Spain

GDPR 'Glasnost': The Spanish AEPD Raises the Transparency Bar and Sanctions Two Banks

*Julien Levis and Philipp Fischer**

I. Introduction

What degree of detail do regulators expect in a privacy policy notice? Two recent decisions of the Spanish Data Protection Agency (Agencia Española de Protección de Datos, AEPD) with which it respectively fines Spanish banks Banco Bilbao Vizcaya Argentaria (BBVA)[1] and CaixaBank[2] with 5 and 6 million euros, set a high bar. Both decisions – issued one month apart – essentially highlight similar aspects and grievances primarily drawn from the alleged lack of clarity in the two banks' privacy notifications to their clients as well as in the process of obtaining consent.[3]

Both decisions illustrate a new trend in enforcement by Data Protection Authorities (DPAs). Sanctions issued over GDPR's first two years of implementation have largely focused on sanctioning manifest disregard for GDPR such as a lack of appropriate technical and organisational measures or the absence of a lawful basis for personal data processing. Recently, however, DPA scrutiny has become both more stringent and more focused on form. In that context, an emerging area of focus is data controllers' duty of information. The AEPD appears to be following a similar path to that of the Commission nationale de l'informatique et des libertés (CNIL) the French DPA, which decided on a similar matter just a few weeks earlier.[4] While the two AEPD decisions are primarily remarkable in their substantive reasoning (II.), this report will also highlight some particularly interesting procedural aspects (III.).

II. Substantive GDPR-based Reasoning of the Decision

This report will focus on three aspects regarding the substantive data protection rules, namely (i) the duty of information, (ii) the obtaining of a valid consent and (iii) the justification of data processing based on a legitimate interest.

1. Duty of Information

In its two decisions, the AEPD conducts a detailed review of the (publicly available) documents used by both banks to meet their duty of information under Article 13 GDPR and sets a high threshold for meeting that duty.

The AEPD criticizes both banks for providing unclear and non-systematic information on the data processing activities and their purposes. The Spanish authority highlights that the expressions used in the relevant privacy notices (such as processing of information "to provide new services", "to conduct investigations" or "to provide personalised services")

DOI: 10.21552/edpl/2021/2/14

* Julien Levis, Privacy practitioner, for correspondence: <julien.levis@protonmail.com>; Philipp Fischer, attorney-at-law, OBERSON ABELS SA (Geneva), for correspondence: <pfischer@obersonabels.com>.

1 PS/00070/2019 (December 11, 2020), available at <https://www.aepd.es/es/documento/ps-00070-2019.pdf>.

2 PS/00477/2019 (January 13, 2021), available at : <https://digitalesrecht-datenrecht.iusnet.ch/de/system/files/DOWNLOADS/ENTSCHEID/AEPD%2C%20Caixabank%20fine%2C%20PS-00477-2019%2C%2006.01.2021.pdf>.

3 The two examined decisions were issued a few weeks apart and each of them is obviously specific to the facts of the respective matters. They are nonetheless widely similar in their motivation. Therefore this report mainly focuses on the elements that are common to the two decisions. It will discuss the elements of reasoning that are common to both decisions, whilst mentioning differences where relevant.

4 See CNIL, Carrefour Banque decision of November 18th 2020, <https://www.cnil.fr/en/cnil-fines-carrefour-france-2-25-million-eu-and-carrefour-banque-800000-eu>; Cf. on this also Fischer/Levis, La CNIL sanctionne une banque pour des atteintes à la protection des données, <https://swissprivacy.law/47/>, English version available at <https://www.linkedin.com/posts/activity-6757195279901978624-XWCg>.