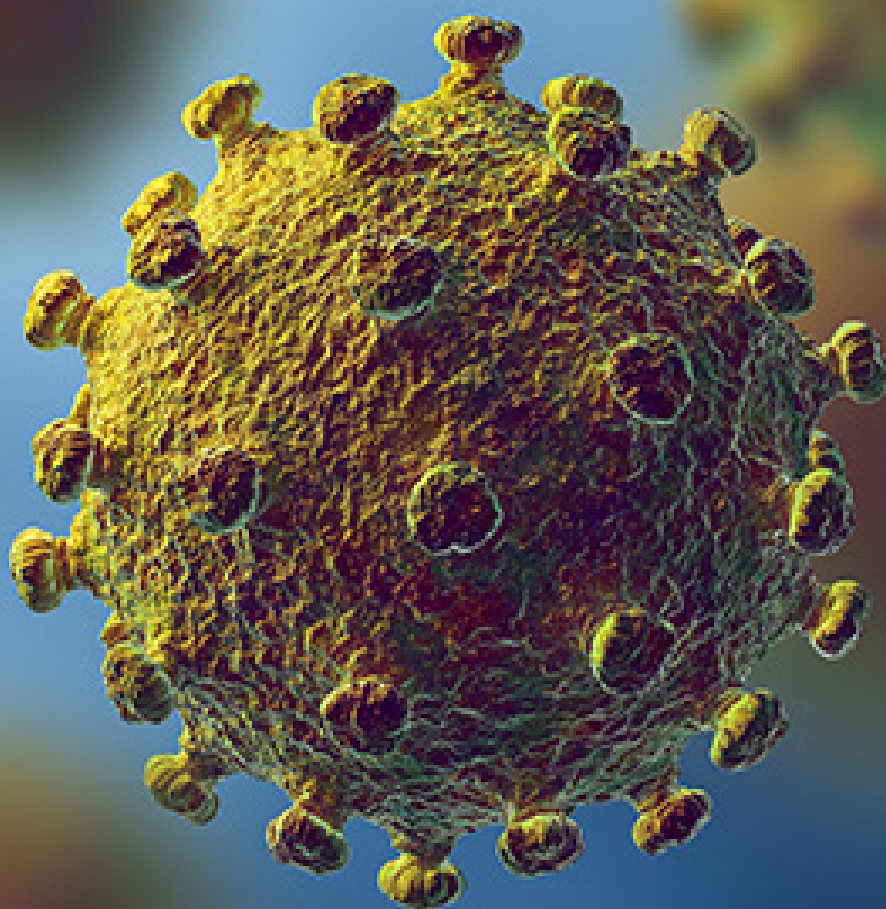


C/M/S/

Law . Tax



Key considerations for conducting internal investigations remotely

CMS Risk & Investigations Group

April 2020



Risk &
Investigations



The armchair investigator

With so many businesses in lock-down, many internal investigations will have to be conducted remotely, with investigation teams, employees, external counsel and other providers working from home for the foreseeable future. As well as the technological requirements and the practical and interpersonal challenges they will entail, there can be additional legal risks to consider.

Many of the tasks involved in fact-gathering investigations are normally carried out at a desk or in front of a screen. Once gathered, much of the work is about sifting material for relevant evidence, identifying connections and gaps and reconstructing the story based on the available material. As one very famous detective put it:



One does not, you know, employ merely the muscles. I do not need to bend and measure the footprints and pick up the cigarette ends and examine the bent blades of grass. It is enough for me to sit back in my chair and think. It is this – ” he tapped his egg-shaped head – “this, that functions!

Hercule Poirot, in Agatha Christie's Five Little Pigs

Using the “little grey cells” will be particularly important when conducting remote investigations (particularly those involving regulatory or criminal issues, or in multiple jurisdictions), using novel or alternative techniques to overcome current restrictions around collecting evidence – both documentary and from witnesses. This guide looks at the key practical and legal issues that investigators should have in mind when carrying out their work on internal investigations remotely. Some of those issues arise in non-remote investigations too, particularly in multi-national investigations, but their significance and extent may be different when operating remotely. It should be noted that different considerations may apply where there is a parallel regulatory or external authority investigation into the same matters. We focus on:

Planning



Privilege



Interviews & employment rights



Data gathering & protection



Reporting



Key takeaways

1

It may be prudent to postpone the investigation

Consider the benefits and risks of progressing with a remote internal investigation, including whether lack of remote capabilities, or access to data or people could lead to an ineffective investigation which may later be criticised by a regulator or enforcement body. Conversely, consider whether pausing may exacerbate any existing risk or create regulatory risk, or compromise existing data sources. Any decision to pause/delay the investigation should be documented with a full justification.



2

Plan and scope the investigation to avoid delays, excessive costs and legal exposure

In addition to normal investigation planning, consider the appropriate investigation and oversight teams based on expertise and location. Review and update internal policies to align with remote working. Ensure software for communicating with the internal investigation team and interviewees is secure. Seek approval from internal stakeholders when changing protocols and strategies to conduct internal investigations, and share best practices amongst legal, compliance and investigations teams.



3

Understand privilege risks

In circumstances where interviewees, interviewers and team members may be communicating from different jurisdictions, consider the extent or lack of privilege protection over those communications and work and plan accordingly, based on the sensitivity of the matters under investigation. Continue to re-evaluate the position as the investigation progresses and new facts are learned.



4

Prepare for remote interviewing

Ensure secure videoconferencing software is in place (and tested in advance) for effective interviews. Consider data privacy issues and local law obligations/restrictions before recording the video interview. Inform interviewees not to record interviews themselves or copy any documentation shown to them and to keep discussions confidential, but be alive to the increased risk of this happening. Lawyers conducting interviews should be mindful of their professional duties and not take advantage of interviewees.



5

Data preservation and gathering

As with all investigations, take steps to control and preserve relevant company data. Consider employment law and data privacy obligations when collecting and reviewing data, including personal data held in employees' corporate email accounts. As it may not be possible to collect company devices, drives etc. that hold relevant data (unless courier recovery is available), ensure clear instructions requiring preservation and non-deletion/accessing of potentially relevant data are sent to all those holding such items. Consider whether remote access and copying of the device data can be undertaken safely in the meantime. Keep a record of all steps and decisions taken to provide later justification if required.



6

Internal reporting

Obtain local disclosure/privilege advice before reporting across different jurisdictions, even if only orally so that risks are understood. Place restrictions on (1) printing written reports and (2) circulating written reports externally or through unsecure networks.



Should you postpone the investigation?

Businesses should consider the benefits and risks of progressing with an internal investigation during office lockdowns. Relevant considerations include:

- whether an effective and thorough investigation can be conducted (albeit with some limitations) into the issues, given the location and nature of evidence and witnesses and relevant legal requirements or restrictions
- whether delaying an investigation into serious allegations could exacerbate any existing risk for the business or create a regulatory risk
- whether delaying the investigation could compromise existing sources of potentially relevant data and/or inhibit access to key employees and witnesses
- the risk that the issues to be investigated become public or lead to external investigations before the business has been able to understand its risk and exposure by investigating
- whether ploughing ahead with an investigation could result in a compromised investigation which could lead to later criticism or sanction from regulatory or enforcement authorities, or increase risk of claims.

If the investigation is paused, companies should still regularly monitor the matter for any significant developments and take steps to preserve relevant data. Companies may also wish to implement interim compliance measures to address any existing risks – including, for example, pausing any payments to third parties and/or discontinuing business elements to which the investigation may relate or suspending implicated employees. There should be a clear interim plan to manage the issue during any abeyance and a documented justification for the delay. Businesses will need to be prepared to justify any delay to regulators/authorities in due course, depending on the outcome.



Planning the investigation

Careful planning at the outset to avoid mistakes and exposing the business to additional risk, while always best practice, will be more important than ever. It is likely that the investigation team will be learning how to do certain tasks differently; it will be unfamiliar and that creates risk. As well as notification, reporting and PR considerations, and assessing whether anything urgently must be done or stopped, key planning issues include:

What needs to be investigated?

- Can any or all issues be investigated remotely?
- Does the investigation need to be protected by privilege (if possible)?
- Who should be in the team (taking account of their location)? How can the team communicate effectively and confidentially? What external support is required?

Who needs to be interviewed?

- Where are they and can they be interviewed remotely?
- Will it be legal and compliant with policies?
- What record can be taken?
- How sensitive is each interview? Will interviewees need access to legal representation or support during the interview?
- Do all interviews need to be carried out at the same time? Could some be delayed until after the lockdown?

What sources of evidence/ documents are there?

- Where are they? Electronic or hard-copy? On servers, hard-drives, memory sticks, mobile or personal devices?
- Can the data be preserved and collected? Can it be done without damaging metadata? And without alerting potential suspects?

What reporting is appropriate?

- Does it need to be in writing?
- Can it safely be shared?
- Is it envisaged that it will be shared with a regulator or investigatory authority?



As those conducting and overseeing the investigation will be in different locations and possibly different jurisdictions, extra care needs to be taken to consider whether this fact alone should impact on who is in the team.

- Could sharing information or documents with people in country X create a risk of loss of privilege (if it exists) or exposure to disclosure or seizure by authorities that would not exist in other jurisdictions?
- Do all team members have the hardware and software they need to be able to help the investigation run smoothly and securely? If not, can they get it quickly and easily?

These issues should feed into the scoping and team building. Getting the planning wrong can lead to delay, cost, legal and reputational exposure, as well as a compromised investigation.

Are your policies fit for purpose?

Businesses should review their internal investigation policies and protocols, as well as data and monitoring policies, to take account of remote working and its limitations. For example, a separate policy on using systems or software to record conversations may be worthwhile. Any necessary changes should be approved by internal stakeholders. As businesses start conducting investigations remotely, it is essential that they gather all useful learning from each investigation and use it to enhance their investigation protocols and internal controls, and to share best practice among their legal, compliance and investigation teams.

Privilege

The availability of legal privilege protection (and its non-UK equivalents) over interview materials or investigation work product can be an important consideration when structuring investigations, depending on the issues involved. However, its availability generally depends on the documents in question remaining confidential. If that is lost, then any available privilege is unlikely to survive. Conducting remote investigations makes it harder to control the dissemination and security of the investigation work and so creates a greater risk of loss of confidentiality and, thereby, loss of any available privilege. Companies should consider that risk and its significance when conducting and/or structuring a remote internal investigation.

For example, an interview conducted by telephone or video call may be recorded by anyone on the call (including the interviewee) despite promises to the contrary. What happens to such recordings afterwards may be very difficult to control, even if the recording was made in breach of promises or obligations. As noted above, it may be possible and prudent in some investigations to delay some or all interviews, particularly where there are concerns about the interviewee, until they can be conducted face-to-face in a more secure manner and/or the availability of privilege protection may be clearer.

Further, the existence and extent of privilege-type protections differs between jurisdictions; some countries have no equivalent concept at all. Where investigations are being conducted remotely, depending on the business and issues involved there may be a greater need to deal with people and documents in different countries. As noted above, even having investigation team members based in different countries (and thus sending and receiving investigation materials) can raise complex legal questions around privilege protection and/or disclosure of documents, including to governmental authorities or regulators in different countries. Similarly, interviewers and interviewees may be in different countries, which may take different approaches to privilege and powers to order disclosure of documents in legal proceedings or investigations by regulators and law enforcement authorities.

It will be essential to understand how all relevant local laws will approach the issue and plan accordingly to mitigate risk.

Interviews

Videoconference, while far from perfect, will be the next best thing to face-to-face interviews. Anyone with a phone and an internet connection can participate in a video call, which has some of the face-to-face benefits unavailable with telephone calls. It allows the interviewer:

- to hold a more natural conversation and build rapport, demonstrating empathy and understanding
- to observe the interviewee's facial expressions and some body language (a huge part of communication and crucial in assisting the interviewer to assess credibility)
- to ensure the interviewee is reviewing the correct documents and to try to ensure that they are not copying the documents in some way
- to assess whether the interviewee is alone or being coached, or even to identify if the interviewee is recording the conversation.



Practical tips

Before the interview, make sure all involved have the same software required to conduct the call and view or access any documents to be shown or shared. Try to use reputable software with good security and, ideally, end-to-end encryption.

Consider having a pre-call to check everything works and the video/sound quality is acceptable. This can be used to ensure everyone understands the process and to agree rules for avoiding interruptions and multiple people talking at once. Streamline attendee numbers to assist with this. Use the opportunity to understand whether the interviewee may need additional support due to other responsibilities they may have – e.g. child-care obligations.

A pre-prepared interview script can help to make sure all appropriate information is provided to the interviewee and that consistent messaging is given to all interviewees. This could be provided in writing up front, as long as it does not detail any of the issues under investigation.

If a translator is needed, interviewers will need to consider the logistics of having the translator participate by phone or videoconference from a different location than the interviewee.



Confidentiality

To preserve confidentiality and any available privilege, interviewees should confirm they are not recording the interview and are alone (also to avoid distractions or interruptions). If headsets can be used, all the better. While it may be impossible to prevent interviewees covertly recording (and businesses will need to accept this is a greater risk when conducting remote interviews), at least ensure you have a record that the interviewees confirmed they were not doing so and you communicated your efforts to preserve confidentiality.

Even if interviewees don't record the call, be mindful that any written record is likely to contain personal data and, under the GDPR¹, data subjects have various rights in relation to their personal data, including the right to request access to their personal data or even erasure of it. Refusal is possible in limited circumstances.



Recording the interview

- **Get consent:** Given the technology to record video interviews and even generate transcripts of the call, there may be a temptation to do so, particularly if the interviewer does not have the support of a note-taker. If a recording/transcript is to be made, the interviewee should be told in advance and asked for consent, which should be recorded. Indeed, this may be a legal requirement in the jurisdictions where the interviewers or interviewee are based, but may not be sufficient on its own.
- **Local law requirements:** Where video interviews cross jurisdictions, it is critical to understand the rules in each jurisdiction as to whether the interview can be recorded or transcribed, whether it will be open to disclosure and even whether there are any restrictions on conducting the interview at all (e.g. if local bar rules prevent non-local lawyers from conducting interviews).
- **Data privacy:** Any recording is likely to involve processing personal data. It must therefore comply with the GDPR. Companies must have a valid lawful basis in order to process personal data and the lawful basis must be determined before processing begins, which should be documented. Similar requirements may exist in non-EU jurisdictions where the interviewer or interviewee are based.

Should a recording be made, it should be securely stored and protected to prevent misuse or unauthorised access.

¹ European General Data Protection Regulation



Screen sharing

It may be necessary for the interviewee to be shown documents as part of the interview. Any such documents should be clearly numbered for ease of reference.

Software can allow screen-sharing to show interviewees relevant documents or they can be provided on a secure portal or file transfer site (which should ideally be “view only”, preventing downloading, printing or sharing with others). Interviewees should be reminded not to copy any documents shown to them and their confirmation should be obtained, ideally in writing (e.g. by email) prior to the interview.

It is impossible to prevent all risk of the interviewee copying documents, e.g. by taking photos or screenshots of them. But save where the interviewee is intent on flouting such restrictions, these steps will help demonstrate you tried to highlight and protect confidentiality.

As always, sharing documents that an interviewee has not previously seen (e.g. because they sent or received it at the time) should be avoided if at all possible.

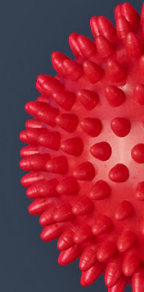
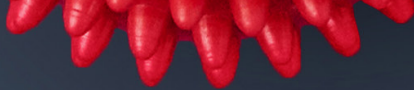


Duties of counsel towards interviewees and employment protections

Lawyers conducting investigations should be mindful of their duties under Codes of Practice or professional bar rules. For example, solicitors in England & Wales must not abuse their position by taking advantage of others and must act with honesty and integrity. While an interviewee is not the interviewing solicitor’s client, the interviewer must be mindful not to mislead interviewees or allow them to incriminate themselves in respect of criminal offences without caution and without notifying them of their right to take legal advice.

In the UK, employees have a duty to cooperate with reasonable instructions from their employer and a refusal to do so could lead to disciplinary action and/or be considered gross misconduct. That said, employment contracts and internal policies will need to be reviewed, as these may contain more specific obligations on employees to co-operate, or conversely contain contractual protections which narrow an employee’s duty to participate remotely and/or face-to-face. Employees may feel unable to effectively engage in a remote investigation due to their personal situation (for example availability of childcare or lack of a private space at home). These types of practical issues will need to be considered on a case by case basis.





In certain jurisdictions employees will have a legal entitlement to be accompanied at an investigation meeting or interview (for example by a colleague or their own counsel). Even where no legal requirement exists, this may be necessary under the organisation's policies and/or deemed appropriate having regard to the circumstances of the investigation. Where an employee wishes to invoke such a right, this will give rise to practical difficulties. Due to social distancing rules in place across much of the world it would not be possible for the employee to be accompanied in the physical sense and the employee may not feel that their right to be accompanied can be meaningfully accommodated in the context of a virtual investigation. In the current circumstances, there may be an increased risk of potential redundancies and furloughing (which may operate differently in different countries). Particular attention should be given to the preservation of data and documents in the possession of employees exposed to that risk. Additionally, if it will be necessary to secure a former employee's participation in the investigation following their redundancy, agreements should be put in place with that individual to ensure that their cooperation continues even after they have left that company, along with appropriate confidentiality obligations. In the current circumstances, it may not be practical for a redundant employee to return all company documents and materials in a secure and safe manner and so it may be prudent or necessary instead to agree with them that they will hold onto such materials (but not access relevant data or devices) in the meantime.

In the UK it is not permissible for furloughed employees to carry out any work (this is a strict requirement) and as such it may be difficult to engage with staff who are furloughed without first bringing them back to work. This will give rise to practical challenges including their entitlement to pay and conditions (something ordinarily adjusted during a period of furlough). Similar or very different rules on furloughing may apply in other countries where relevant staff are based.



Dealing with difficult interviewees

As with all internal investigations, not all interviewees will be willing to cooperate. Interviewees could end the virtual interview or fake technical difficulties to avoid answering questions. They could covertly communicate with others during an interview to 'get their stories straight'.

It is prudent to remind an uncooperative interviewee of their legal, regulatory and/or contractual obligations to assist with the investigation. These requirements should be clearly communicated, in writing, to the difficult interviewee.

Detailed records of all communications and attempted communications with uncooperative interviewees should be documented so they can be produced to the board or a regulator / authority as appropriate.

Data gathering and protection

Use of personal email, messaging apps and devices

While working remotely, employees may have difficulty accessing company systems. Some businesses may not have systems that can be fully accessed remotely and employees may not have been supplied with work devices to do so. Employees may turn to personal email accounts, ephemeral messaging apps (like What's App) and/or use personal devices for their work during the lockdown. Businesses need to review employment terms and policies (if not done already) to clarify what is permissible during this unprecedented situation and to demonstrate they have taken effective steps to ensure they mitigate risk and are able to control company data.

This may be less of an issue when considering historical (i.e. pre-lockdown) data that is the relevant subject matter of an investigation. However, the investigation may be compromised if members of the investigation team have to, or are permitted to communicate on non-secure email, or using ephemeral messaging services. Similar issues arise when communicating with others (e.g. employee interviewees) via similar channels. Where use of personal email cannot be avoided, at the very least the relevant service should be a secure and encrypted one and all sent materials should be password protected. Businesses should also emphasise that any account used should be accessible only by the employee and that they should label all work emails as such and label legal communications as "Privileged and Confidential" (to assist with evidencing the purpose of the document). In addition, thinking ahead (and this applies generally, not just to investigation work product), businesses should design a protocol for ensuring that the business will later have a record of all work communications made or received by employees on personal accounts, apps and devices— this may be as simple as copying all relevant emails to a work email address so that they get onto the work server.

Messaging apps present a particular problem as they are not normally accessible by the business, are not designed as enterprise-based products, and so policies will often discourage or proscribe their use. Some regulatory bodies, notably in the United States, have indicated that they will expect corporates, as part of having effective systems and controls, to have mechanisms for capturing and storing all such communications. That is easier said than done, but businesses who know their staff are using such products for work purposes (even against company policy) should design processes that at least demonstrate reasonable steps were taken to try to prevent such use or secure such communications.



Data preservation & collection

When conducting remote investigations, businesses should ensure that they have the capabilities to preserve and collect relevant data (including metadata) remotely. Third party specialists can assist with this. Where there may be regulatory/criminal issues, it is essential that any data capture is done forensically to preserve metadata and that a full record of the steps to gather the data is retained.

As noted above, securing physical devices and hard copy documents will be more difficult during office shutdowns. It is important to get legal advice in all relevant jurisdiction(s) so that employment law and data privacy risks can be managed.

Co-operation from the custodian may be necessary, unless employees do not store data on the device itself, or where all data is stored in the cloud or on remotely accessible company servers. In the meantime, document preservation notices should be issued to make clear that there should be no disposal of documents or data, even if held on personal devices.

Businesses will need to give thought to how best to secure physical locations where relevant physical evidence is present, to prevent its loss or destruction until the evidence can be properly gathered. All steps should be documented.

Data protection

As with any investigation, access data (e.g. employee work email accounts) which may contain personal data must conform with employment contracts and policies, as well as data protection and human rights or other laws. Data protection should not be seen as a barrier to remote investigations, but it will be necessary to consider the kinds of security measures required in these circumstances.

Businesses should consider whether documents can legally be transferred to another jurisdiction – even if only via screen-sharing with an interviewee in another jurisdiction – and the risks of doing so.

Reporting

If you are using third party non-secure software for calls or videoconferences, be aware of any security risks they pose before proceeding with sensitive calls or conferences through that channel. Nevertheless, daily secure calls to share information, findings and questions could be useful. These can be used also to reflect on the approach being taken and to ensure that the investigation is being conducted in the most effective way in light of ongoing findings and experience of conducting the investigation.

As physical meetings cannot be convened to report on findings, consider whether reporting can be provided on a video or tele-call and displayed via an electronic screen share. Clear instructions on taking notes should be provided in advance, based on disclosure/privilege risk.

If written reporting is required, consider only making reports available securely, for example on a portal, with restrictions on printing, onward circulation and with the capability to track access. As a minimum they should be encrypted and provided by secure email through VPN; again this at least enables some degree of tracking access. Sharing reports through non-enterprise email channels, such as webmail, should be avoided. As noted above, local law advice should be obtained for all jurisdictions of recipients of the reports.



Key contacts

Competition Raids and Investigations



Caroline Hobson
Partner, London
T +44 20 7367 2056
E caroline.hobson@cms-cmno.com



Brian Sher
Partner, London
T +44 20 7524 6453
E brian.sher@cms-cmno.com

Employment Investigations and Whistleblowing



Catherine Taylor
Partner, London
T +44 20 7067 3588
E catherine.taylor@cms-cmno.com



Steven Cochrane
Partner, London
T +44 20 7367 3746
E steven.cochrane@cms-cmno.com

Financial and White Collar Crime



Omar Qureshi
Partner, London
T +44 20 7367 2573
E omar.qureshi@cms-cmno.com



Colin Hutton
Partner, Edinburgh
T +44 131 200 7517
E colin.hutton@cms-cmno.com

Data Protection



Emma Burnett
Partner, London
T +44 20 7367 3565
E emma.burnett@cms-cmno.com

Environment, Health & Safety Risks and Investigations



Jan Burgess
Partner, Aberdeen
T +44 1224 267151
E jan.burgess@cms-cmno.com



Graeme MacLeod
Partner, Edinburgh
T +44 131 200 7686
E graeme.macelod@cms-cmno.com

Education, Social Care and Professional Risks



Chris Horsefield
Partner, Sheffield
T +44 114 279 4118
E chris.horsefield@cms-cmno.com



Olivia Jamison
Partner, London
T +44 20 7367 2055
E olivia.jamison@cms-cmno.com



Elisabeth Bremner
Partner, London
T +44 20 7367 3356
E elisabeth.bremner@cms-cmno.com

Financial Services Regulatory Investigations and Enforcement



Rachel Cooper
Partner, Manchester
T +44 161 393 4760
E rachel.cooper@cms-cmno.com



Lukas Rootman
Partner, Sheffield
T +44 114 279 4022
E lukas.rootman@cms-cmno.com



Alison McHaffie
Partner, London
T +44 20 7367 2785
E alison.mchaffie@cms-cmno.com

Life Sciences Regulatory



Shuna Mason
Partner, London
T +44 20 7367 2300
E shuna.mason@cms-cmno.com



Your free online legal information service.

A subscription service for legal articles
on a variety of topics delivered by email.

cms-lawnow.com

.....
CMS Cameron McKenna Nabarro Olswang LLP
Cannon Place
78 Cannon Street
London EC4N 6AF

T +44 (0)20 7367 3000
F +44 (0)20 7367 2000

The information held in this publication is for general purposes and guidance only and does not purport to constitute legal or professional advice.

CMS Cameron McKenna Nabarro Olswang LLP is a limited liability partnership registered in England and Wales with registration number OC310335. It is a body corporate which uses the word "partner" to refer to a member, or an employee or consultant with equivalent standing and qualifications. It is authorised and regulated by the Solicitors Regulation Authority of England and Wales with SRA number 423370 and by the Law Society of Scotland with registered number 47313. It is able to provide international legal services to clients utilising, where appropriate, the services of its associated international offices. The associated international offices of CMS Cameron McKenna Nabarro Olswang LLP are separate and distinct from it. A list of members and their professional qualifications is open to inspection at the registered office, Cannon Place, 78 Cannon Street, London EC4N 6AF. Members are either solicitors or registered foreign lawyers. VAT registration number: 974 899 925. Further information about the firm can be found at cms.law

© CMS Cameron McKenna Nabarro Olswang LLP

CMS Cameron McKenna Nabarro Olswang LLP is a member of CMS Legal Services EEIG (CMS EEIG), a European Economic Interest Grouping that coordinates an organisation of independent law firms. CMS EEIG provides no client services. Such services are solely provided by CMS EEIG's member firms in their respective jurisdictions. CMS EEIG and each of its member firms are separate and legally distinct entities, and no such entity has any authority to bind any other. CMS EEIG and each member firm are liable only for their own acts or omissions and not those of each other. The brand name "CMS" and the term "firm" are used to refer to some or all of the member firms or their offices. Further information can be found at cms.law