DAWN RAIDS
EXPECT THE UNEXPECTED

Alex Nourry and Chandralekha Ghosh of Clifford Chance LLP explain how to prepare for an unexpected visit from competition authorities.

In recent years there has been a steady increase in enforcement of competition infringements, with higher fines by competition authorities across jurisdictions including the EU and the UK. The EU and UK competition authorities' powers of investigation include the ability to conduct unannounced inspections or dawn raids. Since the Modernisation Regulation (*1/2003/EC*) (2003 Regulation) came into effect in 2004, a number of decisions by the European Commission (the Commission) and the EU courts have helped to clarify some of the powers of the Commission in relation to a dawn raid so that companies can, to some extent, better know what to expect in case of the unexpected arrival of competition officials.

This article describes what companies might expect if subjected to a dawn raid by the Commission or the UK's Competition and Markets Authority (CMA), and other UK regulators with concurrent competition powers, and how companies might best prepare themselves to deal with a dawn raid before, during and after the event in light of recent developments in the practice and procedures of the Commission and the CMA (*see box "Regulators with concurrent powers"*).

LEGAL FRAMEWORK

In the UK, dawn raids in connection with competition investigations may currently be carried out by the Commission or UK competition authorities if they suspect that a company has breached:

- The prohibition on agreements or concerted practices which have as their object or effect the prevention, restriction or distortion of competition within the EU under Article 101 of the Treaty on the Functioning of the European Union (TFEU) (Article 101) or within the UK under Chapter I of the Competition Act 1998 (1998 Act).
- The prohibition of the abuse of a dominant position by companies of their market position in the EU, or a substantial part of the EU, under Article 102 of the TFEU (Article 102) or insofar as it affects trade in the UK under Chapter II of the 1998 Act.

However, the UK's withdrawal from the EU might potentially bring about changes to the legal framework in the near future (*see box "The impact of Brexit"*).

Competition authorities

Dawn raids may follow a complaint to the competition authority regarding the company or information received by the competition authority from a potential whistleblower. In addition, a competition authority may carry out unannounced inspections at the premises of companies in a particular sector if it has reason to suspect anti-competitive practices in that sector, for instance, before launching or after completing a market investigation or enquiry into that sector. For example, the Commission conducted dawn raids during the course of and following

its enquiry into the pharmaceutical sector, and opened a number of investigations into pharmaceutical companies following the publication of its final report in 2009 (*www.practicallaw.com/8-380-8892; www.practicallaw.com/8-518-6089; www.practicallaw.com/w-008-7799*).

Competition authorities often co-operate closely in investigations. In particular, the Commission may seek the assistance of national competition authorities, such as the CMA in the UK, to carry out a dawn raid on its behalf (*Article 22(2), 2003 Regulation*). Other national competition authorities may request similar assistance from the CMA, although not from the sectoral regulators (*Article 22(1), 2003 Regulation*). Competition authorities have the power to impose significant penalties on a company for its failure to co-operate during a dawn raid (*see box "Penalties for failure to co-operate"*).

Inspection of premises

In order to enforce Articles 101 and 102, the Commission may conduct all necessary inspections of any premises, land and means of transport of a company, examine and copy books and other records, and interview representatives of the company (*Article 21, 2003 Regulation*). An inspection of business premises may be conducted either under a formal decision or an authorisation, which is issued without the approval of the full Commission. While it is possible for a company to refuse to submit voluntarily to an inspection based on an authorisation, in practice, a refusal is likely to result simply in the adoption of a formal decision imposing a duty to co-operate.

Officials may enter both business and domestic premises during a dawn raid by the Commission, the CMA or the Serious Fraud Office (SFO). However, the inspection of domestic premises by the Commission requires a decision from a national judicial authority, for example a warrant from the High Court (*Article 21(3), 2003 Regulation*).

Civil and criminal dawn raids

The CMA may carry out a civil dawn raid to investigate suspected infringements (*sections 25, 27 and 28, 1998 Act*). While an unannounced inspection of the premises of a company suspected to have infringed competition law may be carried out without a warrant, this would allow the CMA only to request the company to produce information. A warrant from the High Court in England and Wales or a Court of Session in Scotland is necessary for the CMA to be able to search the premises or to use force to enter them. Certain sectoral regulators in the UK, such as the Financial Conduct Authority (FCA), have the same powers of inspection as the CMA in relation to the sectors in which they operate (*section 54 and schedule 10, 1998 Act*). For example, in April 2017, the FCA carried out a series of dawn raids at the premises of insurance brokers in connection with its investigation into the aviation insurance broking sector.

In addition, the CMA has the power to carry out a criminal dawn raid where it has reasonable grounds to suspect that an individual has agreed with one or more other persons to make or implement a cartel by fixing prices, limiting or preventing the supply of goods or services, limiting markets or bid rigging (the cartel offence) under section 188 of the Enterprise Act 2002 (2002 Act). In order to carry out a criminal dawn raid, the CMA must obtain a warrant from a High Court in England and Wales or a sheriff in Scotland (*section 194, 2002 Act*). The Criminal Justice Act 1987 (1987 Act) also grants the SFO powers to investigate a suspected cartel offence, including the power to carry out a dawn raid after obtaining a warrant from a justice of the peace (*section 2, 1987 Act*). However, this article focuses on the role of the CMA.

Regulators with concurrent powers

The following regulators hold competition powers concurrently with the Competition and Markets Authority:

- Civil Aviation Authority.
- Financial Conduct Authority.
- Gas and Electricity Markets Authority (Ofgem).
- NHS Improvement.
- Northern Ireland Authority for Utility Regulation.
- Office of Communications (Ofcom).
- Office of Rail and Road.
- Payment Systems Regulator.
- Water Services Regulation Authority (Ofwat).

ARRIVAL OF INVESTIGATORS

The nature of dawn raids means that a company being investigated will not have any notice of the investigators' arrival. Investigators typically arrive at the start of the business day but dawn raids in relation to criminal cartel investigations may start even earlier. In order to ensure that any unexpected event is handled efficiently, it is important for a company to be aware of best practice and to have trained key employees, including reception staff, in dawn raid procedure.

Role of contact persons

When the investigators announce themselves at reception on arrival, they will present their credentials and the authorisation, decision or warrant (mandate) for the inspection. They may ask to speak to a senior executive, for example the CEO, and decide to start searching offices immediately. The reception staff should check the credentials and the mandate to confirm which authority is seeking to carry out the inspection, request that the investigators wait and immediately inform the pre-designated contact persons, for example, the general counsel, in-house legal department or the CEO. Once notified by reception, the contact persons must attend to the investigators immediately and will have to be in charge of initial tasks such as checking the mandate (*see box "Checking the mandate"*).

The contact persons will also want to get in touch with external legal counsel without delay. Although investigators are not obliged to wait for the arrival of external legal counsel, Commission and CMA investigators are usually prepared to wait for a short period of time unless in-house lawyers are available or the CMA is conducting a criminal dawn raid. The competition authorities are clear that any delay in starting the inspection has to be kept to a strict minimum. In *Koninklijke Wegenbouw Stevin (KWS) v Commission,* the EU General Court held that a delay of 47 minutes amounted to a failure to submit to the Commission's inspection and upheld the Commission's fine (*T-357/06*) (*www.practicallaw.com/9-205-5623*). The European Court of Justice (ECJ) dismissed KWS's appeal (*C-586/12*).

Even if the investigators have not started to review documents, the company will already be under an obligation not to destroy or conceal documents as this would obstruct the inspection. Given the serious consequences of any failure to co-operate, effective internal communications are vital and external communications should be managed carefully (*see box "Internal communications"*).

Key practical steps

The company should be prepared to take certain practical steps as soon as the investigators arrive in order to ensure co-operation with the investigators while protecting the company's legal position in relation to the alleged infringement.

Shadow investigators. Investigators may search desks, cabinets and offices all over the premises. They must be shadowed by a person familiar with the dawn raid procedure and the subject matter of the mandate at all times. This should ideally be done by external or in-house lawyers. In practice, investigating teams can be large, comprising ten or more officials, and a company will want to ensure that there are sufficient resources to shadow the investigators adequately. External legal counsel can play a key role in this regard.

Ensure support from IT staff. Investigators expect access to appropriate representatives or staff members who are able to explain the organisational structure of the company and the IT environment. Inspections now rely heavily on electronic searches of emails and other documents and, although the authorities will have an IT specialist as part of the team, the investigators will expect access to and support from an IT staff member to assist with specific tasks such as temporary blocking of individual email accounts, temporarily disconnecting running computers from the network, removing and re-installing hard drives from computers and providing "administrator access rights" support. It would be helpful to have pre-designated contacts in this regard.

Record what was taken. Investigators typically take away copies of electronic or physical documents during the inspection. A note should be taken of all documents copied by the investigators, and an additional copy made for the company to keep.

Prepare for employee interviews. Investigators may ask employees questions, including additional oral explanations in connection with documents. It is reasonable to request that an external or in-house lawyer be present during these discussions. However, in criminal cartel investigations, there may be a conflict of interest between the company and individual employees, and so the company might consider helping key individuals subject to the investigation by arranging independent representation before responding to the investigators. Detailed records should be kept, including of any questions asked to, and responses given by, any employee.

DURING THE INVESTIGATION

Investigators have a wide range of powers and can carry out both desk searches and electronic searches. In practice, the powers of the Commission and the CMA are broadly similar and so only major distinctions have been highlighted in this article. In particular, if the CMA conducts an investigation on behalf of the Commission or another authority, its investigators will have the same powers as Commission investigators if it does not have a warrant, but will have the same powers as a standard CMA investigation if it has obtained a warrant.

During the course of desk searches, investigators may examine books and records related to the business and can take away copies of seized documents. In addition, the CMA has the power to seize and take away original documents where there is a warrant for the dawn raid. In practice, the CMA usually takes copies unless it appears necessary to take original documents in order to prevent destruction of the documents or if it is not practicable to copy large numbers of documents.

IT searches

Given the prevalence of electronic communications in modern businesses, inspections increasingly focus on IT searches. The Commission updated its explanatory note in relation to procedures in 2013, and again in 2015, emphasising its ability to search the IT environment and devices, including storage media (*http://ec.europa.eu/competition/antitrust/legislation/explanatory_note.pdf*). It also provided some guidance on the typical procedures that the Commission will follow in relation to IT searches.

Impact of Brexit

Following the UK's EU referendum on 23 June 2016, the government issued a notice under Article 50 of the Treaty on the Functioning of the European Union (TFEU) on 29 March 2017 that triggered a two-year period, at the end of which the UK will officially exit the EU. Depending on the legal framework of the post-Brexit relationship with the EU, the level of co-operation between the UK and the European Commission (the Commission), and with national competition authorities in the EU, might change.

After Brexit, the Commission therefore might not have jurisdiction to carry out dawn raids in the UK and might have to rely on greater co-operation with the Competition and Markets Authority (CMA) (whether formal or informal) in order to gather evidence for any investigations into UK companies for conduct which might infringe Articles 101 or 102 of the TFEU with an effect on trade in the EU. It is possible that companies might find themselves subject to parallel investigations by the Commission and the CMA. While the legal and procedural framework for the conduct of dawn raids might change as a result of Brexit, the practical impact of any of these changes would need to be assessed once the post-Brexit relationship between the EU and the UK has been agreed.

Penalties for failure to co-operate

The European Commission (the Commission) can fine a company up to 1% of its group worldwide turnover in the previous year if it intentionally or negligently:

- Fails to submit to an inspection ordered by a Commission decision.
- Produces the required books or other records related to the business in incomplete form.
- Fails to provide answers to questions asked during an inspection, or gives incorrect or misleading answers to questions and fails to rectify those incorrect or misleading answers within a given time limit.
- Breaks a seal applied by a Commission official (*Article 23(1), Modernisation Regulation (1/2003/EC)*) (2003 Regulation) (Article 23(1)).

The Commission can also impose a daily fine of 5% of the company's average daily turnover in the preceding business year for each day the company refuses to submit to an inspection ordered by a Commission decision (*Article 24(1), 2003 Regulation*).

In 2008, the Commission imposed its first fine under Article 23(1) on E.ON for the breach of a seal. Although E.ON denied having broken the seal and submitted that there might have been accidental displacements or malfunctions of the seal, the Commission's fine of €38 million was upheld by the EU General Court as well as the European Court of Justice (*www.practicallaw.com/1-504-5535*).

The Competition and Markets Authority (CMA) may impose fines on a company for failing to comply with information requests, to allow inspectors to enter premises or any other reasonable requirements of an investigating officer.

Also, it is a criminal offence under the Competition Act 1998 and the Enterprise Act 2002 (2002 Act) if a person:

- Fails to comply with a requirement imposed by the CMA.
- Intentionally obstructs an official carrying out an inspection, with or without a warrant.
- Intentionally or recklessly provides false or misleading information.
- Intentionally or recklessly destroys, disposes of, falsifies or conceals documents (*sections 42-44, 1998 Act; section 201, 2002 Act*).

Investigators will search the company's IT systems (for example, servers, desktop computers, laptops, tablets and other mobile devices) and all storage media (for example, CD-ROMs, DVDs, USB storage keys, external hard disks, backup tapes and cloud services) of the company and its employees. Even personal devices and media belonging to employees that might be used for professional reasons can be searched by investigators.

The investigators, while co-ordinating with the company's IT specialists, will typically use their own dedicated forensic IT software tools, including for keyword searches of electronic documents and emails. The investigators might request additional hardware from the company but are not obliged to use it.

During the search, the investigators will typically require the temporary blocking of individual email accounts, the temporary disconnection of running computers from the network, the removal and reinstallation of hard drives from computers, and the provision of "administrator access rights" support. In 2012, the Commission imposed a fine of €2.5 million on two Czech energy companies for obstructing an inspection (*www.practicallaw.com/3-502-6343*).

According to the Commission, one company had failed to block employees from accessing email accounts and the IT staff had, at the request of an employee, agreed to divert incoming emails for specific accounts so that these could not be reviewed by the Commission officials during the inspection. The General Court upheld the Commission's decision in 2014 (*Energetický a průmyslový and EP Investment Advisors v Commission T-272/12*). This is an example of how failing to comply with the investigators' instructions in relation to the company's IT systems, whether intentional or not, can prove costly and it would be prudent to ensure that the IT staff have appropriate training on dawn raid procedures.

Copying data

The storage media being inspected will typically remain under the investigators' control until the end of the dawn raid unless a forensic copy has been made and stored on the investigators' own storage media. At the end of the inspection, investigators will delete all company data from their own storage devices except for that which has been selected as relevant to the investigation and which will be taken away for addition to the case file. Typically, companies will be allowed to retain an identical set of the data taken away by the investigators.

Should the preliminary review and selection of relevant data remain incomplete at the end of the dawn raid, a copy of the data yet to be searched may be taken away by the Commission to be reviewed at a later stage. However, as the company and its legal counsel would not have had the opportunity to shadow the investigators during the keyword searches, this data has to be secured in a sealed envelope. The Commission may then either:

- Invite the company's representatives to be present when the sealed envelope is opened and the inspection continued at the Commission's premises.
- Request the company to keep the sealed envelope (with the seal unbroken) on the premises to allow the Commission to continue the search during a further announced visit.

- Decide to return the sealed envelope to the company without opening it.

When operating under time constraints and acting under a warrant, the CMA may also seize and take away a larger quantity of original documents to sift through.

It is common for raids to continue over more than one day, in which case the investigators may seal the premises. When Commission officials affix a seal, a minute will be made. The company must ensure that the seals are not broken by anyone (including cleaning staff) until they are removed by the investigators the next morning. A separate minute will be prepared to note the time of removal.

Oral explanations

Investigators may request oral explanations on the spot of facts or documents relating to the subject matter of the inspection and these explanations may be recorded in any form. A copy of these recordings will be made available to the company after the inspection. In practice, Commission officials tend to limit questions to explanations about specific documents. However, the Commission has the power to ask wider questions about the subject matter of the investigation. Where explanations might have to be provided by an employee who was not authorised by the company, the Commission might set a time limit within which the company may rectify, amend or supplement the explanations.

In a civil investigation, the CMA's questions are normally limited to those about where a document might be found or oral explanations regarding the contents. However, in a criminal investigation, the CMA has the power to conduct voluntary or compulsory interviews and ask wider questions about the subject of the investigation. The CMA does have powers to conduct compulsory interviews in civil investigations too, but has not tended to use those powers during a dawn raid.

MANAGING THE INVESTIGATORS

While the Commission and the CMA have very wide-ranging powers of investigation during a dawn raid, these are subject to some important limitations. It is crucial that, despite the flurry of activity during a typical dawn raid, the investigators are managed appropriately and do not exceed their powers.

Checking the mandate

When the investigators arrive, they will present their mandate for the inspection. This mandate must be carefully checked by the company to confirm:

- Whether it applies to the company whose premises the investigators are at and is still valid for that period.
- Whether it is the type of mandate which means that the company must submit to an investigation.
- Whether the mandate names the investigators and each investigator has valid identification.
- The subject matter and period of the alleged infringement to which the inspection relates.

It is advisable to keep a copy of the mandate for the records of the company and its external counsel.

Limits of investigators' powers

Commission investigators cannot use force to enter premises unless they have obtained a warrant through the CMA. However, companies are under an active duty to co-operate with the investigation. Therefore, the company will have to actively direct Commission investigators to the relevant documents or help to find requested documents. In practice, the Commission often requests the CMA to obtain a warrant for Commission raids although this will only be used if a company fails to co-operate. The CMA can use force to enter and search premises where there is a warrant.

As a general principle, the Commission cannot require a company to admit to the existence of an infringement or to give an assessment as to whether it is in breach of competition law. Having in-house or external counsel present when employees are being interviewed could help avoid employees having to respond to leading questions. The right against self-incrimination also means that compulsory interviews conducted by the CMA during raids for criminal investigations cannot be used to prosecute that individual. There is no obligation to respond to questions for a voluntary interview.

The personal data of individuals are not the target of the investigations and raids but may be contained in business documents and can be copied by the Commission. However, any personal information can only be used in connection with the investigation and would need to be processed in accordance with the Data Protection Regulation (*45/2001/EU*) (or, from May 2018, the General Data Protection Regulation (*679/2016/EU*) (*see feature article "Data use: protecting a critical resource", this issue*).

Privileged documents

Investigators cannot copy or take away documents that are legally privileged, unless the company has opted to waive privilege (*see feature article "Waiver of privilege: all is not lost", www.practicallaw.com/0-579-7885*). During the time pressures of a raid, it is rare that a company would have the opportunity to assess properly the implications of waiving privilege and so it is important that the company exercises its right to prevent access to all legally privileged documents immediately. However, the concept of legal professional privilege differs under EU and UK law (*see box "Legal privilege"*) (*see feature article "Legal professional privilege: practical tips for in-house lawyers", www.practicallaw.com/2-531-6847*).

During the course of the dawn raid, the persons shadowing the investigators will have the responsibility of identifying any privileged documents and preventing the investigators from taking copies. For practical efficiency, it might be possible to agree some broad parameters for the identification of privileged documents. Although subject to the discretion of the investigating team, Commission officials have on occasion agreed to exclude correspondence which is clearly to or from external legal counsel during the forensic

Internal communications

It is generally advisable to send an email with key instructions immediately to the employees at the premises that are being raided, even where this reiterates key points from previous dawn raid training.

Employees should not disclose externally the fact of, or any details regarding, the inspection, including to employees in offices of the company located elsewhere. This could be considered to be "tipping off" other potential suspects or future targets of dawn raids and so could be viewed as obstructing the investigators. Once the relevant authority has made the fact of the dawn raid public, the company may choose to issue a press release.

Employees should co-operate with the investigation. In addition to allowing access to offices, desks and company electronic devices, they might be asked to hand over (and should not refuse access to) personal phones, laptops and other mobile electronic devices. If an employee is approached by an investigator, he should contact an in-house lawyer, external counsel (if available at that point) or other designated person before answering any of the investigator's questions.

Under no circumstances should an employee seek to destroy, conceal or falsify documents that could be relevant to the investigation. In this regard, it might be advisable to suspend any routine document management policy which could result in the destruction of documents during the course of the investigation. Also, employees should not seek to break any seals or circumvent any temporary barriers to access email or temporary storage, whether to read, send or delete emails.

IT searches. While it might help if files or correspondence are marked "legally privileged", this might not be sufficient to convince an investigator, who might need a cursory look at the document to confirm that it is in fact privileged.

Disputes over documents

Disputes regarding whether or not a document is privileged are not unusual. The Commission's usual practice is to:

- Set aside the document for further discussion at the end of the raid.
- If no agreement is reached, take away a copy of the document in a sealed envelope to allow the company to make further submissions. A minute will be made to record the disputed documents.

The hearing officer may subsequently examine the document and the company's submissions before making a recommendation to the Commission regarding the claims of privilege.

The CMA's practice in relation to privileged documents is broadly similar.

The investigators should also not review documents which relate to matters outside the scope of the investigation as set out in the mandate. While the lack of relevance might not always be immediately obvious, the company should confirm that:

- The documents being reviewed and added to the file relate to the time period of the subject matter of the investigation as set out in the mandate.
- If the subject matter of the investigation as set out in the mandate relates to only part of the company's business, the documents being reviewed and added to the file are relevant to that part of the company's business.

In practice, while it is possible to challenge the relevance of a document, the Commission and the CMA have a wide discretion to assess relevance. In addition, the scope of the mandate might be phrased broadly and it might be difficult to argue that it is not sufficiently precise to justify the Commission's search. For example, in 2014 the ECJ held that the Commission was justified in examining documents linked to projects outside the EU in order to assess the impact on trade between EU member states because the Commission's related dawn raid decision provided that the suspected cartel was "probably of global reach" (*Nexans SA and Nexans France SAS v Commission C-37/13 P; www.practicallaw.com/5-575-0569*).

However, an earlier decision by the General Court in connection with the same matter held that, as the Commission had only reasonable grounds for suspecting an infringement in the high voltage cables sector, it had overreached in searching for documents related to other product markets (*Nexans SA and Nexans France SAS v Commission T-135/09*).

If there is no agreement, insisting on excluding the disputed documents might open the company to a charge of obstruction. However, the company may wish to reserve its rights to make further submissions in relation to the disputed documents. For this reason, a minute should be made to record the disputed documents.

AT THE END OF THE RAID

Once the dawn raid has come to an end but before the investigators have left, it is critical that the company:

- Ensures that it has an accurate record of the investigators' actions during the inspection. In particular, it should retain:
  - a copy of the mandate;
  - a list of all documents copied or seized by the investigators;
  - copies of any originals taken away by the investigators;
  - records of any explanations or responses to questions provided by employees to investigators; and
  - copies of any relevant minutes, for example, in relation to the affixing and removal of seals.
- Deals with any outstanding questions relating to potentially privileged or out-of-scope documents. To the extent that the status of any document is still in dispute, the company should agree that these may be resolved at a later stage subject to the documents being taken away in a sealed envelope and further submissions being made by the company.
- Checks whether there are unanswered questions or unavailable documents

which need to be provided to the investigators, and the deadline for the company's follow-up responses.

The company will then need to conduct an immediate debrief with its own team, including external legal counsel. It will be important to have preliminary feedback from each person that shadowed investigators to understand: which documents were requested, reviewed, copied or seized; whether there were any disputes over privileged or out-of-scope documents; and the questions asked and answers provided by employees.

An initial understanding of whether there were any potentially damaging ("hot" or "red flag") documents is also important. In practice, given the prevalence of electronic searches and the large numbers of documents seized in typical dawn raids, a comprehensive report on hot documents might require a relatively lengthy review and not be immediately feasible. However, this should be prepared as soon as reasonably practicable in order to assist the company in assessing the legal risks and preparing any defence (*see "After the raid" below*).

Internal communications

Employees who have been directly affected by the raid, as well as others, will inevitably have questions. The exact nature of the internal communications will depend on the circumstances of each case but it is generally worth keeping these communications brief and high level.

Following the raid, the competition authority might send information requests to the company during the course of the investigation. It is possible that other premises of the company, located in different jurisdictions, might be the target of future raids in connection with the same or related investigations. Therefore, it might be helpful to ensure that all employees have refreshed their knowledge of dawn raid procedures.

In addition, the company should consider with its external legal counsel whether to suspend any existing document management policy to prevent automated or regular destruction of historic documents such as older emails in a chain. These documents might be requested by investigators at a later stage, and they might even contain helpful and exculpatory information which could help in the company's defence in the investigation. Internal communications with employees should make clear that, though the raid has ended, historic documents should not be destroyed until the document management policy has been reinstated.

External communications

The company might also need to consider whether to issue an external press release. Where the company is listed, it might have an obligation to make a statement. Even if the company chooses not to issue a press release, it should be ready to respond to press enquiries following any statement by the investigating authority or any other company which might have been raided at the same time.

AFTER THE RAID

A detailed review of the documents seized as well as other documents which could be relevant to the subject matter of the investigation will be necessary for the evaluation of legal risk. Crucially, the company must first identify whether there is any basis for the alleged infringement of competition law that formed the subject matter of the investigation. Following this, the company will need to establish a strategy in dealing with the allegations and for future submissions to the competition authority.

Risk assessment

The need to reach a risk assessment quickly is potentially greatest where the allegations relate to a suspected cartel. The company may need to consider whether a leniency application is advisable. Among the participants of an alleged cartel, only the first company whose leniency application is accepted receives full immunity from fines. However, others may receive reductions in fines in return for co-operating with the authority.

Legal privilege

Under EU law, legal professional privilege covers confidential written communications if:

- The correspondence is with an independent external lawyer who is qualified to practice in an EU member state.
- The correspondence is in relation to the client's rights of defence in connection with the investigation.

In effect, communications between in-house legal counsel and other employees of a company will not be able to claim the protection of legal privilege in a European Commission investigation.

In contrast, under UK law, legal professional privilege covers:

- Legal advice privilege relating to confidential communications between a legal adviser and his client for the purpose of seeking or providing legal advice.
- Litigation privilege relating to confidential communications which have the dominant purpose of assisting with existing, pending or reasonably contemplated litigation.

While the UK view of legal professional privilege does not exclude communications with in-house counsel, the concept has been narrowly interpreted by the UK courts. In *Three Rivers District Council v Bank of England (No 5)*, the Court of Appeal held that communications with a company's lawyers attract legal advice privilege only where the communication is with those whose role it is to obtain the legal advice, and not where the communication is with those whose role it is to prepare the information required by the lawyers to provide the legal advice (*[2003] EWCA Civ 474*). In addition, the Court of Appeal has held that communications, even with lawyers, for the purpose of merely establishing facts do not attract legal advice privilege (*The RBS Rights Issue Litigation [2016] EWHC 3161 (Ch); see News brief "Legal advice privilege: who is the client?", www.practicallaw.com/3-638-0479*).

Related information

This article is at practicallaw.com/w-012-6285

Other links from uk.practicallaw.com/

Topics

Competition compliance and dawn raids	topic/2-103-2056
CMA investigation and prosecution powers	topic/4-591-9535
Privilege	topic/7-635-9367

Practice notes

CMA powers to enter and search premises	0-204-1447
Competition regime: EU compliance programmes	6-107-3714
Competition regime: EU dawn raids	0-107-3712
Competition regime: UK Procedure, negotiation and enforcement	2-107-3693
The English law of privilege and its application in competition law investigations	8-384-6945

Previous articles

Regulators and disciplinary action: striking a balance (2017)	6-640-8896
UK competition regime: new measures in force (2014)	0-566-2805
Legal professional privilege: practical tips for in-house lawyers (2013)	2-531-6847
Global investigations: managing the risks (2011)	9-505-4470

For subscription enquiries to Practical Law web materials please call +44 0345 600 9355

A criminal dawn raid by the CMA will require the company to consider its strategy in relation to employees who might be targets of the criminal cartel investigation. There might be a potential conflict of interest in the company's legal counsel advising these employees. The company's strategy on the basis of its own risk assessment might vary from that of an employee who risks facing criminal charges (*see feature article "Regulators and disciplinary action: striking a balance", www.practicallaw.com/6-640-8896*). These employees should not be included in the core team reviewing the risk assessment and determining the company's strategy in relation to the investigation. They will also need separate legal representation, although the company might choose to assist them in obtaining independent representation.

Confidential documents

As documents copied or taken might in due course be accessed by third parties, it is important to identify and mark confidential documents during the course of the review. In practice, the investigating authority will seek confirmation as to whether the documents contain any information which should be confidential from a third party before allowing others to access the file. However, it might be efficient to identify these documents at an early stage.

Alex Nourry is a partner, and Chandralekha Ghosh is a senior associate, at Clifford Chance LLP.