



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

**Minutes of Meeting of the Internationale Kommission der Detektiv Verbände held at the Parkhotel
Schoenbrunn, Vienna, Austria on Friday the 16th October 2009**

1. Introduction and welcome by the Secretary General – attendees are set out in the list annexed hereto as “A”.
The list shows 24 out of the 29 member organisations and single members were represented by Delegates plus 2
Honorary members attended in addition to 24 guests. The board in attendance were:

Tony Imossi – Secretary General
George Hirtl – Vice Secretary General
Markus Wegst – Treasurer

Apologies for absence –

Raul Guerreiro – Portugal
Jean Schmitt – France
Villy Verner Andersen – Denmark
2. Ratification of New Members.
The provisional membership of the following 6 organisations were considered in turn and a vote of acceptance was carried: -
 - (a) CII,
 - (b) UPNDPBelgique,
 - (c) ANDEPIPortugal,
 - (d) Col.legi Oficial de Detectius Privats de Catalunya (Spain),
 - (e) PDA-Turkey.An objection was raised by ODV against the following membership and after some discussion it was agreed that the objections would be considered by the board after representations in writing.
 - (f) EURODET-Austria
3. Minutes of the Committee meeting held on 18th April 2008 in Walsall, UK were proposed as a true record by Richard Jacques-Turner and seconded by George Hirtl, subject to a minor amendment to paragraph 3, the proposal was carried.
Matters arising – paragraph 7. The use of Investigators by insurance companies was raised. The SG advised that a document was published by The Association of British Insurance in 2007 entitled Guidelines on the instruction and use of private investigators and tracing agents. The SG said he will make this document available to members. A copy of the publication is annexed hereto at “B”
4. The Secretary General (SG) referred to his written Report on the IKD's activities since the last meeting, annexed hereto as “C”.



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



5. The Vice Secretary General (VSG) gave a verbal Report covering his numerous meetings. Adding to the matters arising from Walsall Minutes (paragraph 7) the VSG advised that there has been no final decision made on whether Private Investigation is included in the wider Security Industry. He advised on the EPIC programme and the huge changes to the web site which included a map based directory, which he demonstrated on screen.
6. To consider the income and expenditure accounts for the year ending 31st December 2008 and to adopt the accounts together with the report of the Treasurer and Auditor. The Treasurer explained that the largest item shown, "Cost Europe development" a sum of €8,202.10 was mostly the expenses involved in the Zaragoza CMS Conference. The Treasurer's report was proposed as accepted Richard Jacques-Turner, seconded by Genuario Pellegrino and carried. The Treasurer's Report was read out. Werner Sachse, the appointed Auditor, reported in writing and supported the Accounts presented and commented that all expenses were in order. The Reports of the Treasurer and Auditor are annexed hereto at "D".
7. There then followed a detailed presentation by Andreas Heims and Matthias Willenbrink on behalf of ZAD GmbH Zentralstelle fuer die Ausbildung im Detektivgewerbe, with a proposal for the IKD to fund the research and work necessary to pursue (a) a bid for further funding from the Da Vinci Project (EU), towards (b) research and work in collating data to establish the CMS on competence. ZAD request for €8,000 support from IKD. ZAD's work on the EPIC project was provided pro bono. Delegates were asked to consider and vote on the request which was carried with BDD, Germany voting against and DZRS, Slovenia abstaining. The SG requested ZAD to formalise the arrangement in a brief contract which should cover an opt-out clause and payment by 4 quarterly instalments each supported by accounts.
8. To consider the reports of the Member Associations. The numerous Reports that had been submitted had been distributed and will be published as usual on the IKD website.
9. Any other business
 - (a) Common Minimum Standard. There were no further matters arising.
 - (b) There followed a discussion on the SG proposal to amend Article 4 in an attempt to deal with the use of the IKD logo, by adding the following: -
 5. The use of the IKD logo is permitted for every member described in paragraphs 1.) to 4.) of Article 4 above, only for as long as the full membership criteria are met.
 6. The logo, as registered with HABM, available for download on www.i-k-d.com, may be used as is or altered in size proportionally, but must not be altered in colour, appearance, design or text. The logo may be used on stationery, business cards, in emails and web appearance by the IKD members as described in paragraphs 1.) to 4.) of Article 4 above and/or their



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



respective duly and properly appointed members, individuals and corporate, and so long as they remain in their respective membership.

7. IKD Members are responsible to control the proper use of the logo by their organisation and/or respective membership
8. No person, individual or corporate, may describe himself/herself/itself, direct or implied, as a member of IKD, without the express permission of the IKD secretariat. For the avoidance of doubt, a member of the IKD which can be described as "A member" are those described in paragraphs 1.) to 4.) of Article 4, above. This does not affect the right to use the logo as aforesaid under Article 4 paragraph 6.).
9. The IKD members' [as described in paragraphs 1.) to 4.) of Article 4 above] respective duly and properly appointed members, individuals and corporate, and so long as they remain in their respective membership, are in addition to the use of the logo as aforesaid, entitled to describe themselves by the use of the word "Connected" and/or "Affiliated", or such suitable translation in the member's first language, when making reference to the IKD in their stationery, business cards, emails and/or website.

David Sanmartin pointed out (amendment 6) that there exists a problem where an Operative who belongs to an IKD world-wide member, such as WAD or CII, yet did not belong to his National association, the IKD member is still permitted to use the IKD logo, which may cause offence to the National association. This was discussed but no solution emerged it being the case that both WAD and CII are IKD members on the understanding the IKD affiliation passes to their respective members. It was agreed this problem will require further consideration.

A vote was taken on the proposal to amend the Article 4 as above and carried, with 14 of the member delegates remaining present voting in favour, 1 against and 3 abstentions.

- (c) Federpol agreed through its President and Delegate, Genuario Pellegrino, to review the IKD Code of Ethics and Code of Conduct. The document produced in Italy appeared to the SG as more in line with a Data Protection Policy and following a pre-meeting discussion between the SG and the FEDERPOL members present, the SG had provided a draft Model Policy for members and their respective memberships' use, which he would amend to suit EU (IKD) members for further consideration. The Model Policy is annexed hereto as "E".

10. To fix the date and venue of the next IKD Congress in 2010. The meeting received 3 bids to host the 2010 Congress, namely, from Romania (in May or October in Bucharest), Hungary (in October in Pecs being 215 Km from Budapest but the hosts will organise transfers) and Italy (in October in Venice). After a short discussion the Italy proposal was withdrawn and a vote followed whereby it was decided that the 2010 Congress will take place in Hungary on a date to be confirmed.

Close of Conference



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

“A”

Delegates & Guests

Registration

INTERNATIONALE KOMMISSION
DER DETEKTIV-VERBÄNDE

INTERNATIONAL FEDERATION
OF ASSOCIATIONS OF PRIVATE DETECTIVES

IKD

IKD

Executive Meeting 16 October 2009 - Vienna
REGISTRATION

MEMBERS

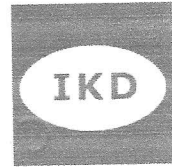
| Country | Member | Delegate | Signature |
|-----------------|---|-------------------------|------------------|
| Austria | Osterreichischer Detektiv-Verband | Bernhard MATER | |
| Austria | EURODET | MANUUS SCHWABER | |
| Belgique | UPNDPB | TI DECUYER | |
| Czech Republic | Czech Chamber Of Detective Services | | |
| Denmark | Foreningen Danske Detektiver & Erhvervsretterforskere | LIPPE BODEHOLT | |
| Finland | Suomen Yksityisetivä-Ja Lakitoimistolittori | | |
| France | Syndicat National Des Agents De Recherches Privees | MIGUOT Pascal | Apology received |
| Germany BDD | Bundesverband Deutscher Detektive | Bodo Scholl | |
| Germany BID | Bund Internationaler Detektive | LOTHAR KUMM | |
| Hungary HDA | Hungarian Detective Association | ✓ | |
| Hungary Chamber | Hungarian Chamber of Bodyguards, Property Protection and Private Detectives | ESATARI TIDOR SANDOR | |
| India | Association of Private Detectives & Investigators- India | | |
| Israel | Israeli Bureau of Private Investigators | RON TEVEL | |
| Italy | Federpol | | GSUARI/SCUSARI |
| Japan | Mr. Sumio Hiroshima (Single Member) | | |
| Latvia | Bizness Droshiba (Single Member) | ✓ MIHAILS HESINS | |
| Netherlands | V.P.B./Sectie A.R.S | PETER VAN RIJN | |
| Norway | Norsk Forening for Etterforskning og Sikkerhet | John Grottem | |
| Portugal | R. Guerreiro Detectives (Single Member) | | |
| Portugal | ANDEPIP | FERNANDO OLIVEIRA | |
| Romania | Asociatia Nationala A Detectivilor Din Romania | MARIA BUMBAREU | |
| Slovenia | Detektivska Zbornica Republike Slovenije | MITJA KLAVORA | |
| Spain | Asociacion Profesional De Detectives Privados De Espana | DAVID SERRAÑA | |
| Spain | Col.legi Oficial de Detectives Privats de Catalunya | ENRIQUE DE MADRID | |
| Switzerland | Fachverband Schweizerischer Privat-Detektive | WEGST Markus | |
| Turkey | PDA | YUSUF VELIB DALIN | |
| United Kingdom | Association of British Investigators | Tony Imossi | |
| World Wide | World Association of Detectives Inc | RICHARD JACQUES-TURNER | |
| World Wide | Council of International Investigators | | |

LN: Richard Jacques - Turner
Werner Sachse

Bank: Zurcher Kantonalbank, Bahnhofstrasse 9,
CH-8022 Zurich, Switzerland



INTERNATIONALE KOMMISSION
DER DETEKTIV-VERBÄNDE



INTERNATIONAL FEDERATION
OF ASSOCIATIONS OF PRIVATE DETECTIVES

Executive Meeting 18 April 2008 – Walsall
REGISTRATION

GUESTS

| Country | Member organisation | Name | Signature |
|-------------|-------------------------|--------------------------|-------------|
| Austria | Öster. Detektiv Verband | Lukas HEMBERGER | [Signature] |
| Austria | ÖDV | Peter LANG | [Signature] |
| ITALY | FEDERPOL | ASCAPI LUCA | [Signature] |
| PAKISTAN | SECURITY 2000 / WAD | RASHID ALI MALIK | [Signature] |
| Den. bdd | BDD / BID | Lotze, Manfred | [Signature] |
| Germany | BID | Engin Akbag | [Signature] |
| Deutschland | BDD / BID | Simon Andreas | [Signature] |
| Germany | BDD | Joachim Erhard | [Signature] |
| UK | W.A.D. | James - James | [Signature] |
| Germany | BID | Andreas Heilm | [Signature] |
| AUSTRIA | BID | Cornelia Haupt | [Signature] |
| UK | W.A.D. | James - James | [Signature] |
| GERMANY | WAD / BDD | MATTHIAS WILLENBRIN | [Signature] |
| UK | C.I.I. | ALAN MARR | [Signature] |
| LATVIA | BIZNESS DROSHIBA | Vukto Slopane | [Signature] |
| UK | ABI | ERIC SHELMERD | [Signature] |
| U.K. | A.B.I | PETER FARRINGTON | [Signature] |
| Switzerland | WAD | Simon Killstone | [Signature] |
| Switzerland | C.I.I. | Katol Stachler | [Signature] |
| UKRAINE | WAD | Yurii KOGUT | [Signature] |
| Norway | IKD - NFES | Grotton | John |
| ISRAEL | SMRP - IBPI | RON TEVEL | [Signature] |
| AUSTRIA | ÖDV | HELENA MNICH | [Signature] |
| AUSTRIA | ÖDV | HERBERT MNICH | [Signature] |

| | | | |
|---------|------------------------------|-----------------------|--------------------|
| Austria | ÖDV | SCHWEITZER | G. Munda |
| ISRAEL | CII / Lapidim | Jacob Lapid. | <i>[Signature]</i> |
| " | CII " | Deborah Allison | D. H. Allison |
| UNGARN | (SZUMSZK) Hungary Chamber | CSATA'RI TIBOR SANDOR | <i>[Signature]</i> |
| BUSETO | LOREZO | FEDERPOL | <i>[Signature]</i> |
| ITALY | SECRETRO DANIELA | FEDERPOL | <i>[Signature]</i> |

1988 1989 1990 1991 1992 1993 1994 1995 1996 1997 1998 1999 2000 2001 2002 2003 2004 2005 2006 2007 2008 2009 2010 2011 2012 2013 2014 2015 2016 2017 2018 2019 2020 2021 2022 2023 2024 2025



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

“B”

Association of British Insurers

July 2007

Guidelines on the instruction and use of Private Investigators and Tracing Agents



Association of British Insurers

Guidelines on the instruction and use of private investigators and tracing agents

July 2007

FOREWORDS

Richard Thomas, Information Commissioner

Respect for privacy is one of the foundation stones of the modern democratic state. Failure to respect an individual's privacy can lead to distress and in some circumstances cause that individual real damage, mentally, physically and financially. In my report 'What price privacy?' I brought to light evidence of an illegal trade in confidential personal information and identified a role for professional bodies to help stamp out that trade. I called on them to take a strong line and influence the industries in which they operate. I welcome these guidelines as a positive step by the insurance industry towards raising awareness and tackling an area where insurers or their agents could be drawn into the illegal trade in personal information.

Stephen Hadrill, Director-General, Association of British Insurers [ABI]

People rightly wish to ensure that their privacy is protected. At the same time they do not want to pay more for their insurance because others are getting away with fraud. Insurers have to strike the right balance, respecting privacy whilst stopping cheating policyholders who add nearly £40 to the average premium.

To protect the interests of our policyholders, it is sometimes necessary for an insurer to use a private investigator to check whether or not a claim is genuine. When this step is taken, it must be taken with care. It is simply not enough to employ a PI company 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 and facing prosecution.

It isn't just about finding the cheats. Insurers will also use tracing agents to find beneficiaries who are due windfalls from long-forgotten policies. Insurers will expect the same high standards to apply to tracing agents, as they do to PIs.

Insurers should also remember that they too can be the victims of deception. So staff, particularly those in call centres, should be suitably trained.

The ABI has worked with the Information Commissioner and the PI industry in developing this guidance. I hope it will provide insurers with the information and tools they need to help track down the cheats while respecting the right to privacy. Insurers who follow it can act safe in the knowledge that PIs working for them will operate to high standards within the parameters set by the law.

CONTENTS

| | |
|--|-----------|
| FOREWORDS | 2 |
| SCOPE | 4 |
| BACKGROUND | 5 |
| Investigation of insurance claims | 5 |
| The views of the Information Commissioner and the Government | 5 |
| Regulation of the private investigator sector | 6 |
| PRIVATE INVESTIGATORS (PIs) | 7 |
| Considering the use of a PI | 7 |
| Entering into a relationship with a PI | 9 |
| Fair processing wording | 12 |
| Instruction to the PI | 13 |
| Access to data collected by a PI | 14 |
| Retention of data collected by the PI | 14 |
| TRACING AGENTS | 16 |
| GLOSSARY | 17 |

SCOPE

These guidelines apply to the instruction of private investigators and tracing agents by insurers in the United Kingdom. They are intended to provide a framework for insurers to devise their own procedures for investigating potential frauds in relation to claims from policyholders and third parties. The guidelines encourage insurers to instruct only private investigators (PIs) who operate within the confines of the law and to high ethical standards, without unduly hindering insurers' efforts to combat fraud.

The guidelines are in two parts. The first, more detailed part, relates to private investigators and the second to tracing agents. Investigations involving PIs tend to be of a more intrusive nature than those involving tracing agents, though the same considerations should apply when the instruction of either is contemplated.

Adoption of the guidelines is voluntary and entirely at the discretion of each individual insurer.

BACKGROUND

Investigation of insurance claims

The vast majority of insurance claims are not subject to investigation. Of the few that are, most are conducted by in-house investigators, covered by FSA regulation, or chartered loss adjusters who are subject to their own professional standards. Most investigations are carried out with the knowledge of the claimant and will often involve standard checks against industry databases, which the customer has been told about at inception of the policy.

It is sometimes necessary to conduct covert investigations. These occur in two main instances: first, where an insurer has good grounds to suspect that a customer is inventing or exaggerating a claim and cannot reasonably accept the evidence that the customer presents; and second, where organised fraud is suspected and alerting the suspected fraudster might prejudice other investigations, including those conducted by the police.

The views of the Information Commissioner and the Government

In May 2006, the Information Commissioner published 'What price privacy?' This report highlighted the existence of a widespread trade devoted to illegally buying and selling personal information causing significant distress, intrusion and harm to individuals. The report identified the insurance industry as one of the sectors with an apparent incentive to acquire confidential personal data, particularly in respect of suspect claims. While these activities already constitute offences under Section 55 of the Data Protection Act (the Act), the report proposed a substantial increase in penalties, including custodial sanctions.

In December 2006 the Information Commissioner published a further report, 'What price privacy now?' that set out the reactions from the media, the security industry, financial bodies and the Government to the initial report. Many organisations have taken positive steps to raise awareness and tighten security. The report explicitly acknowledged the work that the Association of British Insurers (ABI) has undertaken. The FSA has stated that compliance with all relevant legislation is necessary in order to meet the authorisation threshold criteria for firms to act in a fit and proper way. The Information Commissioner's Office (ICO) will be making the FSA aware of any regulated firms that are convicted of Section 55 offences. A conviction or a caution for a Section 55 offence may also be grounds for refusing or withdrawing a PI's licence, when the scheme run by the Security Industry Authority becomes operational.

In early 2007, following a consultation by the Department for Constitutional Affairs, the Government confirmed that it will legislate

to introduce custodial sanctions for Section 55 offences as soon as Parliamentary time permits.

Regulation of the private investigator sector

Insurance fraud is a problem that costs the industry's customers around £1.6bn a year. The vast majority of policyholders are honest and insurers will do all they can to protect their interests and may reasonably investigate suspect claims. However, they will not tolerate illegal access to personal information by those acting for them. Insurers expect the highest ethical and professional standards from private investigators and those acting for them. The ABI has supported regulation of the private investigation sector. Although this will raise costs for insurers, the industry accepts that it is key to raising standards and shutting out a rogue element in that industry.

Under the Private Security Act 2001, PIs will be licensed and regulated by the Security Industry Authority. Licensing is likely to come into effect in late 2008 and will help to ensure that PIs are fit and proper individuals that are competent to carry out their instructions. The competency criteria will not be insurance-specific, so the ABI is issuing these sector-specific guidelines to foster high standards among PIs. This will help to ensure that insurers are able to identify and take action on fraudulent claims swiftly, benefiting the insured population as a whole.

PRIVATE INVESTIGATORS (PIs)

Considering the use of a PI

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 and the information they can obtain is necessary to dispute it. When an insurer is considering whether or not to instruct a PI to investigate an individual, it should assess whether information gathering by the PI is required or whether it would be more suitable to investigate using other sources of information already available to the insurer.

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 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 way of confirming the validity of 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. For example, there are a number of research tools available to the insurer that can play an important role in the claims validation process. These include underwriting and anti-fraud databases such as the Claims and Underwriting Exchange (CUE), CIFAS (the UK's financial fraud prevention service), and credit reference agency databases.

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. Obtaining personal information knowingly and recklessly without the consent of the organisation that holds it, either by deception or bribery, is a criminal offence under Section 55 of the Act. An insurer instructing a PI to gather information that could only reasonably be obtained by these means may be committing a criminal offence, as will the PI.

Where another organisation holds information that is necessary for the insurer to investigate a fraud, and is not available from other legitimate sources, it should be approached directly by the insurer or its agent. It will then be for that organisation to decide whether or not to disclose the relevant information to the insurer or their agent. The organisation approached would have to be satisfied that they had a legitimate basis for the disclosure.

Before a PI is employed, an impact assessment should be completed, documented and retained. Suggested areas to be assessed include:

What are the insurer's grounds for suspicion?

The insurer should state why it believes that the claim might not be genuine.

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

A PI should only be used where there is reasonable suspicion that the claim is not genuine. The insurer should always consider what information it already has at its disposal, or may gain access to, before instructing a PI.

What information needs to be disclosed to the PI so that he can fulfil his instructions?

Only the minimum information necessary to allow the PI to perform their task should be provided to them. It may be inappropriate to inform the PI of the ailment that the claimant is suffering, particularly where this would involve disclosing sensitive data such as an actual illness. The insurer should instead generalise. For example, it should use descriptive terms such as 'restricted mobility', 'ability to drive', etc. But if the insurer is aware that the individual under investigation could endanger the PI, then the PI should be forewarned.

In some circumstances, it would be necessary to inform the PI of the illness, for example in cases of depression, panic attacks, chronic fatigue, incontinence or agoraphobia.

With personal injury cases, it is often necessary to disclose the location on the human body of the injury so that video footage is properly focused on the areas and activity relevant to the claim.

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

The insurer should only request the PI to obtain information that is reasonably necessary to establish the status of the claim and should not request information that could only be obtained by deception or bribery. As part of its impact assessment the insurer should consider what information is required and why it is justified.

This might include:

- 1 **Verification of the claimant's address** - the PI will usually need to verify where the individual lives, and that the person lives at the address supplied. This might be obtained by cross checking against the electoral roll. But remember that those most likely to consider making a fraudulent claim are those least likely to register on the roll. Moreover, it is not uncommon for individuals intent on defrauding insurers to deliberately provide a false address or register at the address of a friend,

neighbour or relative in a determined attempt to avoid surveillance. Not knowing the subject's address might lead to the privacy of an innocent person being breached if the wrong information is supplied.

- 2 **Photographic evidence** – the insurer should consider whether photographic evidence is required for positive verification
- 3 **Video evidence** - this might, for example, demonstrate the claimant's level of mobility or that the claimant is working. The original video tape should be from virgin stock (i.e. new and unused). If the insurer has a specific preference as to how it wants the video evidence edited, the insurer should stipulate this at the time of instruction.
- 4 **PI Report** – this might be required, for example, to register the claimant's movements.
- 5 **Other physical evidence** – such as advertisements offering services, invoices or receipts.

Entering into a relationship with a PI

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 and explicitly require the PI to do so.

It is strongly recommended that there is an appropriate written agreement between the insurer and the PI. It is difficult to see how without this an insurer could limit any additional use of the information, confine its disclosure and ensure its secure destruction at an appropriate time. Without such an arrangement the insurer could find it difficult to justify its compliance with the security requirements placed on it by the Act. At the very least the insurer should ensure that the PI adheres to a code of conduct. However, a code will be non-binding and provides less protection than a legal contract. The advantages of a formal agreement include that it:

- 1 Protects the insurer from financial liability in the event of the insurer being sued and risk to reputation.
- 2 Provides certainty as to the extent of the PI's remit.
- 3 Provides guidelines for the security of documents and information.
- 4 Forms a basis for recovering damages against the PI in the event of improper conduct by the PI

It should be noted that if a PI, when acting on behalf of an insurer, knowingly and recklessly obtains personal information without the consent of the organisation that holds it, this may be an offence under Section 55 of the Act. In these circumstances, the Information Commissioner will investigate both the PI and the insurer with a view to prosecution. For this reason, it is important that the insurer leaves the PI in no doubt that they are to obtain information by legal means

only. It should do this in its instructions and any ongoing contact around the investigation of the case.

Where PIs are operating only on the basis of insurers' instructions, they will ordinarily be data processors for those purposes. Their status will, however, depend on the particular circumstances of the service they provide the insurer. Where a controller-processor relationship exists, it should be documented in a contract. This could be part of the agreement referred to above. PIs will of course be data controllers in their own right.

The insurer should consider including the following provisions in any agreement entered into with the PI:

- 1 The PI company's employees engaged in the provision of the services should be suitably qualified, skilled, experienced, and trained. Many PIs would be involved in activities that are unconnected to claims investigations. So the insurer should ensure that the PI fully understands what is required of him in the particular case. The insurer might wish to establish what checks the PI company undertakes of staff prior to recruitment and should consider seeking references and specimen reports.
- 2 The PI company and its employees should hold any licences required by local legislation.
- 3 The PI company and its employees should act in accordance with all applicable laws, rules, regulations and codes of practice (hereinafter referred to generically as 'The Act') relevant to the services provided.
- 4 The PI company should hold adequate professional indemnity insurance. This reduces the risk borne by the insurer and provides a degree of comfort that the PI company has demonstrated a level of professionalism.
- 5 The PI should complete only the provision of services requested and retain the personal information involved for no other purpose.
- 6 The PI company should obtain agreement from the insurer before sub-contracting to an agent in fulfilling the provision of the service.
- 7 The PI company should take appropriate steps to 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 about the Act and the legal obligations that arise from it.
- 8 The PI company should take appropriate steps to ensure that its employees comply with the Act when obtaining, using and disclosing the data.
- 9 The PI company should take appropriate steps to ensure that neither it or any of its employees or agents shall use any data

other than in connection with the provision of services as instructed by the insurer

- 10 The PI company should have an entry on the register maintained by the Information Commissioner.
- 11 The PI company should hold all data in strict confidence and take all actions, and put in place appropriate security measures, necessary to protect that data from:
 - Any unauthorised or unlawful access; and
 - Any accidental loss, destruction or damage
 - Onward use and disclosure not associated with the investigation

The PI company should also return or ensure the secure destruction of the data when it is no longer required for the investigation, defence of the claim or potential further legal action

The PI company should notify the insurer of those measures on request. These might include steps that the PI company takes to maintain a clear chain of evidence, to store securely all original evidence and to safely dispose of evidence at the appropriate time.

- 12 The PI company should allow the insurer, on request, to carry out an audit of its procedures in respect of the data gathered under this agreement. This might be conducted at the premises of the PI company.
- 13 The insurer has the right to remove from the investigation employees of the PI company 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. Without prejudice to the insurer's right to pursue damages against the PI company in the event of improper conduct by the PI company, the insurer might also seek recovery of any interim fee payments made.
- 14 The PI company should inform the insurer, as soon as reasonably practicable, following receipt of a subject access request from a claimant and should assist the insurer in satisfying that subject access request.
- 15 On completion of the provision of services or on the renewal of the Service Agreement or after a set and agreed period, the PI should return all case material that is not active to the insurer.
- 16 The PI company should not transfer the data, or any part of it, to a country or territory outside the European Economic Area except with the explicit consent of the insurer.
- 17 The PI company should inform the insurer as soon as it becomes aware of any breach of the terms of the Act and advise the insurer of the steps that it intends to take to remedy that breach. The PI company should agree to keep the insurer

apprised as to the progress and completion of those steps. The parties should agree that if the insurer considers the breach to be a material breach of the Act, the insurer is entitled to terminate any agreement that it has with the PI company by notice in writing. Any outstanding instructions at the time of receipt of that notice should be regarded as cancelled.

18 There should be a time limit to the Service Agreement.

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

The insurer should also consider whether the PI has ever given evidence in court or at a tribunal hearing in connection with an investigated claim. It is worth remembering that 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 a surveillance log. Evidence contained within signed contemporaneous surveillance logs is acceptable in court in circumstances where there is no independent video evidence, for example, if a video tape is defective or where an evidential incident may have occurred which could not be documented by video footage.

Fair processing wording

The 1st Data Protection Principle requires data to be fairly and lawfully processed. This would ordinarily require the insurer to disclose to the customer all sources, uses and disclosures of personal data.

A PI will be instructed in order to verify an insurer's reasonable suspicions of fraud. Where PIs are not routinely instructed, a generic reference to the processing of 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 identity of the third parties should they make an enquiry of the insurer.

Where PIs are instructed routinely, the insurer should make that clear to customers in its fair processing notice. The insurer should inform the applicant / policyholder at the earliest stage that a PI might be used.

This might be in the:

- 1 Application form
- 2 Claim form e.g. a group contract where the insurer would not receive any personal data until the claims stage
- 3 Supporting documentation at the proposal stage

A third party claimant, for example, an employee claiming under a group policy or a third party motor accident claimant, should be notified in the initial letter from the insurer following receipt of the claim.

Instruction to the PI

The insurer should decide on the most appropriate medium for issuing instructions.

Sending information via facsimile transmission might be insecure and telephone instructions could be open to interpretation and lack any form of documentation. So it might be prudent for any instructions to a PI to be given in writing and sent securely (e.g. sent by recorded delivery). Alternatively, the insurer could send an email, with the instructions contained in an attachment that is suitably protected against unauthorised access (e.g. by encryption or, at the very least, password protected).

The instructions to the PI must be explicit and transparent, with the subject matter clearly documented. The insurer should request the minimum amount of information needed to gather evidence to support the insurer's suspicions.

The insurer should provide the PI with sufficient information as is necessary to ensure that the investigation focuses on the correct individual. The information provided to the PI should only be that which is necessary and relevant to identify the subject of their investigation and inform them of what type of investigation is required. This might include:

- 1 The claimant's name
- 2 The claimant's sex
- 3 The claimant's address (on file) [which the PI may be asked to verify]
- 4 The claimant's date of birth
- 5 The description of the claimant (this might be obtained, for example, from the nurses' report or other medical report)
- 6 Family circumstances
- 7 A description of the type of data required:
 - Photographs
 - Video recording
 - PI report
 - Original signed surveillance logs
 - Any other information that is reasonably required (and justified) in order 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.

8 Instructions on what to look for:

- The PI should not ordinarily be informed of the medical condition that the claimant alleges they are suffering from. The instructions should instead advise the PI to assess the way in which the claimant acts and may ask for evidence of particular activity. For example, the claimant might have difficulty lifting objects or should not be driving.

The claims handler and the PI might hold regular review meetings. This would help to ensure consistent standards of work, a mutual understanding of what is required from the investigation and provides a forum for providing feedback on the PI's work.

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.

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

- 1 The **reinsurer** who underwrites a proportion of the risk, and may be consulted on the appointment of a PI and as to 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.
- 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.

Retention of data collected by the PI

The insurer should consider the length of time that it might need to hold the data provided by the PI. The 5th Data Protection Principle 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. FSA 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 6 years following the cancellation of the policy or repudiation of the claim. It is vital that the insurer notifies the

PI when a claim has been settled/closed so that the PI can then take steps to dispose of the data securely. The insurer should allow sufficient time for an appeal to be lodged or disposed of.

TRACING AGENTS

Many of the requirements that would apply to employing a PI apply equally in respect of tracing agents. Most tracing agents are employed to find the beneficiaries of wills and do not involve insurers. However, insurers might trace 'gone aways' who are the beneficiaries of life policies.

When contemplating instructing a tracing agent, the insurer should follow the same process as when instructing a PI. The following steps should be considered:

- 1 An impact assessment should be undertaken to establish whether it is necessary to use a tracing agent.
- 2 If a tracing agent is to be instructed, the parties should enter into a written agreement including provisions that are similar to those involving an arrangement with a PI.
- 3 The instruction to the tracing agent should be secure, precise and specify exactly what information is to be obtained.
- 4 The insurer should apply the same considerations to a tracing agent who wished to sub contract as they would in respect of a PI.
- 5 The insurer should be the only party other than the tracing agent who has access to the data.
- 6 The tracing agent should destroy data that it has accumulated from its investigation within 3 months of providing the insurer with its findings. This would provide sufficient time to deal with any enquiries.

GLOSSARY

Blagging: A form of deception by which the ‘blagger’ pretends to be someone they are not in order to wheedle out the information they are seeking, usually by way of a series of telephone calls. Information that is obtained illegally is then sold on.

Data controller (Data Protection Act): A person who determines the purposes for which, and the manner in which, personal information is to be processed. This may be an individual or an organisation and the processing may be carried out jointly or in common with other persons.

Data processor (Data Protection Act): A person, who processes personal information on a data controller’s behalf. Anyone responsible for the disposal of confidential waste is also included under this definition.

Data protection principles: There are eight principles of data protection – these form the core around which much of the Data Protection Act is written. All data controllers must generally comply with all eight, even if they are exempt from notification. The principles are enforceable by the Information Commissioner.

Encryption: The process of obscuring information to make it unreadable without special knowledge, so that the information remains private and secure.

Fair and lawful processing: The first data protection principle requires data to be processed fairly and lawfully. For processing to be considered fair, individuals must be provided with certain information including the controller’s identity, the reasons that their information is being collected and any third parties it will be disclosed to. In addition, it is necessary that all personal data processing must comply with at least one of six threshold conditions. Where sensitive personal data is processed, including information about the health or the commission or alleged commission of an offence, additional considerations for processing must be met. For insurers, this will often be that the individual has provided explicit consent.

‘Gone aways’: A person who has left his/her given address since their data was added to the insurer’s customer contact database and their current whereabouts is not recorded.

Notification (Data Protection Act): The process by which a data controller’s processing details are added to the Information Commissioner’s register. Under the Data Protection Act, every data controller who is processing personal information needs to notify unless they are exempt. Failure to notify is a criminal offence. Even if a data controller is exempt from notification, they must still comply

with the data protection principles. The Commissioner maintains a public register of data controllers at www.ico.gov.uk. A register entry only shows what a data controller has told the Commissioner about the type of data being processed. It does not name the people about whom information is held.

Personal data: Information held in electronic and some highly structured paper files about a living individual who can be identified from that information and other information which is in, or likely to come into, the data controller's possession.

Private investigator: A person privately hired to do investigatory work, for example, to investigate suspicious insurance claims.

Processing (Data Protection Act): Obtaining, recording or holding the data or carrying out any operation or set of operations on data.

Subject access request (Data Protection Act): Under the Data Protection Act, individuals can ask for a copy of information about themselves that is held on computer and in some paper records. If an individual wants to exercise this subject access right, they should write to the person or organisation that they believe is processing the data.

A subject access request must be made in writing and accompanied by the appropriate fee. In most cases, the maximum fee will be £10, but this can vary. A request must include enough information to enable the person or organisation to whom the subject is writing to satisfy itself as to their identity and to find the information.

The request must be fulfilled within 40 days as long as the necessary fee has been paid. A data controller should act promptly in requesting the fee or any further information necessary to fulfil the request. If a data controller is not processing personal information of which this individual is the data subject, the data controller must reply saying so.

Surveillance log: Records or logs of incidents and activities carried out at specific times that serve as memory refreshing documents. They are used by private investigators when giving evidence and should be made on the understanding that they may be produced in evidence.

Tracing agent: Insurers may employ tracing agents to find people or assets, for example, beneficiaries under life insurance policies.



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

“C”

Secretary General Report



REPORT

- Secretary General -

2009

Vienna, Austria

Page 1 of 1

1. Membership

Once again there have been several enquiries over the past year. Six organisations have been granted provisional membership by the Executive which will be considered by Delegates for ratification; they are from Belgium, Portugal, Spain, Turkey, Austria and the CII.

The membership of IKD continues to grow as the world's single representative umbrella body currently made up of 24 National organisations, 2 world-wide organisations and 3 single members.

Problems over communication persist and the Executive now leave the onus largely on each member to take the initiative. Most information of vital importance, Minutes of Meetings and Notice of Meetings is published on the web site so members can monitor events. So too are the profiles for each member published on the web site and members are requested to periodically check that their respective details are up to date.

2. Common Minimum Standard

Efforts to move this project forward continue. The next step is to address the competence criteria. In this respect we have been in talks with ZAD and await their Business Plan and Proposals.

My own attitude to a CMS has been heavily influenced by what will take place in the UK. Whilst licensing should have been implemented by 2009 this has again been postponed currently to 2011/2. However, The Association of British Investigators has not stood idly by waiting for the regulations and has strengthened their own membership selection and criteria to create a feasible and respectable self-regulation alternative, include criminality check, professional indemnity insurance, competency testing and other requirements that mirror closely the IKD CMS template. The new elements are being introduced piecemeal and when finally implemented, anticipated by May 2010, then it may be a good model for the IKD to study as an international CMS.



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

“D”

Treasurer & Auditor Reports

IKD Financial Statement as per December 31, 2008

Balance Sheet

Assets

| | <u>2007</u> | <u>2008</u> |
|-------------------------------------|--------------------|--------------------|
| Bank balance (ZKB) | € 29'260.50 | € 24'214.10 |
| Outstanding membership contribution | € 0.00 | € 0.00 |
| Further assets | € 0.00 | € 90.00 |
| Total | € 29'260.50 | € 24'304.10 |
| | ===== | ===== |

Liabilities

| | | |
|-------------------------------------|--------------------|--------------------|
| Liabilities | € 0.00 | € 30.00 |
| Suspense liabilities | € 0.00 | € 0.00 |
| Association property as per Dec. 31 | € 29'260.50 | € 24'274.10 |
| Total | € 29'260.50 | € 24'304.10 |
| | ===== | ===== |

IKD Financial Statement as per December 31, 2008

Account of Expenses and Proceeds

| | <u>2007</u> | <u>2008</u> |
|-------------------------|--------------------|--------------------|
| <u>Proceeds</u> | | |
| Membership contribution | € 8'730.00 | € 9'820.00 |
| Further proceeds | € 0.00 | € 0.00 |
| Bank interest | € 282.31 | € 229.45 |
| Loss | € 3'442.94 | € 4'986.40 |
| | | |
| Total | € 12'455.25 | € 15'035.85 |
| | ===== | ===== |

Expenses

| | | |
|--|--------------------|--------------------|
| Expense account Secretary General | € 4'454.73 | € 3'821.35 |
| Expense account Vice Secretary General | € 3'906.27 | € 1'012.10 |
| Expense account Treasurer | € 711.80 | € 914.05 |
| Cost IKD Congress | € 280.00 | € 0.00 |
| Internet cost | € 1'728.00 | € 216.00 |
| Presents and donations | € 490.00 | € 117.00 |
| Cost Europe development | € 0.00 | € 8202.10 |
| Bank charges and tax on interest | € 284.45 | € 169.70 |
| Further expenses | € 600.00 | € 583.55 |
| | | |
| Total | € 12'455.25 | € 15'035.85 |
| | ===== | ===== |



Audit report 2008

As elected Auditor I conducted an audit of the books and financial records of the Internationale Kommission der Detektivverbände, IKD, maintained by Treasurer, Markus Wegst. This audit took place in my Office and the necessary documents were forwarded to me by the Treasurer. I reviewed all of the following documents:

- Bank Statements
- Payables and Invoices
- Financial Reports
- Cash Receipts Journal

I reviewed all of the records listed above from January 1, 2008 through December 31, 2008. All of the documents reviewed were correct and in order.

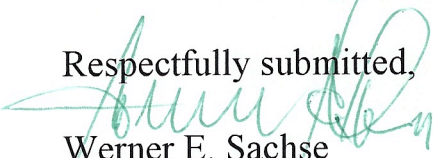
The balance as of 31 December 2008 was € 24.304,10, which is a decrease of € 4.956,40 compared to 2007. The income from dues has risen again. All dues have been paid.

Expenses for the General Secretariat were less again than in 2007. Expenses for the Vice-General Secretary were reduced to a third.

The Cost of Europe development (Saragossa and HABM fees) were € 8.202,10, a one-time-only item.

The Treasurer, Markus Wegst of Zurich, has done again an excellent job and the financial situation of IKD is good. I propose to extend the Executive Committee's recognition and thanks to the Treasurer.

Respectfully submitted,


Werner E. Sachse
Auditor of IKD Funds



**INTERNATIONALE KOMMISSION DER DETEKTIV-
VERBÄNDE**

**INTERNATIONAL FEDERATION OF ASSOCIATIONS
OF PRIVATE DETECTIVES**



MINUTES of Committee Meeting 2009

“E”

Model Data Protection Policy

Data Protection Regulation

European Union

MODEL POLICY FOR MEMBERS USE

Internationale Kommission der Detektiv-Verbände

Internationale Kommission der Detektiv-Verbände



www.i-k-d.com

1. The EU Data Protection Directive 95/46 enhances and broadens the scope of earlier regulations. Its purpose is to protect the rights and privacy of living individuals and to ensure that personal data is not processed without their knowledge, and, wherever possible, is processed with their consent, unless otherwise exempt.
2. This document is a model Data Protection Policy issued by the Internationale Kommission der Detektiv-Verbände for use by its EU members and their member agencies (*The Member*).
3. *The Member* complies with the requirements of the Data Protection regulations in force in *The Member's* jurisdiction with regard to the collection, storage, processing and disclosure of personal information and is committed to upholding the regulation's core Data Protection Principles.
4. *The Member* is committed to a policy of protecting the rights and privacy of individuals (includes staff, course delegates, and others) in particular the data subjects of investigations, in accordance with the Data Protection regulation.
5. *The Member* needs to process certain information about its staff, trainees, sub-contractors and other individuals it has dealings with as clients, subjects of instructions, for administrative purposes (e.g. to recruit and pay staff), and to comply with legal obligations and government requirements.
6. To comply with the law, information about individuals must be collected and used fairly, stored safely and securely and not disclosed to any third party unlawfully.
7. The policy applies to all data subjects. In the event of a breach of the Data Protection regulation or this Policy by a member of staff, *The Member's* employment disciplinary procedures will apply.
8. As a matter of good practice, other agencies and individuals working with and thus affiliated to *The Member*, and who have access to personal information, will be expected to have read and comply with this policy, the terms of which form part of the consultancy/agency agreement between *The Member* and that affiliate.
9. *The Member* is the Data Processor under the regulation, when dealing with its core business as an Investigation Agency and the client is the Data Controller.
10. *The Member* is the Data Controller under the regulation, when dealing with data of staff, clients, contractors, trainees and any other member or affiliate of *The Member* or in circumstances when The

Member determines the manner in which and the purpose for which data is processed. For this purpose *The Member* has duly Notified the Information Commissioner.

11. Compliance with data protection regulation is the responsibility of all members and their contractors who process personal information.
12. Each member of staff, clients, contractors, trainees and any other member or affiliate of *The Member* is responsible for ensuring that any personal data supplied to or handled by *The Member* is accurate and up-to-date.
13. Data Subjects have the following rights regarding data processing and the data that are recorded about them:
 - To make subject access requests regarding the nature of information held and to whom it has been disclosed.
 - To prevent processing likely to cause damage or distress.
 - To prevent processing for purposes of direct marketing.
 - To be informed about mechanics of automated decision taking process that will significantly affect them.
 - Not to have significant decisions that will affect them taken solely by automated process.
 - To sue for compensation if they suffer damage by any contravention of the regulation.
 - To take action to rectify, block, erase or destroy inaccurate data.
 - To request the Information Commissioner to assess whether any provision of the regulation has been contravened
14. Wherever possible, personal data or sensitive data should not be obtained, held, used or disclosed unless the individual has given consent.
15. *The Member* understands "consent" to mean that the data subject has been fully informed of the intended processing and has signified their agreement, whilst being in a fit state of mind to do so and without pressure being exerted upon them. Consent obtained under duress or on the basis of misleading information will not be a valid basis for processing.
16. There must be some active communication between the parties such as signing a form and the individual must sign the form freely of their own accord. Consent cannot be inferred from no response to a communication. For sensitive data, explicit written consent of data subjects must be obtained unless an alternative legitimate basis for processing exists.

17. In most instances consent to process personal and sensitive data is obtained routinely by *The Member* (e.g. when a member of staff or consultant signs a Service or Consultancy Agreement).
18. Any forms (whether paper-based or electronic-based), that gather data on an individual should contain a statement explaining what the information is to be used for and to whom it may be disclosed. It is particularly important to obtain specific consent if an individual's data is to be published on the Internet as such data can be accessed from all over the globe.
19. If an individual does not consent to certain types of processing, appropriate action must be taken to ensure that the processing does not take place.
20. All staff and affiliates of *The Member* are responsible for ensuring that any personal data (on others) which they hold are kept securely and that they are not disclosed to any unauthorised third party.
21. All personal data should be accessible only to those who need to use it. You should form a judgement based upon the sensitivity and value of the information in question, but always consider keeping personal data:
 - in a lockable room with controlled access, or
 - in a locked drawer or filing cabinet, or
 - if computerised, password protected, or
 - kept on disks which are themselves kept securely.
22. Care should be taken to ensure that PCs and terminals are not visible except to authorised staff and that computer passwords are kept confidential. PC screens should not be left unattended without password protected screen-savers and manual records should not be left where they can be accessed by unauthorised personnel.
23. Care must be taken to ensure that appropriate security measures are in place for the deletion or disposal of personal data. Manual records should be shredded or disposed of as "confidential waste". Hard drives of redundant PCs should be securely erased by overwriting the disc space before disposal.
24. This policy also applies to staff and affiliates of *The Member* who process personal data "off-site". Off-site processing presents a potentially greater risk of loss, theft or damage to personal data. Staff and affiliates of *The Member* should take particular care when processing data in other locations outside the offices of *The Member* or its affiliated locations.

25. Members of *The Member* and / or other data subjects have the right to access any personal data which are held by *The Member* in electronic format and manual records which form part of relevant filing system held by *The Member* about that person, subject to exemptions.
26. Any individual who wishes to exercise this right should apply in writing to *The Member* who reserves the right to charge a fee for data subject access requests. Any such request will normally be complied with within 40 days of the receipt of the written request and, where appropriate, the fee.
27. *The Member* must ensure that personal data are not disclosed to unauthorised third parties which includes family members, friends, government bodies, and in certain circumstances, the Police, unless authorised under the terms of the regulation or other statute or Court Order or where disclosure of data is required for the performance of *The Member's* contractual duty. All staff and affiliates should exercise caution when asked to disclose personal data held on another individual to a third party.
28. The regulation permits certain disclosures without consent so long as the information is requested for one or more of the following purposes:
- To safeguard national security;
 - Prevention or detection of crime including the apprehension or prosecution of offenders;
 - Assessment or collection of tax duty;
 - Discharge of regulatory functions (includes health, safety and welfare of persons at work);
 - To prevent serious harm to a third party;
 - To protect the vital interest of the individual, this refers to life and death situations.
29. For reasons of personal security and to protect *The Member* premises and the property of staff, trainees and other visitors, close circuit television cameras may be in operation in several areas. The presence of cameras may not be obvious. This policy determines that personal data obtained during monitoring will be processed as follows:
- any monitoring will be carried out only by a limited number of specified staff;
 - the recordings will be accessed only by approved personnel;
 - covert monitoring should only be carried out temporarily where necessary to address specific issues of a serious nature;
 - personal data obtained during monitoring will be destroyed as soon as possible after any investigation is complete;
 - staff involved in monitoring will maintain confidentiality in respect of personal data.

Definitions

Personal Data

Data relating to a living individual who can be identified from that information or from that data and other information in possession of the data controller. Includes name, address, telephone number, identity number. Also includes expression of opinion about the individual, and of the intentions of the data controller in respect of that individual.

Sensitive Data

Different from ordinary personal data (such as name, address, telephone) and relates to racial or ethnic origin, political opinions, religious beliefs, trade union membership, health, sex life, criminal convictions. Sensitive data are subject to much stricter conditions of processing.

Data Controller

Any person (or organisation) that makes decisions with regard to particular personal data, including decisions regarding the purposes for which personal data are processed and the way in which the personal data are processed.

Data Subject

Any living individual who is the subject of personal data held by an organisation.

Processing

Any operation related to organisation, retrieval, disclosure and deletion of data and includes: Obtaining and recording data. Accessing, altering, adding to, merging, deleting data Retrieval, consultation or use of data disclosure or otherwise making available of data.

Third Party

Any individual/organisation other than the data subject, the data controller (clients) or its agents.

Relevant Filing System

Any paper filing system or other manual filing system which is structured so that information about an individual is readily accessible. **Please note that this is the definition of "Relevant Filing System" in the regulation. Personal data as defined, and covered, by the regulation can be held in any format, electronic (including websites and emails), paper-based, photographic etc. from which the individual's information can be readily extracted.**

Principles - All processing of personal data must be done in accordance with the eight data protection principles.

1. Personal data shall be processed fairly and lawfully.

Those responsible for processing personal data must make reasonable efforts to ensure that data subjects are informed of the identity of the data controller, the purpose(s) of the processing, any disclosures to third parties that are envisaged and an indication of the period for which the data will be kept.

2. Personal data shall be obtained for specific and lawful purposes and not processed in a manner incompatible with those purposes.

Data obtained for specified purposes must not be used for a purpose that differs from those.

3. Personal data shall be adequate, relevant and not excessive in relation to the purpose for which it is held.

Information, which is not strictly necessary for the purpose for which it is obtained, should not be collected. If data are given or obtained which is excessive for the purpose, they should be immediately deleted or destroyed.

4. Personal data shall be accurate and, where necessary, kept up to date.

Data, which are kept for a long time, must be reviewed and updated as necessary. No data should be kept unless it is reasonable to assume that they are accurate. It is the responsibility of individuals to ensure that data held by *The Member* are accurate and up-to-date. Completion of an appropriate registration or application form etc will be taken as an indication that the data contained therein is accurate. Individuals should notify *The Member* of any changes in circumstance to enable personal records to be updated accordingly. It is the responsibility of *The Member* to ensure that any notification regarding change of circumstances is noted and acted upon.

5. Personal data shall be kept only for as long as necessary.

6. Personal data shall be processed in accordance with the rights of data subjects under the Data Protection regulation.

7. Appropriate organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of data.

8. Personal data shall not be transferred to a country or a territory outside the European Economic Area unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data.

Data must not be transferred outside of the European Economic Area (EEA) - the twenty-seven EU Member States together with Iceland, Liechtenstein and Norway - without the explicit consent of the individual. Staff and/or contractors of *The Member* should be particularly aware of this when handling data that may be published on the Internet, which can be accessed from anywhere in the globe. This is because transfer includes placing data on a web site that can be accessed from outside the EEA.

EU States – Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, Netherlands, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, United Kingdom.