COVINGTON

COVINGTON & BURLING LLP

E-ALERT | Antitrust

December 1, 2014

JUDGMENT OF THE GENERAL COURT OF THE EU IN CASE T-272/12 ENERGETICKÝ A PRŮMYSLOVÝ HOLDING A.S. ET AL. VS. EUROPEAN COMMISSION EU POWERS OF INSPECTION GET ANOTHER BOOST

Correctly managing a dawnraid is becoming a critical part of any company's compliance toolkit. The GCEU has confirmed the very broad powers of the European Commission, and any attempt to obstruct a dawnraid can lead to the imposition of substantial fines, even if ultimately no competition infringement is found. Companies are well-advised to maintain stringent controls on their IT departments during dawnraids, and ensure that training incorporates appropriate awareness-raising.

The Judgment

On November 26, 2014, the General Court of the EU ("GCEU") ruled on an appeal brought by Czech energy firm Energetický a průmyslový holding a.s. and its subsidiary (together the "applicants") against a fine of €2.5 million imposed by the European Commission ("EC") in 2012, for failure to comply with the EC's powers of inspection under Article 23(1)(c) of Regulation 1/2003. The applicants essentially contended that it was incorrect that they had refused to submit to the inspection, and that the decision imposing the fine should be annulled. The GCEU dismissed the appeal in its entirety.

Background

In November 2009, as part of an EC investigation into the energy market in the Czech Republic, the EC dawnraided the applicants. The company did not object to the inspection, and it followed the usual routine: the EC team notified the company representatives, had the company describe its organizational structure, and then set out to start the inspection, which in this case involved working with the applicants' IT department, blocking and then reviewing the electronic accounts of four individuals employed by the company. In order to block the accounts, the EC re-set them with new passwords. The company was duly notified, and agreed to comply. However, subsequently, at the request of one of the four individuals, the IT department reset his password. The EC inspectors discovered this the next day. The event was minuted. During the third and final day of the dawnraid, the EC discovered that another account had been tampered with, with the e-mails being diverted to a separate server rather than being routed to the account.

Six months later, in May 2010, the EC initiated proceedings against the company for refusal to submit to an inspection and the production of required records related to the business in incomplete form. It went through various requests for information and state of play meetings, and issued two Statement of Objections (SO) before imposing the €2.5 million fine in March 2012, some 0.25% of the company's turnover in 2010. The appeal was lodged in June 2012.

Discussion and Implications

This is not the first case in which a company has attempted to escape an "obstruction of justice" type allegation arising during an EC dawnraid. The EC imposed a €38 million fine on E.ON in 2008, and an €8 million fine on Suez Environnement in 2011, both for breach of a seal.

The present case may appear minor in terms of the absolute size of the fine imposed -- but that would be an injudicious conclusion. First, in relative terms, the company in the present case was fined 0.25% of its relevant turnover, while E.ON's €38 million fine represented "only" 0.14% of its turnover. Beyond that, however, it really is the focus of this case on dealings with electronic data which makes it important.

The GCEU notably rejects the notion that the fine was disproportionate, linking the unblocking of the account in the present case to doubts about the "*integrity of the evidence in the sealed room*" as per E.ON, and adding that the deterrence aspect of the present fine is "*all the more important in the case of electronic files since, having regard to their particular nature, they are much easier and quicker to manipulate than paper files*". In reaching that conclusion, the GCEU has made a number of findings which should be front of mind for anyone dealing with a compliance effort involving IT related issues.

First, the EC need not prove that data was actually manipulated or deleted, only that (unlawful) access was granted during the blockage:

- It does not matter that the EC inspectors could access the electronic files by means of a server to verify that the data was intact, as the EC is "*under no obligation to investigate whether those files might be intact elsewhere*";
- For the same reason, it does not matter that the (unlawful) access was achieved remotely -- as it was -- such that the individual accessing the account could not alter the data stored on his PC.

Second, attempts to hide behind the IT manager are equally unfruitful:

- The IT manager, after having been duly briefed by the EC, has the responsibility to "*promptly instruct his subordinates in the IT department of those obligations [to block the accounts] and how to implement them as regards IT matters… in order to avoid an infringement of procedural obligations under Regulation 1/2003*". Failure to do so amounts to omission, according to the GCEU;
- It does not matter that IT management is outsourced to an independent service provider, such that the IT manager is not an employee of the company, given that the company had identified the person in question as being responsible for its IT services from the outset of the inspection.

Third, attempts to restore data are also irrelevant.

Fourth, the fact that the diversion of e-mails that (i) related to a very short phase of the inspection (as opposed to the total time period under investigation) and (ii) covered only "*a limited number of non-essential e-mails for the inspection*" is also not a defense: according to the GCEU, "*the quantity or significance of the diverted mails for the subject-matter of the investigation is irrelevant to establishing the infringement*".

In short, companies will be well-advised to maintain stringent controls on their IT departments during dawnraids, and ensure that training incorporates appropriate awareness-raising.

Correctly managing a dawnraid is becoming a critical part of any company's compliance toolkit. The GCEU has confirmed the very broad powers of the EC and any attempt to obstruct the dawnraid can lead to the imposition of substantial fines, even if ultimately no competition infringement is found. This judgment complements the very strict reading by the GCEU of the privilege rules in *Akzo* where only documents produced by external counsel are subject to legal privilege. It also builds on the position of the GCEU and the ECJ supporting the imposition of a fine on E.ON for breaking a seal during a dawnraid. The presence of experienced lawyers during dawnraids is becoming ever more critical, as is the roll-out of a stringent, tried-and-tested compliance program -- with an appropriate focus on IT.

If you have any questions concerning the material discussed in this client alert, please contact the following members of our antitrust group:

Peter Camesasca	+32.(0).25495238	pcamesasca@cov.com
Miranda Cole	+32.(0).25495264	mcole@cov.com
Johan Ysewyn	+32.(0).25495254	jysewyn@cov.com