Shulmans

General Data Protection Regulation (GDPR)

Getting it right

Driven by results

Let our experts support you on your GDPR compliance journey

Data protection compliance in the UK is currently governed by the Data Protection Act 1998 (**DPA**) – a UK statute implementing the UK's interpretation of a 1995 European Directive. The DPA is primarily based on a set of eight key principles which must be complied with whenever handling personal data in the UK.

For a more harmonised approach to data protection, the EU member states have been negotiating for the last few years in an effort to reach agreement on the new General Data Protection Regulation (**GDPR**). The new GDPR came into force on 24 May 2016, with a transition period of two years, meaning it takes full effect on 25 May 2018. It will automatically take effect in all countries which are member states of the EU on that date.

Your compliance journey starts here

Doesn't Brexit change all that?

Now we know the Brexit deadline is in March 2019, organisations in the UK will still need to comply with EU legislation (including GDPR from 25 May 2018) or risk being in breach.

As confirmed by the Queen's Speech in June 2017, the UK will be implementing its own legislation in place of GDPR and the Data Protection Bill (Bill) entered parliament in September 2017. The Bill will try to make the UK's data protection laws fit for the digital age post Brexit. The Bill aims to ensure that the UK will be regarded as a sufficiently compliant country with which the remaining European member states can safely transfer data and conduct business.

We all need to prepare for and adapt our approach to data in order to meet the more stringent regime of the GDPR. Achieving compliance with the GDPR is essential for all organisations handling personal data to ensure they are compliant with the UK's implementation of GDPR upon Brexit.

> We all need to prepare for and adapt our approach to data to meet the more stringent regime of the GDPR

It is worth revisiting some of the key terminology and bearing this in mind when considering your approach to GDPR:

Personal Data

Information relating to an identified or identifiable natural person (so not the name of a company for example). GDPR confirms this can now involve a range of factors specific to that person and can include an online identifier, location data or a name and identification number.

Controller

The organisation which alone or jointly determines the purpose and means of processing personal data.

Processor

The organisation which processes personal data on behalf of the controller.

Data Subject

The living individual who can be identified from the personal data and who is afforded rights in respect of such personal data.

Special categories of personal data

This was previously known, under the DPA, as 'sensitive personal data' and remains largely unchanged by GDPR, as personal data which reveals an individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sex life or sexual orientation. Under GDPR genetic and biometric data used to identify a person is now included in this definition.

Which organisations does GDPR apply to?

Data controllers are organisations which decide how the data they hold is processed, whereas a data processor is an organisation which carries out that processing on behalf of a data controller.

Up until now the DPA has directly applied to all data controllers only and has not applied directly to data processors. This substantial gap has been filled by the new GDPR applying to both data controllers and processors of data.

The GDPR applies to all organisations established within the EU regardless of whether they actually process their data in the EU. So any business incorporated as a company or limited liability partnership or any partnership or sole trader with a registered trading address in the EU will have to be compliant with the GDPR even if the only data they are dealing with relates to individuals located outside the EU.

The GDPR applies to all organisations that process data of individuals who are in the EU, if the processing relates to either offering goods or services to people in the EU (even if no payment required) or monitoring behaviour of individuals if the behaviour occurs in the EU.

So the controller or processor organisation need not be incorporated or have any branch office within the EU at all. For example, a US website capable of accepting orders placed by EU citizens online will therefore now be governed by the GDPR. An Indian call centre accepting calls from consumers located within the EU will be governed by the GDPR. This latter example is regardless of whether the organisation for which the Indian call centre is providing that outsourced service is located within the EU or outside it.

Even if your organisation only trades with other businesses, you are likely to have personal data of the contact at that business and so GDPR will apply to that data.

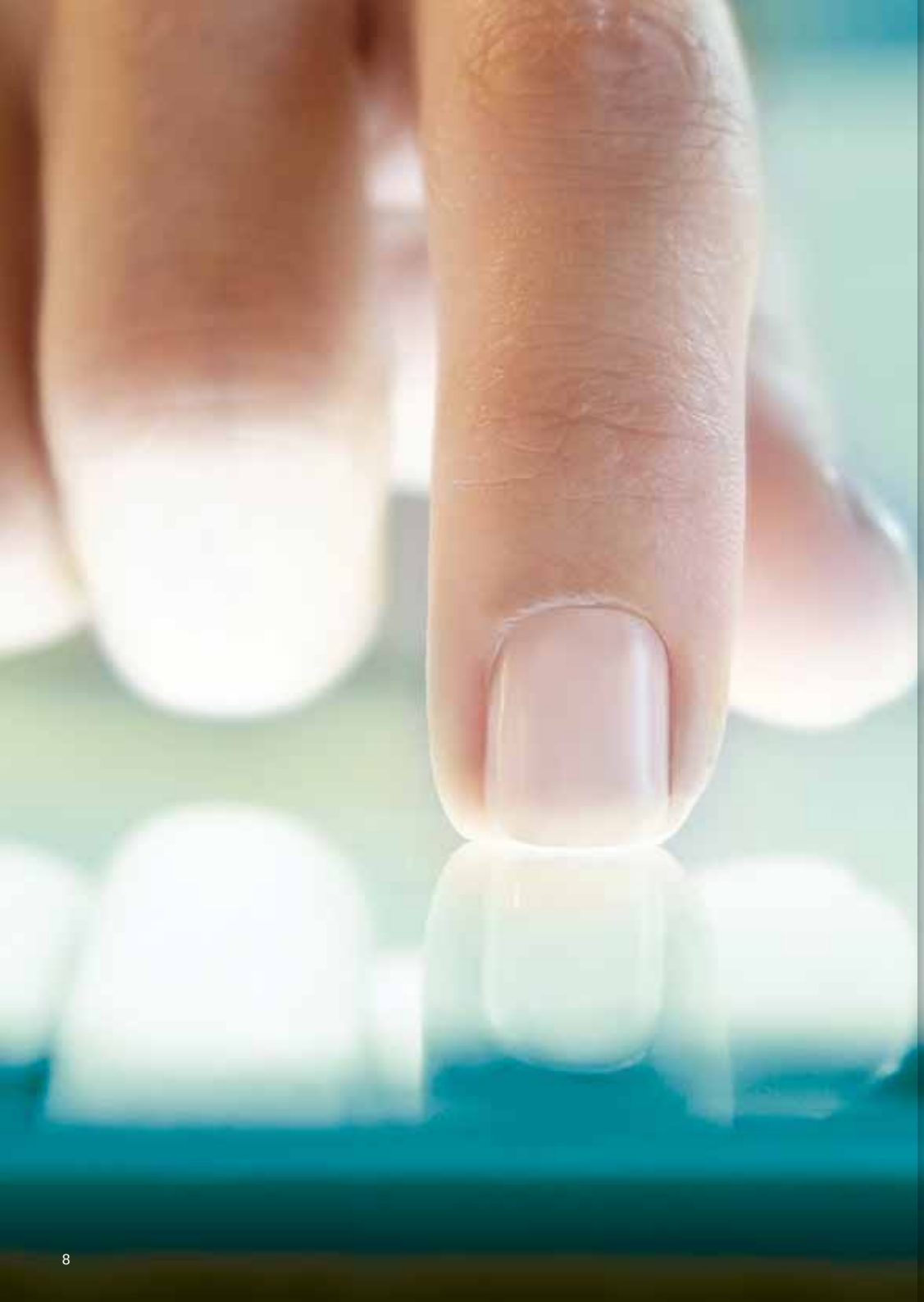
Most organisations hold personal data about its people if nothing else and so GDPR will apply to that data.

Key Features:

What are the key features of GDPR?

If you're already doing things right under the DPA, you're well on the way to GDPR compliance. Lots of concepts will be familiar so we've highlighted here some of the particular issues we know organisations have questions about. Of course, there's much more to it than this, and we'd love to come and talk to you about that detail when you are ready to do so, but in the meantime we think you should at least be aware of the following key issues:

- Data Protection Officer appointment
- Breach notification
- Data Protection by design/by default
- Conditions for processing and consent
- Enhanced data subject rights
- Changes in sanctions



"Don't view getting data protection right as something you're being forced to do; view it as something that you really want to do because it helps you build better, stronger relationships with your customers"

Source: Garreth Cameron, Group Manager (Business and Industry), ICO

Who needs to appoint a Data Protection Officer?

The appointment of a designated individual to be responsible for data protection in an organisation has, to date, been an optional role. The GDPR now makes the appointment of a Data Protection Officer (DPO) a mandatory requirement for both controllers and processors in the following circumstances:

1	If the organisation in question is a public authority (save for judicial courts);
2	If an organisation's core activities involve processing which requires 'regular and systematic monitoring' of individuals on a large scale; or
3	If an organisation's core activities involve processing on a large scale of the particularly sensitive categories of data (including data on criminal convictions or offences).

The independent European advisory body on data protection known as the Article 29 Data Protection Working Party (**WP29**) has issued guidance around the appointment of data protection officers which helps in working through some of the terminology of these criteria.

'Core activities' are those which are key operations for the organisation in question, rather than ancillary functions such as simply managing and paying staff and supporting internal IT systems. However, it is also clear that the intention is for processing which is inextricably linked to the organisation's core activity should be included within that definition.

So, by way of an example given by WP29 in their guidance, whilst a hospital's core activity is clearly providing health care, it cannot perform that core activity without processing patient's health records. Processing such records is therefore to be considered as part of the hospital's core activities.

Similarly, what constitutes 'large scale' is not given a specific definition in the GDPR. However, factors likely to impact on the question will include: the number of data subjects affected, the volume of data or range of data fields being processed, duration or permanence of the data processed and the geographical extent of the data processed.

It's important to remember that even if an organisation chooses to voluntarily appoint a DPO, despite not meeting the mandatory designation requirements, that person will be obliged to meet the criteria and perform the role in accordance with the GDPR.

Therefore, if an organisation doesn't meet the designation requirements and doesn't wish to voluntarily appoint someone as a DPO, it needs to be very careful about clarity around the role, title and status of any other individuals they employ or engage to work on protecting personal data or dealing with privacy matters for the organisation. You don't want them to be accidentally regarded as the DPO and fall under the specific technical requirements of that role if it isn't the intention for them to do so.

Who should be the Data Protection Officer?

The independence and importance of the role of Data Protection Officer under the GDPR is a significant area of change from previous legislation.

Whilst setting out specific criteria for the appointment, the GDPR also affords certain new protections to someone fulfilling the role of the DPO.

A DPO does not take on personal liability for data protection compliance within the appointing organisation; that remains the ultimate responsibility of the organisation which has appointed them to their role. It's up to the organisation to ensure that the DPO is involved in all issues relating to data protection and also that their contact details are published and provided to the Information Commissioner's Office (**ICO**) as the regulatory authority for data protection in the UK.

The DPO can be an employee or be engaged as a contractor on the basis of a service contract and can also be appointed to act in this role for different organisations, provided the DPO is 'easily accessible from each establishment'. It is clear that the requirement is for someone who is personally available to those within the organisation as well as to the regulatory authority.

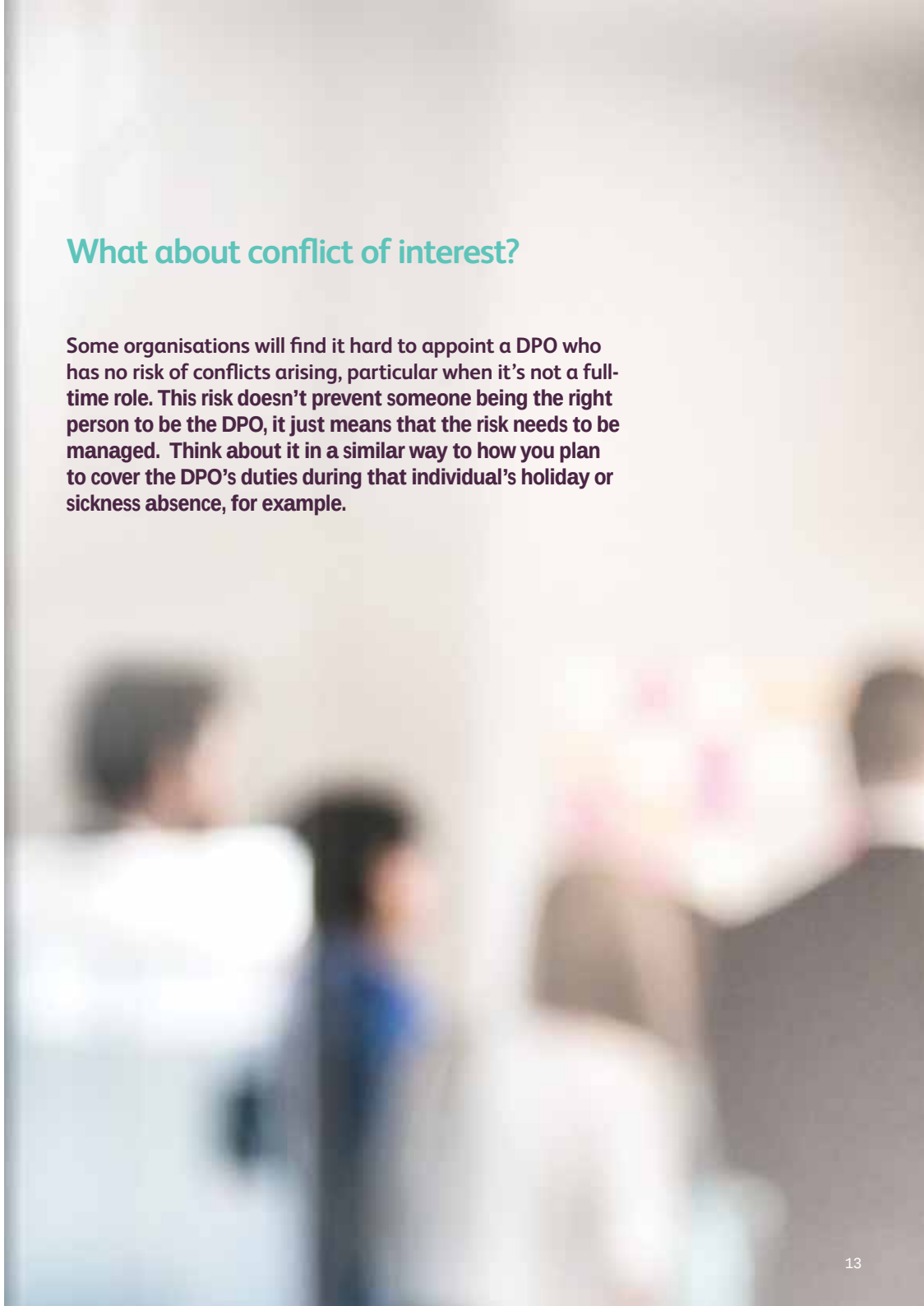
The DPO can fulfil the role alongside other duties within the organisation, so essentially it can be considered a part-time function, provided the other duties or roles undertaken by that individual do not put them in a position of a conflict of interest.

The person fulfilling the role of DPO for an organisation must have sufficient professional qualities and expert knowledge of data protection law to enable them to fulfil the specified tasks required by GDPR. Whilst such concepts as 'sufficient levels' of expertise and precisely what is meant by 'professional qualities' are not defined, this approach has been taken in order to allow organisations to view such questions in light of the complexity of their processing activities, considering factors such as the sensitivity and volume of data being processed, the level of risk to individuals from that processing and nature of protection needed. Being well-versed in the GDPR as well as being able to maintain and regularly update that expert knowledge is clearly a base level expectation.

The protection set out in the GDPR for the role of DPO includes that a DPO cannot be instructed in the exercise of their tasks by the organisation nor can they be dismissed or penalised by the controller or processor appointing them for simply performing their tasks. The organisation appointing the DPO must provide that individual with the necessary resources and support to enable them to fulfil those tasks, including ensuring they have regular access to and directly report into the highest management of the organisation.

What about conflict of interest?

Some organisations will find it hard to appoint a DPO who has no risk of conflicts arising, particular when it's not a full-time role. This risk doesn't prevent someone being the right person to be the DPO, it just means that the risk needs to be managed. Think about it in a similar way to how you plan to cover the DPO's duties during that individual's holiday or sickness absence, for example.



What do organisations have to do if they suffer a data security breach?

The notification requirements if an organisation suffers a personal data breach is a specific area of increased stringency imposed by the GDPR.

To date, under the UK's data protection laws, there has been no general legal obligation to notify either the regulator or the individuals affected by a breach of data security. Making such notifications has, until now, been at the discretion of the controller in consideration of the context of the breach itself. There is guidance, however, from the UK's regulator, the ICO, as to their view of when notification both to them and to affected individuals should be made.

The GDPR takes a much more structured and mandatory approach to this issue. So if a data controller organisation suffers a personal data breach, that is to say, any "breach of security which leads to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of or access to, personal data transmitted, stored or otherwise processed", then it must notify the ICO, without undue delay and not later than 72 hours after becoming aware of it. The only exception to this is if the breach is unlikely to result in a risk to the rights and freedoms of the individuals whose data is breached.

A processor experiencing a personal data breach is now required to notify the controller on behalf of which they process data, without undue delay on becoming aware of such a breach, which again forms a new mandatory obligation under the GDPR.

If a data controller organisation suffers a personal data breach, then it must notify the ICO, without undue delay and not later than 72 hours after becoming aware of it, even if the breach happens over a weekend.

There are some minimum requirements of the notice provided to the ICO, so it must at the very least do the following:

- describe the nature of the personal data breach, including the categories and approximate number of affected individuals and the records concerned;
- provide the name and contact details of the data protection officer or other contact point where more information can be obtained:
- describe likely consequences of the personal data breach; and
- describe measures taken or proposed to address the breach, including to mitigate possible adverse effects.

If you can't provide all the above within the 72 hours, guidance has confirmed that it is possible to phase notification, but you must still tell the ICO within that 72 hours. In terms of when an organisation which has experienced a personal data breach is obliged to notify the affected individuals, this is now mandatory and also must be done without undue delay, but only if the breach is likely to result in a high risk to the rights and freedoms of the affected individuals. This notification must contain, as a minimum, the last three items listed above as well as being required to be in plain and clear language.

The exemptions to the notification requirement to affected individuals apply in any of the following circumstances:

- the controller has implemented measures that apply to the affected personal data and which renders that data unintelligible to any person not authorised to access it, such as encryption;
- the controller has taken subsequent measures which mean the high risk to rights and freedoms of individuals is no longer likely to materialise; or
- it would involve disproportionate effort – in which circumstance a public communication is required instead or similar measure which informs the affected individuals in an equally effective manner.

What is meant by data protection by design or by default?

Any data controller, that is any individual or organisation which determines the purposes and means of processing any personal data, has to not only ensure that processing complies with the GDPR, but also that it can demonstrate such compliance.

This means implementing appropriate technical and organisation measures, including data protection policies, to ensure and demonstrate such compliance.

Part of demonstrating compliance are two concepts known as 'data protection by design and data protection by default'. These concepts are essentially a requirement for data controllers to ensure that at the time of determining and developing any new method of processing, that a commitment to data minimisation as well as compliance with the data protection principles are integral to the process. The authorities want to see a commitment to reducing the amount of data being processed to meet the specific purpose for which it has been collected in the first place.

These concepts of not just complying, but being seen to be complying and data protection by design and by default are all about enabling a deeper interrogation by the regulatory authorities of processes and systems. The aim is to ensure that compliance is really an embedded cultural position rather than something to which an organisation simply pays lip service.

If an organisation is working with another party to determine the processing of data they may well be regarded as joint controllers and, whilst this means they can come to an arrangement between them as to their respective responsibilities, a data subject can exercise their rights against either of them.

What's an impact assessment and when should they be done?

As with so many aspects of data protection legislation, impact assessments are not a new concept, but use of them was not mandatory under the UK's Data Protection Act 1998.

However, under the changes in the GDPR, the use of impact assessments has been made more explicit and compulsory in certain circumstances. They are considered by the ICO to be a key part of the 'data protection by design' approach to compliance.

An impact assessment is a process which assesses the likely impact and risks identified from a particular processing operation on the protection of personal data. Think of it like a health and safety risk assessment, just for data. It needs to be done before starting a new processing operation which is 'likely to result in a high risk to the rights and freedoms' of the affected individuals.

Examples of situations where the GDPR requires an impact assessment to be undertaken include where there is:

- systematic and extensive evaluation of personal data based on automated processing (such as profiling) on which decisions are taken which either produce legal effects or significantly affect the individual concerned;
- processing on a large scale of the special categories of data (what used to be commonly known in the UK as sensitive personal data) or personal data concerning criminal convictions or offences; or
- systematic monitoring of a publicly accessible area on a large scale.

As a minimum requirement the impact assessment must contain the following:

- a systematic description of the envisaged processing operations and the purposes for processing, including where applicable the legitimate interests being pursued by the controller;
- an assessment of the necessity and proportionality of the processing for that identified purpose;
- an assessment of the risks to rights and freedoms of the individuals concerned; and
- measures envisaged to address the risks to ensure the protection of the personal data and to demonstrate compliance with the GDPR.

Reviews of the assessment and compliance with its outcomes are also required in the event of any change to the risk posed by the processing operations.

Does GDPR put a stop to processing data without consent?

No! GDPR isn't about stopping the use of data. It's about using it more responsibly. Your organisation doesn't always need consent to process data, as long as your processing meets one of the other conditions. In fact, consent is the only condition that is significantly different under GDPR.

So it's now more important than ever to remember that consent is not the only justification for processing data. Changes under the GDPR and the guidance issued so far suggest that consent could well become a last resort option, because getting it right is now going to be harder than ever.

Processing is lawful if it's necessary for one of these reasons:

- the performance of or prior to entering into a contract with the data subject;
- compliance with a legal obligation to which the data controller is subject;
- in order to protect the vital interests of the data subject or another natural person;
- the performance of a task carried out in the public interest or in the exercise of official authority; or
- the purposes of the legitimate interests of the controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject in particular where the data subject is a child.

Remember there are different conditions for the special categories of data, but again, these are consistent with the DPA conditions for handling sensitive personal data.

Consent – what are the changes to watch out for?

The concept of consent is one of the really significant areas of change in the GDPR and is very likely to require a change in approach if it's a condition your organisation has been relying on.

GDPR has clarified that to be valid consent must now be:	
1	**Freely given** – so this will not be the case, for example, where a contract is made conditional on consent being given to processing of data which is not necessary for the performance of that contract
2	**Specific** – meaning that simply referring to consent being given to the transfer of data to something as vague as 'our trusted business partners' will not be specific enough
3	**Informed** – as with specific consent, the data subject must be clearly informed of what precisely they are consenting to in order to make an informed decision
4	**Unambiguous** – the consent request needs to be clearly distinguishable from other matters such as accepting terms and conditions and it must be stated in clear and plain language
5	**Statement or clear affirmative action** – consent must be given using a clear positive action, so implied consent or pre-ticked boxes will no longer be compliant

It is important to note that there are special considerations that apply to consent from children.

What rights do Data Subjects have?

GDPR introduces new rights and also enhances some of the existing rights afforded to data subjects. Such rights have various conditions and exceptions, but generally speaking data subjects have the following rights:

- The right of access to the data subject's personal data which existed under the DPA, but under GDPR there are tighter timescales for responding to such access requests and no fees can be charged for responding to them.
- The right to rectification is a right to ask that any inaccurate data about them is corrected. An organisation will therefore need to ensure they have processes in place to do this quickly and prevent processing until such correction has been made.
- The right to be informed about why their information is being used.
- The right to data portability which is the right to obtain some of their personal data in a reusable format.
- The right to object to processing which is based on legitimate interests and/or data being processed for direct marketing purposes.
- The right not to be subject to automated decision making and profiling which is a right to be informed when such decisions have been made and/or require a manual decision to be made.
- The right to erasure (to be forgotten) which means the data subject can request the deletion or removal of personal data, providing there is no legal basis to continue processing.
- The right to restriction of processing of data for limited purposes.

What are the changes in fines for breach of the GDPR?

At present the fines which the Information Commissioner's Office can impose on an organisation breaching the Data Protection Act 1998 in the UK is capped at £500,000 and that limit hasn't yet been imposed, although they did get close with the fine on TalkTalk. Under the GDPR the fines have been re-categorised into two tiers of breach with increased thresholds of:

Up to 2% of annual worldwide turnover of the preceding financial year or **€10 million** (whichever is the greater)

for violations relating to internal record keeping, data processor contracts, data security and breach notification, data protection officers, and data protection by design and default

Up to 4% annual worldwide turnover of the preceding financial year or **€20 million** (whichever is the greater)

for violations relating to breaches of the data protection principles, conditions for consent, data subjects rights and international data transfers

Even if this type of fine feels a little remote, perhaps more close to home is the potential reputational damage of getting this kind of compliance wrong. Individuals have a right to claim damages from a controller or processor and the regulatory body's powers of investigation can be equally disruptive to the running of an organisation.

What next?

Of course, we're going to say, come and speak to us!

We speak to so many organisations that have struggled with their approach to data protection compliance over the years and don't quite realise the extent of the work involved to get up to speed in this space. Often as organisations have grown and the desire to use data in new and exciting ways has taken over, somewhere along the way putting questions of data and privacy compliance into that process has become a secondary matter rather than a fundamental 'proof of concept' stage element.

GDPR, and the regulatory authorities tasked with governing it, envisage a cultural shift in attitudes to managing data protection compliance rather than organisations being able to rely on a one-size-fits-all approach to this issue. We work alongside organisation's own compliance and project teams so the GDPR compliance process is one with which colleagues can be fully engaged and from which they can learn how to address GDPR issues for themselves in future.

So now is a really good time to start thinking about identifying what data your organisation currently holds, where it comes from and where it goes to, in terms of which other organisations it gets transferred to and where they are located as well as looking at what internal policies and external contracts are in place which might benefit from review in light of the changes.

Shulmans' Commercial team aren't overnight GDPR experts. Ours is a team of pragmatic, experienced lawyers who have all worked in the areas of data protection, privacy and cyber security for years; some of them since the DPA first came into effect almost 20 years ago! So they are data protection specialists who can really tailor their approach to help your organisation find the way forward on its GDPR journey.

General Data Protection Regulation (GDPR) www.shulmans.co.uk

Our data protection specialists are here to advise you

Emma Roe
Partner
Commercial, IP & Regulatory

Direct Line: +44 (0)113 288 2817
Mobile: +44 (0)7976 448 773
Email: eroe@shulmans.co.uk

Mark Lumley
Partner
Commercial, IP & Regulatory

Direct Line: +44 (0)113 297 7727
Mobile: +44 (0)7946 780 9897
Email: mlumley@shulmans.co.uk

Helen Goldthorpe
Associate Solicitor
Commercial, IP & Regulatory

Direct Line: +44 (0)113 288 2829
Email: hgoldthorpe@shulmans.co.uk

Sarah Briscall
Solicitor
Commercial, IP & Regulatory

Direct Line: +44 (0)113 831 3954
Email: sbriscall@shulmans.co.uk

Shulmans

Shulmans LLP
10 Wellington Place
Leeds
LS1 4AP
www.shulmans.co.uk

T : 0113 245 2833
F : 0113 246 7326
E : eroe@shulmans.co.uk

Driven by results