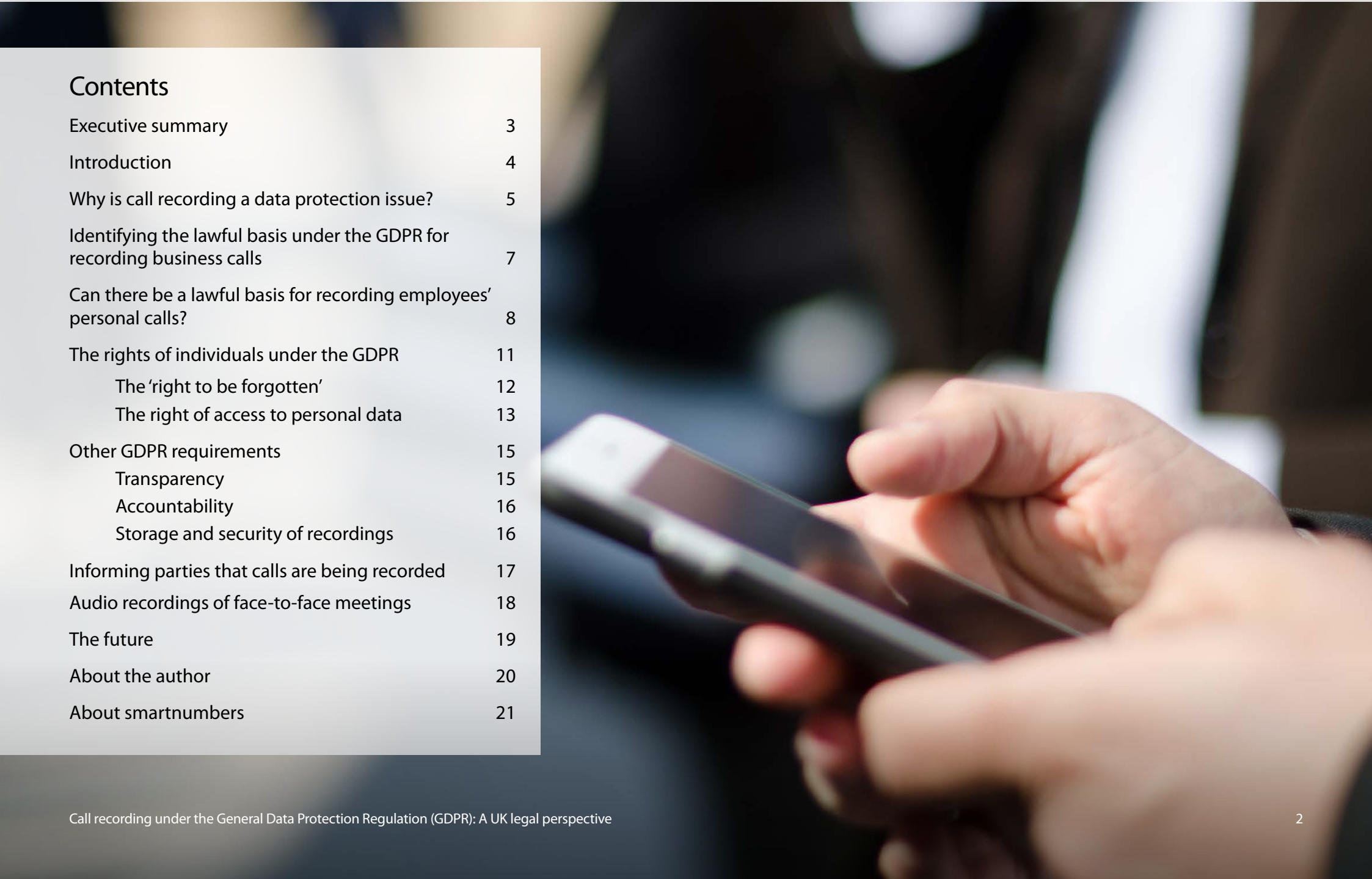
resilient plc

Call recording under the General Data Protection Regulation (GDPR)

A UK legal perspective

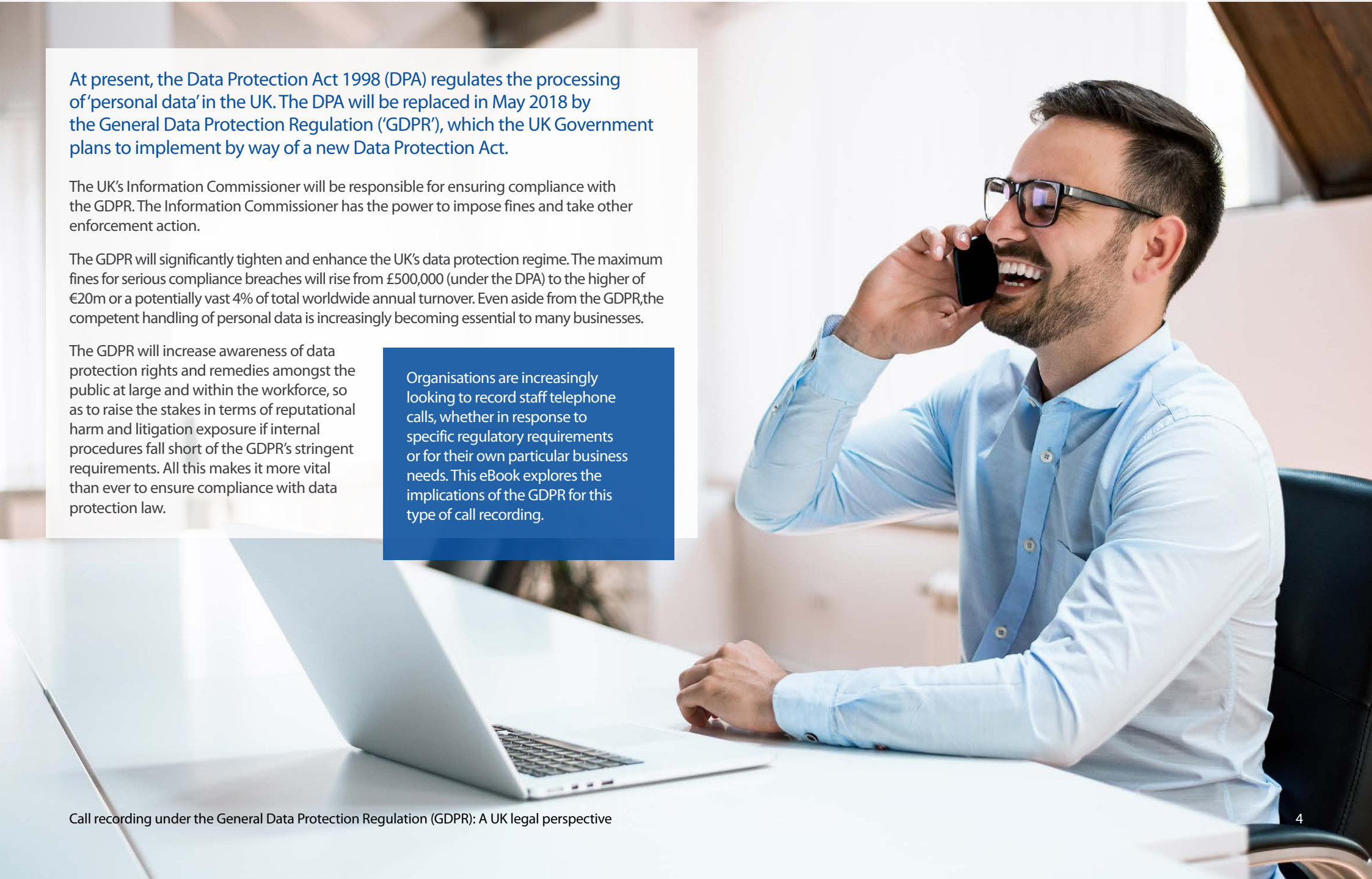


Contents

Organisations are increasingly looking to record calls for compliance, dispute-resolution, training and quality control reasons. In some sectors, such as financial services, there are specific legal requirements to do so.

- From May 2018 onwards, any such call recording will need to comply with the General Data Protection Regulation ('GDPR'). Compliance will be critical – fines under the GDPR will be potentially very substantial.
- The GDPR will apply because recording calls will generally result 'personal data' and, potentially, so-called 'special categories' of personal data being obtained.
- In essence, organisations can record business calls that involve personal data if the legitimate business needs of the organisation which lie behind such recording outweigh any adverse impacts for the individuals in question.
- Organisations can also record calls that involve personal data if that is necessary for compliance with a legal obligation.
- However, if there is a viable option for ensuring that only business calls are recorded, then an organisation that nevertheless adopts a blanket recording policy for the purposes of recording business calls under which personal calls are also inadvertently recorded may well be contravening the GDPR.
- Further, personal calls will be likely to involve special category personal data, and it will generally be very difficult for organisations to justify collecting such data under the GDPR (whether by obtaining explicit consent, or otherwise).
- The GDPR's 'right to be forgotten' will not operate to require the erasure of call recordings if the organisation in question is legally required to make and retain them.
- In all other cases, right to be forgotten requests are likely to cause resource and other difficulties for organisations that record calls, although those difficulties will be lessened if the organisation has taken steps to avoid recording personal calls.
- Similarly, if an organisation records calls, then right of access requests under the GDPR should in general be somewhat easier to navigate if steps have been taken to avoid recording personal calls.

Introduction



At present, the Data Protection Act 1998 (DPA) regulates the processing of 'personal data' in the UK. The DPA will be replaced in May 2018 by the General Data Protection Regulation ('GDPR'), which the UK Government plans to implement by way of a new Data Protection Act.

The UK's Information Commissioner will be responsible for ensuring compliance with the GDPR. The Information Commissioner has the power to impose fines and take other enforcement action.

The GDPR will significantly tighten and enhance the UK's data protection regime. The maximum fines for serious compliance breaches will rise from £500,000 (under the DPA) to the higher of €20m or a potentially vast 4% of total worldwide annual turnover. Even aside from the GDPR,the competent handling of personal data is increasingly becoming essential to many businesses.

The GDPR will increase awareness of data protection rights and remedies amongst the public at large and within the workforce, so as to raise the stakes in terms of reputational harm and litigation exposure if internal procedures fall short of the GDPR's stringent requirements. All this makes it more vital than ever to ensure compliance with data protection law.

Organisations are increasingly looking to record staff telephone calls, whether in response to specific regulatory requirements or for their own particular business needs. This eBook explores the implications of the GDPR for this type of call recording.

Like the DPA, the GDPR regulates the handling of 'personal data'.

Data that is about identifiable individuals generally amounts to their 'personal' data. So, for example, an organisation that records a telephone call in which one party gives his home address is as a result recording personal data about that person (namely, his home address). Further, data can be 'personal' even if the information is not especially private. For example, an organisation that records a call in which an employee mentions that she was present at a meeting earlier that day will be recording personal data about that employee (namely, that she was present at that particular meeting). In addition, data does not need to be accessed or used in any way by a human being before the GDPR can apply. It is enough if an organisation is simply storing the data electronically.

Organisations are increasingly looking to record staff telephone calls, whether in response to specific regulatory requirements or for their own particular business needs. This eBook explores the implications of the GDPR for this type of call recording.

Certain forms of 'personal' data are classified as 'special categories' of personal data under the GDPR. Examples of special category personal data include data that reveals an individual's political opinions or religious beliefs, and data that concerns an individual's health, sex life or sexual orientation.

The special categories are more restrictively regulated by the GDPR than other personal data. It is therefore important to clarify when the recording of a telephone call may result in special category personal data being recorded. It is useful to analyse two types of call in turn – business calls, and personal calls made by employees.

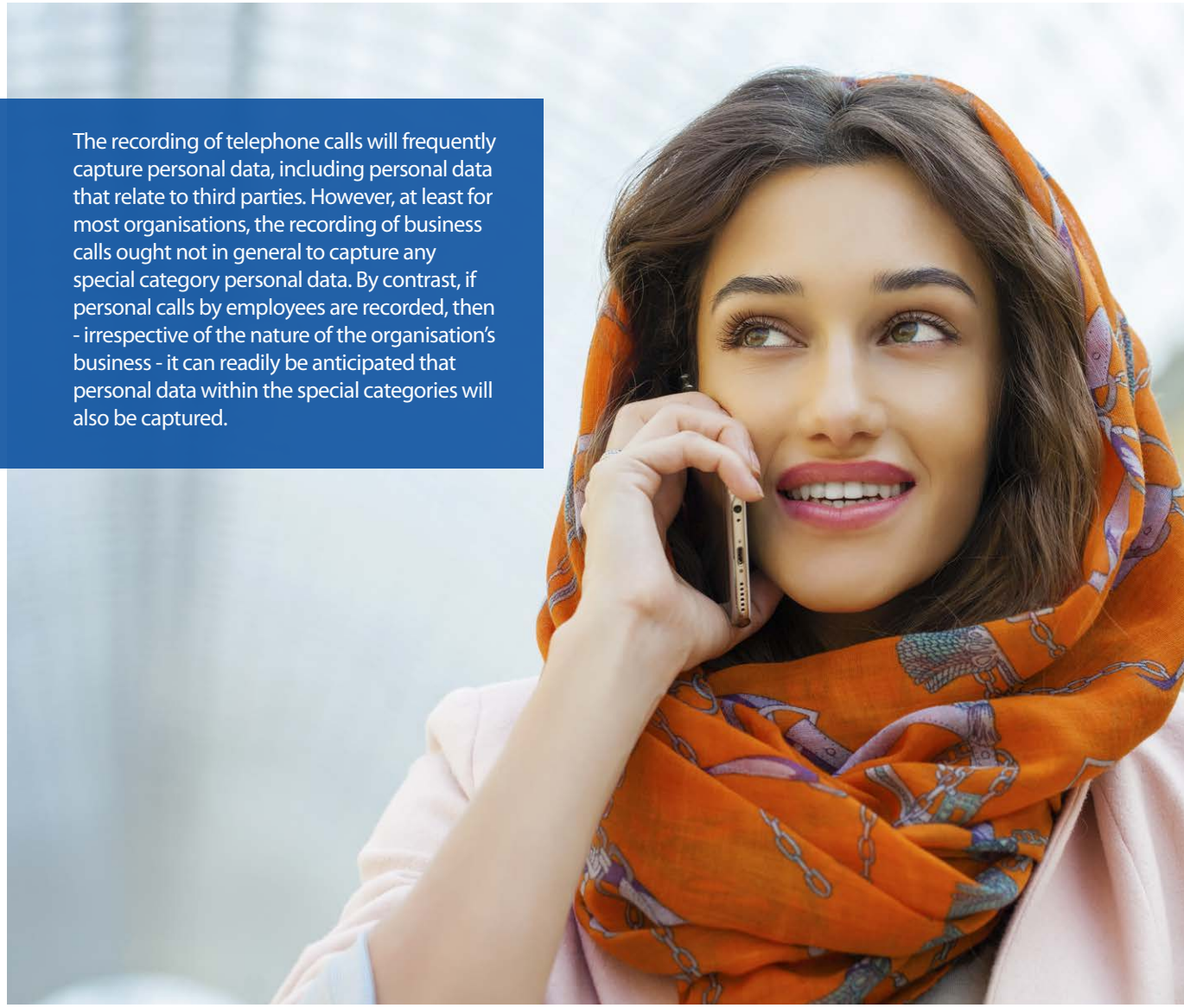
Why is call recording a data protection issue?

The likelihood that business calls will involve special category personal data depends on context. For instance, a health insurance company that records calls with customers will obviously be recording special category personal data - in the form of health information - on a very frequent basis. However, for most organisations, it should in general be unlikely that any given business call will involve special category personal data.

If, however, an organisation records its employees' personal calls (for instance, because the same devices are being used for both business and personal calls) then special category personal data may well be obtained. For instance, an employee may discuss his health in a call with his spouse, or reveal his political opinions in a casual chat about the news with a friend.

One final point should be noted. In the above examples the personal data relate to one or other of the parties to the recorded call. But it is also possible that the personal data or special category personal data will relate to a third party. For instance, during a business call, one employee may tell another than an external consultant was present at a meeting, and so a recording of this call would contain personal data about that external consultant. Similarly, an employee may make a personal call to his spouse to discuss the health of their child. If this call were recorded then the organisation in question would be obtaining special category personal data about the child.

The recording of telephone calls will frequently capture personal data, including personal data that relate to third parties. However, at least for most organisations, the recording of business calls ought not in general to capture any special category personal data. By contrast, if personal calls by employees are recorded, then - irrespective of the nature of the organisation's business - it can readily be anticipated that personal data within the special categories will also be captured.



Identifying the lawful basis under the GDPR for recording business calls

Any organisation that records telephone calls - and so obtains personal data - needs a lawful basis under the GDPR to do so.

As regards business calls, consent is unlikely to provide the requisite lawful basis. First, consent is unlikely to be valid for GDPR purposes if it is obtained from employees who are in effect obliged to consent by their employers. Secondly, there will in general be no practical way to gain the consent of all third parties whose personal data could be obtained by call recording.

By contrast, an organisation can justify recording business calls that potentially involve personal data if that is 'necessary' for compliance with a legal obligation (under article 6(1)(c) of the GDPR). For example, MiFID II will impose a legal obligation on financial institutions to record certain types of telephone call, and that legal obligation will in turn provide a lawful basis for recording those call types.

More generally, an organisation can record business calls that potentially involve personal data if, in essence, the organisation's legitimate business needs makes that 'necessary', and if those business needs are not outweighed by any adverse impacts for the individuals in question (see article 6(1)(f) of the GDPR).

The word 'necessary' in these above contexts means that organisations need to act proportionately. If the legal obligation or business need only applies to certain types of call, then the organisation will have to adopt a recording policy that is reasonably 'targeted' towards recording those types of call. Finding such a suitably targeted policy will require the organisation to consider the various policies and systems that could be used for call recording, and in particular consider the extent to which they minimise the number of other calls that may inadvertently be recorded alongside the types of call that the organisation is obliged, or needs, to record.

In addition, organisations will need to identify the likely benefits of its recording policy, and the likely adverse affects of that policy on individuals and their privacy rights, so as to be able to properly assess whether its business needs are outweighed by those adverse affects. In general, the more the business calls focus on the particular circumstances of individuals, the greater the business need will need to be both to make the recording of those calls 'necessary' and to ensure that those needs are not outweighed by the adverse impacts of call recording.

If, given the particular organisation at issue, business calls are likely to routinely involve special category personal data then specialist advice should be sought on whether call recording can comply with the GDPR.

Can there be a lawful basis for recording employees' personal calls?

resilient plc

It is very unlikely that an organisation would ever have a legitimate business need to specifically record the personal calls of their employees that could outweigh the adverse impacts on the parties to such calls of such recording.

So, even if the personal calls were only to involve personal data and not special category personal data, an organisation could not in general specifically seek to record such calls in the absence of a direct and specific legal obligation to do so.

Could an organisation nevertheless justify recording personal calls on the basis that it has to have, in effect, a blanket recording policy in order to make sure that it successfully records the business calls that it has a legitimate business need to record, or that it has a legal obligation to record?

There are two difficulties with a blanket policy of this type The first is that at least in general a blanket recording policy that leads to the recording of personal calls may well fail the proportionality test. This is the case irrespective of whether the organisation is seeking to rely on the legal obligation basis or the legitimate business needs basis to justify its policy for the purposes of the GDPR.

As regards the legal obligation basis:

- If there is a viable option available that would ensure that only business calls are recorded, then an organisation that is subject to a legal obligation to record certain business calls may well find it difficult to justify - as being 'necessary' to comply with that legal obligation - a blanket recording policy under which personal calls are also recorded.
- In particular, in these circumstances, it is difficult to see how it would be 'necessary' to record personal calls in order to ensure that the business calls that by law have to be recorded are indeed recorded.
- In the absence of some other GDPR justification for recording the personal calls, such recording would in all likelihood contravene the GDPR.

As regards the legitimate business needs basis:

- If the recording policy will lead to personal calls being recorded then the likely adverse impacts for individuals will generally be very significant. This in turn means that the likely adverse impacts of call recording may well outweigh the legitimate business needs that are being relied on.
- Further, and whether or not the adverse impacts outweigh the business needs, no blanket policy that leads to the recording of personal calls is likely to be 'necessary' if there is a viable option available that would ensure that only business calls are recorded.
- Thus, again, in the absence of some other GDPR justification for recording personal calls, such recording would in all likelihood contravene the GDPR.

The GDPR's new requirement of 'data protection by default' makes the above difficulty more acute in that, among other things, this requirement obliges organisations to implement appropriate technical measures to ensure that, by default, only personal data that are necessary for their aims are collected. A system that ensures that only business calls are recorded is an example of the type of 'technical measure' that, if available, data protection by default is likely to require.

The second difficulty with a blanket recording policy flows from the fact that recording personal calls is likely to result in special category personal data being obtained, including special category personal data that relate to individuals who are not parties to the calls in question. These two features of personal calls make it much harder to record them without contravening the GDPR:

- While an organisation may record and store special category personal data if the individual in question has explicitly consented, in practice consent is very unlikely to provide a means for achieving compliance. As already noted, it is difficult for an employer to obtain valid consent from its employees if in reality they are obliged to give their consent. It is harder still to reliably obtain such explicit consent from individuals outside the organisation who are parties to personal calls. Further, it will be all but impossible to obtain such explicit consent from all third parties whose special category personal data might be discussed during personal calls.
- In the absence of explicit consent the GDPR only permits special category personal data to be obtained for certain specified and carefully limited purposes, and in general few organisations will be able to rely upon them in the context of call recording.

Can there be a lawful basis for recording employees' personal calls?

Assume that an organisation wants to record all its business calls, and is considering adopting a blanket recording policy to achieve that, but at least some of the telephone lines in question (whether mobile or fixed-line) are in practice also used for at least some personal calls. A blanket policy will obviously lead to those personal calls being recorded, which in turn means that the organisation is likely to be recording special category personal data about the parties to the calls, and about third parties.

Even if this is only inadvertent, the fact that the organisation is likely to be recording special category personal data will in turn attract much greater scrutiny of its recording policy and, more importantly, give rise to acute compliance issues under the GDPR.

Further, if there is viable approach that avoids recording personal calls then, in general, the organisation will be breaching the GDPR if it fails to take that approach and instead adopts a blanket policy. Any such breach of the GDPR will expose the organisation to the risk of a potentially vast fine, together with other significant reputational and legal risks.

The final issue is whether GDPR compliance can alternatively be achieved by policy only - notably by the creation of a staff policy that prohibits employees from making personal calls on business devices. Anecdotal evidence suggests that some organisations have adopted or at least considered adopting this approach.

If a staff policy of this type is in place, and if it is generally complied with and enforced, then an organisation can reasonably argue that a blanket recording policy is justified because all recorded calls should be business calls.

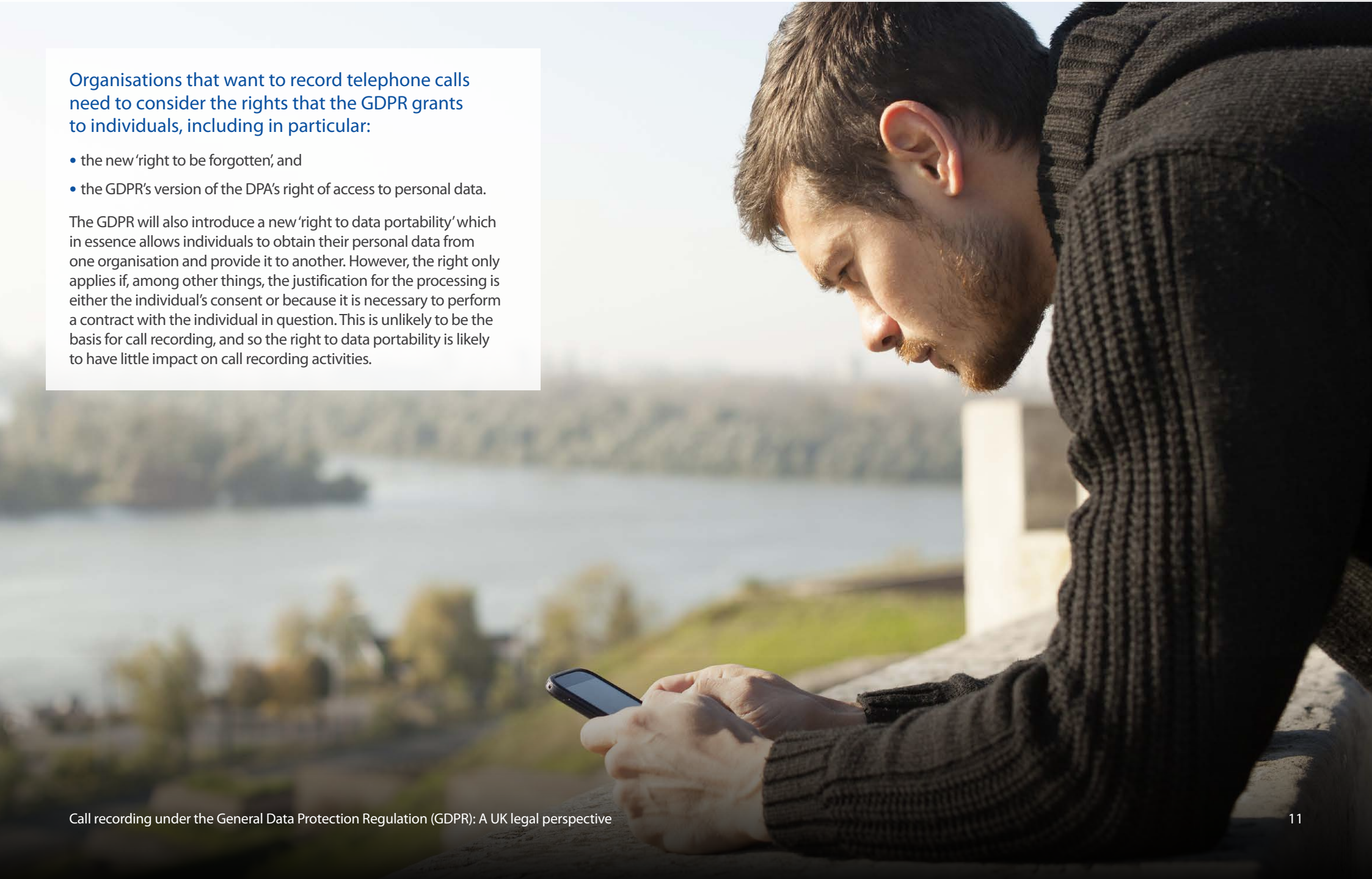
However, if a staff policy of this type is in place but in practice it is not complied with or enforced, then the Information Commissioner's view appears to be that merely having such a policy will not justify blanket recording. In other words, a staff policy that prohibits personal calls but that does not in practice reflect the reality is unlikely to save an organisation that knows or should know that it is recording private and intimate information, and special category personal data, in a way that may well not comply with the GDPR's stringent requirements.

The rights of individuals under the GDPR

Organisations that want to record telephone calls need to consider the rights that the GDPR grants to individuals, including in particular:

- the new 'right to be forgotten', and
- the GDPR's version of the DPA's right of access to personal data.

The GDPR will also introduce a new 'right to data portability' which in essence allows individuals to obtain their personal data from one organisation and provide it to another. However, the right only applies if, among other things, the justification for the processing is either the individual's consent or because it is necessary to perform a contract with the individual in question. This is unlikely to be the basis for call recording, and so the right to data portability is likely to have little impact on call recording activities.



The 'right to be forgotten'

The DPA provides limited opportunities for individuals to require organisations to erase their personal data. By contrast, the GDPR will introduce a much more wide-ranging 'right to be forgotten'. Organisations should not assume that this will remain a technical and obscure data protection right. The right to be forgotten may well become widely known about and frequently exercised, at least if the take-up of an earlier version of this right - as exercised against internet search engines - is any guide.

Where it applies, the GDPR's right to be forgotten gives individual the right to require organisations to erase records of their personal data. Importantly, this would include any parts of any recordings of telephone calls that constitute their personal data.

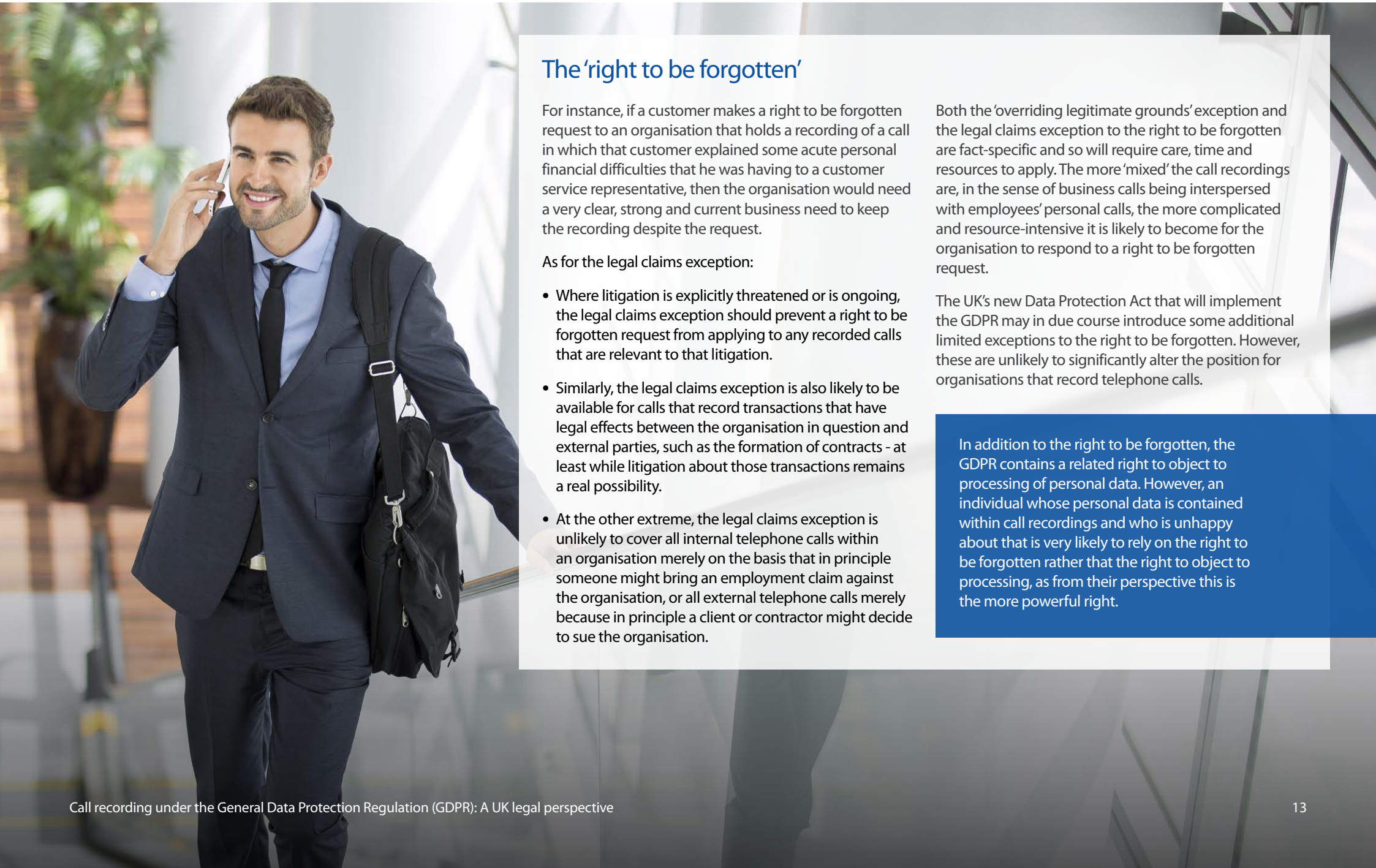
However, the right will not apply to a call if it was 'necessary' to record that call (and keep the recording) in order to comply with a legal obligation. This legal obligation exception to the right to be forgotten will most obviously be relevant for financial institutions that are subject to MiFID II. The exception will in particular mean that the right to be forgotten cannot operate so as to require the erasure of the call recordings that financial institutions are legally required to retain.

What is the position if an organisation is relying on its business needs, rather than a specific legal obligation, to justify recording calls?

Even in this context, the right to be forgotten is not an absolute right. However, in order to be able to retain any particular recordings of personal data in the face of a right to be forgotten request by the individual to whom the data relates,
the organisation will in general either need to establish 'overriding legitimate grounds' to do so, or it will need to be able to show that doing so is 'necessary'
to establish, advance or defend against legal claims.

If the personal data in question is not especially private then the organisation's business need to retain the calls will generally not need to be particularly weighty to be 'overriding'. For instance, an organisation would not need particularly strong reasons to justify retaining personal data that consisted of records of routine business activities by an identified employee in the face of a right to be forgotten request by that employee.

By contrast, if the personal data in call recordings is of a private or intimate nature then the business need to retain those records will need to be much greater if it is to be 'overriding'.



The 'right to be forgotten'

For instance, if a customer makes a right to be forgotten request to an organisation that holds a recording of a call in which that customer explained some acute personal financial difficulties that he was having to a customer service representative, then the organisation would need a very clear, strong and current business need to keep the recording despite the request.

As for the legal claims exception:

- Where litigation is explicitly threatened or is ongoing, the legal claims exception should prevent a right to be forgotten request from applying to any recorded calls that are relevant to that litigation.
- Similarly, the legal claims exception is also likely to be available for calls that record transactions that have legal effects between the organisation in question and external parties, such as the formation of contracts - at least while litigation about those transactions remains a real possibility.
- At the other extreme, the legal claims exception is unlikely to cover all internal telephone calls within an organisation merely on the basis that in principle someone might bring an employment claim against the organisation, or all external telephone calls merely because in principle a client or contractor might decide to sue the organisation.

Both the 'overriding legitimate grounds' exception and the legal claims exception to the right to be forgotten are fact-specific and so will require care, time and resources to apply. The more 'mixed' the call recordings are, in the sense of business calls being interspersed with employees' personal calls, the more complicated and resource-intensive it is likely to become for the organisation to respond to a right to be forgotten request.

The UK's new Data Protection Act that will implement the GDPR may in due course introduce some additional limited exceptions to the right to be forgotten. However, these are unlikely to significantly alter the position for organisations that record telephone calls.

In addition to the right to be forgotten, the GDPR contains a related right to object to processing of personal data. However, an individual whose personal data is contained within call recordings and who is unhappy about that is very likely to rely on the right to be forgotten rather that the right to object to processing, as from their perspective this is the more powerful right.

The right of access to personal data

The GDPR grants individuals a right to be provided on request with the personal data that organisations hold in relation to them. This right is similar to an existing right under the DPA and so is not an innovation on the part of the GDPR. However, given that the GDPR is likely to increase public awareness of data protection issues and rights, it is worth reflecting on the practical impact of this right where personal data is held by organisations in recordings of telephone calls.

The key practical issue is that when providing personal data in response to a request for access an organisation cannot 'adversely affect the rights and freedoms of others'. In simple terms, this means that organisations will not necessarily be able to respond to a right of access request from, for instance, a former employee by simply providing all the recordings of his or her telephone calls. In particular, those calls will in all likelihood contain the personal data of other individuals, and there may be circumstances in which that personal data cannot be disclosed because it might prejudice those other individuals, most obviously where the data in question is particularly private.

This poses resource challenges for any organisation that faces a request for access. Further, and as with the right to be forgotten, this resource challenge is likely to be much greater if the organisation holds recordings of personal calls in addition to business calls. This is because personal calls are generally much more likely to contain the personal data of others that is particularly private in nature, and such data is likely to crop up in unpredictable ways during personal calls.

The risk for an organisation that records personal calls is therefore that a right of access request might require it to listen in detail to all relevant personal calls, and make difficult and time-consuming judgments about what could and could not be disclosed.

The need for a lawful basis for call recording is only one of a number of requirements of the GDPR that needs to be considered.

Organisations that want to record telephone calls also need to comply with the additional requirements that the GDPR imposes in relation to:

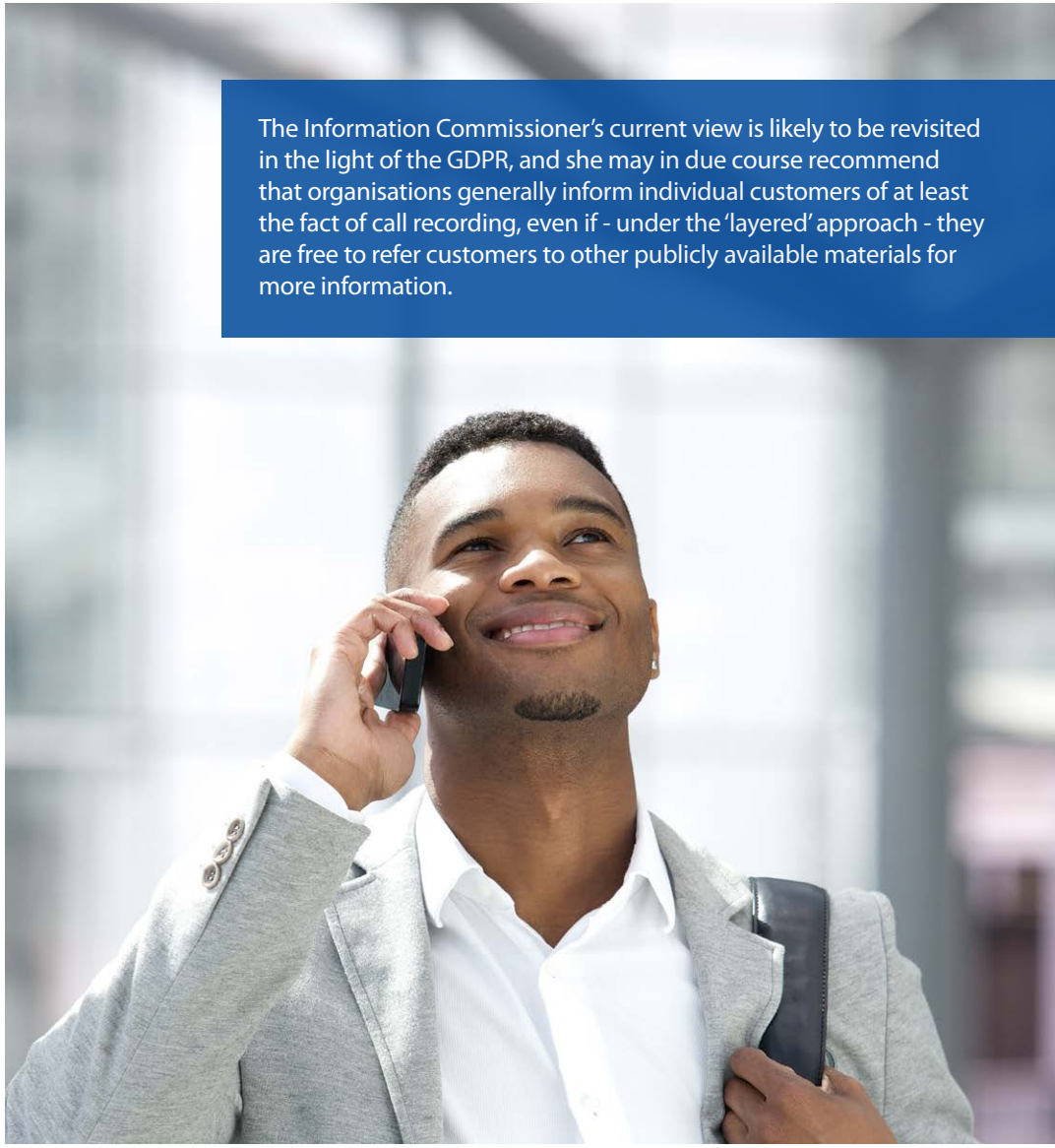
- transparency,
- accountability, and
- data storage and data security.

Transparency

Article 13 of the GDPR requires organisations that obtain personal data directly from individuals to provide information to those individuals on how and why it will process their personal data, including as regards any call recording activities. The information in question is more than was required by the DPA's transparency requirements, and it includes the purpose of the call recording, its legal basis (together, if the organisation is relying on its legitimate business needs, with a statement of those) and the existence of the principal rights granted to individuals by the GDPR. The Information Commissioner has indicated in her latest Code of Practice on Privacy Notices that it may be possible to provide the requisite information in 'layered' form in the sense that individuals can be given the key information upfront and an opportunity to easily obtain the remainder, for instance by clicking on a website link.

As regards telephone call recording, all affected staff should be specifically informed of an organisation's recording policy and all the detailed article 13 information should also be made readily available to them. This may for instance be done by including the detail in intranet staff policies.

An organisation that records calls will also need, at the very least, to make the requisite article 13 information readily available to external callers. For instance, all this information could be included, in 'layered' form, in the privacy / legal section of the organisation's website. When will organisations need to go further and directly inform callers about call recording? The Information Commissioner's current view under the DPA is that organisations do not generally need to tell customers that their calls are being recorded. However, the Information Commissioner's current Employment Practices Code also suggests that if it would not be 'obvious' in the particular context at issue that recording might occur, then organisations should consider ensuring that callers are informed.



The Information Commissioner's current view is likely to be revisited in the light of the GDPR, and she may in due course recommend that organisations generally inform individual customers of at least the fact of call recording, even if - under the 'layered' approach - they are free to refer customers to other publicly available materials for more information.

Accountability

Although not specific to call recording, organisations need to be aware that the GDPR will introduce a new accountability principle that requires them to be able to demonstrate compliance with the key data protection principles in the GDPR. Part of this will involve maintaining documentation that covers the organisation's processing activities, including any call recording.

Further, organisations with 250 or more employees, or which process data in various sensitive ways, will need to maintain specific and relatively detailed records of their processing activities. Again, this would include any call recording activities.

Finally, where the introduction of call recording would give rise to a 'high risk' to the rights and freedoms of individuals, an organisation will first need to carry out a 'data protection impact assessment' (a version of what is currently called a 'privacy impact assessment') and may need to consult with the Information Commissioner. High risk processing includes the processing on a large scale of special categories of data, including health data. It follows that health insurance companies and medical institutions that want to record calls with customers and patients are likely to need to first conduct a formal data protection impact assessment. For most organisations, however, it appears unlikely that the GDPR requirement to conduct a DPIA will apply to any call recording activities that they undertake.

Storage and security of recordings

The recordings must be securely stored with appropriate technical and organisational measures in place to protect them from unauthorised access – both internally by employees and externally by third parties.

The number of employees who are authorised to access the recorded calls should be kept to a minimum, and they should be subject to appropriate confidentiality requirements and given appropriate data protection training to ensure that they handle the recordings appropriately.

Unless there is a legal or regulatory requirement to keep the recordings for a particular time period, the organisation will have to set its own retention period (or periods). This should be no longer than is necessary for the legitimate business needs that the organisation is relying on to justify its recording policy, and it may be that different retention periods are appropriate for different categories of call. The recordings must be securely erased after the end of the relevant retention period or periods.

Informing parties that calls are being recorded

Both the DPA and the Lawful Business Practice regulations (LBP) requires that employees be informed of any systematic recording policy that will affect them.

However, should individuals outside the organisation who make calls to, or receive calls from, employees also be informed of the recording policy?

The LBP Regulations do not require this. As regards the DPA, any call recording policy should be referred to in an appropriate section of the organisation's website (such as the 'contact us' page).

Is anything else required?

The Information Commissioner has stated that individuals should generally expect that organisations will record calls, so that they do not need to be specifically informed of this during calls (for instance, by way of a recorded message). There are signs that business practice increasingly reflects this. In general, therefore, if individuals outside an organisation would generally expect that their calls might be recorded by that organisation then the DPA is unlikely to require that those individuals be specifically informed of any recording policy during each call. The Information Commissioner's position on this issue is not however entirely clear, and if it would not be 'obvious' in the particular context at issue that recording might occur, then the Code of Practice advises organisations to consider using a recorded message, or instructing its employees, to inform callers of this.

What if an organisation wants to record face-to-face meetings?

Assuming that such meetings are only recorded as a result of some human intervention (by, for instance, the pressing of a 'record' button), then organisations can ensure that only business meetings are recorded by instructing employees to only use the recording devices for such meetings. Accordingly, the difficulties associated with inadvertently recording personal calls are unlikely to arise in the case of recordings of face-to-face meetings.

Aside from this, the above GDPR analysis of call recording applies equally to recording face-to-face meetings, with one exception.

The exception is that it is possible that the transparency requirements for recording face-to-face meetings may be greater than in the case of call recordings. This is because customers are less likely to be familiar with meetings being recorded than telephone calls being recorded.

At present, no GDPR analysis can be fully definitive. The picture is evolving - regulators have not yet finished issuing their guidance on the GDPR, and the text of the UK's new Data Protection Bill has not yet been published. The analysis in this eBook is therefore subject to future changes and developments.

When it occurs, Brexit will require some amendments to the UK's data protection regime. In all likelihood, however, the stringent requirements of the GDPR will continue to underpin the UK's approach to data protection in the years that follow.

At present, the Lawful Business Practice Regulations (LBP Regulations) provide a basis for recording business calls without falling foul of the Regulation of Investigatory Powers Act 2000 (which places limits on when telephone calls can be recorded). In essence, the LBP Regulations permit a call recording policy so long as staff are informed and the policy is solely for the purpose of recording calls that are relevant to the organisation's business. Thus the LBP Regulations in general add nothing to the GDPR analysis. The Regulation of Investigatory Powers Act 2000 is in the process of being replaced by a new Act, the Investigatory Powers Act 2016. At some stage the LBP Regulations will similarly be replaced. However, there is at present nothing to suggest that the eventual new replacement will significantly alter the effect of the LBP Regulations.

Ben Hooper is an independent consultant specialising in data protection and privacy, and the strategic implications of the regulatory regimes that operate in those areas.

He principally advises companies in the technology and telecoms sectors.

Between 2000 and 2015, he was a barrister at 11KBW, a leading set of chambers in public and information law. At 11KBW Ben specialised in data protection law and the right to privacy, and he acted for and advised the UK Government, the Information Commissioner and regulated entities in a broad range of industry sectors.

About smartnumbers

smartnumbers mobile is the first mobile service in the UK that enables firms to achieve compliance with GDPR for their mobile call recording. By ensuring that whilst business calls are recorded, personal calls remain private, firms can meet both the MiFID II and GDPR regulations.

This eBook is not intended to be a source of legal advice, and should not be relied on as such.

Ben Hooper
29 August 2017