Get ready for the Dutch Competition Authority's new dawn raid guidelines

March 10, 2014

The ACM has published new digital dawn raid guidelines specifying how it uses its powers to inspect and copy digital media. The guidelines also contain safeguards regarding legally privileged data. The ACM, like the European Commission, has been increasing its focus on digital data during dawn raids. It is thus important to take steps in preparation for a potential dawn raid regarding not only a company's hard copy files, but also its IT system. A designated IT representative and a general document management policy are advisable.

Only documents which:

- are not of a private (i.e., non-business) nature
- are not covered by legal professional privilege (LPP)
- are relevant for the subject matter and purpose of the investigation

can be claimed by the ACM inspectors during a dawn raid. The new dawn raid guidelines lay down the legal safeguards the ACM inspectors will observe while collecting digital data. Different from the European Commission officials, who usually inspect digital data on the spot, the ACM will secure the data at the company to be further investigated at the ACM's premises.

Given the ACM's and European Commission's increased focus on digital data, it is advisable for companies to designate an IT staff member as "dawn raid IT representative" beforehand to assist the European Commission and/or the ACM inspectors during their digital data search. This IT representative should be well informed about the company's IT environment, including the company's document retention policy and different IT systems used over time. In addition, as explicitly stated in the European Commission's guidance, the IT representative should be able to carry out specific tasks, such as the temporary blocking of individual email accounts, temporarily disconnecting running computers from the network, removing and re-installing hard drives from computers and providing support for "administrator access rights". The IT representative should also have insight into those other individuals authorised to block email accounts to prevent accidental "de-blocking" and, in the case of IT outsourcing, should have a contact ready there to avoid unnecessary delays in providing access to digital data.

The ACM's new guidelines also provide safeguards for data covered by LPP. Companies can claim LPP for documents during the on-site investigation. The ACM official will want to verify this claim by skimming through the document. However, in case of a dispute on LPP coverage or if the company refuses to allow ACM officials to have a cursory look at the document, a "sealed envelope" procedure similar to that known from EU case law applies. The ACM official will place the document in a sealed envelope and hand it to an independent ACM official, the "LPP officer". If the LPP officer, after having given the company opportunity to substantiate its LPP claim, is not convinced of the validity of the claim, the data will be provided to the ACM's case team within 10 business days. In those 10 business days, the company can initiate interlocutory proceedings concerning this matter. Similarly, if a company objects to having to hand over its documents to the LPP officer in the first place, it remains free to bring preliminary relief proceedings instead. If no summons is served on the ACM within 10 business days, the ACM official will hand over the sealed envelope to the LPP officer.

The Dutch rules on LPP, we note, differ from the EU rules. Under Dutch national rules, correspondence exchanged with lawyers admitted to the Bar – regardless of the country of establishment – is covered by LPP. In European Commission investigations, however, communications between in-house counsel and companies remain unprotected by LPP, regardless of whether the in-house counsel is a member of the Bar. Consequently, if the ACM inspectors conduct investigations on the basis of Dutch competition law, the Dutch national rules apply and the correspondence with both in-house and external lawyers is covered by LPP. The same applies to investigations by the ACM at the request of the Commission.

However, if the ACM inspectors only assist the Commission officials, the European rules apply and correspondence with in-house lawyers has no LPP coverage. It is therefore imperative for companies to verify at the very start of a dawn raid, which authority and, more importantly, in what capacity the authority is conducting the dawn raid to determine the level of LPP protection. Similarly, it is advisable for companies to introduce a general document management policy to avoid accidental disclosure during a dawn raid. Legally privileged materials, including (legally privileged) faxes and emails, should be kept separately from other documents in a marked file. It may also be wise to introduce policy rules to avoid cross-disclosure of LPP information in parallel international dawn raids.