GDPR

An Overseas Perspective

The Professional Investigator

Summer 2018

FULL SCREEN

The Institute of Professional Investigators

IPI
Jubilee House
3 The Drive
Brentwood
Essex
CM13 3FR

Tel: 0870 330 8622
Fax: 0870 3308612
Email: admin@ipi.org.uk

David Palmer FIPI
Editor

Contents

Annual General Meeting

Early Notice

The Board has decided that the Annual General Meeting will take place on the **26th of October** at **Regus House, Herald Way, Pegasus Business Park, Nottingham DE74 2TZ.** The event will convene at 10am for a 10.30am start. A buffet is available for anyone seeking to leave shortly after the event.

The venue is accessible by road in central UK rather than London, taking advantage of our Regus contract to reduce costs. If you can keep that date free and consider travelling to meet and greet your peers, we would like some advance notice of your intent so that we can ensure that the venue can accommodate those who attend. Please let us know at admin@ipi.org.uk if you already know you wish to attend based on the admittedly limited information provided.

James Harrison-Griffiths, Immediate Past Principal Passes Away

On the 4th of May 2018, our friend and colleague James Harrison-Griffiths collapsed while out walking. A passer-by was able to contact the Institute because Jim was carrying his IPI identification card, and we were able to contact his beloved wife Maureen as he was taken to hospital. Sadly, Jim passed away.

James Harrison-Griffiths FIPI

James W. Harrison Griffiths, Hon Life Member, Fellow and Immediate Past Principal. (friend, colleague, mentor and leader)

By Simon Smith FIPI

Jim was born in January 1946, the son of a senior Army NCO, at Colchester Garrison. Those who do not remember, nowadays, the trauma of War and its aftermath, will not appreciate how tough, mentally and physically, life was then. Fathers having nightmares, having to adjust to family life after years away, exacerbated, in Jim's case, by his father having been a Prisoner of War. His early life and that of his siblings, was typical of service families, uprooted to far flung corners, often at fairly short notice.

He was eventually settled in Cheshire where, after school, he initially worked in the Manchester Ship Canal Docks at the mouth of the Mersey, then busy Ports and before the conversion to Marinas and expensive flats. Seeing no immediate future other than toil and more toil, interspersed with a pointless existence, he followed in his father's footsteps in taking the Queen's shilling, adjusted for inflation.

The "cold war" was at its height, his duties placed him close to the front line, as it was in all but name.

He served over seven years in Royal Signals, achieving junior NCO status. Very rapidly, at initial training, he was recognised as above average, and earmarked for the more serious end of the Corps. he was stationed in Bahrain and Germany, and the Germany posting was important. The "cold war" was at its height, his duties placed him close to the front line, as it was in all but name. Jim never talked about this period as the Official Secrets Act requires, but he was deployed, literally, Yards or metres short of the wire, monitoring Warsaw Pact traffic, relaying information to the little known British Frontier Service and the "I Corps", as well as BRIXMIS, which readers are encouraged to reference for further detail. This was dangerous work, had the cold war gone "hot" they were, by their very nature, both

continued ▶

the canary in the cage for setting up warnings and, frankly, the first to suffer if positions were over run. It is hard, today, to grasp what sort of strain that put on to the job he did. He only acknowledged, to me, that, had it gone “hot” he’d have been one of the first casualties.

In 1974, he left the Army and successfully joined the Metropolitan Police. Save for a short transfer, in the mid-1970s, when he transferred to Cheshire to nurse his Mother, who was frail and alone, when he, selflessly, put his career on hold, went back to uniform and drove a “ Panda “ car, he spent the rest of his career with the “ Met “. As a DC, initially in Division, he saw the advantage of the concept of Criminal Intelligence, then in it’s infancy, and specialised in that when he could. He was one of the first to take courses and, ultimately, years later, help to design programmes for intelligence analysis. Of course, for those who were not there in the 1970s, it is hard to regard intelligence-led policing as other than routine but when Jim first espoused it, it was not universal. It recognised the interoperability of criminals, who would rob a Bank to fund a drug deal, whereas police structures were not so fluid. Divisional Collators, at the time, were a mixed bunch, some excellent, some ageing PCs, well past their prime, looking for non-shift work.

As an ex-Soldier, having been involved in basic Intelligence, he recognised the difference between Political and Military Intelligence and criminal

For those who were not there in the 1970s, it is hard to regard intelligence-led policing as other than routine but when Jim first espoused it, it was not universal.

intelligence. He wanted either to gain evidence or advanced knowledge of criminal activity so as to catch them red handed. His transfer to C11, subsequently SO11, was testament to this approach, and he subsequently became a Detective Sergeant in that post. He was transferred for two years to SO13, then the Anti-Terrorist Squad and returned to command the Special section of SO11 as it then was in the 1980s. On promotion to DI, in the early 1990s he was sent to Bethnal Green as DI, Proactive where, again, the value of information was the main criteria. By then, of course, DIUs were in place,

His promotion to DCI and training as an SIO in the Murder team was his last job. His team, based in his heartland of North East London, swept into the East End to clear murders

civilian analysts the norm, and computerisation used to track and trend. At Bethnal Green, he also stepped in as acting DCI when there was a personnel crisis and ran the entire Borough CID, as it had become. During the 1990s, a difficult time for the Met, gun and knife crime was high, Bethnal Green was a centre of gang trouble, drug dealing and associated robberies and burglaries. More Senior Officers at Area and Division levels were for TSG deployment, armed patrols and generally treating the area as a minor war zone. Jim successfully resisted this trend, kept TSG in its box, steadily promoting informant use, gathering the facts, slowly and surely bringing in the bad guys. A combination of old style methodical work and new style computer recording.

His promotion to DCI and training as an SIO in the Murder team was his last job. His team, based in his heartland of North East London, swept into the East End to clear murders. The writer remembers him from then, appearing at Poplar Coroner’s Court to brief the Coroner on the latest Murders. Most were crimes falling into the “operation Trident” category where, again, Intelligence is key to solution. Knowing who “ran with” who, and why. This also was where Jim showed his management skills. Once he had competent personnel, provably good at what they were doing, he was generous in both praise and ensuring their recognition for their work. He quickly built a team which solved every case they were

continued ▶

assigned, where all officers and civilian support staff felt valued. This, by the way, is the way he ran IPI as its Principal, years later.

On retirement, he ran his own small business, where he was effective and very helpful. He also built, around him, the contacts which facilitated others to achieve. His loyalty to his friends was legendary.

He was an IPI Member from October 2004, achieved Fellowship in 2012, spending hours on making our already excellent Course compliant with the whims of the Examining body, again painstaking work, hour after hour, interspersed with smoothing the way with people by getting the best out of them to achieve the goal. His motto, “You slide further on Bull **** than on gravel” was put to good use in meetings with the examiners. He appeared on behalf of the IPI on TV, at the Parliamentary Select Committee and, through Byron DAVIES, an Honorary Life Member and former Met Copper who’d become an MP, in trying to move the Home Office. A job that continues, lots of Bull being needed to move that monolithic lump.

Jim, himself became an Honorary Life Member in 2017, recognising all his work for IPI. As Principal from late 2014, he motivated the Board during times that were, initially, difficult in that there had to be financial control. His “no nonsense” approach was backed by his urging of appropriate members to step up and join the Board. (He told this writer not to complain unless he was prepared to try to help, a gentle but necessary kick up the rear end!)

He was an IPI Member from October 2004, achieved Fellowship in 2012, spending hours on making our already excellent Course compliant with the whims of the Examining body

He left the Board in October 2017, in better shape than he found it, having encouraged younger people to step up and do things

He left the Board in October 2017, in better shape than he found it, having encouraged younger people to step up and do things, having, as one of our Trainers, “talent spotted” new members who had come for the training and stayed, indeed, some now on the Board, and having been the constant support of money saving and money making. Ironically, his last training Course, as it transpired to be, was on the morning of his death. By all accounts, he enjoyed it, had a good chat with the candidates and invigilator, was happy when he left the venue. It appears that, as often when the weather was fine, he was walking from the Railway Station to his home, when he died. He enjoyed that walk, it was a nice day and we can hope that he remained upbeat.

James was a very committed family man, doting on his wife and daughter, who was the apple of his eye, and considered himself very lucky in that respect.

In his life, he achieved a lot. He put the bad guys away, we can ask for nothing more of a detective, he served his Country and his community, to us in IPI he was the no nonsense chap who’s support for what was right, and his people, was solid, he left everything he could better than he found it, and you cannot ask for more. If we can carry on the work, with the strong Board we have, then that will be his best memorial. He would want everyone to keep plugging on, do their best, step by step.

Bless him.

Other Board Members wrote:

I have only just got back from travelling and seen the terrible sad news about James. I am really moved by the loss. What a lovely man. We have lost one of life's true star's, a genuine and forthright man with a great sense of humour. There are not many people in my life that I can genuinely say that I always enjoyed being in their company but without doubt I can say that about James. He was a true role model. From a personal perspective I know that James, along with Simon, were the driving forces behind me not only becoming a member of the IPI but also joining the board and for that I will be eternally grateful. My thoughts are with his wife and family at this very sad time. **Brian Collins**

How very, very sad. A wonderful man who certainly gave me support throughout my time as an IPI member. He will be missed by all who had the pleasure of knowing him. **Susan Ward**

The first time I met Jim was at an AGM where I also met Simon, and it was within minutes that I realised that we had a dynamic duo who were to serve the Board magnificently over the next few years. Jim's sense of humour matched my own, as does Simon's, so we would shoot the breeze with some common recollections of misdemeanours and derring-do, putting the policing world to rights. Jim's most amusing tale for me was when he accosted a well-known gangster by arresting him with a firearm pressed firmly into the miscreant's lower back. Or, as Jim put it, his .45-calibre index finger.

Jim's dedication to the Institute matched Simon's and Jim Cole's – nothing was too much effort for his colleagues and peers. It was he who managed to do the work that converted a Manual and a course into a qualification, no small feat. He oversaw the exam-day Refresher Courses for us, making lots of friends, raising the profile – and the membership numbers – of the IPI as he did so.

Like Simon, I will miss Jim and his laconic sense of humour – I am so glad he never made ACPO rank! **David Palmer**

And a student wrote:

If you could forward my condolences to his family as I remember him talking time, especially to go through and test my knowledge in the pre-lesson leading up to the exam and was generally pleasant and helpful.

It made the experience of traveling to London to do my exam a little easier and more enjoyable. **Ben Youngs**

James' funeral took place in Brentwood on the 30th of May and was well attended by family, friends and colleagues from all over the UK. Your Board was well-represented by current and past members, too. Some amusing stories – the 'admissible' ones – were told, and some tributes and emotional speeches were also provided. On behalf of his daughter, Hannah, the poem 'My Father, My Friend' was read, and we left to Frank Sinatra's 'My Way' It was a fitting tribute to a lovely bloke.

British Standards Institution 2018 Review Update

By David Palmer FIPI

Members will by now be aware that the Institute chairs the BSI panel for the review of BSI 102000-2013 British Standard for the Provision of Investigative Services. This document remains the source document for the SIA in terms of business registration, and while smaller firms may not seek 'inspected status', they may conclude that compliance through membership of a professional body such as ours will be desirable if/when licensing and registration become a reality.

Earlier this year we announced that the BSI Standard Review draft was available for comment. Three people had provided 17 comments on the draft, which the panel reviewed on the 25th of June. From the author's perspective some were a bit pedantic and some were quite reasonable observations. The results of the final panel's musings were that some changes were called for and were made at the meeting. Such changes were essentially cosmetic and need not be detailed here, but there was a lot of discussion – and I mean a LOT – about the influence of BSI 7858 on the vetting of people working in a secure environment.

The issue had arisen in part because this standard was for people working in a secure environment and not in the security field, an important distinction. The SIA wanted it kept in, which would have meant that someone seeking BSI certification would have had to spend an extra couple of hundred on buying and complying with it. They see it as a cross-sector vetting standard, which is not an unreasonable aim, but it seemed to half of the attendees that it was excessive for our sector's needs – imagine having to vet yourself or have yourself vetted at cost (in a one-man consultancy), or paying for the vetting your business partner with whom you'd spent 30 years in CID. The final result was a compromise whereby compliance with a '7858 Light' that is detailed in the Standard would be acceptable, while compliance BS7858 would still be desirable.

The issue had arisen in part because this standard was for people working in a secure environment and not in the security field, an important distinction

The final draft, if approved, will be circulated for final publication soon after the 6th of July. Those who already hold certification will be pleased to note that nothing spectacular has been added that requires investment in a new copy before re-inspection. In fact, the only major addition was the 'definition' of investigation provided by the IPI and edited with the input and assistance of the panel.

As an individual, I have to say that the experience and quality of the debate, listening to some excellent professional, researching the answers to questions raised and having to fight our corner has been an absolute pleasure.

SIA Finally Publishes It!

This just in as of the date of preparation. The SIA has finally got around to publishing its 2016 Review. The introductory paragraphs say:

"The Review concluded that the PSI is an important part of the economy in how it protects people and property. It can also make a significant contribution to public safety, protection of the vulnerable, and national security. The Review found that the risk profile across the public safety, safeguarding and national security spaces regulated by the SIA have all increased, and that effective regulation of the PSI will help mitigate that risk.

The Review made the following recommendations. (Edited for relevancy. Ed.)

R1. Regulation of the Private Security Industry – In general the PSI operates effectively, and regulation plays a large part in this. Regulation is still required; it should be retained and improved.

R2. Performance of the Regulator – The SIA has performed to a satisfactory standard as a regulator and should be retained, but now is the time to focus on how it can make changes to achieve regulatory best practice.

R3. Improving Standards – A systemic and systematic approach to securing and improving standards should be the focus of the regulatory system. The SIA should be given the necessary tools, including sanctions, to lead the industry improving.

Subject to mandatory business licensing. Business licences should only be issued to companies who meet the voluntary revised Approved Contractor Scheme (ACS) standards

R4. Risk Based Approach – The SIA should improve its risk-based approach to PSI regulation. In turn the SIA should reduce regulatory burdens where appropriate.

R6. Business Licensing – All businesses offering security services, whether operating under contract **or operating in-house**, where there is a risk to public protection, safeguarding and national security, should be **subject to mandatory business licensing. Business licences should only be issued to companies who meet the voluntary revised Approved Contractor Scheme (ACS) standards.**

R7. Approved Contractor Scheme (ACS) – The current ACS needs to be refreshed and strengthened. It should be streamlined with existing industry schemes and enhanced to provide a single set of graduated (bronze/silver/gold/platinum, or similar) standards offering buyers clear differentiation. ACS should be industry owned and administered, with the SIA setting standards and overseeing compliance.

R8. De-regulation – While remaining focused on risk, the SIA should develop a strategy to enable

continued ▶

individual licensing to be progressively replaced with business licensing where it is safe and appropriate to do so.

R10. ***Private investigators – Private Investigators should be treated as businesses and subject to the revised ACS."***

At this time the Board has yet to discuss it – it is literally hot in the Editors hands – but your observations to ipitrain@aol.com will be considered.

One thought – as the PSI Act refers consistently and repeatedly to individuals being licensed, are they proposing a change in the Act to accommodate that change to Parliament's stated intention? And whose idea is it? I'm guessing it hasn't come from a sole trader or small business.

The full 76 page document outlining the results of the 2016 Review completed by the SIA is available at **https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/703258/Security_Industry_Authority_Review_2016-17.pdf**

but we have reproduced the final 2 paragraphs from the investigation section, which reads as follows and indicates a willingness, albeit tardy and probably further delayed by Brexit:

"Private investigators are licensed in the USA, Canada, Australia and New Zealand though in most of these countries the regulatory regime varies by state. In Europe, there are a range of approaches to regulation, with at least some countries such as the Netherlands regulating private investigator companies. The Republic of Ireland has recently introduced regulation and it will be useful to learn from their experience both in preparing for regulation and the effect of the introduction of regulation.

There is therefore a case for introducing regulation, supporting the Home Secretary's earlier commitment during the previous coalition Government. The SIA should keep under review the need for regulation of certain sectors. Coupled with potential deregulation elsewhere within PSI, the potential exists to allow regulation of the private investigation sector. Departments such as DCMS would need to be consulted to identify the best approach to defining PIs and distinguishing them from those the Government would not wish to regulate. Current provisions in the 2001 Act may need to be reviewed, and the Home Office may wish to introduce legislation to proceed with regulation."

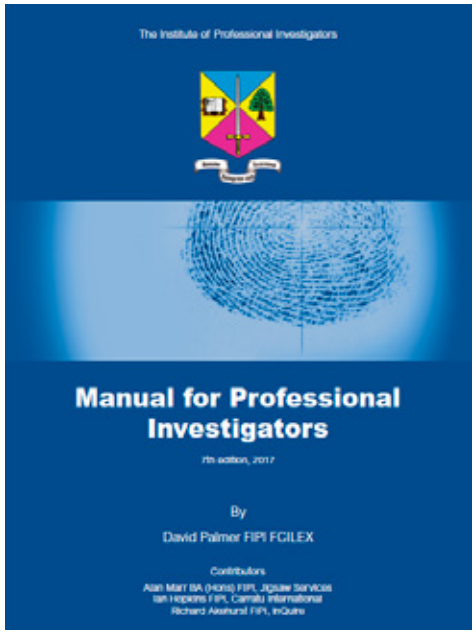
In due course we will read it fully and perhaps take action with a view to making our feelings known – particularly since WAPI and the ABI get a mention and we don't, despite our slightly more active role in deliberations since 2001!

Our thanks to Richard Cumming FIPI for attending the Security Commonwealth meeting at which the full document was discussed and made available.

IPI Manual Updated

Following enactment of The Data Protection Act 2018 the IPI Manual has been updated, as has the training course. It is available from the IPI Website and is frequently edited to take into account any legislative changes.

http://ipi.org.uk/investigator-publications



Byron Davies Awarded Honorary Fellowship of the Institute

Byron Davies, an MP that lost his seat in Theresa May's badly thought through 2017 election, has been awarded an Honorary Fellowship of the Institute.

Byron was a member of the Institute some years ago. He was educated at Gowerton Boys' Grammar School and holds an honours degree in Law.

He served as a Police officer with the Metropolitan Police, and gained extensive experience on secondment to the EU advising on organised crime and helping prepare countries for accession.

He represented South Wales West in the Welsh Assembly from 2011 to 2015.

Byron wrote:

"Dear Simon,

Firstly, a huge apology for the delay in responding to your correspondence awarding me the Honorary Fellowship of IPI. The correspondence has been on a circuitous tour of Wales in someone's briefcase but eventually reached me just recently.

Can I say how delighted and frankly humbled I was to receive this and I would naturally like to pass on my sincere thanks to all concerned at IPI. I have great admiration for the work undertaken by the organisation and those who ensure that the highest of standards are maintained in this area of work.

As you know, I failed to get returned to Parliament last June after a particularly nasty campaign against me by Momentum on social media, the participants of whom choose to remain anonymous. That said my belief in democracy remains and who knows what may be around the corner!

Keep up the good work and I look forward to remaining in contact and providing any assistance to IPI that you may consider useful.

With very best wishes and thanks to all at IPI,

Byron"

WAPI Investigator Workshop

On the 26th April 2018 Brian Collins MIPI, Board Member, attended the Investigator work shop run by Apex Seminars on behalf of WAPI. He wrote this report.

The event was well organised with excellent communications pre-event. The event consisted of two guest speakers, each with a 2½ hour slot. This was all delivered to approximately 35 delegates.

The two speakers were;

- GDPR Best Practice - Ray Snow
- OSINT Techniques - Neil Smith

We were given the following biographies in relation to the two speakers;

Ray Snow - GDPR-BEST PRACTICE
Ray Snow, a GDPR Practitioner from Thrive2Distinction, became a successful business owner by managing his own IT support firm specialising in the legal industry. Ray is now utilising his thirty years of knowledge and experience to assist businesses in achieving GDPR compliance for which the deadline is 25th May 2018. Ray's UK and Corporate International business experience have enabled him to understand how various business sectors need to adapt their processes and marketing in order to meet the May deadline.

Ray's unique understanding of IT structures and cyber security are a valuable asset when ensuring that the new laws and procedures are now leaving companies open to significant fines. Ray has studied both the principles of compliance and legislation when designing processes that help businesses function effectively within the law.

Ray Snow

Ray's presentation was constantly interrupted as he batted away and answered every query from the floor including interpretation of principles, contracts, terms of agreements, data controllers, penalties, fines, blagging ...

His presentation showed that he is a very knowledgeable individual who has clearly developed an outstanding knowledge of the principles of GDPR. His presentation was limited due to the time he was allotted to deliver on a wide-ranging subject. I found the input invaluable not having spent sufficient time self-researching GDPR. Ray gave what I would describe as a high-level overview rather than a workshop approach. I can fully appreciate why this approach was taken. He was addressing a receptive audience of investigators but within this field the roles varied considerably from groups of corporate investigative teams to sole trader investigators, and where the can of worms was opened Ray took incoming fire from every angle as everyone started to work this little bit of new acquired knowledge into their own particular work scenarios. Ray's presentation was constantly interrupted as he batted away and answered every query from the floor including interpretation of principles, contracts, terms of agreements, data controllers, penalties, fines, blagging and, inevitably, it did cover vehicle tracking.

continued ▶

Ray did include regular Q&A sessions which were answered by table groups. This enabled each subject to be reinforced; however, it also had the downside of introducing debate after answers were presented and explanations challenged.

Ray finished about 30 minutes over his allotted time and in reality, he could have covered the subject all day and he still would have fielded multiple questions as it was quite apparent that neither legislation or the ICO can yet provide answers to many of the questions raised.

Overall an excellent presentation but needed more time.

On to Neil Smith – OSINT Techniques

After serving over 10 years as a police officer in a UK police force and then spending time working as a counter-fraud specialist for a government department and as a fraud investigator for insurance companies, Neil has spent most of the last 14 years as a full time investigative researcher for a mixture of clients, from insurance companies to law enforcement agencies and journalists.

During these last 14 years Neil has also taught many hundreds of investigators, mostly from law enforcement but also from local authorities and insurance companies, as well as private investigators and journalists, in the art of using the Internet as an Investigative Tool. These courses have mostly been in the UK but have also been given in a number of different countries around the world.

One of the most valuable sites was a free site run by Neil's company Qwarie, I have used it on a number of occasions since the course www.uk-OSINT.net

Neil also regular speaks on the subject of Open Source Intelligence and in Using the Internet as an Investigative Tool at a number of conferences and events both in the UK and around the World. to groups from law enforcement, local authority investigators, commercial & corporate investigators and people from the compliance and insurance industries.

In 2016 Neil helped form Qwarie (www.qwarie.com) to build on what he was doing previously but in a bigger company to offer OSINT research and training to more clients around the world. As well as having a team of full-time in-house researchers, who undertake online enquiries for our clients, Qwarie now has a number of trainers to deliver OSINT & Cybercrime courses around the world.

OSINT

The approach taken by Neil was far more relaxed and interactive. He is a vastly experienced investigator and expert in his OSINT field. Rather than working to a clear structure he put it to the floor to fire questions at him that we felt could assist us in our roles in relation to the lawful application of OSINT research.

I have to say that I consider myself relatively computer literate and I always thought I was able to assist clients with a reasonable standard of OSINT research. I know now that I am an absolute amateur at it having seen from Neil what can be achieved without the tools of GCHQ or the NSA! It was truly

continued ▶

an eye opener - all legal and even GDPR compliant.

The presentation had a really good mix of questions answered and practically demonstration to reinforce the answer. We covered enhanced Google searches, Facebook, historic Facebook entries, cached versions, Twitter searches, twitter user locations, Skype searches and financial research. We were provided with various useful websites, some free, some paid for and some very expensive that could achieve various results for us. One of the most valuable sites was a free site run by Neil's company Qwarie, I have used it on a number of occasions since the course, so I would also recommend it; www.uk-OSINT.net.

Overall, I would say this was again an excellent workshop presentation by an expert in his field. I would add that Neil could easily have filled a whole day and his audience would still have been left wanting more time with him. His value to us as Investigators in a social media world cannot be underestimated. Many hours sat in watching front doors could be saved if we truly harness the capabilities of OSINT.

I would like to thank Apex seminars and WAPI for putting on a really useful and relevant workshop day which I would recommend to my fellow investigators.

Apex Seminars can be contacted at:
andy@apexseminars.co.uk

WAPI can be contacted at:
mail-generalsecretary@wapi.com

Brian Collins MIPI

A Bit of History

From John D Grant Companion and Fellow

Newer members may not know, and older members may well have forgotten, just how much work the Institute did and does on their behalf. John recently sent me a paper outlining some of the major work done in the early days.

In 1976 he, and the Institute, engaged a Parliamentary Draughtsman – no cheap feat – to assist us with the drafting of the Private Investigators (Registration) Bill 1984, which received support from 182 MPs, the Law Societies of England, Wales and Scotland, the Police Federation and many other important organisations and individuals. Unfortunately, the Bill wasn't introduced, in part due to lack of Parliamentary time.

When the Leveson and Home Affairs Select Committee went through their motions in 2011-2012, John responded to the latter with his own submissions, at 75 years old still showing an active interest in the process of licensing for the industry. He submitted responses still in his capacities as founder of the Scottish Investigators' Forum, including a specific response to the Scottish Parliament when they considered their own introduction of licensing north of the border. In fact, it was a petition based on the fact that there were some differences between the two separate legal systems. In addition, John submitted responses to The Younger Committee on Privacy (1972); the Consultation Paper relating to the Code of Practice under the Crime and Punishment (Scotland) Act 1997; to the Scottish Legal Aid Board Proposals for Private Public Defence Solicitors Office (1997); the Data Protection Act 1984 and 1998; the Draft Criminal Legal Aid Fixed Payments (Scotland) Regs (1998); The Scottish Law Commission Breach of Confidence (committee) in 1977 and 1982; The Scottish Law Commission – Right to Privacy; The Private Security Industry Discussion Paper (1979), a Response to the Government's proposals for the Private Security Industry (1999); and a number of recommendations and reports to the Scottish Justice Department, and submissions to the Joint Security Industry Council, SITO (now SfS) and other agencies.

The IPI continues to liaise with bodies on your behalf and welcomes input and support from the membership.

Data Protection – the new Access Provisions

As reported in the24th May Newsletter the Data Protection Bill is now an Act. It was granted Royal Assent on the 23rd of May 2018 – just in time for GDPR

The bill can be downloaded from: http://www.legislation.gov.uk/ukpga/2018/12/contents/enacted

The Editor's LinkedIn readers may be aware that as of the 23rd of May, the only person who knew the following was him, as despite requests that his employers enlighten its 800+ investigators about the new access provisions, they were still only disseminating information designed to avoid organisational responsibility for failings to comply with subject access requests, and about ill-advised opinions. How to obtain information was not being disseminated, possibly waiting for the College of Policing to publish its own advice – again, not received as of the 23rd of May.

My question was - after GDPR/DPA, what replaces Ss 29 and 35 of the old Act? In fairness, the following was provided to the Editor, who disseminated it locally.

For ease of reference for investigators, the following is a comparison chart.

The comparison table will help you find your way through the familiar exemptions via which investigators already obtain or disseminate data. This has been edited as the original chart because the original chart was based on the Bill and not the final Act. Apart from that note, the chart has been accepted on trust save the references to Ss29 and 35.

The comparison table below will help you find your way through the familiar exemptions via which investigators already obtain or disseminate data

Comparisons between DPA 1998 and the DP Bill (GDPR)

DPA 1998	Data Protection Act 2018
Third party data - SAR - Section 7(4) & 7(6)	Schedule 2, Part 3, 16(1 -3) (relates to NOT having to disclose)
	Part 3 exemption - Part 3, Chapter 3, 44 (4) (e)
Section 29 (general) e.g. crime and taxation	Schedule 2, Part 1, section 2(1)
Section 29(3) – which seems to be the same general exception under 29?	Schedule 2, Part 1, section 2(1)
Section 35(1) - disclosure by law (releasing data)	Schedule 2, Part 1 section 5 (1 - 3)
Section 35(2) - disclosure for legal proceedings (obtaining data)	Schedule 2, Part 1 section 5(3)

continued ▶

Please read the Act yourselves – the Editor believes the following to be accurate but is not an expert in this field and the chart may also be incomplete for readers' purposes.

As an aside, your Editor has spent the last 5 months chasing his employer for GDPR/DPA information, concerned that all would be left to the last minute. On the 31st of May – 8 days after the DPA came in - he was tasked to obtain medical records of a deceased party. The documents were produced, but only after the provider checked with the ICO the request to ensure that my enquiry was GDPR-compliant, only to be asked whether my request was 'excessive'. Now, given that the DPA does NOT apply to the dead, why they should ask if my request was excessive I do not know. Neither did the controller, who accepted the logic of my request.

In addition (and as expected) the organisation still only had a S.29/35 Request Form available (I edited it to make it compliant myself). In conclusion, therefore, and as expected – the role of an investigator in that organisation, and the need to obtain data lawfully, has been forgotten about in favour of the more urgent 'protecting the organisation' from errors it may never make. Despite the fact that BOTH could have been addressed more than adequately in the past 5 months.

Other stories abound. On the 12th of June I attended a doctor's surgery. Considering the GDPR and the aforementioned experience with a surgery who checked before assisting, I was amused to see a big screen upon which Mr Matthew Jones' name was displayed, along with the fact he was to go to treatment with Carole. I now knew that Mr Jones was at that surgery, could take a photo if I was clandestinely interested. I could probably identify Carole's specialism (if she had one) and thereby potentially deduce Mr Jones' ailment. I could follow him out to his car, perhaps. And so on and so on.

The sender cc'd in all other freelance representatives whose services they use , therefore disclosing my email address to about 60 other people and providing me with the email addresses of all the other freelance representatives used by their firm

And an IPI colleague who shall remain nameless to avoid identification through non-compliance with GDPR, wrote, "We have had a number of GDPR letters to sign in relation to client's data in relation to when we accept instructions from solicitors when we , as freelance agents, represent their clients in xxxxx. We had to sign too, re confidentiality; 'keeping all data secure and not passing on to a third party without the client's authorisation.'

I had to smile when I saw that the sender who had sent the email had cc'd in all other freelance representatives whose services they use , therefore disclosing my email address to about sixty other people and providing me with the email addresses of all the other freelance representatives used by their firm !! When I brought this to her notice she said she did not realise that everyone's details would be seen by all the other recipients - and she signed herself off as the 'GDPR Compliance Co-ordinator ' !!

You really don't have to make things up.

An Overseas Perspective on GDPR

By Michele Palmer FIPI CII and R. Palmer

(Please note the following article is published in entirety and should not be read as accepted or disputed by the Institute of Professional Investigators.)

We are NOT lawyers; we are NOT offering this as legal advice; and, we encourage all the members to investigate these issues themselves. Rather, we are simply providing you with the information we have encountered to date, as we are currently negotiating agreements with EU partners. We are hoping to encourage open GROUP discussion of these matters.

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union (EU)and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). The 261-page English language version of the document has 99 articles, is vaguely written in several areas; and should be used in conjunction with personal data protection laws for each EU member state – many of which are still being drafted and/or amended. This still imperfect combination of laws carries with it large penalties for persons and companies around the world who process personal data regarding EU residents. Aside from imposing many complex and rigorous requirements on investigators and those ordering such investigations on a world-wide basis, these legal requirements and penalties are enforceable throughout much of the world – certainly in North America.

As was recently written by an Israeli tech company security officer, "While much has been written about GDPR's rules, sanctions, and fines, it appears GDPR is often treated as if its effect is equal to any company regardless of size. On paper, it seems that any company that violates the new data privacy regulation will suffer the same international sanctions. GDPR, however, will not have the same effect on every size company. *For smaller companies, the smallest fine could likely be like a death penalty.*"

The majority of the professional investigators effected by the GDPR are NOT multimillion dollar companies with their own dedicated IT security staff, legal staffs or even affordable and constant access to a consultant on GDPR matters. Therefore, understanding even some major concepts of the GDPR is critical to the survival of our companies and our industry. It also illustrates what happens when a bureaucracy pursues extreme data protection without considering how this can damage the rights of self-protection of its citizenry and its effects on the investigative industry. We do not address all of the requirements stemming from the GDPR such as data storage, secure transport of the information, extensive logs of all actions, and reporting data breaches. While the penalties for these issues are equally punitive, we tried to restrict ourselves to the key areas in which we believe non-EU investigators will encounter the most likely conflict in accepting this law.

For smaller companies, the smallest fine could likely be like a death penalty

I would like to thank the many colleagues who responded to our first email – to the group as well as offline directly to us - regarding our suggestion for a discussion of the impact of the GDPR on our industry and the membership. We would like to reiterate that we are not experts in this subject matter and are only looking to start a professional group discussion of what this law will mean to the investigative industry.

continued ▶

To be more explicit, we are attempting to look at a new law in the EU and determine how it will affect the investigation industry – as well as non-EU investigators, because that is what we are. Recognizing that this is a new law that has quite apparently not yet been fully analyzed, we noted that several respondents provided answers that were contradictory – each claiming to have the real insight. Therefore, we encourage the members to reply to the membership on this link so that we can consider all the views on these questions.

Simply put, we are looking for ways to work with our EU colleagues, without endangering them, ourselves, or our businesses. I believe that most non-EU investigators do not do enough business in or for the EU to justify hiring lawyers, consultants or attending classes at professional conventions. It is a simple matter of cost versus benefit.

Therefore, we need to attempt to work together to discuss these matters if we are to keep these professional ties alive and healthy.

In the past, non-EU investigators could simply rely on their EU based clients – usually EU based investigators or lawyers – to direct the investigation in such a way as to be in conformance with national and EU laws. However, this has now changed into a situation in which the GDPR and other new and/or evolving national data protections laws may not be clear to the client (Controller or Processor in GDPR speak). Further, there is also the matter that several national jurisdictions within the EU may be involved – of which the clients may not be totally expert.

While the penalties for these issues are equally punitive, we tried to restrict ourselves to the key areas in which we believe non-EU investigators will encounter the most likely conflict in accepting this law

Consequently, we would like to comment on our observations of the responses we received and then specifically address some questions that we believe could be of interest to the entire membership. With that in mind, a few key points became apparent in reading these responses.

Basic Terms

From the UK ICO online guide noted below, "Data Controllers and Processors: The Data Controller is usually the client who requests the investigation. The Data Processors are usually the investigators and sub-contractors who process the PII and other personal data. The GDPR refers not only to the establishment of data controllers, but also of data processors (i.e. of the entity that processes personal data on behalf of the data controller) which, if located in the EU, triggers the applicability of EU data protection laws, regardless of where the data processing (e.g. location of the servers) takes place." Sub-data processors would be sub-contracting investigators to the primary data processor. The "Instructing Attorney" may or may not be the Data Controller.

According to the GDPR:

- a Controller is a natural or legal person or organization which determines the purposes AND means of processing personal data; and
- a (Data) Processor is a natural or legal person or organization which processes personal data on behalf of a controller.

According to the GDPR, a Data Processor has specific legal obligations which require you to at least maintain records of all personal data and processing activities and you will be responsible for any personal data breaches.

Data Controllers have similar legal obligations as well as for ensuring that all contacts with the Data Processors are documented and comply with the GDPR.

Personal Identifiable Information (PII) is any data that could potentially identify a specific individual. Any information that can be used to distinguish one person from another and for de-anonymizing anonymous data, can be considered PII. (The term PII and personal data are often interchanged. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people. It can also include IP and MAC addresses, cookies and RFID tags; all of which can be combined with

continued ▶

unique identifiers and other information to identify data subjects.)

There Is Still Considerable Confusion About The GDPR

We found it interesting that several respondents seemingly experts and consultants on the GDPR, had opposing views on aspects of the law. In fact, it is estimated that 50 % of all EU firms still have "major information gaps" regarding the GDPR. We presume this will continue for some time, but we hope that an open discussion of the law will smooth out some of these conflicts. I believe that is all new and it is a game changer for many us outside of the EU. Therefore, it is incumbent on us non-EU members to try to get a handle of this as soon as possible. After all, this appears to be a murky area and there are several unsettled areas – as was shown by many of the responses received, containing contradictory information re the GDPR. We also know that some EU member states are currently revising their data protection laws to come into better conformance with the GDPR.

As an example, one respondent wrote "Despite supposedly being a unified legislation, organisations (sic) will still need to consider local laws in deciding how to process personal data under GDPR. While it's doubtful that a company would get away without some form of penalty if caught processing information from one EU country in another EU country with less restrictive legislation, there will undoubtedly be some that try."

In fact, it is estimated that 50 % of all EU firms still have "major information gaps" regarding the GDPR

Therefore, it is a matter of professional prudence to ensure that we non-EU members have a more thorough understanding of the GDPR (and related laws) for which we will be assuming a higher level of liability and serious penalties than ever before.

Question

We have seen two different views on the question of whether a notice of GDPR compliance is required at the bottom of each professional email by an investigator who handles GDPR personal data.

Can anyone confirm this to be true?

Does the organisation have any suggestions as to what notice would satisfy this requirement – if it is true?

The GDPR Is Not New

The general tenor of several of the responses of the EU based investigators re the GDPR was that "this is not new for us" or "we have been doing this for years" or "our national laws are even more stringent". As I pointed out in my first email (OBSERVATION #1), we understand that the GDPR was actually passed two years ago, and we are also aware that there are various data protection laws in individual states of the EU.

I was born and raised in Europe and we have done business there for well over 30 years. We are generally aware of the various Data Protection laws, although we usually count on our European partners to ensure that their requests meet ever changing local and EU standards. Conversely, we do not expect members outside of the U.S. to be expert on our laws. In the past, we have counted on our European partners to be aware and cognizant of their state and EU laws. However, the GDPR is a game changer in that it attempts to create legal liabilities for us outside of the EU.

Therefore, as our EU based colleagues have a "head start" in looking at this matter, our observations below are addressed to both EU and non-EU based investigators. We believe many of the latter will be surprised at the responsibilities and obligations resulting from EU law(s) and how their liability can be drastically increased based upon the contracts required as well as the judgement of the primary client or investigator ("controller") who initiates and manages the cases.

All Investigators Are Aware Of The GDPR And Its Requirements

There appears to be a prevailing perception that if the EU members are aware of these laws, the rest of the members are as well. That is certainly not the case. I am willing to wager that over 90 % of the non-EU members are NOT aware that the GDPR will add legal liability and very specific data processing

continued ▶

requirements when investigating an EU subject for whom the GDPR applies. While some professional organizations have had some excellent general articles regarding the GDPR, there are several areas yet to be touched on and that should be brought to the attention of the general membership.

The GDPR Will Probably Not Go Into Effect On 25 May

In this same vein, several respondents opined that the GDPR will not go into effect on 25 May, and it may be some months before it actually goes into effect. The point is that the new GDPR - will de jure if not de facto - go into effect on 25 May 2018. This new law attempts to extend the EU laws to control the activities of investigators outside of the EU. That is a fact that cannot be avoided or ignored. The details may not be worked out and enforcement may be spotty at first, but like any bureaucrat or lawyer will tell you – that is the "effective date". Any alleged violations will be considered as being valid any time after May 25. I doubt there will be any official "grace period".

The Need For Additional Contracts

Several respondents stated that there is *no need* for additional contracts. We are currently dealing with three different partners in the EU and each is asking for additional agreements. You will note that the key resource GDPR EU.org "Web learning resources for the EU General Data Protection Regulation' located at https://www.gdpreu.org/the-regulation/key-concepts/ recommends that new contracts be negotiated with all processors (vendors) to insure compliance with the GDPR.

This new law attempts to extend the EU laws to control the activities of investigators outside of the EU. That is a fact that cannot be avoided or ignored.

Further, according to the GDPR, there must be a written Data Processor Agreement (DPA) contract when one business processes personal data on behalf of another business, which obligates the businesses to at least comply with the absolute minimum legal requirement concerning the procedures and safeguards to be used in processing this data. Further, any Controller (client) that is subject to GDPR will need to have in place an appropriate Data Processing Agreement (DPA) with any third party that he shares data with where that third party is a Processor as defined under GDPR.

In fact, the UK ICO online guide states:

The GDPR states at Article 28.3 that Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller ...

This means that you need a written contract every time you employ a processor to process personal data. This includes both:

- when you directly employ a processor; and
- when a processor, with your written authority, employs another processor.

A non-disclosure agreement (NDA), also known as a confidentiality agreement (CA), confidential disclosure agreement (CDA), hush agreement, proprietary information agreement (PIA) or secrecy agreement (SA), is a legal contract between at least two parties that outlines confidential material, knowledge, or information that the parties wish to share with one another for certain purposes but wish to restrict access to or by third parties. We are also being asked to execute these agreements so that the Controller/Processor can document his protection of the personal data.

Contracts between controllers and processors:

- ensure that they both understand their obligations, responsibilities and liabilities;
- help them to comply with the GDPR;
- help controllers to demonstrate their compliance with the GDPR; and
- may increase data subjects' confidence in the handling of their personal data.

The GDPR imposes a legal obligation on both parties to formalise (sic) their working relationship. Aside from the legal requirements, this makes practical and commercial sense.

By having a contract in place with the required terms:

continued ▶

- you are ensuring that you are complying with the GDPR;
- you are protecting the personal data of customers, staff and others; and
- both parties are clear about their role in respect of the personal data that is being processed and there is evidence of this."

Although not mandated in the GDPR, we are being asked to sign a separate General Cooperation Agreements (GCA) with our EU partners. These agreements set our legal relationships as well as exactly what services we are being asked to provide. We have been told that this agreement is necessary for each assignment to ensure that the exact parameters of the investigation are memorialized. We suspect that this is another measure to document how the data processing came about and is being carried out – as a matter if legal protection.

However, much more important, it is our belief that a very strong Non-Competition Agreement (NCA) is a must. As we discuss below, it appears that the GDPR requires that the data controller (the client) be aware of the sources used in carrying out these investigations. If we were to name our sources to the client or investigator who hires us, why would they come back to us in the future?

Therefore, a non-EU investigator will need to sign at least one and probably multiple contracts when agreeing to work on a case involving a person protected under the GDPR. Therefore, below, we will look at the risks undertaken by signing such contracts.

However, much more important, it is our belief that a very strong Non-Competition Agreement (NCA) is a must.

Mandatory Contract Brings Many Duties And Liabilities

An investigator (processor or sub-processor in GDPR speak) must at a minimum sign a Data Processor Agreement (DPA) – which immediately subjects us to EU data processing and contractual laws. The DPA ensures that personal data is processed lawfully, fairly and transparently; collected for specified, explicit and legitimate purpose; adequate, relevant and limited to what is necessary; accurate and kept up-to-date; kept for no longer than is necessary in relation to the purposes for which it was collected; processed in a manner that ensures appropriate security. It also stipulates how we store the data on a subject, communicate this data, are prepared to every trace of the data if so directed, it is necessary for us to identify each and every source of information, all extraneous data must be destroyed, and we could become involved in legal liabilities if the client (controller in GDPR speak) makes a judgment error. This is indeed new.

In the three proposed DPAs we have seen, we are asked to agree to not only comply with the GDPR but with the local national EU member state's data protection laws – which are then indicated by a URL link to the actual law. In other words, we are being asked to certify that we are totally familiar and in compliance with these state laws. As most of the "legal experts" we have seen in the EU have not agreed on the meaning of various sections of the GDPR, we believe that a non-EU investigator must take this into account before making such a certification and undertaking this significant liability.

This is even more so in the case of the local national EU member states data protection laws (at least 14 we have found), some of which date back to 1976 and have been amended or superseded on multiple occasions. Some of the DPAs we have received cite multiple jurisdictions and contain multiple URL's.

We also understand that a key misconception regarding GDPR concerns where and how data is stored. Some investigators believe that if their collected data does not reside inside a European Union data center, they are exempt from the regulations. This is a false assumption. It's about the data, not the location where that data is stored. Much of GDPR was written specifically to handle data collection of organizations based outside the EU. We doubt most non-EU investigators know where their servers are located. Iceland is a popular location for servers. Iceland is not a member of the EU, but it is a member of the single market by being a member of the European Economic Area (EEA). Switzerland is not a member of the EU or the EEA but is a member of the single Market.

continued ▶

Question

1. If we were to use a server in Iceland for our email (millions do), what would we need to do to be sure that we were GDPR compliant?
2. The same question for Switzerland.

GDPR and the Many State Laws

The GDPR calls for each member state of the EU to enact their own Data Protection law. It is our understanding that only 14 of the 28-member states have thus far passed such a law, and that several states are still developing their laws. For example, Poland and the U.K. are reportedly making changes, and Norway is currently rewriting their regulations on Data Protection Agreements. Further, many states have even more stringent national data protection laws than the GDPR. Although, as noted above, a non-EU investigator like we are, must sign a DPA stating that they are cognizant regarding the GDPR and individual national data protection laws now and any future changes, the reality is that we normally rely on the client or local investigator to provide guidance on their local laws. (Conversely, EU investigators have normally relied on us to advise them regarding legality under U.S. laws.) Obviously, this means that non-EU investigators will have to rely on their EU clients to be totally up-to-date with the pertinent laws in the EU. Further, non-EU investigators having signed the DPAs stating that they accept responsibility for complying with these laws, will have the *sole* liability in the event of any inadvertent violation of these laws.

We learned that, for example, Germany has consistently had some of the strictest data protection laws in Europe and is preparing even more stringent changes. Poland and Norway are preparing to broaden the scope of processing employee personal data law; Norway is currently revising their requirements DPAs; and the UK is planning to make some personal data, such as that belonging to people with criminal convictions, exempt from requiring consent.

Further, non-EU investigators having signed the DPAs stating that they accept responsibility for complying with these laws, will have the sole liability in the event of any inadvertent violation of these laws.

Questions:

Regarding this issue of overlapping laws, we have two questions which we believe would be of general interest:

1. In the event of contradictory or overlapping laws in the EU, which law is dominant and takes supremacy: The GDPR or the EU member state national law?
2. Can an EU member state's national data protection law have lesser standards than the GDPR, or can they only be more restrictive?

Who Is Protected By The GDPR

To us, a key question is who is protected under the GDPR? (We understand that this question can also vary according to national members state laws, but we are inquiring only about the GDPR.)

Initially, we understood that the GDPR applies to EU citizens residing in the EU or temporarily residing outside of the EU.

We have now been informed that foreign citizens residing in the EU will have the same rights under the GDPR. Further, EU citizens serving at an embassy or consulate in a non-EU Country are similarly protected.

Questions:

Regarding this issue who is protected by the GDPR, we have four questions which we believe would be of general interest:

1. Does an EU citizen who resides for several months in another country but does not have a residence permit enjoy the protection of the GDPR? (I.E. – For example, if someone travels to the US and remains here for three months every year, they do not need a residence permit.) Is it the length of time out of the EU or the receipt of a foreign residence permit that decides the jurisdiction?
2. When does the EU citizen lose the GDPR protection?
3. Is it in fact correct that a foreigner residing in

continued ▶

the EU receives the same protections from the GDPR as an EU citizen?

4. If so, how long does foreigners have to reside in the EU before they are protected?

Source Protection

It is our understanding that the GDPR requires that the entire chain of the data processors (investigators) know the sources involved. For example, it is now our understanding of GDPR Article 28 (2) that if a private investigator was working as a data processor, the private investigator would be required to inform the instructing attorney or controller as to the identities of which sub-processors (vendors) they had utilized. Further, no matter who acts as the Data Controller, the GDPR requires that all sub processors (sub agents) in the processing must be declared and identified to the Data Controller, i.e. the client. In fact, the GDPR adds that "The Processor must not use sub Processors without consent of the Controller."

To put this into a more understandable context, I will use an excellent example written by colleague in a professional investigators' association newsletter:

> *"Example – I'm employed by US Investigator to do a due diligence project in Germany, the end client is (a) US Bank. The US Bank would be the data controller and my client (the US investigator) and I would be data processors. GDPR apparently requires the data controller to know who is in the processing chain, therefore my client needs to disclose in their contract that they have employed me with my contact details, and I would need to disclose my German resource with contact details."*

In fact, the GDPR adds that "The Processor must not use sub Processors without consent of the Controller.

This would clearly make an investigator uncomfortable. Part of our brand or "added value" are our sources. Traditionally, clients came to you because you could offer a better product – usually based upon your sources. Under the GDPR, it appears that most investigators will be using the same non-proprietary / non-confidential sources. As we noted above, if an investigator were to agree to name their sources, they would at least need a very strong NCA.

Questions:

We imagine that this will be a matter of considerable concern to many investigators. Therefore, we especially encourage comments and discussion on this issue.

1. For example, if I supply the public marriage records of an EU citizen from the public registry in Albuquerque, New Mexico, is it enough to say that they came from the registry, or must I also state that John Smith went there to obtain a copy?
2. Are we correct that everyone above us on the chain of data processing will receive this information (i.e., controller and data processor) or just the person above us in the chain (i.e., the primary data controller)?
3. Is the source information provided to the data subject along with a copy of the report or only if requested in a legal action?

As everyone can imagine, the answer to this question will have a major impact on investigators and/or their sources.

Consent

Under the GDPR, consent needs to be 'freely given, specific, informed and unambiguous'. Explicit consent of the data subject is one of the key elements of the GDPR.

Article 6 of the GDPR lists six possible justifications for data processing personal information on an "EU person". The most commonly named by respondents for investigations such as pre-litigation, asset searches, reputational and background checks, etc. was the so-called "legitimate interest" justification listed in Article 6.1 (f). These investigations can become increasingly complicated because the personal data of third parties can also become involved.

continued ▶

Article 6(1) identifies six lawful grounds for processing personal data:

a. Consent
b. Contract
c. Legal obligation
d. Vital interests
e. Public interest task
f. Legitimate interests

We note that several respondents noted that advance consent for an investigation is not always required – in some limited circumstances. In fact, Article 6 of the GDPR provides some exceptions. The most commonly referred to was Article 6.1(f) which refers to "legitimate interests".

It is our impression that many investigators see this as a means to conduct investigations without notifying the data subject or being able to use other than public sources.

We note that the GDPR EU.org website "Web learning resources for the EU General Data Protection Regulation" (GDPR) located at

https://www.gdpreu.org/the-regulation/key-concepts/legitimate-interest/ makes the following comments:

> "Legitimate interest" may be among the most confusing concepts written into the GDPR, which is not helped by the amount of incorrect interpretations available when you search for the term online.

It is our impression that many investigators see this as a means to conduct investigations without notifying the data subject or being able to use other than public sources.

"Article 6.1(f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular, where the data subject is a child.

Like all other subparagraphs in this section, (f) sets a high bar that the processing must be necessary. In other words, if an alternative approach could meet the same end without processing personal data, then said processing would not be lawful without consent.

Even when data processing is necessary to the controller, such legitimate interests must be weighed against "the interests or fundamental rights and freedoms of the data subject". ***Should data controllers justify processing without consent based on this subparagraph, they will need to be prepared to prove legitimate interests (a higher burden) relative to the implied general interests of data subjects.*** (*Emphasis added.)*

For further confirmation, take a look at the April 2017 opinion posted by the Article 29 Data Protection Working Party, an independent advisory body to the EC commissioned by Article 29 of the current Directive (thus the name):

> In this context, the Working Party also supports the principled approach chosen in the Proposed Regulation of broad prohibitions and narrow exceptions and ***believes that the introduction of open-ended exceptions along the lines of Article 6 GDPR, and in particular Art. 6(f) GDPR (legitimate interest ground), should be avoided.***
>
> Note the explicit call-out that the legitimate interest ground under 6(f) in the GDPR should be avoided"

Some investigators stated that Article 6 (f) of the GDPR allows you "to collect etc. data if you have a legitimate reason, which can be anything from legal, to economic interests. And you have to notify the Person."

Others noted that "if the legal interests of the other Party are higher or you are preventing a crime, defending your civil rights etc., then you don't have to notify the Person." (Emphasis added.)

However, per the UK ICO online guide, "If you obtain personal data from other sources, you must provide individuals with privacy information within a

continued ▶

reasonable period of obtaining the data and no later than one month." Other respondents have stated that it is only 2 weeks.

One of the few reference sources we found that discussed some pertinent hypothetical details of "legitimate interests" was in a guide published by the The International Association of Privacy Professionals (IAPP).

https://iapp.org/media/pdf/resource_center/DPN-Guidance-A4-Publication.pdf

Regarding "Legitimate Interests and the obligation to inform individuals", it states that "Controllers need to be aware that if they use Legitimate Interests rather than other Lawful Bases, ***individuals must be told about those Legitimate Interests and there is also an obligation to tell individuals about their right to object."***

The study notes that "legitimate interests" can be considered necessary for "the purpose of preventing fraud." It goes on to note that "An individual who may be engaged in alleged illegal activity, or whose data is processed in relation to an age restricted or regulated environment, still has rights and freedoms. However, where processing addresses illegal activity it may tip the balance in favour (sic) of the Controller, as the Legitimate Interest ***could be compelling***." *(Emphasis added.)*

Some of the other listed general hypothetical areas in which the "legitimate interests" basis might be acceptable are "Fraud, Risk Assessment,

individuals must be told about those Legitimate Interests and there is also an obligation to tell individuals about their right to object."

Due Diligence, Ethical, Profiling and Evidential Purposes…."

However, this guide also states that the GDPR requires that "The processing of personal data strictly necessary for the purposes of preventing fraud", also constitutes a legitimate interest of the data controller concerned.

- Controllers that rely on "legitimate interests" should maintain a record of the assessment they have made, so that they can demonstrate that they have given proper consideration to the rights and freedoms of data subjects.
- Controllers should be aware that data processed on the basis of legitimate interests is subject to a right to object - which can only be rejected where there are "compelling" reasons.

Where "legitimate interests" are relied on, ensure this is included in the

information that must be supplied to data subjects pursuant to Articles 13 and 14. Information notices must now set out legitimate interests where "legitimate interests" are relied on in relation to specific processing operations, this will now need to be set out in relevant information notices, by virtue of Article 13 (1)(d) and 14 (2)(b).

Article 13: EU GDPR: "Information to be provided where personal data are collected from the data subject"

1. Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

(a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

(b) the contact details of the data protection officer, where applicable;

(c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

(d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

Article 14: EU GDPR: "Information to be provided where personal data have not been obtained from the data subject"...

continued ▶

2. In addition to the information referred to in paragraph 1, the controller ***shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:***

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

In short, from these guides, it appears that you must notify the data subject of at least your "legitimate interests". Despite this, several investigators opined that you would not have to notify a data subject of your investigation or the basis for it. Further, you could refuse to confirm your investigation if the data subject exercised their right to access. Therefore, we have this key question below.

Question:

1. If you are basing your investigation on the "legitimate interest" exception, when do you have to notify the subject of the investigation that you are conducting or have conducted this inquiry? (We have received four different viewpoints on this point! Two weeks; four weeks; never; or if the matter goes to court.)
2. What do you have to notify them of?

The answer to the above question is critical for several reasons. First of all, depending upon the

At that point, all of the sources used, and information obtained would be provided to the subject – which could then lead to civil action against the Controller and processors involved

case, the subject could flee, move or conceal his assets, do damage to a firm's reputation, etc. Secondly, the GDPR states that "Controllers should be aware that data processed on the basis of legitimate interests is subject to a right to object - which can only be rejected where there are "compelling reasons". Obviously, if the subject objects, the investigation can very likely be terminated and the ICO would be called upon to review your records explaining the decision to utilize the "legitimate interests" exception. At that point, all of the sources used, and information obtained would be provided to the subject – which could then lead to civil action against the Controller and processors involved. At that point the person could also seek redress under Article 82 of the GDPR, which makes it possible for data subjects to sue firms for any breach of their rights under the GDPR, even if the breach did not cause a material loss.

"Under the GDPR, individuals will have the right to obtain:

- confirmation that their data is being processed;
- access to their personal data; and
- other supplementary information – this largely corresponds to the information that should be provided in a privacy notice (see Article 15).

This "right of access" ……. clarifies that the reason for allowing individuals to access their personal data is so that they are aware of and can verify the lawfulness of the processing (Recital 63)"

The other two points we noted were raised in the following guide: Taken from the U.K. ICO on-line guide to the GDPR:

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

It states that:

"You may be able to rely on legitimate interests to lawfully disclose personal data to a third party. You should consider why they want the information, whether they actually need it, and what they will do with it. You need to demonstrate that the disclosure is justified, but it will be their responsibility to determine their lawful basis for their own processing.

You should avoid using legitimate interests if you are using personal data ***in ways people do not understand and would not reasonably expect,*** or if you think some people would object if you

continued ▶

explained it to them. ***You should also avoid this basis for processing that could cause harm, unless you are confident there is nevertheless a compelling reason to go ahead which justifies the impact.***" *(Emphasis added.)*

In short, we see two issues here:

First, the Controller (client and/or primary investigator) will need to make some judgment calls that are based on rather vague legislation. (Certainly, lawyers will profit from these new data protection laws.)

Secondly, you will have to perform a ***legitimate interests assessment*** (LIA) that considers legitimacy, necessity and balance. Once again, these areas are very subjective. The UK IOC online guide also notes "***Legitimate interests will not often be the most appropriate basis for processing which is unexpected or high risk***… You must tell people in your privacy information that you are relying on legitimate interests and explain what these interests are."

Third, also according to the UK ICO online guide, "If your LIA identifies significant risks, consider whether you need to do a DPIA to assess the risk and potential mitigation in more detail……. Data Protection Impact Assessments (DPIAs) – you must carry out a DPIA when what you are doing with personal data is likely to result in a high risk to individuals' rights and freedoms, particularly when new technologies are involved. You can use your record of processing activities to help flag when a DPIA is required, to keep a track of its progress, and to link to the completed report."

it seems to us that any processors or sub-processors working under a Controller who makes such a decision are leaving themselves liable if the Controller's decision is disputed by the subject of the inquiry.

In other words, it is our understanding that the Controller will be required to complete a DPIA where their processing is "likely to result in a high risk to the rights and freedoms of natural persons". However, there is no statutory requirement for Data Processors to complete a DPIA.

Fourth, all aspects of this decision and data processing procedure must be saved in the event of any future disputes regarding this decision to "legitimate interests".

Finally, it seems to us that any processors or sub-processors working under a Controller who makes such a decision are leaving themselves ***liable*** if the Controller's decision is disputed by the subject of the inquiry.

In this area of data processing exceptions, there seem to be many opinions but little data so far.

We are told by a German fellow investigator that the German Data Protection Law has a provision allowing an investigator to carry out an investigation without the consent of the person of interest if it "would prejudice the assertion, exercise or defense (sic) of civil claims, or that the processing contains data from civil law contracts and serves to prevent damage by criminal offenses, unless the data subject's legitimate interest in the provision of information is outweighed…"

Does the GDPR have such a provision? Is Article 9 (2) (f) of the GDPR the equivalent where it gives the exception "Necessary for the establishment, exercise or defense (sic) of legal claims or where courts are acting in their judicial capacity."?

In the past, you could legally conduct a discreet search for the person and his assets. Once successful, you could seek a Mareva injunction to freeze their funds without prior notice. (A Mareva injunction is an exceptional form of interlocutory relief, designed to freeze the assets of the defendant, in appropriate circumstances, pending determination of the plaintiff's claim.) ***It is critical to our profession to know if this type of investigation is still possible in the EU.***

Key Question

In simple terms, for example, if a person from one of the developing countries embezzles $100 million dollars and moves to the EU, can you conduct a civil search for him and his assets ***without*** giving him notification? Obviously, if the embezzler is alerted, he will flee or conceal his assets.

continued ▶

This leads us to the next two keys areas: penalties and effective jurisdiction.

Penalties

To understand as to why a non-EU based investigative company would be interested in the GDPR, please note that the EU takes the view that this new law applies to ***any business anywhere*** (including those businesses located in the U.S. and Canada) wishing to do business in the EU or regarding personal data concerning an EU citizen. In any event, the EU considers this privacy legislation to be legally binding. ***Please note that the GDPR provides penalties for certain violations of up to 20 million euros ($24.6 million) or 4 percent of a company's worldwide profits, whichever is greater.*** The significant potential financial penalties provide reason enough for companies in the EU and beyond to be aware of the GDPR requirements.

Ignorance of a partner's noncompliance will not save a company from the 4% fines of global annual turnover.

GDPR Jurisdiction Regarding The U.S.

Again, we are not lawyers and our observations do not constitute legal advice. Rather, we hope to spur open professional group discussions and further research.

From what we have read in research as well as been informed by colleagues, U.S. companies that conduct business overseas also have to comply with the GDPR or face the same fines as EU businesses.

When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. Each violation of such an order may result in a civil penalty of up to $40,654.

In March 2016, the Judicial Redress Act of 2015 was passed and went into effect. The Judicial Redress Act of 2015, 5 U.S.C. § 552a note, extends certain rights of judicial redress established under the Privacy Act of 1974, 5 U.S.C. § 552a, to citizens of certain foreign countries or regional economic organizations. This gave EU citizens the right to seek legal redress in the US as part of a new EU-US data protection agreement, covering instances where EU citizens' personal data is involved in US criminal and terrorism investigations. The deal brings rights of EU citizens in line with those of US citizens, who can sue in European courts for similar privacy breaches.

On December 2, 2016, the European Union (the "EU") undertook the final steps necessary under EU law to approve an executive agreement between the U.S. and the EU (the "Parties") relating to privacy protections for personal information transferred between the U.S., the EU, and the EU Member States for the prevention, detection, investigation, or prosecution of criminal offenses. The Agreement, commonly known as the Data Protection and Privacy Agreement (the "DPPA") or the "Umbrella Agreement," established a set of protections that the Parties are to apply to personal information exchanged for the purpose of preventing, detecting, investigating, or prosecuting criminal offenses. Article 19 of the DPPA establishes an obligation for the Parties to provide, in their domestic law, specific judicial redress rights to each other's citizens. The Judicial Redress Act is implementing legislation for Article 19 of the DPPA.

In 2016, three major U.S. corporations were successfully sued in U.S. courts for not protecting personal data under the EU-US Shield law.

In September 2017, an additional three U.S. companies agreed to settle Federal Trade Commission (FTC) charges that they misled consumers about their participation in the EU - US Privacy Shield framework, which allows companies to transfer consumer data from EU member states to the United States in compliance with EU law. The Commission issues an administrative complaint when it has "reason to believe" that the law has been or is being violated, and it appears to the Commission that a proceeding is in the public interest. When the Commission issues a consent order on a final basis, it carries the force of law with respect to future actions. ***Each violation of such an order may result in a civil penalty of up to $40,654.*** The key factor in this decision was that the companies were not only violating contracts that they signed, but that they had also misrepresented

continued ▶

their participation and compliance with the EU - US Privacy Shield framework.

Finally, Article 82 of the GDPR makes it possible for data subjects to sue firms for any breach of their rights under the GDPR, even if the breach did ***not*** cause a material loss. It states that any person who has suffered "material or non-material damage" as a result of a breach of GDPR, has the right to receive compensation (Article 82(1)) from the controller or processor. The inclusion of "non-material" damage means that individuals will be able to claim compensation for distress and hurt feelings even where they are not able to prove monetary loss.

We believe this clause will introduce the concept of accepting lawsuits on a contingency basis.

Certainly, any one of these laws could be invoked to sue not only the Instructing Attorney and/or Controller and/or processors if – for example – the subject of the inquiry was to dispute the use of "legitimate interests" under Article 6.1 (f) to conduct an investigation without prior consent and notification.

In summary, as we understand it, EU residents with no physical presence in the U.S. do have many individual rights and remedies they can pursue against a U.S. investigation company before U.S. courts. For example, a breach of tort law can also be claimed either through privacy tort violations, or through claims of misrepresentation where the defendant can be found to have concealed a material fact about its compliance with privacy laws or has made a misleading representation because of some material fact that wasn't disclosed.

as we understand it, EU residents with no physical presence in the U.S. do have many individual rights and remedies they can pursue against a U.S. investigation company before U.S. courts

Furthermore, U.S. companies are not immune from a claim by an individual in the EU, in addition to claims by the FTC and other U.S. Federal agencies under Federal law, as well as by State Attorneys General under State law.

Finally, under the GDPR, U.S. companies acting as subcontractors to companies that are directly accountable to EU data protection authorities and EU individuals by virtue of their processing activities, will also be liable under the law and may be subject to direct claims in connection with their sub processing activities.

As an aside, with the GDPR going into effect on 25 May 2018, we note that data transfers will no longer be governed by the existing EU-US Privacy Shield arrangement - or - EU-US Umbrella Agreement.

Additional Information Regarding "Legitimate Interests" Which You May Find Useful

Obtained from the U.K. ICO on-line guide to the GDPR

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/lawful-basis-for-processing/legitimate-interests/

At A Glance

- Legitim ate interest's clause is the most flexible lawful basis for processing, but no one can assume that it will always be the most appropriate.
- It is likely to be most appropriate where you use people's data in ways they would reasonably expect, and which have a minimal privacy impact, or where there is a compelling justification for the processing.
- If you choose to rely on legitimate interests, you are taking on extra responsibility for considering and protecting people's rights and interests.
- Public authorities can only rely on legitimate interests if they are processing for a legitimate reason other than performing their tasks as a public authority.
- There are three elements to the legitimate interests' basis. It helps to think of this as a three-part test. You need to:

continued ▶

- identify a legitimate interest;
- show that the processing is necessary to achieve it; and
- balance it against the individual's interests, rights and freedoms.
- The legitimate interests can be your own interests or the interests of third parties. They can include commercial interests, individual interests or broader societal benefits.
- The processing must be necessary. If you can reasonably achieve the same result in another, less intrusive way, legitimate interests will not apply.
- You must balance your interests against the individual's. If they would not reasonably expect the processing, or if it would cause unjustified harm, their interests are likely to override your legitimate interests.
- Keep a record of your legitimate interests' assessment (LIA) to help you demonstrate compliance if required.
- You must include details of your legitimate interests in your privacy information.

Please direct any comments to the Group rather than directly to us as, due to our caseload, we will not have time to answer them individually. Thank you!

The Professional Investigator

Institute of Professional Investigators
Jubilee House
3 The Drive
Brentwood
Essex
CM13 3FR

Tel: 0870 330 8622
Fax: 0870 3308612
Email: admin@ipi.org.uk