DMH Stallard

Data Protection: Getting you ready for 25 May 2018

DMH Stallard

DMH Stallard

Introduction

We all hold personal data about clients, suppliers, professional contacts, employees, and prospective clients (eg names, contact details and possibly bank details). Our collection, use and storage of personal data has been regulated since 1998 by the Data Protection Act (DPA). But the world we live in today is very different to the world of 1998 and the DPA has struggled to keep up over the last 5-10 years, particularly with advances in technology, social media, mobile devices and targeted advertising.

From 25 May 2018, the DPA will be replaced by the EU General Data Protection Regulation 2016 (GDPR). Some similarities will remain but there will also be new and different requirements. The UK Government has confirmed that, despite Brexit, the GDPR will be implemented into UK law and it will either remain as is once we exit the EU, or remain but with some changes.

Before we delve into the detail of some of the fundamental changes that are on the horizon for data protection, here are some of the key terms you'll need to be familiar with together with some of the things that you need to start thinking about doing now:

Key terms

Broadly speaking, the aim of our current data protection laws and the GDPR is to regulate the *'processing'* of *'personal data'*.

The term *'processing'* is very broadly defined and covers almost anything that can be done with or to personal data, including collecting, accessing, transferring, amending, storing and destroying that data. *'Personal data'* are data relating to a living person (known as the *data subject*) who can be identified from that data alone (eg name, telephone number, email address, national insurance number) or in conjunction with other information in or likely to come into the possession of the controller of that data (known as the *data controller*). A data controller decides how personal data will be processed (eg a company using employee personal data to pay their salaries into their bank accounts) A person who processes data on behalf of a data controller is known as a data processor (eg if a company uses a cloud services provider to host certain data then the company would be the data controller and the cloud service provider would be the data processor).

What do businesses need to do now?

Although the GDPR is not yet in force, businesses (both controllers and processors) should not underestimate the extent of changes which they will need to make, and the financial costs which they will incur. For example:

- internal and external systems, processes, policies and procedures will need updating/upgrading
- consider if any tools need to be developed or procured to help reduce privacy risks and assist with applying the controls necessary for compliance with the GDPR
- review and update project and risk management methodologies and policies – or draft if there are none
- data processing contracts will need amending to ensure that there is an appropriate apportionment of risk and liability as the GDPR imposes obligations on processors as well as controllers and
- regular and ongoing training for staff will need to be implemented (if it isn't already).

The sanctions alone for non-compliance should be enough to push this to the top of the Board agenda. Fact finding, careful thinking, planning and operational implementation will all be needed. Businesses can't collect every conceivable piece of personal data from an individual, keep it forever and worry about it later. Businesses need to start assessing their level of awareness and readiness for compliance now – waiting for 2018 to arrive will be too late!

This booklet contains a number of recent articles that we have written on some of the fundamental changes that are on the horizon. If you would like any further information, or advice on the GDPR, please contact:

John Yates
Partner
T +44(0)1293 605591
E John.Yates@dmhstallard.com

Anthony Lee
Partner
T +44(0)207 8221522
E Anthony.Lee@dmhstallard.com

DMH Stallard

What's all the fuss about?

The main changes will:

- place greater obligations on businesses eg tougher requirements to satisfy 'consent' to data processing, security breach notifications, carrying out regular data protection audits, maintaining data processing records, conducting privacy impact assessments and (possibly) having to appoint a data protection officer
- introduce substantial fines if businesses do not comply with the GDPR – depending on the type of breach:
  - greater of €10m or (for undertakings) 2% of a company's total annual turnover
  - greater of €20m or (for undertakings) 4% of a company's total annual turnover
- apply to non-EU based businesses which offer goods or services to EU citizens, or monitor the behaviour of EU citizens (eg profiling)
- apply to data processors
- give individuals:
  - better control of, and access to, their personal data, and
  - extended and enhanced rights in relation to the processing of their personal data eg the right to restrict or object to processing of their personal data in certain circumstances and the right to transfer their personal data from one provider to another,
- create a 'one-stop shop' for businesses operating in more than one EU Member State – who will therefore have one 'lead' data protection supervisory authority rather than multiple.

The GDPR modernises and unifies our existing data protection rules into a single set of rules applicable across the EU which will make data protection compliance simpler and cheaper in the long run. The DPA is derived from the EU Data Protection Directive of 1995. Each EU Member State has implemented the 1995 Directive in its own way, and over the years this has caused confusion and difficulties, particularly for multi-national businesses and anyone dealing with businesses in different parts of the EU. The GDPR will apply directly throughout the EU, with no need for EU Member States to implement their own laws to comply with it.

Shhhh "what breach"?

The number, frequency and impact of data security breaches – has been steadily increasing since 2005. An overwhelming majority occur in the US, but the UK has, and is having, its fair share – from HMRC losing two CDs which contained details of 25 million child benefit claimants, through to T-Mobile sales staff selling an unknown number of customer records to a third party broker, and TalkTalk suffering a cyber security hack in 2015 which saw 157,000 customer records stolen.

Cyber-attacks have become one of the most common types of data security breaches. To help combat the threat and to make the UK the best protected country in cyber space, the UK Government announced in 2016 that it would be investing £1.9bn into cyber security over the next five years. It commissioned a cyber security breach survey in 2016 which found that, amongst other things:

- 65% of large firms detected a cyber security breach in the past year, with 25% of these firms experiencing a breach at least once a month
- the average cost of a breach to large businesses is £36,500 and
- 68% of cyber security breaches/attacks come from viruses/spyware/malware.

These figures and other details published in the survey are alarming. However, this information on cyber security attacks and information on all types of personal data breaches which is available from the ICO is just the tip of the iceberg. Notification requirements under the DPA are woefully inadequate. But this will change under the GDPR and we therefore expect to see details of even more personal data breaches being published.

What does the DPA say about personal data breaches?

The UK has two main laws which protect personal data: the DPA and the Privacy and Electronic Communications Regulations 2003 (PECR).

Under PECR, individuals have specific privacy rights in relation to electronic communications (eg telephone calls, emails, text messages, video messages and internet messaging) and providers of these services are required to notify the ICO if a personal data breach occurs. A personal data breach is 'a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed in connection with the provision of a public electronic communications service'. There is no seriousness threshold – all breaches must be notified to the ICO within 24 hours of detection (ie when the provider has acquired sufficient awareness that a security breach has occurred that led to personal data being compromised). Furthermore, individuals must be notified without undue delay if the breach is likely to adversely affect their privacy. A log of security breaches must also be kept.

Under the DPA, businesses must have in place appropriate physical, technical, management and operational security measures to prevent personal data from being accidentally or deliberately compromised, together with robust security policies and procedures, and well-trained employees. Unlike PECR, there is no express obligation to notify the ICO if a personal data breach occurs. However, guidance from the ICO recommends that serious personal data breaches are notified to it. A serious personal data breach is described by the ICO as a breach:

- that could cause significant threat of harm to individuals
- where large volumes of data are involved (generally affecting at least 1000 people) and
- where sensitive data is involved, such as financial or medical records or unencrypted personal data.

The ICO can also impose fines on data controllers (but not data processors) of up to £500,000 for a serious personal data breach under the DPA or PECR.

How will these laws change?
Under the GDPR:

- personal data must be *'processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures* and
- a personal data breach must be notified by the:
  - data controller to the ICO within 72 hours of becoming aware of a personal data breach (unless the breach is unlikely to result in a risk to the rights and freedoms of affected individual(s))
  - data controller to the affected individual(s) without undue delay (unless the breach is unlikely to result in a high risk for the rights and freedoms of those affected individual(s)) and
  - data processor to the data controller without undue delay.

In due course, guidance will be provided by the European Data Protection Board (which will replace the Article 29 Working Party) on what 'without undue delay' and 'high risk' mean.

The GDPR also carries a substantial fine for data controllers and data processors which experience a personal data breach – the greater of €10,000,000 or 2% of total worldwide annual turnover. In addition, affected individual(s) will be able to pursue the data controller and/or the data processor for compensation (which is not financially capped) if they suffer any loss or damage as a result of a personal data breach. Both data controllers and data processors will be liable unless they can prove that they were not in any way responsible for the damage suffered by the affected individual(s).

What rights do individuals have?

What rights do data subjects have under the DPA?
Data subjects have the following rights:

1. A right of access to a copy of information held about them including a description of the personal data, the reasons it is being processed, and whether it will be, or has been, given to any other third parties (this is known as a data subject access request).

   The copy must be provided within 40 days of the request and is subject to a maximum charge by the data controller of up to £10 (although for copies of paper-based health and education records a fee of up to £50 can be charged)
2. A right to have inaccurate personal data rectified, blocked, erased or destroyed but not to alter or remove opinions unless those opinions are based on inaccurate factual information
3. A right to stop being sent direct marketing. The data controller will have no discretion in this case about whether or not to stop processing for direct marketing purposes. They simply must not continue to send direct marketing. However, the data subject's personal data wouldn't be deleted, it would be supressed so that the data controller retains enough information to ensure that they don't get direct marketing materials in the future
4. A right to object to processing that is likely to cause unwarranted and substantial damage or distress. The data subject must specify why the processing is causing unwarranted and substantial damage (eg financial loss or physical harm) or distress (eg a level of upset, or emotional or mental pain, which goes beyond annoyance or irritation, strong dislike, or a feeling that the processing is morally abhorrent). However, data subjects can't stop their personal data being processed if they have consented to the processing or if the processing is necessary:
   - in relation to a contract that the data subject has entered into with that data controller or because the data subject has asked for something to be done so they can enter into a contract with that data controller
   - because of a legal obligation that applies to that data controller (other than a contractual obligation) or
   - to protect the data subject's 'vital interests' (eg life or death cases)
5. A right to claim compensation for damages caused by a breach of the DPA (damage is not defined by the DPA, but if a data subject has suffered financial loss they would be entitled to compensation)
6. A right to object to decisions being taken by automated means where there is no human intervention (eg website algorithms and credit searching facilities which determine whether to approve an online loan application) where that decision has a significant effect on the data subject (so not trivial or negligible effects). They have 21 days to ask the data controller to reconsider the decision or to take a new decision on a different basis. This right to object is not available where the automated decisions:
   - are authorised or required by law, or are taken in relation to (or preparation for) a contract with the data subject and
   - are to give the data subject something they've asked for or to safeguard the data subject's legitimate interests.

DMH Stallard

The UK regulator of the DPA, the Information Commissioners Office, can also impose fines on data controllers of up to £500,000 for failure to comply with these data subject rights.

What rights will data subjects have under the GDPR?

Under the GDPR, no real substantial changes will be made to the concepts of processing, personal data (the definition has been expanded slightly, consistent with how the EU has been interpreting the DPA definition over the last few years), data subjects or data controllers and data processors given under the DPA.

The rights data subjects have under the DPA remain but with a few enhancements:

- General principles relating to a right of access – data controllers:
  - *must be clear:* information provided to data subjects must be concise, transparent, intelligible and in an easily accessible form using clear and plain language
  - *must be prompt:* information must be provided to data subjects without undue delay but, in any case, within one month (two months for complex requests) and
  - can no longer charge a fee to data subjects for providing them with this information save where the request is manifestly unfounded or where the data subject makes excessive requests.
- More specifically:
  - data controllers will need to put a lot more content their into privacy notices eg information setting out the purposes for processing as well as the legal basis of processing, how long personal data will be stored for and all of the data subject's rights under the GDPR
  - data controllers will need to provide not only a copy of their personal data but also supplemental information about the processing eg how long they intend to hold onto the data (the envisaged retention period – or if this is not possible, the criteria that will be used to determine this), how the personal data was sourced (if not collected from the data subject), and details of anyone receiving the data in third countries to international organisations)
  - the right to object to decisions being taken by automated means works in a similar way to the existing DPA rights, but under the GDPR the concept of profiling is explicitly mentioned (it isn't in the DPA). Profiling is carried out on a data subject's personal data and is done to evaluate personal aspects about the data subject. Under the GDPR, a company must now inform data subjects specifically about any profiling activities that they undertake. Furthermore, personal data which are sensitive (eg race, religion, sexual orientation etc) can't be subject to automated decision making without the explicit consent of the data subject unless the processing is necerssory for reasons of substantial public interest on the basis of EU or national law
  - a new right for data subjects to be forgotten in certain specified situations (eg personal data are no longer necessary for the purposes for which they were collected, or the data subject withdraws his consent and the data controller has no other justification for processing it). If a data controller receives such a request, it has to notify anyone to whom it has disclosed that personal data, unless this would be impossible or involve disproportionate effort
  - a new right to data portability in relation to data processed by automated means. This is mainly targeted at online service providers and is an attempt to promote further interoperability between online systems. At the data subject's request, data controllers must (free of charge) provide a copy of all personal data that it processes about the data subject (and which has been provided by the data subject) in a structured, commonly used and machine readable format. This would not apply to personal data that has been provided to the data controller by a third party;
  - there is a strengthened right for data subjects to object to processing (for specific purposes) regardless of whether it is likely to cause or is causing damage or distress. The burden is now on the data controller to show compelling legitimate grounds which override a data subject's right to object.

The GDPR also carries a substantial fine for companies who fail to comply with these data subject rights – the greater of €20,000,000 or 4% of total worldwide annual turnover.

Extending its reach to non-EU businesses

A data controller that is not established in the UK will only be subject to the DPA if it uses equipment (automated or otherwise) situated within the UK, except where that equipment is used only for the purposes of mere transit through the UK. Data processors are not subject to the DPA. So, if a US website operator uses servers in the UK to host its website, then that is likely to count as using equipment within the UK and would mean the US website operator must comply with the DPA. If it merely uses those servers as a conduit to transfer personal data to another country and doesn't carry out any substantive processing then it may not have to comply with the DPA.

Under the GDPR data controllers and data processors who are not established in the

DMH Stallard

UK (or another EU country) will be subject to the GDPR (irrespective of whether or not the data processing itself takes place in the UK (or another EU country)) if their processing activities relate to:

- offering goods or services to data subjects in the UK (or another EU country), irrespective of whether or not payment is required or
- monitoring behaviour of data subjects in the UK (or another EU country) as far as their behaviour takes place within the UK (or another EU country) (eg profiling).

Therefore, many non-EU based businesses may find themselves subject to the GDPR when it comes into force.

If so, the GDPR requires data controllers (but not data processors) to appoint a representative '*in one of the Member States where the data subjects', whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are in the EU*'. The representative will be the point of contact for data subjects and the relevant supervisory authorities (either in addition to or instead of the data controller) on all issues related to processing.

Extending its reach to data processors

All obligations under the DPA fall on the data controller and not the data processor. You would think that it would be pretty straightforward to determine whether a party is a data controller or a data processor. You would need to look at:

- how much independence each party has in deciding how and in what manner the data are processed and
- the degree of control each party has over the content of personal data.

Although the DPA doesn't apply to data processors, it does require the data controller to enter into a written contract with the data processor which requires the data processor to:

- act only on the instructions of the data controller and
- take appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss or destruction of or damage to personal data.

Under the GDPR, data processors will no longer escape and will be subject direct obligations under the GDPR. However, the following obligations will primarily fall on the data controller:

- principles relating to the processing of personal data set out in Articles 5-11
- rights given to data subjects eg provision of information, information access rights, and the right to rectification, erasure and data portability (Articles 12-22)
- requirement to follow the concept of data protection by design and default (Article 25)
- requirement to maintain records of all categories of personal data processing activities carried out (but this will apply to data processors who have more than 250 employees) (Article 28)
- requirement to notify personal data breaches to data subjects (Article 34) and
- requirement for data protection impact assessments to be carried out prior to any processing (Articles 35 and 36).

The data controller can only use data processors which provide "sufficient guarantees to implement appropriate technical and organisational measures in such a manner that processing will meet the requirements of this Regulation and ensure the protection of the rights of the data subject". Under the GDPR a data processor cannot subcontract its processing activities without the prior written consent of the data controller.

As with the DPA, there must be a written contract with the data processor but the GDPR goes further and specifies what must be included in that written contract (Article 28(3)) as well as placing an obligation on the data processor to immediately inform the data controller if any instructions given by the data controller breach the GDPR (Article 28(3)(h)).

A data controller is also likely to want to place obligations on the data processor to ensure that it is able to meet the GDPR obligations which it is primarily responsible for complying with.

Having statutory obligations as well as contractual obligations will not only be a major cultural change for data processors but it will create substantially more risk. This is because failure to comply with the GDPR attracts:

- substantial fines (depending on the breach, this could either be (i) the greater of €10m or 2% of total annual turnover or (ii) the greater of €20m or 4% of total annual turnover) and
- payment of compensation to data subjects who have suffered damage as a result of the data processor not complying with obligations under the GDPR specifically directed to it or where it has acted outside or contrary to the lawful instructions of the data controller.

The fines and compensation would be in addition to any contractual liability owed to the data controller.

DMH Stallard

What will privacy notices look like under new data protection laws?

The current situation

Under the DPA, privacy notices are a way for companies to tell data subjects how their personal data (eg name, address, telephone number and email address) will be collected, stored and used. They allow companies to:

- comply with their fair processing obligations under the DPA (ie only using personal data in a way that a data subject would reasonably expect, considering how that use would impact the data subject and ensuring that they know how their personal data will be used) and
- obtain data subject's consent (which must be freely given, specific and informed) to the collection, storage and use of their personal data – the recommended approach is to use an unticked opt-in box (so the individual needs to tick it to show consent). However, the majority of websites either use a pre-ticked box consenting to the privacy notice (which then needs to be unticked by the data subject if they don't consent) or merely contain a link to the privacy notice on each page where personal data is collected (but without the need to tick or untick a box). The latter two examples would not be sufficient if a website was collecting sensitive personal data (eg race, ethnic origin etc) – explicit consent would be required (ie unticked box which the data subject needs to tick).

As a minimum, privacy notices should therefore include:

- information about the data controller (eg company name and address)
- details about the type of personal data that will be collected (eg information given by data subject when they fill in online forms, and information about what pages they have viewed or products they have searched for)
- whether the website uses cookies
- how the data controller will use and store the collected personal data (eg to provide the data subject with the information they've requested, or to process an order they've placed via the website) – you can't just produce a long list of possible future uses if, in reality, you aren't going to use them
- details as to a data subject's right to object to any direct marketing
- whether the collected personal data will be disclosed to/shared with any third parties (eg advertisers, and analytics and search engine providers), including if it will be transferred outside the EEA and
- details of how the data subject can obtain a copy of information held about them.

The ICO can impose fines on companies of up to £500,000 for serious personal data breaches under the DPA.

Greater obligations coming under GDPR

Under GDPR privacy notices will need to contain a lot more information because the GDPR is prescriptive about what information needs to be given to data subjects.

Personal data must be *'processed lawfully, fairly and in a transparent manner in relation to the [data subject]'*. The inclusion of *'in a transparent manner'* goes further than the above fair processing obligations under the DPA.

The transparency requirements under the GDPR are set out over 6 pages and require data controllers to provide data subjects with extensive information about how their personal data is collected, stored and used. Furthermore, this information must be provided to data subjects in a *'concise, transparent, intelligible and easily accessible form, using clear and plain language'* (in particular where the data subjects is a child). In practice, this means that data controllers will need to include more information in their privacy notices, as well as retaining more detailed records of their data processing activities in relation to data subjects.

To comply with the GDPR, privacy notices will therefore need to include:

- the identity and the contact details of the data controller (same as the DPA)
- the contact details of the data controller's nominated data protection officer, where applicable (new information to be provided)
- how the data controller will use and store the collected personal data (same as the DPA) as well as the legal basis for the collection, use and storage thereof (new information to be provided)
- whether the collected personal data will be disclosed to/shared with any third parties (same as the DPA)
- whether the personal data will be transferred to a third country or international organisation (same as the DPA) including how the personal data will be safeguarded and the means by which the data subject can obtain a copy of those safeguards (new information to be provided)
- details as to how long personal data will be stored, or if that is not possible, the criteria used to determine that period (new information to be provided)
- details of how the data subject can obtain a copy of information held about them (same as the DPA) and details of all the other rights they have under the GDPR (new information to be provided)
- details of the data subject's right to lodge a complaint with a supervisory authority (eg the ICO) (new information to be provided) and
- details of whether the provision of personal data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the data subject is obliged to provide the personal data and of the possible consequences of failure to provide such personal data (new information to be provided).

DMH Stallard

A number of the above GDPR information requirements are also currently recommended by the ICO – but as they go further than the requirements imposed under the DPA, they are only recommended currently.

Consent will be much tougher to obtain

Under the GDPR, a data subject's consent to processing is defined as *'freely given, specific, informed and unambiguous indication of the [data subject's] wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her'*. A data controller must be able to demonstrate that consent was given to its privacy notice and this could include the data subject *'ticking a box when visiting an internet website, choosing technical settings for information society services or by any other statement or conduct which clearly indicates in this context the [daat subject's] acceptance of the proposed processing of their personal data. Silence, pre-ticked boxes or inactivity should therefore not constitute consent'*.

Although the GDPR removes the possibility of opt-out consent (thereby creating additional hurdles for consent over what is currently required by the DPA), the data subject may consent by *'choosing technical settings for information society services'*. How this will be interpreted remains to be seen, but it could leave provisions of the e-Privacy Directive relating to cookies and other tracking technologies intact.

The GDPR also deals with obtaining a child's consent to data processing – something lacking under the DPA. Processing personal data of a child is only lawful where the child is at least 16 years old. Where the child is under 16 years, processing is only lawful if and to the extent that consent is given or authorised by a parent or legal guardian. The GDPR allows EU Member States to legislate for a lower age provided it is not below 13 years.

Fines

Fines under the GDPR will be substantially higher than the DPA. Some breaches of the GDPR are subject to fines of up to the greater of €10m or 2% of a company's global annual turnover, while other breaches will be up to the greater of €20m or 4% of a company's global turnover. Breach of the rules around information to be given to data subjects in privacy notices and how consent is obtained are subject to the higher level although breach of the rules concerning age of consent are subject to the lower level.

Embracing privacy by design and default throughout your business

For a number of years, the ICO has encouraged and promoted 'privacy by design' for all activities that involve data processing. Unlike the ICO, the DPA doesn't specifically recognise the concept of 'privacy by design and default'.

The ICO's concept of privacy by design simply recommends businesses take a pro-active approach to designing projects, processes, products and systems by promoting privacy and data protection compliance from inception and throughout their lifecycle. The ICO regards it as an essential tool for minimising privacy risks for businesses because it can, for example, identify potential issues or problems early on (when it is much simpler and less costly to fix) and help businesses meet their legal obligations under the DPA.

Although also not recognised under the DPA, privacy impact assessments (PIAs) are an integral part of the ICO's privacy by design approach and are also encouraged to help identify and reduce privacy risks. In 2014, the ICO produced a Code of Practice which can be integrated into project and risk management methodologies and policies.

Under the GDPR, the concepts of 'privacy by design and default' and 'data protection impact assessments' (DPIAs) will be mandatory for data controllers (ie individuals, organisations and other corporates/unincorporated bodies) who determine the purposes for which and the manner in which any personal data are, or are to be, processed. The GDPR embraces and builds on the ICO's concepts.

In terms of privacy by design and default, data controllers will need to 'implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for the specific purposes of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the data subject's intervention to an indefinite number of natural persons'. Although this is fairly straightforward and easy to understand, in practice it could be quite time consuming and costly to implement. However, this obligation needs to be balanced alongside available technologies and implementation costs – there needs to be an element of reasonableness.

Whether a data controller needs to undertake a DPIA will depend on whether the particular processing operation is likely to result in a high risk to the rights and freedoms of an individual. The GDPR specifies instances when DPIAs must be carried out eg processing operations which involve (i) systematic monitoring of a publicly accessible area on a large scale (eg CCTV, drones and body-worn devices) or (ii) systematic and extensive evaluation of personal aspects relating to individuals which is based on automated processing and on which decisions are based that produce legal effects concerning individuals or similarly significantly affect them (eg profiling and other data analysis activities).

The added complication with DPIAs is that the data controller must consult with the ICO before processing any personal data if the DPIA indicates that its processing operations would, in absence of safeguards, result in a high risk to the rights and freedoms of individuals and the data controller can't mitigate those risks by reasonable means in terms of available technologies and implementation costs.

The GDPR also carries a substantial fine for companies who fail to comply with these obligations – the greater of €10,000,000 or 2% of total worldwide annual turnover.

DMH Stallard

What does this mean in practice for businesses?

The GDPR clearly has more teeth than the ICO's approach to privacy by design and PIAs under the DPA.

As well as starting to take a pro-active approach now to designing projects, processes, products and systems by promoting privacy and data protection compliance from inception and throughout their lifecycle, businesses should also:

- identify any new or near-complete projects which involve data processing and factor in these mandatory requirements
- consider if they need to develop or procure any tools to help reduce privacy risk and assist them in applying the necessary controls
- review and update project and risk management methodologies and policies – or draft if there are none – which should also integrate DPIAs and ensure that the approach to identifying risks and solutions to avoid or mitigate risks can be clearly documented to enable them to demonstrate compliance with the GDPR and
- start training relevant staff (eg design and implementation teams, project managers).

How can anonymous and pseudonymous data help you comply with data protection laws?

Anonymous data is data which doesn't identify living individuals – so it is not personal data, and therefore not subject to the DPA. The concept of anonymised data is not expressly referred to in the DPA (although it is mentioned in the recitals of the governing Data Protection Directive) but it has for a long time been recognised as a way to ensure the availability of rich data resources, whilst protecting individuals' personal data.

Pseudonymised data is data that can't be attributed to a specific individual without the use of additional information which is kept separate from it. The concept of pseudonymised data is not expressly referred to in the DPA or the governing Data Protection Directive.

Under the GDPR, anonymous and pseudonymised data are both recognised.

The GDPR states that *'the principles of data protection should ... not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable. This Regulation does not therefore concern the processing of such anonymous information, including for statistical or research purposes.'* However, despite this statement many view anonymised data as unsafe because even the most sophisticated techniques can be reversed or bypassed with the right data sets. Re-identification is therefore a key, and realistic, threat to anonymised data.

Pseudonymised data is referred to in much greater detail in the GDPR. 'Pseudonymisation' is defined as the *'processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person'*. Thus personal data which has undergone pseudonymisation is still personal data and subject to the GDPR. As with anonymised data, re-identification is a key, and realistic, threat for pseudonymised data – but, unlike anonymised data, re-identification could happen in two ways:

- a data breach might enable an attacker to acquire the key for identifying the induviduals whose personal data has been pseudonymised or otherwise connect the pseudonymised data to individual identities or
- even if the key is not acquired, an attacker may be able to identify individuals by linking information (eg gender and date of birth) in the pseudonymous database with other available information

If done correctly, the process of pseudonymisation can help businesses comply with the GDPR because it:

- can reduce the risks to data subjects and help data controllers and data processors meet their data protection obligations (it is not by itself a sufficient measure to exempt data from the GDPR)
- is a central feature to the concept of privacy by design and default – pseudonymisation is a way of implementing appropriate technical and organisational measures to ensure appropriate data security
- allows personal data to be processed for purposes other than that for which it was originally collected
- could allow for relaxed data breach notification rules because pseudonymisation reduces the risks of harm to data subjects (notification of data breaches only needs to made to the ICO and data subjects if the breach is likely to create a risk (high risk in the case of notification to data subjects) to the rights and freedoms of the data subject)
- may require less strict data subject access, rectification, erasure or data portability obligations a data subject can no longer be identified and
- allows greater flexibility to conduct data profiling (defined in the GDPR as *'any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements')*.

DMH Stallard