The ABI
Together Driving Change

Guidelines on the instruction and use of Private Investigators

November 2026

The ABI | 30 Fenchurch Street, London, EC3M 3BD
T +44 (0) 207 600 3333 | abi.org.uk

Statement of Principles

This Statement applies to the instruction and use of Private Investigators (PIs) by insurers or their appointed lawyers or other authorised agents in the UK. It should be read in conjunction with the ABI Guidelines on the instruction and use of Private Investigators. These documents are intended to provide a framework for insurers to devise their own policies and procedures:

1. I**nsurers should only appoint PIs in appropriate circumstances.** Appropriate circumstances can include; to obtain independent, objective evidence where there is reasonable suspicion that a claim might be fraudulent or reasonable grounds to require validation of a claim. Prior to appointing a PI, insurers should look to explore other options including whether they can obtain information from other sources such as databases, credit reference agencies and open source intelligence.
2. **Insurers should only appoint PIs who operate within the confines of the law and to high ethical standards.** This will ensure insurers do not fall foul of the law, fail to meet their regulatory requirements or face adverse reputational impacts.
3. **Before a new PI is employed, the insurer should undertake appropriate due diligence on the PI.** Due diligence checks may include ensuring the PI complies with relevant legislation and standards, has appropriate security procedures and equipment, and staff receive appropriate training and screening. Insurers should consider performing a data protection impact assessment prior to appointment. Where the relationship is ongoing, due diligence should be carried out on an ongoing basis.
4. **The insurer should always enter into a written agreement with PIs, which should take account of legislative and regulatory requirements.** The agreement may cover issues such as compliance with applicable legislation and regulations, data protection and security, remit of the PI, and renumeration of the PI.
5. **Insurers should consider adopting their own code of practice that could also be incorporated into the agreement with the PI**, the aim of which is to ensure that the insurer is represented in a professional and proper manner, thereby minimising reputational risk.
6. **The insurer should take appropriate steps to ensure they and the PI comply with data protection legislation**, in particular, the principles concerning data accuracy, data security, data minimisation, access to data and retention of data. The insurer should:
    a. ensure instructions to the PI are explicit and transparent and decide on the most appropriate and secure way for issuing instructions, for example, via a standard form template.
    b. require the PI to obtain the minimum information reasonably necessary to establish the status of the claim, based on an assessment of the circumstances of the case.
    c. be transparent to consumers about the uses and disclosures of personal data.
    d. establish procedures to ensure that access to the information collected is restricted to relevant employees and, where appropriate, third parties (e.g. reinsurers, legal and medical advisers, police and other law enforcement agencies and counter fraud bodies).
    e. consider the length of time that it should hold personal data bearing in mind data protection and FCA regulatory requirements, and the statute of limitations.

Contents

Introduction **4**

Private Investigators (PIs) **5**

Considering the use of a PI 5
Due diligence checks prior to the appointment of a PI 6
Entering into a relationship with a PI 8
Fair processing wording 12
Instruction to the PI 12
Access to data collected by a PI 13
Retention of personal data collected by the PI 14

APPENDIX I - FCA REGULATORY REQUIREMENTS **15**

APPENDIX II - DATA PROTECTION PRINCIPLES **17**

GLOSSARY **19**

Introduction

The vast majority of insurance claims are not subject to investigation for fraud purposes. Of those that are, most are conducted by in-house counter-fraud specialists. Most investigations are carried out with the knowledge of the claimant and will often involve standard checks against fraud indicators, open-source data (e.g. social media) and industry databases, as well as personal interviews.

In 2025, insurers uncovered dishonest insurance claims worth £1.34bn. Despite the insurance industry investing around £200m every year to counter fraudulent activity, it is estimated that at least a similar amount of insurance claims fraud goes undetected each year, which leads to increased premiums and wastes public resources. It is incumbent upon insurers to do all that they can to protect honest consumers against the actions of fraudsters and thieves.

In certain circumstances an insurer may decide to instruct a private investigator (PI) to check whether a claim is genuine or not, or for other purposes such as liability investigations. When this step is taken, it should be taken with great care. It is simply not enough to employ a PI just because it 'gets results' - any organisation that fails to check the credentials and working practices of a PI runs the risk of falling foul of the law, not meeting their regulatory requirements, facing prosecution and hefty monetary fines as well as dealing with the associated reputational damage.

These guidelines apply to the instruction of PIs by insurers or their appointed lawyers or other authorised agents in the United Kingdom. They are intended to provide a framework for insurers to devise their own procedures for investigating claims and to deliver a framework where insurers appoint only PIs who operate within the confines of the law and to high ethical standards.

The 2014 version of these guidelines were updated in 2020. The changes made then reflected then-recent legislative, regulatory and market developments. Further updates were made in 2023 to reflect changes in how PIs store digital media and the introduction of FCA Consumer Duty, which introduced new standards for assessing, evidencing and delivering good customer outcomes, and in 2026 to reflect introduction of the Association of British Investigators UK GDPR Code of Conduct.

These guidelines are not confirmed by the Financial Conduct Authority (FCA). However, the FCA and the Association of British Investigators have been consulted in their development. Adoption of the guidelines is voluntary and entirely at the discretion of each individual insurer, but given the continuing absence of statutory regulation, we strongly encourage ABI members to adopt them.

Private Investigators (PIs)

Considering the use of a PI

There are many different reasons why an insurer might employ the services of a PI. These include:

- Undertaking surveillance in relation to a fraud investigation
- Liability disputes
- Validation of damages
- Credit hire enquiry services
- Tracing services to support motor recovery claims or to find beneficiaries under life policies
- Motor theft, vehicle and accident enquiries
- Claims screening
- Training

The use of PIs for surveillance purposes will occur primarily in two main instances:

- Where an insurer has grounds to suspect that a customer or third-party claimant is inventing or grossly exaggerating a one-off claim and cannot reasonably accept the evidence presented.
- Where organised fraud is suspected and alerting the suspected fraudster might prejudice other investigations, including those conducted by the police. Such investigations are most often used where there is scope to fabricate or exaggerate bodily injury, or in some cases of organised property damage (e.g. motor 'crash for cash').

The use of PIs for surveillance is likely to be an intrusion into that individual's privacy. So, a PI should only be employed where there is reasonable suspicion that the claim might be fraudulent or there are reasonable grounds for requiring validation of a claim and the information they can obtain using surveillance is deemed appropriate and necessary in the circumstances.

When an insurer is considering whether or not to instruct a PI to investigate an individual, it should consider all other options first, such as using other sources of information available to the insurer and assessing whether information gathering by the PI is strictly necessary.[1] The use of surveillance should not be considered as the first and only response. The purpose of surveillance, as recognised by the courts, is to obtain independent, objective evidence in order to prove, disprove or validate a claim. Properly authorised surveillance is often the only effective method of securing the evidence necessary for a fair trial.

There might be circumstances where the use of a PI might not be an appropriate, or the best, way of confirming the validity of a claim or where liability sits for a claim, for example, because an individual is alleging an illness that could not be verified through surveillance of that individual. So the insurer should consider what alternative courses of action might be appropriate in the particular circumstances of the case. There are a number of research and open-source intelligence tools available to the insurer that can play an important role in the claims validation process. These include underwriting and anti-fraud

[1] If Open Source Intelligence (OSINT) is used to conduct claimant profiling, to ensure compliance with data protection legislation, insurers should ensure that human control of the profiling and profile report is maintained, can justify the purposes for which the data are required and there are sufficient processing condition in place as well as having safeguards in place to ensure that only the minimum amount of required data is processed and transferred.

databases including, but not limited to, the Insurance Fraud Register, the Claims and Underwriting Exchange (CUE) and credit reference agency databases. In relation to bodily injury claims, insurers can also obtain much useful information from independent medical reports. In relation to liability disputes, insurers can obtain information from eyewitness accounts and CCTV footage if available.

In some cases, the information that may impact upon a claim cannot be obtained by surveillance of the individual but is held securely by another organisation for its own purposes. If this information is necessary to investigate the claim and is not available from other legitimate sources, the organisation should be approached directly by the insurer or its agent. That organisation should then decide whether or not to disclose the relevant information to the insurer or their agent. Obtaining personal information knowingly and recklessly without the consent of the data controller, is likely to be a criminal offence under Section 170 of the DPA 2018 and would be a breach of the data protection principles set out in the UK GDPR.[2]

The insurer should have a clear strategy to manage cases of suspected fraud so that PIs are only appointed in appropriate circumstances.

For claims which are handled on behalf of an insurer by an appointed law firm or authorised agent, the appointment of a PI should be approved in advance by the instructing insurer. This applies equally for claims at the pre or post litigation stage. We would ordinarily expect law firms and authorised agents to only appoint PIs who are already contracted with the insurer and use the same instruction process for a claim where a PI is appointed directly by the insurer.

Due diligence checks prior to the appointment of a PI

Before a new PI is employed the insurer should undertake appropriate due diligence on the PI itself. This should include actions such as ensuring:

- The PI has the recognised certification (e.g. BS 102000)
- The PI is a member of a reputable trade association (e.g. Association of British Investigators)
- The PI complies with relevant legislation and standards (e.g. demonstrates compliance of sector specific key areas through verified membership of the Association of British Investigators UK GDPR Code of Conduct)[3]
- Staff are DBS checked for criminal convictions
- Staff are trained and competent in all areas and equipped with secure technology (e.g. laptops, phones, email)
- The PI is able to securely store and securely dispose of personal data and has appropriate security procedures in place

[2] Insurers should also be aware of the principles set out in the:

- European Convention on Human Rights
  - Article 5 – Right to liberty and security;
  - Article 8 – Right to respect for private and family life;
  - Protocol 1, Article 1 – Protection of property
- Regulation of Investigatory Powers Act 2000

[3] More information on the Association of British Investigators UK GDPR Code of Conduct can be found in Appendix II.

It is likely that many investigations conducted by PIs will involve the processing of special category criminal offence data. This requires additional protection and additional legal conditions to be met.[4] Insurers and PIs should ensure that all relevant staff have sufficient understanding of what constitutes criminal offence data as the definition is wider than merely data about criminal convictions and extends to allegations, investigations and proceedings.

Insurers should also undertake appropriate due diligence to assess whether the appointment is necessary, taking account of relevant FCA regulatory requirements and data protection principles. This could include performing a data protection impact assessment prior to appointment or completing a 'reason for instruction' note.[5] Areas to be assessed and included are:

What are the insurer's grounds for using a PI?

The insurer should state why it believes that the claim might not be genuine, liability or damages are disputed, or a person needs to be traced, etc.

What means have been explored, other than the use of a PI, to verify the insurer's suspicions?

A PI should only be used to undertake surveillance or make enquiries where there is reasonable suspicion that the claim is not genuine, there is a dispute over liability or damages, or to assist with a tracing service, etc. The insurer should always consider what information it already has, or may gain access to, before instructing a PI.

What information needs to be disclosed to the PI so that they can fulfil their instructions?

Only the minimum information should be provided to the PI to enable them to perform their task. Sufficient background information should be provided but the insurer should be careful when providing sensitive personal data. Ordinarily, it is acceptable to provide a brief summary of the injury and the alleged limitations or disability the claimant has suffered. The insurer may also want to give the PI specific instructions as to the area of the body where the injury occurred so that the PI can focus on that area. Additionally, the insurer may ask the PI to comment on specific tasks that the claimant has alleged that they cannot do (e.g. lifting or driving).

Ordinarily, it will be inappropriate to disclose to the PI special category data such as an actual illness. Where a PI will not be able to undertake the task without that information (e.g. where the claimant is said to be suffering from depression, panic attacks, agoraphobia, etc) careful consideration should be given to disclosure.[6] The Insurance Derogation (Schedule 1, Paragraph 20) in the Data Protection Act (DPA) 2018 outlines when special category data can be processed for insurance purposes. The Derogation allows special category data to be processed when it 'is necessary for an insurance purpose' which can include claims handling activities such as the use of a PI. If the processing of special category date in this context cannot reasonably be said to be necessary for an insurance purpose, then unless an alternative legal condition can be met the processing of special category data shall be prohibited.[7]

[4] See Article 10 UK GDPR & Schedule 1 Data Protection Act 2018

[5] Although a data protection impact assessment is not mandatory for the use and instruction of PIs, such an assessment can be a useful method of assessing data protection risk and demonstrating that you have done so. If PIs are being instructed on a frequent basis then it would be advisable to complete and maintain such an assessment.

[6] http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/paragraph/20/enacted

[7] Potential alternative conditions include Article 9 (2) (f) of UK GDPR if the processing is necessary for the defence of legal claims and Schedule 1, Para 10 of the Data Protection Act 2018 if the processing is necessary to prevent or detect unlawful acts.

Entering into a relationship with a PI

The insurer, appointed law firm or third-party claims administrator acting on behalf of the insurer should ensure that it chooses a PI that will act in an appropriate manner, both in compliance with the law and with standards of ethics.[8] Prior to entering into a formal business relationship, the insurer should undertake appropriate due diligence as outlined above.

Although there may be occasions when PIs act as data processors, for example when the insurer exerts full control over the processing, in the majority of cases PIs will act as data controllers given the degree of autonomy and influence that they have in determining how an investigation is managed and what information is collected. In either case, a written agreement should exist between the insurer and the PI. The advantages of a formal agreement or contract include that it:

1. Helps to ensure that the insurer and/or PI complies with the requirements and principles of the UK GDPR and DPA 2018, and FCA regulation.
2. Helps to protect the insurer from financial liability in the event of the insurer being sued and from reputational risk.
3. Provides certainty as to the extent of the PI's remit.
4. Provides guidance on security of documents and information.
5. Forms a basis for recovering damages against the PI in the event of improper conduct.

To comply with the requirements of the FCA's Consumer Duty and Insurance Distribution Directive (IDD) which together require insurers to deliver good customer outcomes and act honestly, fairly and professionally in accordance with their customer's best interests, the insurer should leave the PI in no doubt that they should only obtain information by legal means. The insurer should emphasise this in its instructions to the PI.[9] A PI, when acting on behalf of an insurer, who knowingly and recklessly obtains personal information without the consent of the organisation that holds it, is likely to be committing an offence under Section 170 of the DPA 2018. The Information Commissioner may investigate both the PI and the insurer with a view to prosecution in these circumstances.

When entering into an agreement with a PI, the insurer, or appointed law firm or authorised agent, should consider the following[10]:

1. The PI company's ('the PI') employees engaged in the provision of the services should be suitably qualified, experienced, and trained.
2. The insurer might wish to establish what checks the PI undertakes of staff, and any sub-contractors or agents they may from time to time use, prior to recruitment and should consider seeking references and specimen reports.
3. The PI and its employees should hold any licences required by legislation and / or British Standards.

[8] Insurers should be aware that the onus is on the PI to examine each individual case to ensure that any investigations undertaken and all information collected is proportionate to the nature of the investigation and that appropriate safeguards are implemented to prevent leakage of personal data and to confirm that it is appropriate to send and fully compliant with the relevant legislation.

[9] Insurance Distribution Directive, Article 17, https://eur-lex.europa.eu/legal-content/en/TXT/?uri=CELEX:32016L0097

[10] The provisions contained in sub-paragraphs 1-15 are characteristics of the Association of British Investigator's Code of Ethics and Professional Standards, now also covered in BSi 102000/2018.

4. The PI and its employees should act in accordance with all applicable laws, rules, regulations and codes of practice, including in relation to health and safety and data protection, relevant to the services provided.
5. The PI should maintain adequate systems and controls to ensure that all of its personnel receive adequate training and are properly supervised in relation to requirements of the contract and relevant legislation. If possible, records should be kept of all training and insurers should seek evidence of regular testing of PI staff on their knowledge of relevant legislation, regulation and policies.
6. The PI should perform all services to the same standards as if they were all regulated activities, notwithstanding that some services will not be regulated activities.
7. The contract should clearly set out the basis on which the PI is being remunerated.
8. The contract should clearly set out how matters relating to breaches of contractual terms and conditions are to be remedied.
9. The PI should hold adequate professional indemnity insurance. This reduces the risk borne by the insurer and provides a degree of comfort that the PI has demonstrated a level of professionalism.
10. The PI should hold other relevant insurances as appropriate, such as employers' liability and public liability.
11. The PI should complete only the provision of services requested and retain the personal information involved for no other purpose.
12. The PI should obtain prior agreement from the insurer or law firm (as appropriate) before sub-contracting to an agent in fulfilling the provision of the service. The insurer should reserve the right to carry out due diligence on any sub-contractors and ensure that a suitable agreement is in place between the PI and the sub-contractor.
13. The PI should ensure that, if it sub-contracts to other agents in the provision of services to the insurer, those agents are bound by the same requirements as the PI. This should include full awareness training and periodic testing about applicable laws, rules, regulations and codes of practice and the legal obligations that arise from them.
14. The PI should take appropriate steps to ensure compliance with the UK GDPR and DPA 2018 when obtaining, using and disclosing data.
15. The PI should take appropriate steps to ensure that neither it or any of its employees or agents shall use any personal data other than in connection with the provision of services as instructed by the insurer and should not process the personal data for any other purpose.
16. The PI should have an entry on the register maintained by the Information Commissioner.
17. The PI should hold all personal data in strict confidence, take all actions, and put in place appropriate security measures, necessary to protect that personal data from unauthorised or unlawful access and accidental loss, destruction or damage and onward use and disclosure not associated with the investigation.
18. The PI should also have a clear personal data retention policy and return, or ensure the secure destruction of the personal data, when it is no longer required for the investigation, defence of the claim, potential further legal action, or accounting purpose. The PI should notify the insurer of those measures on request.
19. The PI should keep complete and accurate records of the services it carries out under its control and store all documents, information and personal data (in whatever form) in an intelligible format for an appropriate period from the termination of the contract or, on request by the insurer, return the records to the insurer in an intelligible format.[11]

[11] The UK GDPR and DPA 2018 do not give a definitive limit on 'appropriate period' but state 'personal data be kept for no longer than is necessary for the purpose for which personal data it is processed'. The insurer may wish to stipulate the retention period (bearing in mind the data protection requirements).

20. The PI should allow the insurer, on request, to carry out an audit of its procedures in respect of the personal data gathered under this agreement. The PI should cooperate fully, and supply promptly, relevant information, data and records of whatsoever nature as may be reasonably requested by the insurer. The PI should grant to relevant regulators the same rights as those granted to the insurer in relation to auditing rights.
21. The PI should submit agreed management information (MI) to the insurer on a regular, agreed basis and in an agreed format.
22. The insurer has the right to remove from the investigation employees of the PI or sub-contractors, if they are found to be acting inappropriately or if there are reasonable grounds for suspecting that they may be acting inappropriately.
23. In the event that the investigation of the PI is compromised, or there is suspicion of it being compromised, the operatives conducting the investigation should be immediately withdrawn and the matter referred to the instructing insurer.
24. If the PI receives any complaint, notice or communication which relates directly/indirectly to the processing of personal data (or to either party's compliance with the UK GDPR and DPA 2018), it should immediately notify the insurer and provide full cooperation and assistance in relation to the matter.
25. The PI should inform the insurer, as soon as reasonably practicable, following receipt of a data subject access or other data protection rights request from a claimant, in order that the PI and the insurer can decide upon the most appropriate party to satisfy the request.[12]
26. The PI should not transfer the personal data, or any part of it, to a country or territory outside the European Economic Area except with the explicit consent of the insurer.[13]
27. The PI should inform the insurer as soon as it becomes aware of any breach of data protection legislation and advise the insurer of the steps that it intends to take to remedy that breach. The PI should agree to keep the insurer informed as to the progress and completion of those steps.
28. There should be a time limit to the Service Agreement or contract.

Other Considerations

Reinsurance

Where there is reinsurance in place, the insurer should also consider whether the agreement should also reflect any conditions imposed by the reinsurer.

Giving evidence in court

The insurer should consider whether the PI has any experience of giving evidence in court or at a tribunal hearing in connection with an investigated claim. Evidence might not be heard for several years, so the PI should be asked what measures are taken to ensure that the evidence can be supported several years after the investigation e.g. maintaining the original surveillance log. All events that occur during the surveillance operation should be recorded in longhand in the surveillance log. The evidence should be recorded contemporaneously or as soon as reasonably practicable after the event (and, in any case, while the events are still fresh in the PI's memory).

[12] https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

[13] When transferring data to a country or territory outside the European Economic Area, the use of the international data transfer agreement (IDTA) and the international data transfer addendum to the European Commission's standard contractual clauses for international data transfers (Addendum) are recommended by the ICO.

Evidence contained within signed contemporaneous surveillance logs is usually acceptable in court in circumstances where the original media has been lost or damaged or where there is no independent film evidence, for example, if technology such as a DVD/CD/memory stick is defective or where an evidential incident may have occurred which could not be documented by footage. To avoid any suggestion of malpractice, a copy of the original surveillance log should always be attached to the surveillance report as an appendix.

Insurer Code of Practice

Individual insurers might also adopt their own code of practice, which can also often be incorporated into the agreement or contract with the PI. The aim of the code is to ensure that the insurer is at all times represented in a professional and proper manner by the PI, thereby minimising the risk of reputational damage to the insurer. The code might cover issues such as:

- Ethics - the PI should ensure that its employees and agents are subject to appropriate vetting procedures, such as carrying out a DBS check.
- Interviews and surveillance – the PI and its agents should only conduct interviews or surveillance in accordance with the insurer's specific instructions and relevant legislation.
- Surveillance and minors – The PI and its agents should take all reasonable steps to avoid filming third parties or, if avoidance is not possible, to protect their identity, in particular minors.
- Filming in other sensitive locations – The privacy of third parties should be respected in sensitive locations.
- Representations to insurer customers/third parties – Unless acting under the explicit instruction of the insurer, the PI and its agents should not make a direct approach to the customer, claimant or their representatives.

What information would be required from the PI to verify suspicion?

Schedule 2 Part 1 (2) of the DPA 2018 ('crime and taxation exemption') allows for covert operations to take place and disapplies the claimant's right to be informed, providing that the processing is both necessary for the prevention or detection of crime and if informing the claimant would cause prejudice.

In order to adhere to Article 5(1)(c) of the UK GDPR concerning data minimisation, the insurer should only request that the PI obtains information that is reasonably necessary to establish the status of the claim and should not request excessive information. As part of its assessment, the insurer should consider what information is required and why it is justified.

This might include:

1. **Desk-based profiling of claimant** - the PI will usually need to verify where the individual lives, and that the person lives at the address supplied. This might, for example, be obtained by cross checking against the electoral roll. Not knowing the individual's address might lead to the privacy of an innocent person being breached if the wrong information is supplied. The PI might also be instructed to carry out County Court Judgment (CCJ) screening; Directorship/Company Secretary searches; other open-source intelligence inquiries and police telephone enquiries.[14]
2. **Pre-surveillance enquiries** – the insurer might ask the PI to undertake pre-surveillance enquiries to verify the identity of the claimant under investigation, to establish whether it is likely that the claimant travels to a place of employment, their general demeanour and physical capabilities and

[14] Enquiries of the police are legitimate where, for example, the interest of the police in the person who is the subject of the investigation is known and related to the claim. Police officers can also be formally interviewed for the likes of motor vehicle accidents.

other pertinent information. Such enquiries should only be used in very carefully controlled and exceptional circumstances – they should never be a routine activity. If relevant, justified and proportionate, the PI might visit the locality of the claimant's place of residence to make enquiries of neighbours or at the property directly. The use of pretext enquiries for this purpose are, by definition, deceptive and may constitute a Section 170 offence. The Information Commissioner expects a detailed audit trail to be kept of the authorisation and investigation so that the insurer can fully demonstrate its reasons for using a PI and authorising pre-surveillance enquiries.

3. **Photographic evidence** – the insurer should consider whether photographic evidence is required for positive identification/verification.
4. **Digital Media** - Any digital or physical media gathered by PIs (e.g. surveillance footage) should be transferred and stored securely.[15] It may be necessary to download and edit a copy of the evidence (e.g. to preserve the anonymity of third parties, in particular minors). If working copies are to be downloaded and edited, this should be done in a secure manner. If the insurer has a specific preference as to how it wants the evidence edited, the insurer should stipulate this at the time of instruction.[16]
5. **PI Report** – this might be required, for example, to register the claimant's movements.
6. **Other physical evidence** – Evidence, other than photographic or surveillance footage, such as advertisements offering services, invoices or receipts.
7. **Other PI work** - The PI should be transparent around what other work they undertake, and the insurer should be satisfied that this does not conflict with their interests or create a reputational risk.

Fair processing wording

The UK GDPR requires data to be fairly and lawfully processed in a transparent manner. This would ordinarily require the insurer to disclose to the customer all sources, uses and disclosures of personal data.

Where PIs are frequently instructed, the fair processing notice should reflect this and provide transparency. Where PIs are not frequently instructed, a generic reference to the processing of personal data, including disclosures to third parties, for the prevention, detection and investigation of crime (including fraud/attempted fraud) might be sufficient. This information should be included in the notification given to customers. The customer would have the right to be informed of the recipient (or categories of recipient) should they enquire.

Instruction to the PI

The insurer should decide on the most appropriate medium for issuing instructions, such as a mandatory standard form template which might, for example, include the rationale for appointment of the PI and the desired outcome.

[15] Many PIs now use cloud-based media storage systems. These systems allow for media to be securely and remotely uploaded, stored and transferred in real time with strict data security processes and controls, thus reducing risk of loss of or damage to media and meaning media can be accessed quicker for use.

[16] Insurers and PIs should be aware (and be able to demonstrate such awareness) that although photographs and video footage are not considered by data protection legislation to be special category data, if technological means are specifically applied in order to uniquely identify an individual, then the resultant data is likely to be considered biometric data, a form of special category data that requires additional protections and compliance measures (See Article 9 UK GDPR & Schedule 1 Data Protection Act 2018).

The insurer should ensure that instructions are provided to the PI company by secure medium. It is prudent for any instructions to a PI to be given in writing and sent securely. The insurer might provide instructions via a secure portal or email, with the instructions contained in an attachment that is suitably protected against unauthorised access (e.g. by encryption or password protected).

The instructions to the PI should be explicit and transparent, with the subject matter clearly documented. The insurer should only request the necessary and appropriate amount of information needed to gather evidence to support the processing of a genuine claim or to confirm the insurer's suspicions.

The insurer should provide the PI with the minimum amount of information necessary and relevant to ensure that the investigation focuses on the correct individual, to identify the subject of their investigation and inform them what type of investigation is required. This might include:

1. claimant's name (and any known aliases or previous identities)
2. claimant's sex
3. claimant's address (and any known previous addresses) (on file) [which the PI may be asked to verify]
4. claimant's date and place of birth
5. claimant's occupation (if employed) and occupation history
6. Details of the claimant's known hobbies or interests
7. Description of the claimant (this might be obtained, for example, from a medical report)
8. Family circumstances
9. Brief explanation of illness or disability
10. Details of claimant's vehicle
11. Description of the type of data required[17]:
    - Photographs
    - Video footage
    - PI report
    - Any other information that is reasonably required (and justified) to help the insurer resolve the case. If the insurer is in any doubt as to whether further information is required or is justifiable, the insurer's data protection officer should be consulted.
12. Any other relevant information obtained through open-source intelligence (OSINT).

Access to data collected by a PI

The insurer should establish appropriate procedures to ensure that access to the information collected is restricted to relevant employees.

There might also be a number of organisations that the insurer needs to consult in connection with the claim (e.g. to gather evidence) which might involve disclosure of some of the information obtained by the PI. These may include:

1. The reinsurer who underwrites a proportion of the risk and may be consulted on the appointment of a PI and whether the claim should continue following receipt of the PI's evidence.
2. The employer who, as the policyholder on a group policy, might have the right to ascertain whether a claim should continue.

[17] See "what information will be required from the PI to verify suspicion" [page 11].

3. The legal advisers who might be involved in advising on whether the claim should be repudiated, involved in subsequent legal action or in advising on legislative requirements.
4. The medical advisers who might need, for example, to give an expert opinion as to whether certain behaviour or activity might be possible if the claimant is suffering from the condition claimed.
5. The police, other Law Enforcement Agencies and dedicated insurance fraud agencies such as the Insurance Fraud Enforcement Department (IFED) and the Insurance Fraud Bureau (IFB).

Individuals who are the subject of investigation by a PI are entitled to see the personal data obtained about them from the insurer who has instructed the PI. All disclosures made under the data subject access request right will be subject to lawful exemptions, where appropriate.[18] The confidentiality of other individuals about whom the PI may have inadvertently collected additional information should be redacted from any disclosure.

Retention of personal data collected by the PI

The insurer should consider the length of time that it might need to hold the personal data provided by the PI. UK GDPR Article 5(1)(e) states that personal data processed for any purpose or purposes shall not be kept for longer than is necessary for that purpose or those purposes. FCA guidance on systems and controls similarly provides that the general principle is that records should be retained for as long as is relevant for the purposes for which they are made.

For evidential purposes, in line with the Limitation Act 1980, it might be prudent to hold data for six years following the cancellation of the policy or repudiation of a claim. The insurer should also allow sufficient time for an appeal to be lodged or disposed of. It is important that the insurer notifies the PI when a claim has been settled/closed so that the PI can then archive the file, taking account of the need to ensure security of the information. When sufficient time has elapsed, the PI should take steps to dispose of the data securely.

[18] The lawful exemptions are available here: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/exemptions/

APPENDIX I - FCA REGULATORY REQUIREMENTS

FCA Handbook

It is important that insurers are aware of how the FCA Handbook applies to work outsourced to PIs when handling claims as part of their regulated activities and are able to demonstrate how they monitor and mitigate any potential risks to customers arising from outsourcing claims functions and/or activities to PIs.[19]

When using a PI, insurers are outsourcing part of the regulated activities they perform as the work falls within the FCA Handbook Glossary definition of outsourcing, which is '*.....the use of a person to provide customised services to a firm.....*'

The FCA expects insurers to ensure that the work performed by PIs, which impacts upon their claims handling practices, is consistent with their regulatory obligations under SYSC, PRIN and ICOBS, and they are able to evidence this.

ICOBS 8.1.1R - https://www.handbook.fca.org.uk/handbook/ICOBS/8/1.html

PRIN 2.1.1R - https://www.handbook.fca.org.uk/handbook/PRIN/2/1.html

SYSC 3.2.3G - https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html

SYSC 3.2.4G - https://www.handbook.fca.org.uk/handbook/SYSC/3/2.html

SYSC 13.9.1G - https://www.handbook.fca.org.uk/handbook/SYSC/13/9.html

SYSC 13.9.4G - https://www.handbook.fca.org.uk/handbook/SYSC/13/9.html

SYSC 13.9.5.G - https://www.handbook.fca.org.uk/handbook/SYSC/13/9.html

SYSC 13.9.9.G - https://www.handbook.fca.org.uk/handbook/SYSC/13/9.html

Consumer Duty

The new rules set out in the FCA Consumer Duty were finalised in July 2022 and take effect from 31 July 2023 for open products and services and from 31 July 2024 for closed products and services. The Duty sets higher and clearer standards of consumer protection than under the existing Principles 6 and 7 across financial services and requires firms to act to deliver good outcomes for consumers. The FCA wants to see firms deliver a higher standard of customer care and protection, and to go further to equip consumers to make effective decisions in their interests.

Main Provisions

The new Principle 12 requires firms to act to deliver good outcomes for retail customers.

[19] For more information on FCA regulatory requirements can be found here: https://www.fca.org.uk/firms/outsourcing-claim-activities-private-investigators

Cross-cutting rules require firms to:

- act in good faith towards retail customers;
- avoid causing foreseeable harm to retail customers; and
- enable and support retail customers to pursue their financial objectives.

Outcomes and associated rules:

1. Products and services
2. Price and value
3. Consumer understanding
4. Consumer support

Scope

The Consumer Duty applies to the regulated activities and ancillary activities of all firms authorised under the Financial Services and Markets Act 2000 (FSMA), the Payment Services Regulations 2017 (PSRs) and E-money Regulations 2011 (EMRs), in respect of products and services for prospective and actual retail customers.

For insurers, the scope follows that of the Insurance Conduct of Business Sourcebook (ICOBS).

APPENDIX II - DATA PROTECTION PRINCIPLES

It is important that insurers are aware of how the Data Protection Principles, as set out in the UK GDPR, applies to work outsourced to PIs.

The ICO expects insurers to ensure that the work performed by PIs is consistent with their legal obligations under the UK GDPR and DPA 2018. It is particularly important that insurers are aware of the following sections of the UK GDPR and understand the impact they have on their practices in this area:

UK General Data Protection Regulation (UK GDPR)

Article 5 – Principles relating to processing of personal data - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/data-protection-principles/a-guide-to-the-data-protection-principles/

Article 6 – Lawfulness of processing - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/a-guide-to-lawful-basis/

Article 9 – Processing of special categories of personal data - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/lawful-basis/special-category-data/

Article 24 – Responsibility of the controller - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-controller/#1

Article 26 – Joint controllers - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-joint-controllers/

Article 28 – Processor - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1

Article 29 – Processing under the authority of the controller or processor - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/controllers-and-processors/controllers-and-processors/what-does-it-mean-if-you-are-a-processor/#1

Article 35 – Data protection impact assessment - https://ico.org.uk/for-organisations/uk-gdpr-guidance-and-resources/accountability-and-governance/data-protection-impact-assessments-dpias/

Data Protection Act 2018 (DPA 2018)

Part 6, Section 170 – Unlawful obtaining etc of personal data:
http://www.legislation.gov.uk/ukpga/2018/12/section/170

Schedule 1, Part 2, Paragraph 10 – Preventing or detecting unlawful acts:
http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/2/crossheading/preventing-or-detecting-unlawful-acts

Schedule 1, Part 2, Paragraph 20 – Insurance:
http://www.legislation.gov.uk/ukpga/2018/12/schedule/1/part/2/crossheading/insurance

Schedule 2, Part 1, Paragraph 2 – Crime and taxation: general:
http://www.legislation.gov.uk/ukpga/2018/12/schedule/2/part/1/crossheading/crime-and-taxation-general

The Association of British Investigators UK GDPR Code of Conduct

The purpose of the Association of British Investigators UK GDPR Code of Conduct for Investigative & Litigation Support Services is to enable PIs to demonstrate compliance with specific areas of data protection law in the provision of investigative and litigation support services.

The ICO-approved Article 40 code aims to provide sector-specific guidance to help PIs comply with data protection laws and to increase accountability in handling personal data. It includes advice, guidance, and practical examples in relation to:

- Roles and responsibilities of code members when acting as data controllers, joint controllers or processors
- Conducting Data Protection Impact Assessments
- Determining a lawful basis for data processing
- Performing legitimate interests assessments
- Obtaining consent to share when tracing and locating individuals in certain cases

Code membership is managed by an independent ICO-approved and UKAS-accredited monitoring body. PIs who are code members must satisfy the monitoring body that they meet the requirements covered in the code.

GLOSSARY

Claim - A claim for compensation when the insured has suffered a loss or is liable for causing a third party to suffer a loss.

Compromise - An unplanned or unexpected event, which leads to a person becoming aware that they are the subject of observation.

Contemporaneous Surveillance Log - A detailed handwritten log of events, which are observed during any period of surveillance. In the absence of any corroborative evidence of the event, such as video or photograph, courts will allow details of the event to be admitted into evidence, provided that the event was recorded at the time, or as soon as reasonably practicable after the event and while details of the occurrence were still fresh in the mind of the observer.

Covert - An enquiry which is hidden or secret, without the subject of the investigation being aware that it is taking place.

Data Controller - The natural or legal person, public authority, agency or other body which alone, or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

Data Processor - A natural or legal person, public authority, agency, or other body which processes personal data on behalf of the controller.

Data Protection Legislation – The UK General Data Protection Regulation (UK GDPR) and the Data Protection Act 2018.

Data Subject - An individual who is the subject of Personal Data, as defined by the UK GDPR.

Digital Investigation - Low cost, office-based techniques, using information technology such as self-serve templates to validate, or video interviewing to investigate claims.

Investigation - The act or process of examining an insurance application, claim, statement, etc, by digital, desktop or field enquiries to establish the truth.

Investigation by Exception - An investigative process utilising omni-channel communications starting with desktop and digital triage of evidence. The process establishes genuine claimants and lost causes quickly, with minimal disruption to customers and eliminates the need to pursue expensive investigations or draft Civil Procedure Rules statements that will never be used in defence of a claim.

Liability Investigation - An investigation carried out in order to determine fault and the extent of the insurer's liability for loss.

Personal Data - Any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or

more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Pre-Surveillance Enquiries - An extension of a Lifestyle Profile, undertaken as part of an Intelligence Surveillance operation through the acquisition of intelligence in order to maximise the chances of observing the subject and minimising no-shows by choosing the best dates, times and places to carry out the surveillance.

Private Investigator - A person who conducts investigations into cases where the police service will not act. It is ordinarily, but not necessarily, restricted to offences or attempted offences perpetrated against businesses as opposed to individuals.

Special Category Data – Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.

Surveillance - The covert observation of a person or place, in order to establish independent, objective evidence as to the physical condition and/or disabilities displayed by that person; the level of care they are receiving; the activities occurring at and persons frequenting a particular place; the association between individuals, or the location of property which is the subject of a claim.

Tracing - To find someone or something by searching using lawful, ethical means, either desktop or through enquiries in the field.

Tracing Agent - A business or individual offering a tracing service.

Disclaimer

This document has been produced by the ABI for general information purposes only. While care has been taken in gathering the information and preparing the document, the ABI does not make any representations or warranties as to its accuracy or completeness and expressly excludes to the maximum extent permitted by law all those that might otherwise be implied. The ABI accepts no responsibility or liability for any loss or damage of any nature as a result of acting or refraining from acting as a result of, or in reliance on, any statement, fact, figure or expression of opinion or belief contained in this document. This document does not constitute legal or financial advice of any kind.