# Act now to adopt voluntary code that upholds accountability

Engaging professional investigators requires a strategic approach in order to safeguard IPs from reputational and legal liabilities, says **Tony Imossi**

The term 'private investigator' often conjures up images of a lone sleuth working in the shadows, evoking a stereotype of an individual in a trench coat and fedora engaging in covert surveillance and unravelling mysteries through cleverness, intuition and resourcefulness. In reality, there is a high level of professionalism in carrying out this crucial function and the sector is obligated to ensure that investigative methods and the scope of enquiries comply with data protection requirements.

Having worked in the investigation field for 45 years, I find the term 'private investigator' no longer accurately reflects the services we provide to the legal sector. I prefer 'professional investigator'.

## Largely unregulated

I understand why legitimate agencies continue using the more widely recognised term, as their business models likely rely on visibility to potential clients. Unfortunately, this terminology is also used by less reputable and unaccountable elements in the largely unregulated industry. This highlights the importance of distinguishing between those who adhere to ethical investigative practices and those who engage in unscrupulous tactics. For simplicity, I will refer to all operatives in the investigative sector, as 'PIs'.

A significant portion of PI assignments arise from insolvency professionals. In insolvency practice and contentious business law, the engagement of PIs is often a pivotal component in navigating complex cases. Locating absconding debtors, tracing attachable assets, unravelling fraud scenarios and providing ongoing litigation support, such as process serving, interviewing witnesses or assisting with complex discovery issues, are just a few of the areas in which IPs benefit from investigative and litigation support services.

> **Determining purpose and means for data processing is not always clear, and they are quite often interpreted for convenience without a legal basis**

Yet, surprisingly, the PI sector is not regulated by statutory licensing. Despite being included in the Private Security Industry Act 2001, licensing of PIs has never been introduced due to insufficient political will. This creates a conundrum for insolvency practitioners that may rely on investigators' reports to meet their own strict regulatory conditions or provide evidence in legal cases.

Following the introduction of the UK GDPR, and the Information Commissioner's Office's (ICO) implementation of the Code of Conduct scheme (under article 40(5)), the Association of British Investigators (ABI) seized the opportunity to move towards establishing a regime of good order and accountability by developing a code of conduct for PIs. This initiative aims to protect the public and other stakeholders, such as insolvency professionals.

Working in collaboration with the ICO, the ABI developed the ABI UK 'GDPR Code of Conduct for Investigative and Litigation Support Services'. This good practice guide was approved by the ICO and published on 13 November 2024, the first of its kind in the UK, within one of the most complex sectors to regulate. Who would have thought that PIs would be the first to have achieved the ICO's approval?

## Evaluated annually

Opting to sign up to the code allows PI agencies to demonstrate adherence to best practices, data protection compliance and accountability. Those companies will be evaluated annually by an independent monitoring body for the code, pending final approval from the ICO.

The ABI code represents industry-specific accreditation, forming a unique, government-supported self-regulatory framework. Professionals in the investigative sector who study data protection laws recognise that data protection laws govern PI activities. After all, processing personal data is the sector's core business activity.

While the code scheme is voluntary, due diligence remains necessary when selecting a service provider. However, the code register will offer a reliable source for identifying compliant agencies that have also met the strict fit and proper assessment by the independent monitoring body. Ideally, investigative agencies outside the scheme will at least adhere to the code's guidance.

The success of the code as an industry standard will depend on market forces encouraging investigative agencies to adopt it in order to earn the trust and credibility that the sector often struggles to achieve. The legal and financial services professions, including IPs as the primary source of assignments for investigators, will likely drive this adoption, given their reliance on investigators, process servers and related services.

The ABI seeks to motivate competent agencies to join the code scheme through the influential market pressures of client preferences, rather than excluding them.

## Breaching rights and freedoms

Recent court cases highlight the increasing scrutiny of investigative techniques involving personal data processing.

• In one recent High Court case, the background of which concerned an allegedly fraudulent scheme said to involve misrepresentation, forgery and asset misappropriation, a law firm that presented its investigative service provider's report into evidence was later embarrassed to have to withdraw the report in its entirety when the factual accuracy of the information was questioned.

• In another pending case, the judge, unhappy with the lack of transparency, required an explanation of the data processing involved in a 'smoke and mirrors' investigation report on financial assets submitted into evidence by a man's ex-wife following private investigation. Everyone involved in the case is now shuffling to reposition their role to try to escape responsibility.

• In a case in Spain reported in the press, (and let's not forget the UK GDPR mirrors the EU regulation), an investigator's very helpful surveillance report commissioned by the defendant's employer was thrown out for breaching the rights and freedoms of the data subject. The investigator had been frequently recording the employee in a number of private settings.

Overturning the shadowy PI stereotype: The 'GDPR Code of Conduct for Investigative and Litigation Support Services' is a good practice guide for PIs, and is the first of its kind in one of the most complex sectors to regulate

> **The greatest risk emerges from the reckless activities of unaccountable PIs, some of whom could also be your service providers**

Call yourself what you like under GDPR (data controller or processor), but it is the data processing activity that will determine your position. Determining purpose and means is not always clear, and they are quite often interpreted for convenience without a legal basis. Had the investigators had the luxury of a code of conduct and adhered to it, they may have found themselves in a stronger and more authoritative position, and, of course, their professional clients would be in less discomfort.

There is now a noticeable show of interest within the investigative sector following the ICO's press release about the code's approval. The industry's realisation that the imminent implementation of the ABI UK GDPR Code of Conduct affords the investigative and litigation support service providers an opportunistic punctuation point. There has never been a better moment for all stakeholders to grasp the chance to be part of this legacy.

After 100 years of lobbying, 25 of which were conducted under the mistaken belief by the PI industry that statutory licensing held great significance, it is time to embrace a code of conduct to ensure compliance and reassurance. The voluntary scheme on the table potentially offers a better, and certainly more relevant, form of level playing field and accountability than a state licence was ever going to be capable of achieving.

I listened to Jonathan Hall KC on the radio recently. He is the UK's independent reviewer of terrorism legislation and state threats. He mentioned the dangers to the nation's security from the unchecked and unaccountable activities of some PI agencies when accepting assignments from hostile foreign governments, probably unwittingly. This threat, now covered in the National Security Act 2023, is currently being widely publicised by the Home Office. The greatest risk emerges from the reckless activities of unaccountable PIs, some of whom could also be your service providers. But this risk can be mitigated with the code's regulatory regime.

If the UK government were to be persuaded to revisit applying some regulatory control, it would only be to address the harm being caused to the public by poor or illegal practices. It has not escaped the attention of the officials looking at licensing that this is exactly what the ICO-approved code of conduct is designed to address by providing guidance on the area of the PI sector's activities causing harm (data protection abuse). Why would this not be important to the insolvency profession and other stakeholders?

## Strategic approach

Engaging professional investigators in the fields of insolvency and contentious business requires a strategic approach. By choosing investigators who adhere to the ABI's UK GDPR Code of Conduct, insolvency practitioners can ensure compliance, maintain ethical investigative standards, and safeguard themselves from reputational and legal liabilities. It is crucial to act now to adopt a regulatory model that upholds accountability and professionalism, securing the integrity of the investigative sector for the future.

**Tony Imossi** is head of the secretariat at the Association of British Investigators