Corporate Co-operation Guidance

This document is for guidance only. It assists in assessing the co-operation from business entities (herein referred to as "organisations"). Decisions in each case will turn upon the particular facts and circumstances of that case.[1]

Co-operation by organisations benefits the public and advances the interests of justice by enabling the Serious Fraud Office ("SFO") more quickly and reliably to understand the facts, obtain admissible evidence, and progress an investigation to the stage where the prosecutor can apply the law to the facts.

Co-operation will be a relevant consideration in the SFO's charging decisions to the extent set out in the **Guidance on Corporate Prosecutions** and the **Deferred Prosecution Agreements Code of Practice**. According to the Guidance on Corporate Prosecutions, it is a public interest factor tending against prosecution when management has adopted a "genuinely proactive approach" upon learning of the offending. Co-operation can be an important part of such a genuinely proactive approach (**DPA Code** 2.8.2(i)).

Co-operation means providing assistance to the SFO that goes above and beyond what the law requires. It includes: identifying suspected wrong-doing and criminal conduct together with the people responsible, regardless of their seniority or position in the organisation; reporting this to the SFO within a reasonable time of the suspicions coming to light; and preserving available evidence and providing it promptly in an evidentially sound format.

Genuine co-operation is inconsistent with: protecting specific individuals or unjustifiably blaming others; putting subjects on notice and creating a danger of tampering with evidence or testimony; silence about selected issues; and tactical delay or information overloads.

It is important that organisations seeking to co-operate understand that co-operation – even full, robust co-operation – does not guarantee any particular outcome. The very nature of co-operation means that no checklist exists that can cover every case. Each case will turn on its own facts. In discussing co-operation with an organisation, the SFO will make clear that the nature and extent of the organisation's co-operation is one of many factors that the SFO will take into consideration when determining an appropriate resolution to its investigation. The SFO will retain full and independent control of its investigation process.

---

[1] "Organisations" includes corporate entities such as limited companies, limited liability partnerships, etc.

ID163 Version OGW v1, Published August 2019

Any enquiries regarding this publication should be sent to the Serious Fraud Office, 2-4 Cockspur Street SW1Y 5BS email: information.officer@sfo.gsi.gov.uk

Many legal advisers well understand the type of conduct that constitutes true co-operation. This will be reflected in the nature and tone of the interaction between a genuinely co-operative organisation, its legal advisers and the SFO. Nonetheless, some indicators of good practice are listed below, as are examples of steps which the SFO may ask an organisation to take. This is not a complete list; some items will be inapplicable (or undesirable) in certain cases and it is not intended to, nor does it, create legally enforceable rights, expectations or liabilities:

Preserving and providing material

1. Good general practices

i. Preserve both digital and hard copy relevant material using a method that prevents the risk of document destruction or damage.
ii. As and when material, especially digital material, is obtained, ensure digital integrity is preserved.
iii. Obtain and provide material promptly when requested, to respond to SFO requests and meet agreed timelines.
iv. Provide a list of relevant document custodians and the locations (whether digital or physical) of the documents.
v. Provide material in a useful, structured way, for example:
    a. Compilations of selected documents (including hard copy records, digital communications, records showing flow of cash) as requested by the SFO;
    b. Particularly relevant materials sorted, for example, by individual or specific issue;
    c. Relevant material gathered during an internal investigation;
    d. Basic background information about the organisation, including organograms; lists, job titles, and contact and personal information of relevant persons; and what categories of data exist (e.g. emails, audio, chats).
vi. Provide material on a rolling basis in an agreed manner.
vii. Inform the SFO without delay of suspicions of, and reasons for, data loss, deletion or destruction.
viii. Identify relevant material that is in the possession of third parties. The SFO may ask the organisation to facilitate the production of third-party material.
ix. Provide relevant material that is held abroad where it is in the possession or under the control of the organisation.
x. Promptly provide a schedule of documents withheld on the basis of privilege, including the basis for asserting privilege.

If an organisation decides to assert legal privilege over relevant material (such as first accounts, internal investigation

interviews or other documents), the SFO may challenge that assertion where it considers it necessary or appropriate to do so.

xi. Assist in identifying material that might reasonably be considered capable of assisting any accused or potential accused or undermining the case for the prosecution.

2. Digital evidence and devices

i. Provide digital material in a format the SFO requests that is, in a format ready for ingestion by and viewing on the SFO's document review platforms. The SFO may ask an organisation to provide schedules of relevant documents that it is producing and details of search terms, "seed sets" or other search methodologies applied to extract the documents.
ii. Create and maintain an audit trail of the acquisition and handling of digital material and devices, and identify a person to provide a witness statement covering continuity.
iii. Be alert to ageing technology or bespoke systems, and preserve means of reading digital files over the life of the investigation and any prosecution and appeal.
iv. Alert the SFO to relevant digital material that the organisation cannot access – for example, relevant private email accounts, messaging apps or social media that have come to light in an internal investigation.
v. Preserve and provide passwords, recovery keys, decryption keys and the like in respect of digital devices.

3. Hard-copy or physical evidence

Create and maintain an audit trail of the acquisition and handling of hard copy and physical material, and identify a person to provide a witness statement covering continuity.

4. Financial records and analysis

i. Provide records that show relevant money flows.
ii. Provide relevant organisational financial documents in a structured way, including bank records, invoices, money transfers, contracts, accounting records and other similar documents.
iii. Alert the SFO to relevant financial material that the organisation cannot access – for example, bank accounts into which monies flowed from the organisation.