# Your Witness

*Newsletter of the UK Register of Expert Witnesses published by J S Publications*

## Some further thoughts on the GDPR

Following my call for specific questions on the General Data Protection Regulation (GDPR) in the last issue, we had a member write to say:

*'In 'Your Witness' issue 91 you wrote about GDPR which was useful but rather general, e.g. 'carry out an information audit' and 'publish privacy notices'. I don't know how to do these things!'*

Well, these things aren't too complicated, as I'll explain. But first I think a quick reality check may be in order. While the GDPR makes no distinction between your business, my business and Google, the Information Commission's Office (ICO) most certainly will! It has nothing like the resources to deal with small businesses. In our view, the most likely response if a jobbing expert witness was to come across the ICO's horizon would be a bit of guidance from them on how to do better. Having said that, I think the purpose of GDPR is a good one and it makes sense for us all to get to grips with how we use personal data.

### Data audit

The data audit is simply about **documenting the personal information you collect**. It does not need to be complicated or long winded. Just think about your business and write down:

- What data do I collect? *e.g. name, email address, location, IP address, cookies*
- Where do I store the data? *e.g. e-mails, filing cabinets, databases, backups, email lists*
- How do I protect and document the data I have? *e.g. passwords, encryption, locked safes*
- How long do I plan to keep the data for?
- Do I have a reason for every piece of data I collect? *e.g. name: to provide customer service*
- What is the process if someone asks to be removed from my records? *What records need to be checked?, etc.*

Once you know what data you hold, prepare an audit form along these lines:

- Type of data
- Description of data
- Person responsible
- Legal basis for processing it
- If by consent, date of consent
- Where the data are stored
- Source of the data
- Purpose of the data
- How the data are protected in storage
- Usage restrictions
- Usage rights
- Usage frequency
- Retention period

### Privacy notice

Your privacy notice is simply a **short document explaining what personal data you gather, why you gather it, how you store it and how you share it**. Our own privacy notice is available at *www.jspubs.com/privacy.pdf*. I suspect that for most expert witness businesses, a shorter privacy notice than ours would suffice. Once you have completed your data audit, you will find that your privacy notice almost writes itself.

With the 25 May deadline behind us, you will start to see many privacy notices appearing on the web. So if you really are unable to come up with your own version, there will soon be many you can use as a template!

### 'Data Controller' or 'Data Processor'?

Whether an expert witness is to be considered a 'data controller' or 'data processor' was also a hot topic on the *Register* helpline. For example, one expert wrote:

*'A firm of solicitors for whom I have worked has sent me an agreement that they want me to sign in relation to GDPR in which they identify themselves as the data controller and me as the data processor. This seems incorrect to me because, if they are the data controller, then as a data processor, I am simply doing their bidding, whereas I would consider myself to be an independent expert to the Court, so from that perspective, I see this agreement as potentially undermining my professional autonomy...'*

A 'controller' determines the purposes and means of processing personal data. A 'processor' is responsible for processing personal data on behalf of a controller. Before GDPR, only data controllers were liable in law for any infringements or breaches. This has changed significantly. Data processors now have specific responsibilities under law, and the potential for direct liability to regulators and data subjects.

Our initial thinking on this issue has been that experts are instructed by the lawyers, and the work they do on the lawyer's case, and the processing of the particular set of personal data the lawyer gives the expert, would not be undertaken at all without that instruction. The questions lawyers ask experts to address in the report control the way in which the expert will process the data. So, on this analysis, the lawyer is the data controller and the expert is the data processor. But that question of **independence** struck a cord with us.

We were, then, much interested in the view expressed by the Bar Council about barristers. It has said that **self-employed barristers are data controllers because they need to be able to act independent of instructing solicitors. That must hold for expert witnesses as well.**

It is, in the end, a decision for each expert to make in each case. But if you favour being the 'controller', the Bar Council's view will be one to remember.

*Chris Pamplin*

## Inside

**e-docs and experts**
**Unsafe convictions**
**Dirty tricks**
**GDPR thoughts**

**Issue 92**

*June 2018 © J S Publications*

# Electronic documents and experts

*Proliferation of electronic documents is a boon to some expert witnesses*

In our modern world, fewer documents are being printed on paper and many communications are only produced and stored in electronic format. This has created a number of issues for the courts and parties to litigation.

The essential difference between e-documents and their paper predecessors is that e-documents can be produced in vast numbers. Once created, they are also difficult to destroy. What's more, they are relatively easy to search and can often reveal information beyond the mere textual content. All of these 'features' may require expert involvement. For example, expert assistance may be sought:

- to retrieve deleted documents
- to analyse metadata contained within the document (which can show whether a document has been changed since the original date of creation and by whom)
- to look at metadata contained on the medium on which an electronic document is stored to reveal valuable information about a document's provenance
- to preserve or filter data, and
- to search through millions of documents using 'predictive coding'.

### Regulatory guidance sparse

Specific provision in relation to e-disclosure is something that is quite recent. In 2006, the Cresswell Report gave some consideration to emerging problems surrounding e-documents and their disclosure. It identified the classes of electronic data that were potentially relevant as:

- active or on-line data
- embedded data (metadata)
- replicant data
- back-up data, and
- residual data.

Such data could include:

- the contents of a user's email in-box
- the contents of a user's email sent items
- files on a hard drive, and
- the contents of network or server drives.

It is acknowledged that such data are not necessarily stored near the point of access. They can be stored on distant or remote servers, sometimes in a different country, requiring the consideration of country-specific data protection laws.

*Expert witnesses are often used to help parties prepare for disclosure*

In October 2010, directions were given in relation to the specific disclosure of e-documents. They are contained in Civil Procedure Rules (CPR) Practice Direction (PD) 31B. This practice direction introduced an Electronic Documents Questionnaire (EDQ) designed to resolve technical and legal issues, including:

- the extent of a reasonable search (including date ranges, custodians and types of electronic document)
- methods of searching (using keywords or other types of automated search)
- document preservation
- potential problems regarding accessibility of electronic documents
- inspection by electronic exchange, and
- expectations regarding the other side's e-disclosure.

Although use of the EDQ is not mandatory, the Court has the power to give directions requiring its completion in whole or in part.

PD31B.24 states that the primary source of disclosure of electronic documents is normally 'reasonably accessible data'. Data that are not reasonably accessible will frequently require some form of expert assistance in their extraction, interpretation or preservation, which is likely to involve time and expense. Consequently, any party requesting the specific disclosure of electronic documents which are not reasonably accessible must be able to show, to the satisfaction of the court, that these are both **relevant and material** *and* that the cost and burden of retrieval is **proportionate**.

It should be noted also that some courts, e.g. the Technology and Construction Court (TCC), have their own protocols on e-disclosure.

### Case law developing fast

The case law on e-documents and their disclosure is, of course, relatively young and evolving. However, there have already been some decisions given by the courts specifically regarding the role and involvement of experts in the search and disclosure process.

In *Mueller Europe Ltd -v- Central Roofing Ltd*[1], Coulson J ordered that the defendant's e-disclosure exercise should be carried out on its behalf by an IT expert because the defendant did not have the necessary expertise. In *Mueller*, although the majority of the communications between the parties had been by e-mail, the defendant had disclosed almost no e-mails. The defendant sought to explain this by saying that it had moved premises and had replaced its computer systems. The defendant had, however, removed some of the electronic data to backup tapes or discs. The claimants had applied for, and had been granted, an order that the defendant should make a keyword search of this backup data and serve a statement confirming the method whereby this had been undertaken. The defendant duly served such a statement but failed to disclose any documents resulting from the search. This was not a deliberate obstruction by the defendant, and the court recognised that non-compliance with the order was simply due to the defendant's lack of technical expertise. Following a further application, the court made an order for the searches to be performed by an expert on the defendant's behalf.

It is, of course, one thing for the search to be carried out by that party's own expert, but quite another for the search to be made by an opponent's expert. In *CBS Butler Ltd -v- Brown*[2], an application was made by the claimant that it should be permitted to instruct its own

expert to make a search of the defendant's e-document data. Tugendhat J distinguished the circumstances leading to the decision in *Mueller* and said that an order granting permission for an expert to search an opponent's data would be an unnecessarily intrusive order that would be contrary to normal principles of justice. However, he did not rule this out entirely, and opined that such an order might be made if there was a paramount need to prevent a denial of justice.

As the storage and retrieval of data becomes more time consuming and complex, recent cases have addressed the methods permitted for making a search. Tradition has favoured a physical search of every document and the application of some direct consideration to assess its relevance to disclosure. Keyword searches have long been permitted because such searches still require consideration and input by the searcher to decide whether documents thus revealed are relevant and of a class that should be disclosed. However, the task can become Herculean when vast quantities of data have to be trawled through or the data are contained on media or systems that are not easily accessible or are arranged in a complex way.

### Algorithmic searching being developed

In *Pyrrho Investments Ltd -v- MWB Property Ltd*[3], the court recognised that traditional search methods were not the answer in some complex disclosure cases. The case involved a very high-value monetary claim and the review of more than three million electronic documents. It was impossible for a satisfactory and thorough review to be carried out by traditional means. Consequently, the parties had reached agreement that the documents be searched by means of a technology known as **predictive coding**. Put simply, a team of lawyers familiar with the case would examine a sample, or 'seed', set of documents which were marked up indicating their relevance to disclosure. Coded data from that sample were then used to produce a predictive coding algorithm, designed to predict the likely relevance of the remaining documents. The coding and production of the algorithm was a process that needed expert input. The use of such predictive coding did, of course, require the express permission of the court.

Considering the application, Master Matthews reviewed its use in other jurisdictions where it had been found useful. He could see nothing in it that was likely to be less reliable than a manual or keyword search. Indeed, in some cases he thought it could be more reliable. He considered that, in addition, predictive coding could assist searching at **proportionate cost** where manual searches might be too time consuming or disproportionate. It was not contrary to CPR PD31B.25 in the light of the parties' agreement and the relatively early stage in proceedings.

The decision by Master Matthews was the first in the English High Court to approve the use of predictive coding. Indeed, it has opened the way for further development in this area.

In *Brown -v- BCA*[4], the court went so far as to order a search using predictive coding, despite strong objections by one party to its use. Amongst other matters, the case established that, in the event of objection to the use of the technology, the court is likely to favour the views expressed by the party that would bear the greater burden of disclosure.

This year, in *Triumph Controls UK Ltd -v- Primus International Holding Co*[5], Coulson J emphasised a number of important points in relation to e-documents and their disclosure. These included the need for **cooperation between parties** and the importance of having a **robust, well-documented methodology** to support the approach adopted for the search and review of documents. He was concerned that there should be **transparency** in relation to both the **extent of any searches** and the **methods used**. These, he said, should be **independently verifiable**, and any sampling exercise undertaken should be identified and made clear.

In *Triumph Controls*, a mixture of search techniques had been used. The first was a keyword search which had identified 450,000 potentially relevant documents. The claimants made a further search of a little over half of these documents using a combination of computer-aided review (CAR) and manual processes. Subsequently, 16,000 documents were disclosed as a result of these searches, but the remaining 220,000 documents were not searched (because CAR analysis of a very small sample indicated they were less likely to be relevant and the cost of further searches was considered to be disproportionate).

Ordering further searches to be carried out, Coulson J expressed a number of concerns. If a party takes a unilateral decision to use CAR, or some other computer-aided search technology, into which the other party had no input, it is incumbent on that party to provide details of how this was set up and how it was operated. Similarly, if a sampling exercise is undertaken, transparency requires that details be provided of, for example, stated tolerances and the number of rounds of sampling.

The judge observed that the evidence had indicated that a significant number of documents (~2,000) had been disclosed because they were documents that the disclosing party's own expert had identified and wished to rely upon. With regard to other documents, the disclosing party had been too ready to accept the CAR prediction that only a small number (0.38%) were relevant when in fact the evidence indicated that the real figure was likely to be substantially higher.

### Conclusion

E-disclosure is a rapidly developing area of litigation procedure in which the role of the IT expert is, we suggest, likely to increase.

***Transparency required on the scale and method of searching***

**References**

[1] *Mueller Europe Ltd -v- Central Roofing (South Wales) Ltd* [2012] *EWHC* 3417 *(TCC).*

[2] *CBS Butler Ltd -v- Brown & Others* [2013] *EWHC* 3944 *(QB).*

[3] *Pyrrho Investments Ltd & Another -v- MWB Property Ltd & Others* [2016] *EWHC* 256 (Ch).

[4] *Brown -v- BCA Trading Limited* [2016] *EWHC* 1464 (Ch).

[5] *Triumph Controls UK Ltd & Another -v- Primus International Holding Co & Others* [2018] *EWHC* 176 (TCC).

# Does expert's breach of duty render c

*Could fresh evidence have changed the jury's verdict?*

An expert's duties to the criminal court are set out in the Criminal Procedure Rules (CrimPR) Part 19, and every expert practising in the criminal arena should be familiar with them. The **purpose of expert evidence in criminal courts is to assist jury members with matters likely to be outside their experience and knowledge**. Evidence will only be admissible as 'expert' if it falls **within the expert's area of expertise**. Evidence outside the relevant area of expertise will be of no use to the jury and corrosive of the trust placed in experts. But in what circumstances will an expert's breach of duty be a ground for rendering a conviction unsafe? And what is the test applied by the court?

### What the Appeal Court has to decide

In general, the test for safety – or otherwise – of a conviction is the same, no matter what the nature of the concern. Accordingly, expert evidence of doubtful or tainted probity will illicit the same test as, for example, the concealing of evidence by the prosecution or the availability of entirely fresh evidence that was not available at trial.

The leading case in relation to this was *R -v- Stafford*[1], which was an appeal on the ground of fresh evidence. *Stafford* established the principle that when considering whether a conviction is unsafe or unsatisfactory in the light of fresh evidence, the law does not require the court to decide in every case what they think the jury might have done if it had heard that evidence. Where the Court of Appeal has no reasonable doubt of the appellant's guilt, it should not quash the conviction even if it thinks a jury might reasonably take a different view. In short, the **Court of Appeal has to decide whether the verdict was unsafe, and no different question has to be decided**, e.g. whether the defendant was guilty.

In the more recent case of *R -v- Pendleton*[2], an appeal against a conviction for murder was made on the grounds of fresh psychological evidence and documents not produced at trial. It was held that the **scope of the appeal court's duty was limited to an assessment of the safety of the conviction**, because the primacy of the jury decision precluded judicial intrusion upon the issue of an appellant's guilt. It would usually be wise for the Court of Appeal, in a case of any difficulty, to test its own provisional view by **asking whether the evidence, if given at trial, might reasonably have affected the decision of the trial jury to convict**. In the light of the fresh evidence, it was impossible to be sure that the conviction was safe because the jury had never had the opportunity to hear the true defence, nor were the jury members allowed to assess the reliability of the admissions made in the undisclosed documents.

What is clear from these cases is that **when considering the safety or otherwise of a conviction, the appeal court should not, when reviewing the evidence, seek to usurp the role of the jury and make its own determination on the issue of guilt**. What the court should do is to **assess the impact that evidence might have had on a jury if it had been put to the jury at trial**.

### Banker on trial

In March 2018, in *R -v- Pabon*[3], the Court of Appeal was asked to adjudicate on whether unsatisfactory expert evidence given in a fraud case was sufficient to render a conviction unsafe.

The appellant in *Pabon* was a derivatives trader who had been convicted with five others of conspiracy to defraud in respect of his part in dishonestly manipulating the London Interbank Offered Rate (LIBOR). In his original grounds for appeal, he admitted seeking to move the LIBOR rate to suit his book and favour the bank for whom he worked. However, in doing so, he claimed that he had not acted dishonestly. The central issue for the jury had therefore been dishonesty. Subsequently, at the retrial of two of his co-defendants, it emerged that the expert witness instructed by the Serious Fraud Office (SFO) had failed to comply with his CrimPR duties in several glaring ways.

The expert's evidence had been seriously deficient. He had strayed well beyond his field of competence, and in some areas had sought the advice of a colleague. There was concern, in particular, regarding his lack of experience and expertise in the field of short-term interest rate trades. He was criticised by the Court for, among other things:

- **straying into areas that were beyond, or at the outer edge of, his expertise**
- **failing to inform the SFO, or the court, of the limits of his expertise**
- **obscuring a colleague's role** in preparing sections of his report, and
- **flouting the judge's instruction not to discuss his evidence with third parties** when he was still under oath.

The appellant submitted that if evidence of the expert's deficiencies had been available to him at trial, it would have enabled devastating cross-examination of the expert which, it was argued, would have led to the defendant's acquittal, as it had done in the retrial of two of his co-defendants. It was argued, therefore, that this was sufficient to render his conviction unsafe.

In an interesting and elegant application of the tests in *Stafford* and *Pendleton*, Gross LJ said that the word 'unsafe' connoted a risk of error or mistake or irregularity that exceeded a certain margin. It involved a risk assessment. The Court was required only to answer the direct and simply stated question of whether it thought the conviction was unsafe. The judge observed that, at trial, the appellant had faced considerable difficulty in dealing with the initial questions of the genuineness of the LIBOR submissions, and the SFO had presented a strong case. There had also been damaging evidence of e-mails passing between defendants, to which must be added the appellant's own admissions. The central issue

**References**

[1] *R -v- Stafford (Dennis) (No 2)* [1974] *AC* 878.

[2] *R -v- Pendleton (Donald)* [2001] *UKHL* 66, [2002] 1 *WLR* 72.

[3] *R -v- Pabon (Alex Julian)* [2018] *EWCA Crim* 420.

# conviction unsafe?

remaining was whether the appellant had acted dishonestly.

The judge observed that, although the expert's conduct and evidence were deficient in many respects, he did have a general expertise in banking and finance. Many of the issues dealt with by the expert were not controversial and were not matters in dispute. The manner in which the appellant had chosen to defend himself at trial meant that there had been little need to conduct an in-depth analysis of short-term interest rate trades or related expert evidence matters. Had this not been the case, then the situation might have been different. However, in reality, there was little in the expert's evidence that addressed the key question of the appellant's honesty. That conclusion, said the judge, was fact sensitive and turned on a consideration of the expert's evidence in the round, evaluated in the context of the trial as a whole.

While the evidence relating to the expert had been very damaging to the prosecution at the co-defendants' retrial, there was nothing to suggest that this would have been replicated if it had been produced at the appellant's original trial. To transpose the outcome of the retrial to the original trial, or to try to predict how the jury might have reacted, would be purely a speculative exercise and one that did not satisfy the test laid down by *Stafford*.

### No causal link saves the expert's bacon

There were many courses the original trial might have taken if the shortcomings of the SFO's expert had become known, including the possibility that the expert would not have been called. However, there was nothing to suggest that this would have impacted on the final outcome. Dismissing the appeal, the judge held that there was no causal link between the expert's failings and the issue of the appellant's dishonesty, which was the key focus of the trial. Further, while not determinative, the Court was satisfied that if the new material had been available at trial, it would not reasonably have affected the jury's decision to convict.

Although the failings of the expert were not, in this case, considered sufficient to render the conviction unsafe, Gross LJ's judgment contains a useful guide to judicial thinking and identifies the parameters that would need to be established for defective expert evidence to lead to this outcome.

In this case, the judge said that the expert had '*signally failed to comply with his basic duties as an expert. ... he signed declarations of truth and of understanding his disclosure duties, knowing that he had failed to comply with these obligations*'. Faced with such strident criticism, even if the outcome of the trial was, in the end, not rendered unsafe, the banker concerned can perhaps expect some need of his professional indemnity insurance in the not too distant future! This all goes to remind us, as if a reminder was needed, that experts should be vigilant in staying strictly within their areas of expertise.

# Dirty tricks

The Machiavellian tricks sometimes employed in relation to expert evidence never cease to amaze, although we should, by now, have become inured to such inventiveness.

A potential area for high jinx, and one that is new to us, was at the heart of a case before the International Centre for Settlement of Investment Disputes. This tribunal is part funded by the World Bank Group, and is designed to offer dispute resolution and conciliation services between international investors. The case under review was an arbitration between Switzerland and Venezuela under the bilateral investment treaty.

In the course of the hearing, the tribunal was asked to consider an application to disqualify an expert appointed by the respondent and to exclude his expert report. It was claimed that the expert instructed by Venezuela had previously been considered by the claimant as a potential expert in its own cause. The claimant had sent the expert certain papers and documents but hadn't gone on to instruct him. It was argued that the expert had thus acquired knowledge of confidential information concerning the damages claim. There was, argued Switzerland, a real danger that the expert might have disclosed this knowledge to Venezuela.

In dismissing the application, the tribunal observed that the claimant had taken no steps to indicate the confidentiality of the information it had provided and had done nothing to preserve this. Moreover, there was nothing to indicate that the expert had actually accessed the information sent by Switzerland or had any knowledge in relation to its content.

There is, perhaps, nothing in the tribunal's ruling that is surprising, but there was another rationale that is novel and worthy of comment.

Commentary to the tribunal's decision highlights the possibility that, if the tribunal had allowed the application purely on the basis that confidential information had been sent – and regardless of whether or not the expert had accessed it or made use of the information – this would open the way for unscrupulous parties to **taint a pool of experts by providing them with unsolicited information**. It would be of particular concern in narrow fields of expertise where the number of suitably qualified and available experts was few. Indeed, in some circumstances it might be possible for confidential information to be sent to all the readily available experts and thus drastically reduce or exclude the pool of experts from which an opponent could draw.

Although we have never heard of a case in which such a tactic has been employed (and there was no suggestion that this had been the claimant's intention in this case), it does, nevertheless, provide some food for thought and, for those of a mischievous bent, a frisson of amusement.

*If an expert is sent, unbidden, information about a case...*

*... can a party argue the expert is thereby tainted?*

# GDPR – the problem with consent

*Data must be collected lawfully, or not at all*

In our *Factsheet 68: Data Protection and the Expert Witness*, which we have completely rewritten to account for the GDPR (General Data Protection Regulation), we explain that there must be a lawful basis for any personal data processing. These lawful bases are:

- consent
- contract
- legal obligation
- vital interest
- public task
- legitimate interest.

It's often said that consent is the obvious lawful basis – which is why we are all being deluged with requests to give explicit consent to all those companies whose e-mails routinely clog our in-boxes. [*Am I alone in having a near visceral joy in deleting such e-mails? Ed.*] While *consent* may seem the natural choice to many experts, it is definitely worth considering the alternative of *legitimate interest*. This lawful basis will often be simpler to handle than battling through the strengthened requirements imposed by GDPR to gain fully informed consent. We'll look in some detail at legitimate interest later in this article, but first there's an important caveat contained in GDPR than can save expert witnesses a lot of time. Let's consider three examples.

### Right to object to processing

Article 21 of the GDPR allows a person to object to further personal data processing if the lawful basis for any processing is legitimate interest. The **legitimate interest** for expert witnesses lies in the **instruction from the lawyer and the needs of the litigation**.

So what happens if you have written your report, served it on the other side and then the person whose data is contained in the report suddenly starts to object?

### Processing health data

Article 9 of the GDPR prohibits the processing of certain categories of personal data, including those:

> *'... revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade-union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation'.*

*Relying on consent to process data is problematic for expert witnesses*

Imagine the situation, raised by another of our members, who asked what consent is needed by an expert instructed by the defence to consider health data on a claimant? In these circumstances, the defence-instructed expert obtaining informed consent from the claimant could be a bit tricky.

By using legitimate interest, rather than consent, as the lawful basis for processing, the defence expert (and, indeed, the claimant expert) can avoid the problems of trying to get fully informed consent. But that still leaves the issue of how to overcome the ban on processing health data in any event. How can an expert get around that barrier?

### Right to be forgotten

We had a member expert witness contact the helpline to ask about the right to be forgotten in the context of legal proceedings. Our expert said:

> *'I am wondering about the right of erasure in relation to court reports. It seems to me that there is a conflict here between this right and the needs of the court. I mean, if a data subject (i.e. someone I assessed for court) asked me to erase their file, I don't think I am at liberty to do that as the court has an interest in that data, surely?'*

The right to erasure exists when, for example, the lawful basis for processing is consent and the data subject withdraws consent. It is contained in Article 17

### Vital exemption all experts should know

The answer to all three conundrums lies in an important exemption. It is contained in Articles 9(2f), 17(3e) and 21(1) of the GDPR. Each states that **the right under consideration is not absolute where the data is being processed 'for the establishment, exercise or defence of legal claims'**.

So, when expert witnesses handle personal data solely for the purpose of the establishment, exercise or defence of legal claims, they can more easily justify **using legitimate interest instead of consent as the lawful basis for processing the personal data**, and thereby avoid a whole bag of issues surrounding consent.

### Legitimate interest

We have highlighted here the important exceptions of legitimate interest and processing for the purpose of establishing or defending a legal claim.

Legitimate interest is not a new concept and has always existed as a potential basis for the processing of private and confidential personal data. Indeed, under the Data Protection Act 1988 (DPA), it was relatively easy to establish this as a lawful basis, and it often appeared to favour business over the rights of individual data subjects. However, under the GDPR, legitimate interest will become more formalised and its application will fall under rather more precise scrutiny and control.

Under the DPA, a controller's legitimate interests would be overridden only if unwarranted prejudice was caused to the rights and freedoms or legitimate interests of individuals. Effectively, this placed an onus on the data subject to demonstrate prejudice. The situation under the GDPR is somewhat different because the element of prejudice is no longer applicable.

Article 6(1)(f) provides that processing will be lawful where it is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, *except* where these interests are overridden by the interests or the fundamental rights and freedoms of the data

subject, *in particular* where the data subject is a child. It will be apparent, therefore, that under the GDPR the mere existence of the data subject's interests or fundamental rights and freedoms (which require the protection of personal data) may be sufficient to override a data controller's interest. This fundamentally switches the burden of demonstrating legitimate interest, compliance and transparency to the controller.

Consequently, although legitimate interest is the most flexible legal basis available under the GDPR, it may not be justifiable in all situations if it cannot be clearly shown to be appropriate under the Regulation.

The guidance notes to the GDPR indicate that relying on this ground will place more responsibility on controllers to justify any impact on individuals. As part of the transparency requirements under the GDPR, controllers must set out details of the legitimate interests that they pursue in processing personal data.

With this in mind, the Information Commissioner's Office (ICO) has advised that data controllers should carry out a 'legitimate interests assessment' before using it as a basis for processing. Unlike the 'data protection impact assessment', this assessment is not mandatory but is seen more as a matter of good practice. It will, in any event, be very difficult to show that the controller has complied with the accountability principles if the assessment is not completed.

The ICO has issued guidance on the methodology of the **legitimate interests assessment**. It is a three-stage process based on tests for **purpose**, **necessity** and **balancing**.

- The **purpose test** considers the interests pursued by a processing activity. Interests do not have to be compelling to be legitimate, but they must be specific. Vague or generically formulated interests will not satisfy this test.
- The **necessity test** considers whether the processing activity is a targeted and proportionate way of achieving the stated purpose. Controllers must think about whether there is any less intrusive way of meeting the objectives of the processing activity.
- The **balancing test** requires a light-touch risk assessment to be undertaken to ensure that any risks to individuals' rights are proportionate. Controllers should consider the reasonable expectations of individuals at this stage.

As a matter of best practice, controllers may provide data subjects with information about how the balancing test under Article 6(1)(f) has been performed. It is also recommended that controllers should inform individual data subjects that they can request this information.

Of course, even if the legitimate interest ground is fully justified and established, controllers will still need to comply with all the requirements made by the GDPR. They will still need to have a system in place for reporting breaches, etc., and will still need to properly address any request from the data subject for the removal of data.

*Consider using 'legitimate interest' instead*

### What happens to the DPA?

With GDPR in effect, does the DPA become obsolete? The answer is, generally, yes – but with some minor provisos.

The final text of the GDPR was published in the *EU Official Journal* on 5 May 2016 and entered into force on 24 May 2016. The idea was that there would be a two-year transition period and that the GDPR will apply directly in all Member States from 25 May 2018. This was intended to give data controllers and processors sufficient time to adapt their data processing activities to ensure compliance with the new legal framework.

From 25 May 2018, the EU GDPR replaced the regime established by the DPA. It will be supplemented by the Data Protection Bill – once it receives Royal Assent.

The GDPR will become directly applicable before the UK leaves the EU (scheduled for 29 March 2019). Once the UK leaves the EU, it will become a 'third country' for the purposes of personal data transfers from the EU. It will be required to have an 'adequate' level of data protection to that of the EU so that personal data transfers from the EU to the UK can continue to take place. The government has confirmed that the UK will implement the GDPR.

The Data Protection Bill is proceeding through the parliamentary process, having had its first reading in September 2017. It serves a number of functions. Once it receives Royal Assent, it will:

- replace the DPA
- fill in the gaps in the GDPR
- address data processing in law enforcement and the intelligence services, and
- attempt to ensure that on leaving the EU, the UK has an 'adequate' data protection regime compared with that of the EU.

Currently the Bill is still at the Public Bill Committee stage.

There has also been some discussion on an 'immigration exemption', giving the government the power to remove data protection rights from anyone whose details are processed for 'effective immigration control'. We suspect that, in the light of the Empire Windrush debacle, this proposal will be handled with caution.

*Don't forget the 'defence of legal claims' exemption*

In addition, during a House of Lords debate on the Cambridge Analytica investigation, Lord Ashton noted that the Information Commissioner has requested stronger enforcement powers. The power of audit is already in the Bill, but the Information Commissioner has proposed additional criminal sanctions.

So, back to the key question. Once the Bill has passed through parliament and has received Royal Assent, will the DPA be obsolete? Yes!

# Services for registered experts



Expert witness members of the *UK Register of Expert Witnesses* have access to a range of services, the majority of which are free. Here's a quick run down on the opportunities you may be missing.

### Your Witness – FREE

First published in 1995 and now fast approaching 100 issues, *Your Witness* was the first newsletter dedicated to expert witnesses. All quarterly issues are freely available to members online.

### Factsheets – FREE

Unique to the *UK Register of Expert Witnesses* is our range of factsheets (currently 70). All are available and searchable on-line. Topics covered include expert evidence, terms and conditions, getting paid, training, etc.

### E-wire – FREE

Now exceeding 100 issues, our regular condensed e-wire is our fast link to you. Containing shortened articles, as well as conference notices and details of urgent changes that could impact on your work, it is free to all members.

### Little Books series – DISCOUNTED

Distilled from three decades of working with experts, our *Little Books* offer insights into different aspects of expert witness work. Point your browser at *www.jspubs.com/LittleBooks/lbe.cfm* to find out more.

### Court reports – FREE

Accessible freely on-line are details of many leading cases that touch upon expert evidence.

### LawyerLists

Based on the litigation lawyers on our Controlled Distribution List, *LawyerLists* enables you to buy recently validated mailing lists of UK litigators. A great way to get your marketing material directly onto the desks of key litigators.

### Register logo – FREE

If you are vetted and a current member, you may use our undated or dated logo to advertise your inclusion.

### General helpline – FREE

We operate a general helpline for experts seeking assistance in any aspect of their work as expert witnesses. Call 01638 561590 for help, or e-mail helpline@jspubs.com.

### Re-vetting

You can choose to submit yourself to regular scrutiny by instructing lawyers in a number of key areas to both enhance your expert profile and give you access to our dated logo. The results of re-vetting are published in summary form in the printed *Register*, and in detail on-line.

### Profiles and CVs – FREE

Lawyers have free access to more detailed information about our member experts. At no charge, you may submit a **profile sheet** or a **CV**.

### Extended entry

At a cost of 2p + VAT per character, an extended entry offers you the opportunity to provide lawyers with a more detailed summary of expertise, a brief career history, training, etc.

### Photographs – FREE

Why not enhance your on-line entries with a head-and-shoulders portrait photo?

### Company logo

If corporate branding is important to you, for a one-off fee you can badge your on-line entry with your business logo.

### Multiple entries

Use multiple entries to offer improved geographical and expertise coverage. If your company has several offices combined with a wide range of expertise, call us to discuss.

### Web integration – FREE

The on-line *Register* is also integrated into other legal websites, effectively placing your details on other sites that lawyers habitually visit.

### Terminator – FREE

Terminator enables you to create personalised sets of terms of engagement based on the framework set out in Factsheet 15.

### Surveys and consultations – FREE

Since 1995, we have tapped into the expert witness community to build up a body of statistics that reveal changes over time and to gather data on areas of topical interest. If you want a say in how systems develop, take part in the member surveys and consultations.

### Professional advice helpline – FREE

If you opt for our Professional service level you can use our independently operated professional advice helpline. It provides access to reliable and underwritten professional advice on matters relating to tax, VAT, employment, etc.

### Expert Search App – FREE

If you choose our Professional service level you can access our Expert Search App for highly flexible searching of the *Register*.

### Discounts – FREE

We represent the largest community of expert witnesses in the UK. As such, we have been able to negotiate with publishers and training providers to obtain discounts on books, conferences and training courses.

### Expert Witness Year Book – FREE

Containing the current rules of court, practice directions and other guidance for civil, criminal and family courts, our *Expert Witness Year Book* offers ready access to a wealth of practical and background information, including how to address the judiciary, data protection principles, court structures and contact details for all UK courts.

**Address**
J S Publications
PO Box 505
Newmarket
Suffolk
CB8 7TF
UK

**Telephone**
+44 (0)1638 561590

**Facsimile**
+44 (0)1638 560924

**e-mail**
yw@jspubs.com

**Website**
www.jspubs.com

**Editor**
Dr Chris Pamplin

**Staff writer**
Philip Owen