data transfer matters, and regular review of the data commitments of third parties.

The decision also, practically speaking, requires companies to regularly audit the effective implementation of technical compliance measures. The fact that Vodafone had allegedly implemented a routing system to prevent marketing messages from being sent to data subjects that had opted out of marketing communications did not shield the company from enforcement scrutiny. Examples of such technical compliance systems include self-service portals for data subjects to exercise access and deletion requests, cookie consent mechanisms, and automated marketing consent recordkeeping.

This is just the first significant shot across the bow from European regulators for companies transferring personal data outside of the EEA, but it almost certainly not be the last. It will be important to carefully review your organization's data processing, subcontracting and transfer policies in order to avoid becoming the next regulatory target.

Footnotes

---

[1] See Sarah Coble, S*panish Data Protection Authority Issues Highest Fine*, Info. Security (last accessed on March 22, 2021), https://www.infosecurity-magazine.com/news/aepd-issues-highest-ever-fine/; Neil Hodge, *Vodafone Spain Fined Record $9.72M for Data Protection Failures*, Compliance Week (March 15, 2021), https://www.complianceweek.com/regulatory-enforcement/vodafone-spain-fined-record-972m-for-data-protection-failures/30162.article#:~:text=Vodafone%20Spain%20was%20fined%20a,fine%20against%20CaixaBank%20in%20January.