The European General Data Protection Regulation

A guide for the health and social care sector
IMPORTANT NOTE: This guide is based on the text of Regulation (EU) 2016/679 and the guidance available on 1 September 2016. This guide is not exhaustive. It is provided solely for general information purposes and should not be relied upon as legal advice. No liability is accepted for errors of fact or opinion this guide may contain. Professional advice should always be obtained before applying the information to particular circumstances. The copyright in this guide is retained by DAC Beachcroft.

© DAC Beachcroft
## Contents

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>An introduction from Anne Crofts</td>
<td>3</td>
</tr>
<tr>
<td>Brexit and the GDPR</td>
<td>5</td>
</tr>
<tr>
<td>An employment law perspective from Khurram Shamsee</td>
<td>7</td>
</tr>
<tr>
<td>Journey so far and journey to come</td>
<td>9</td>
</tr>
<tr>
<td>Summary of key changes</td>
<td>12</td>
</tr>
<tr>
<td>Definitions and data processors</td>
<td>13</td>
</tr>
<tr>
<td>Fair processing information</td>
<td>15</td>
</tr>
<tr>
<td>Processing conditions and exemption</td>
<td>17</td>
</tr>
<tr>
<td>Profiling</td>
<td>19</td>
</tr>
<tr>
<td>Data portability</td>
<td>20</td>
</tr>
<tr>
<td>Right of erasure</td>
<td>21</td>
</tr>
<tr>
<td>Data subject rights - the best of the rest</td>
<td>22</td>
</tr>
<tr>
<td>Accountability</td>
<td>23</td>
</tr>
<tr>
<td>Data protection by design and by default</td>
<td>24</td>
</tr>
<tr>
<td>Privacy impact assessments</td>
<td>25</td>
</tr>
<tr>
<td>Data protection officers</td>
<td>26</td>
</tr>
<tr>
<td>Breach notification</td>
<td>27</td>
</tr>
<tr>
<td>Security measures</td>
<td>28</td>
</tr>
<tr>
<td>Anonymous and pseudonymous data</td>
<td>29</td>
</tr>
<tr>
<td>International transfers</td>
<td>30</td>
</tr>
<tr>
<td>Enforcement</td>
<td>31</td>
</tr>
<tr>
<td>Compensation</td>
<td>34</td>
</tr>
<tr>
<td>Extra territorial effect</td>
<td>35</td>
</tr>
<tr>
<td>Our data protection team</td>
<td>37</td>
</tr>
</tbody>
</table>
I never thought that I would look back on the Data Protection Act with fondness. Over time we have got to know its ways and how to navigate its maze of provisions. But all good things must come to an end. On 4 May 2016 the General Data Protection Regulation – Regulation (EU) 2016/679 or the GDPR – was passed. We now have a new maze to negotiate.

This manual is designed to be your guide: to help you walk the maze with a firmer sense of direction and purpose, to side-step some of the pitfalls and avoid the wrong turns.

All EU member states will need to comply with the GDPR by 25 May 2018. It is likely that after Brexit the requirements of the GDPR will apply in the UK. The countdown to compliance has begun.

You will want to get it right. The maximum fine for non-compliance has risen from £500,000 to €20,000,000 – about £17 million at today’s exchange rates.

This manual gives an overview of the likely impact of the GDPR in health and social care. We have looked at each of the main provisions and compared them to current law, ICO guidance and common practice. We provide advice on the practical steps that should taken to prepare and what to prioritise given the uncertainties.
Much of the GDPR will be familiar territory. It builds on old concepts (personal data, data controller etc.), enhances existing rights and obligations and in places makes best practice a legal requirement.

But I’m afraid there is still a lot to be done. There is a new requirement on organisations to demonstrate compliance, which means there will be a lot of paperwork. There are new rights for data subjects too, which are easier to enforce. Contracts and data sharing protocols will need to be reviewed in light of the changes.

“The countdown to compliance has begun”
Brexit and the GDPR

Brexit means Brexit, to quote Theresa May as she entered Downing Street. But quite what Brexit means for data protection in the UK remains unclear. There are a few reasons why it is very likely that the rules set out in the new EU General Data Protection Regulation (GDPR) will apply in the UK.

The GDPR applies to organisations outside the EU marketing goods and services to people in the EU and processing their personal data. After Brexit, that will include UK companies. The easiest way to ensure that UK companies comply with the GDPR, and are able to continue to trade, is to pass UK legislation equivalent to the GDPR. The government intends to pass a new Data Protection Act to address this.

The GDPR also places restrictions on when organisations based in the EU can transfer data out of the EU. It will only be possible to transfer personal data if the level of protection provided by UK law is considered “adequate”. The UK will undoubtedly want to be deemed an “adequate” jurisdiction by the European Commission.

Any rules that apply to data flowing in and out of the EU would most likely cover processing of data within the UK. In practice it would be cumbersome to have different rules for domestic and international processing. And it would be odd for the stronger protections of the GDPR not to apply to the very sensitive data used within UK health and social care.

Throughout this guide we have highlighted the areas in which it would be prudent to take steps now, and those where implementation can wait a little longer.

“Brexit means Brexit”
The GDPR has particular challenges for health and social care organisations in their capacity as employers.

A key consideration for all employers is the continued reliance upon consent to legitimise the processing of the ordinary and sensitive personal data of its employees. For a number of years, doubt has been cast on whether the employee/employer relationship is compatible with the requirement that consent is freely given, not least as it has become common practice for employers to include blanket consent provisions in their standard employment contracts (so that the employee has no real choice in the matter). As such, with the encouragement of the ICO, in recent years there has been a move away from employers relying upon consent to instead ensuring that it can satisfy one of the other conditions provided for the processing of ordinary or sensitive personal data. The GDPR reinforces this principle, and it is difficult to see how the more stringent requirements for securing consent will be workable in the employment context. Employers would therefore be well advised to abandon their standard consent clauses and instead to audit their data processing to confirm other processing conditions apply. Employee privacy notices will also need to be updated to cover the information prescribed by the GDPR, along with any separate notice provided to job applicants at the recruitment stage.
Subject access requests from current or former employees that require the extensive retrieval of archived e-mails and other electronic files are common in health and social care, as in other sectors.

Employers are no longer able to charge a fee for responding to such requests, a change which will increase the number of requests. The timescale for an organisation to respond has been reduced to just one month. However, it is possible to extend this by a further two months. One new tool in the toolbox for handling employee requests is an exemption that applies if a request is “manifestly unfounded or excessive”, which is likely to cover repetitious requests. It might also cover requests that use data protection rights to deliberately bypass court rules and disciplinary processes about disclosure: we will need some case law to guide us.

There is little comfort for employers on how to tackle subject access requests from current or former employees, which require the extensive retrieval of archived emails another electronic files. Given the increase in potential sanctions, employers who regularly receive these requests should implement a clear protocol to reduce the burden of responding.

“Employers would be well advised to abandon their standard consent clauses and instead to audit their data processing to confirm other processing conditions apply.”
## Journey so far

<table>
<thead>
<tr>
<th>Date</th>
<th>Development</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>13 December 1995</td>
<td>Directive entered into force</td>
<td>Publication date in the Official Journal + 20 days</td>
</tr>
<tr>
<td>January 2012</td>
<td>Reform proposed</td>
<td>The European Commission proposed a comprehensive reform of data protection rules within the EU, including a new draft data protection regulation, which would become the GDPR</td>
</tr>
<tr>
<td>May 2012 – May 2015</td>
<td>Negotiations</td>
<td>Negotiations between the European Commission, EU Parliament (including its Civil Liberties Justice and Home Affairs Committee or LIBE Committee) and the Council of the EU and national parliaments on what the GDPR should include</td>
</tr>
<tr>
<td>June – December 2015</td>
<td>Trilogue discussions</td>
<td>Trilogue discussions between the European Commission, EU Parliament and Council of the EU to agree a final text of the GDPR</td>
</tr>
<tr>
<td>15 December 2015</td>
<td>Informal political agreement on consolidated text of GDPR</td>
<td>The EU Parliament’s LIBE Committee approved the politically agreed text</td>
</tr>
<tr>
<td>17 December 2015</td>
<td>LIBE Committee approval</td>
<td></td>
</tr>
<tr>
<td>14 April 2016</td>
<td>The EU Parliament approved the agreed text. The decision was made in plenary without a vote as there were no amendments or motions to reject</td>
<td></td>
</tr>
</tbody>
</table>
## Journey to come

<table>
<thead>
<tr>
<th>Date</th>
<th>Development</th>
<th>Actions</th>
</tr>
</thead>
<tbody>
<tr>
<td>4 May 2016</td>
<td>Publication of the finalised GDPR in the Official Journal</td>
<td></td>
</tr>
<tr>
<td>25 May 2016</td>
<td>GDPR comes into force</td>
<td>Organisations now have a two year implementation period to ensure compliance</td>
</tr>
<tr>
<td>23 June 2016</td>
<td>The UK votes to leave the EU</td>
<td>Uncertainty about what rules with apply to the UK</td>
</tr>
<tr>
<td>25 May 2018</td>
<td>GDPR to apply (2 years after the date the GDPR comes into force)</td>
<td>Organisations must be operating in full compliance with the GDPR</td>
</tr>
</tbody>
</table>
## Summary of key changes

### Enforcement
- Maximum fine for a breach increased from £500,000 to €20,000,000
- Easier for data subjects to make a claim
- Data subjects have the right to compensation from a data controller or data processor

### Accountability
- New principle of accountability means need to demonstrate compliance. So can be fined even if no harm has occurred
- Must keep a record of processing
- All new systems should be designed in accordance with privacy by design and privacy by default

### New data subject rights
- No more fees
- New right to restrict processing
- New right of data portability
- Enhanced right of erasure
- New right to object to the processing of data for risk stratification or case finding if this amounts to profiling

### Data protection officers
- All NHS bodies, local authorities and organisations whose core business is the delivery of health and social care must appoint a DPO
- DPO must be independent and must not be instructed on how to carry out their role
- DPO must report directly to the highest level of management

### Conditions for processing
- Public authorities can no longer rely on the legitimate interests condition BUT can rely on carrying out a public function instead
- The Schedule 3 medical purposes condition is expanded to expressly include social care
- New Schedule 3 condition for public health, quality and safety of health care and quality and safety of drugs and medical devices

### Breach Notifications
- New duty to inform data subjects of high risk breaches
- Duty to notify ICO within 72 hours of breaches unless they are unlikely to result in a risk to the rights and freedoms of natural persons
- Duty to report to the ICO even if only small numbers of service user affected

### New duties for data processors
- Duty under the GDPR to act in accordance with controller instructions
- Data processors become a data controller if they act beyond instructions
- Extra requirements for data processing agreements
- Restrictions on sub-contracting by data processors

### Fair processing notices
- Extra information to be included in privacy notices including data retention periods, source of data and processing conditions relied on
- Privacy notices to be understood by children whose data is processed

### Best of the rest
- PIAs for projects involving the processing of sensitive personal data on a large scale
- International transfer mechanisms largely unchanged save for formal recognition of binding corporate rules
- European Data Protection Board to replace Working Party 29 with remit for guidance and consistent application of the GDPR
Key concepts

Definitions and Data Processors

Current position under the DPA and ICO Guidance

The DPA applies to the processing of personal data wholly or partly by computer. Personal data is defined as data from which you can identify a living individual.

Under the DPA, only data controllers have direct obligations in relation to personal data (although ICO guidance widened the scope of what organisations would be considered data controllers). A data controller is defined as a person who determines the purpose and the manner of the processing of personal data. Data controllers are differentiated from data processors who act on the instructions of the data controllers and to whom no obligations under the DPA apply. Data controllers are obliged to put contracts in place with their data processors which require the data processors to have adequate security in place and to act only on the instructions of the data controller.

The DPA also distinguishes between personal data and sensitive personal data.

Sensitive personal data is defined in the DPA and includes health data, criminal convictions, trade union membership and ethnicity.

Position under the GDPR

The definition of personal data now refers to identifiers such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Biometric data is added to the list of sensitive personal data, now called "special categories of personal data" and criminal data has been left for member states to legislate on.

The data controller’s obligation to manage its data processors is maintained, but the GDPR also introduces direct obligations on data processors.

A data processor’s obligations include:

- obtaining data controller authorisation before sub-contracting out any data processing. The original data processor remains fully liable for data protection failures of the sub-processor (Article 28);
- maintaining a record of processing activity which (amongst other things) needs to include details of the processor and instructing controller, out of EU transfers and (where possible) a description of data protection security measures in place (Article 30);
- co-operating with the ICO (Article 31);
- ensuring that appropriate technical security measures are in place (Article 32); and
- notifying the data controller of any data breach (Article 33).

Article 28 also sets out the requirements of the contract between data controllers and data processors, which is much more prescriptive than those under the DPA.

Under the GDPR, data processors as well as data controllers will now be directly liable to data subjects for breaches.

Data subjects who have suffered damage as a result of a data processor’s breach may now:

- complain to the supervisory authority (Article 77);
- seek compensation from the data processor (Article 82); and
- bring a court action against the data processor (Article 79).

Data processors can also be subject to fines under the GDPR (see page 31 for more information).
Key concepts

Definitions and Data Processors

Impact on the health and social care sector

The definition of personal data no longer refers to a health record. Instead, the GDPR applies to personal data that is process wholly or partly by computer, and personal data that is part of a filing system or intended to be part of a filing system (see Article 2(1)). The definition of filing system broadly matches how "relevant filing system" under the DPA has been interpreted.

If data is held on paper and is not even partly processed on computer, in a structured filing system or intended to be entered into a structured filing system there will be an argument that it is not personal data. It is unlikely that much data falls within this description.

It is often seen as an unfair burden on data controllers to manage their own data protection compliance obligations as well as the activities of their processors. The application of the GDPR to data processors strikes a more even balance between data controllers and data processors.

The new obligations are similar to those that controllers often try and impose on their processors under contract to redress the balance. Therefore controllers are likely to find the new provisions helpful.

For processors, many will already be subject to similar requirements regarding sub-contracting and breach notification under the terms of the contracts negotiated with their controllers. The new liabilities to data subjects and the potential for ICO fines are significant developments.

IT companies and CSUs providing data processing services to the health and social care sector will now have direct obligations under the GDPR and will require clear contractual provisions detailing:

- the agreed relationship between the parties with respect to each aspect of the processing activity;
- sub-contracting arrangements;
- what will happen to the data at the end of the contract;
- how the processor will demonstrate compliance with the GDPR obligations;

We are also likely to see more data processors requesting warranties from data controllers (e.g. that an accurate fair processing notice has been given).

We anticipate that such requirements will make data processing agreements and negotiations much more complex and lengthy.

Practical steps

- Identify any data processing agreements that are likely to be in place on 28 May 2018 when the GDPR comes into force.
- Review these agreements to ensure they contain:
  - all of the requirements set out in Article 28; and
  - appropriate allocation of liability for data breaches between data processors and data controllers, including claims by data subjects.
- Any new data processing agreements should also contain appropriate GDPR provisions – it is worthwhile updating any template documents. This will save you time later on.

Contract reviews should be prioritised taking into consideration volume and sensitivity of personal data that is processed.

It is often seen as an unfair burden on data controllers to manage their own data protection compliance obligations as well as the activities of their processors. The application of the GDPR to data processors strikes a more even balance between data controllers and data processors.
Principles and Processing

Fair Processing Information

Current position under the DPA and ICO Guidance

The DPA states that in order for the processing of personal data to be fair, the data controller must provide fair processing information which states:
- the identity of the data controller;
- the purposes of the processing; and
- any further information which is necessary to make the processing fair.

This obligation does not apply if providing the information would involve disproportionate effort or if the data are processed to meet a legal obligation of the data controller.

There are also a number of exemptions in the DPA which mean that the information does not need to be provided in specific circumstances. For example, if the provision of the information would prejudice the prevention or detection of crime.

The Directive however contained more prescriptive obligations which did not make it into the DPA including that:
- if the data are obtained directly from the data subject, the notice must state whether replies to questions are obligatory or voluntary, as well as the possible consequences of the failure to reply; and
- if the data are not obtained directly from the data subject, the notice must list the categories of data being processed.

The DPA also does not prescribe any format requirements for notices, although the ICO has provided some guidance in its Privacy Notice Code of Practice. The Code of Practice contains general principles regarding the format and drafting style of privacy notices which broadly align with the GDPR; for example stating that notices should be drafted clearly in an easy to understand manner for the intended recipient.

Position under the GDPR

The GDPR requires a significant increase in the information to be provided by data controllers to data subjects.

Article 12 states data controllers shall have transparent and easily accessible information notices. Information must be provided in a concise form, using clear and plain language, particularly where information is addressed to a child.

In addition to the requirements contained in the DPA, data controllers must also provide:
- the contact details of the data controller;
- the contact details of the Data Protection Officer (see further page 26);
- the Schedule 2/Article 6 and Schedule 3/Article 9 condition relied, the purpose of the processing and:
  - whether the provision of personal data are required by law or for a contract, as well as whether the data subject is obliged to provide the data and the possible consequences of the failure to provide such data; or
  - if the processing is based on the controller’s legitimate interests, an explanation of those interests; or
  - if the processing is based on consent, the right to withdraw consent at any time;
- the data retention period;
- a reference to the rights to erasure, to object to processing, data portability and to complain to the ICO, (see further page 20-22);
- information on international transfers and the safeguards applied to such transfers (see further page 30); and
- the existence of automated decision making (including profiling) and the envisaged consequences of such processing for the data subject (see further page 19).

Where the personal data are not obtained directly from the data subject, the notice should also identify the categories of personal data concerned and the source of the data.

There are also detailed requirements for when such information should be provided (which depend on whether the data are collected from the data subject themselves or from a third party).
Principles and Processing

Fair Processing Information

Impact on the health and social care sector

All privacy notices will need to be reviewed and amended in preparation for the implementation of the GDPR. Most of the information required by the GDPR is typically included in fair processing notices issued by health and social care providers.

On the inclusion of data retention periods, NHS Digital has recently updated its guidance on document management – see the Records Management Code of Practice for Health and Social Care 2016. This is a useful starting point.

More challenging is the requirement to make sure that children can understand the notice if their data is being processed. It may be that organisations need to have two versions of relevant notices – one for children and one for adults.

Privacy notices will now need to specify the source of the information. It is not clear if the source will need to be specifically identified, or whether a generic reference to the source, for example “your GP”, will suffice.

There is some tension between the requirement for notices to be clear and concise and the long list of items to be included, which includes some technical concepts like out of EEA transfers.

It is likely that the ICO will continue to favour a layered approach, with key initial information presented in a simple form and the ability to click through and find more detail if wanted.

Practical steps

- Organisations should begin reviewing their privacy notices to assess what information is required by the GDPR but is not currently provided.
- Data retention periods should be confirmed ready for inclusion in privacy notices.
- Data sharing arrangements will need to be reviewed to ensure that data subjects are provided with all the relevant information at the right time. Organisations sharing information can take advantage of the fact that the information need only be provided once (see Article 14.5).

“

All privacy notices will need to be reviewed and amended in preparation for the implementation of the GDPR

“
Principles and Processing

Processing Conditions and Exemptions

Current position under the DPA and ICO Guidance

**Principles**
The DPA contains eight data protection principles. In summary personal data must:

I. be processed fairly and lawfully;
II. be obtained for a specified purpose and not processed for any purpose that is incompatible with that purpose;
III. be adequate, relevant and not excessive;
IV. be accurate and up to date;
V. not be kept longer than necessary;
VI. be processed in line with data subject rights; and
VII. be protected by appropriate security; and
VIII. not be transferred outside the EEA unless appropriate restrictions are in place.

**Processing Conditions**
In order for processing to be fair (i.e. in accordance with the first data protection principle) the relevant processing conditions must be met.

A processing condition from Schedule 2 of the DPA is always required for the processing of personal data. Where sensitive personal data is being processed, a Schedule 3 condition is also needed. The Schedule 3 conditions are set out in the DPA itself and in a number of additional statutory instruments.

**Exemptions**
The DPA provides exemptions to certain obligations in specific circumstances. These exemptions broadly relate to:

- registration with the ICO;
- granting access to a data subject’s personal data;
- the obligation to process personal data fairly (i.e. to give privacy notices); or
- the restriction on disclosing personal data to third parties.

Position under the GDPR

**Principles**
The principles remain largely untouched, with the exception of the addition of a new principle of accountability (see page 23 for further details).

Principles 6 and 8 of the DPA remain in substance, but no longer in the form of a principle.

**Processing Conditions**
The Schedule 2 (now Article 6) conditions are largely unchanged. One significant development is that public authorities can no longer rely on the legitimate interests condition. There is also the addition of a new Schedule 2/Article 6 condition that applies if the processing is necessary for the performance of a contract with the data subject, or in order to enter into such a contract. This is relevant to the delivery of privately funded care.

It will be harder to rely on the consent condition in Schedule 2/Article 6 and the explicit consent condition in Schedule 3/Article 9. Extra requirements now apply and these are outlined in Articles 7 and 8 (children’s consent).

On the Schedule 3 (now Article 9) conditions, the medical purposes condition has been expanded to expressly include both health and social care. It continues to apply both to treatment and management of services. The requirement for the processing to be carried out by someone owing a duty of confidentiality remains but it no longer has to be equivalent to the duty owed by regulated healthcare professionals.

There is a new Schedule 3/Article 9 condition for processing in the area of public health, to ensure the quality of health care or to secure the quality of medicinal products or medical devices. The requirement for the person doing the processing to owe a duty of confidentiality does not apply.

There is a new Schedule 3/Article 9 condition that can apply to processing for scientific research purposes.

**Exemptions**
The GDPR gives member states a large amount of discretion to determine their own exemptions to the provisions of the GDPR in respect of processing data for various ‘public interest’ purposes such as national security.

Further legislation and guidance on this is awaited but we think it is unlikely that the exemptions set out in the DPA will be narrowed in any material way.
Principles and Processing

Processing Conditions and Exemptions

Impact on the health and social care sector

Schedule 2/ Article 6 conditions

Many health and social care organisations rely on the sixth condition of Schedule 2 to justify processing. Once the GDPR applies public authorities will not be able to rely on this condition any more. However, public sector organisations and those delivering services commissioned by the public sector will be able to rely on the Schedule 2/ Article 6 public function condition, which applies where processing is necessary for “the performance of a task carried out in the public interest”.

Those involved in the delivery of privately funded care can rely on the new condition for processing that is necessary for the performance of a contract to which the data subject is a party. The consent condition can only be relied upon if the requirements of Article 7 are complied with. In particular, consideration will need to be given to Article 7(4). This requires data controllers to take “utmost account” of whether the performance of a contract is conditional on the provision of consent. In such cases there is a question mark over whether consent is freely given and valid. It appears easiest to rely on the performance of a contract condition instead.

Schedule 3/ Article 9 conditions

The re-wording of the medical purposes condition to refer to social care is very welcome. There has been some uncertainty about the extent to which social care providers and commissioners could rely on the condition when processing personal data internally or when sharing with others. The amended wording removes this uncertainty.

It is also helpful that the wording requiring a duty of confidence equivalent to that of a health professional has been removed. The equivalence test has caused uncertainty about whether an individual who is not regulated by a professional body can fulfil the condition by having a contractual duty of confidence.

The addition of the research purposes condition is also a welcome development.

Consent and the law of confidence

Although it is unlikely that health and social care organisations will need to rely on a consent condition, the new requirements regarding consent are likely to have an impact. The existence of tight and clearly worded rules around what counts as consent under the GDPR is likely to lead to further consideration of consent issues in the context of the common law duty of confidentiality.

The law of confidentiality is separate to DPA/ GDPR rules. Today, we use the concept of implied consent to justify the wide range of processing that takes place for direct care. That will continue to be the case under the law of confidence once the GDPR has been passed, even though it does not sit easily with the new GDPR rules on consent.

Link with data subject rights

Some of the data subject rights are triggered by relying on particular conditions. For example, the right to data portability if the data controller is relying on consent or performance of a contract.

Under the DPA if more than one condition applies the data controller has been free to choose which one to rely on. Case law will need to establish what will happen under the GDPR.

Practical steps

- Consider your data flows and what conditions you are relying on. Bear in mind that if you deliver a mix of private and public services different conditions will apply.
- Remember that you will need to put details of the conditions that you are relying on in your privacy notices.

The re-wording of the medical purposes condition to refer to social care is very welcome.
Data Subject Rights

Profiling

Current position under the DPA and ICO Guidance

The DPA does not define “profiling”; instead it refers to “automatic decision making”.

A data subject is entitled to require a data controller to ensure that no decision which specifically affects him or her is made solely based on automatic means unless such decision is made in the course of entering into or performing a contract or is authorised or required by law.

Additionally, if a decision is made by automated means, a data subject is entitled to know the methodology behind such decision as part of a subject access request.

Position under the GDPR

The GDPR introduces a new definition of “profiling” (Article 4(4)) which is defined as “any form of automated processing of personal data consisting of the use of personal data to evaluate 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 or interests, reliability or behaviour, location or movements”.

Article 22 introduces a new right not to be subject to a decision based solely on profiling which produces a legal or other similarly significant effect.

The restriction does not apply if the decision is:

- necessary for a contract;
- expressly authorised by law; or
- has the explicit consent of the data subject.

There is an absolute restriction on profiling using sensitive personal data unless the data subject has given explicit consent or it is necessary for reasons of substantial public interest.

In circumstances where profiling is permitted, the data controller must implement suitable measures to safeguard the data subject’s rights and interests. Additionally, a data controller who uses profiling techniques must implement appropriate technical and organisational measures to safeguard against inaccuracies and prevent discrimination.

The data subject should be informed in the privacy notice of the existence of profiling, the logic used and the significance and likely consequences of such profiling.

Impact on the health and social care sector

Most health and social care organisations do not use profiling. There is usually some human intervention before any decision affecting an individual is made. There are some exceptions to this.

Risk stratification decisions may involve profiling e.g. if a patient is asked to an appointment based on data analysis without any human intervention.

Organisations delivering private care may use profiling to target customers, make decisions to offer services or collect debts. Such activities will be permissible if they are necessary for entering into or the performance of a contract. But profiling for marketing purposes will always require explicit consent.

Practical steps

- Identify whether your organisation carries out profiling. If so:
  - how will you comply with the GDPR requirements?
  - update privacy notices to refer to profiling activities.

- Ensure appropriate measures are in place to prevent profiling which produces inaccurate outcomes and measures which guard against discrimination.
Data Subject Rights

New Right of Data Portability

Current position under the DPA and ICO Guidance

There is no right of data portability or other equivalent right under the DPA. However, data subjects have a right to receive a copy of their personal data in response to a subject access request in an intelligible format.

Impact on the health and social care sector

This right is unlikely to apply to those solely concerned with publicly funded services. Such organisations will not need to rely on the consent condition in Schedule 2/Article 6. They can rely on the public function condition instead.

Providers of private sector services are likely to need to comply, as they are likely to need to rely on the compliance with a contract condition in Schedule 2/Article 6. This will trigger the right to data portability.

The right only applies to data that the data subject has provided to the data controller that is processed automatically i.e. without human intervention. This could cover information supplied by wearable medical devices that monitor health data about an individual and transmit it to a data controller.

Position under the GDPR

Article 20 introduces a new right for data subjects. On request, a data controller must:

- provide the data subject with a copy of his or her personal data which was provided by him or her to the data controller (not data which has been generated by the data controller itself) in a structured, commonly used and machine readable format; and
- not hinder the data subject’s transmission of personal data to a new data controller.

Where technically possible, a data subject also has a right to require that their personal data is transmitted directly between data controllers.

The right of data portability only applies where:

- data is processed by automated means; and
- the data subject has provided consent to the processing; or
- the processing is necessary to fulfil a contract.

Practical steps

- Consider whether your organisation will be relying on the consent or compliance with a contract conditions.
- If so, identify what data is gathered from data subjects and whether this is processed automatically.
- If such data exists and is processed automatically, establish policies and procedures for responding to requests.
Data Subject Rights

New Right of Erasure

Current position under the DPA and ICO Guidance

Principle 5 of the DPA obliges data controllers to ensure that personal data is not kept longer than necessary.

Data subjects have a right to have their personal data erased:

- if the data subject can prove substantial unwarranted damage or distress; or
- by court order, when the personal data is inaccurate.

This is a high threshold and, as such, this is currently a little used right.

Impact on the health and social care sector

With the balance of power now shifted from data controller to data subject, the burden of proof is on the data controller to demonstrate the legitimate interest and/or legal and regulatory reason for data retention.

Most health and social care organisations already have robust data retention policies in place that are broadly in line with national NHS guidance. These will be put under scrutiny.

We expect data subjects will have high expectations of their right to erasure. Therefore data controllers need a clear and documented reason why they are keeping personal data.

Position under the GDPR

Article 17 provides data subjects with a new enhanced right to request erasure of their personal data. Data subjects do not need to prove substantial unwarranted damage or distress or inaccuracy.

Data controllers must delete personal data on request where specified grounds apply. Such grounds include:

- where the personal data are no longer necessary for the original purpose for which the data were collected/processed; and
- if the data subject withdraws their consent and no other legal ground for processing applies.

However, there are a number of grounds on which data controllers can rely to keep personal data. These include if the data is needed for:

- the delivery of public services;
- the protection of public health; or
- the establishment, exercise or defence of legal claims.

Where a request for erasure has been received in respect of personal data which has been disclosed by the data controller to a third party, the data controller must take all reasonable steps to inform any onward data controllers of the request.

There are other provisions throughout the GDPR which require increased transparency as to how long data controllers are to keep personal data.

For example, Article 13 requires that a privacy notice contains details of the period for which the personal data will be stored. The right of subject access in Article 15 obliges a data controller to inform data subjects on request of the envisaged period for which personal data will be stored or the criteria used to determine the period.

Practical steps

- Ensure you have an appropriate data retention policy in place and that it is implemented. Review your policy in light of the NHS Digital guidance ‘Records Management Code of Practice for Health and Social Care 2016’.
- Policies and procedures should be put in place documenting how erasure requests are to be handled.
Data Subject Rights

The Best of the Rest

Current position under the DPA and ICO Guidance

Data subjects have a right to:

- receive their personal data in response to a subject access request in an intelligible format within 40 days of request, for a fee of £10. They also have a right to certain limited information about the processing undertaken;
- rectification of their personal data if it appears to a court to be based on inaccurate data. This requires a court order to enforce;
- prevent processing of their personal data in certain defined circumstances and where they can show such processing would cause unwarranted substantial damage or distress; and
- object to direct marketing.

Impact on the health and social care sector

The removal of the ability to charge for subject access requests is likely to lead to an increase in such requests. There is a possibility that the new exemption for requests that are manifestly excessive could be used to refuse requests from solicitors or employees in dispute with the data controller. In these cases it could be argued that as there is another, more appropriate route to obtaining the information the request is excessive.

With an increased public awareness of rights data controllers may receive an increased number of requests for restrictions on processing or rectification.

The right to restriction of the processing of personal data may be difficult to implement. IT systems may not be able to exclude data from analysis, or retain it when it would otherwise be deleted.

Practical steps

- Amend subject access request policies and procedures to take account of the new provisions.
- Investigate how you might implement a request to restrict processing.
- Put processes in place to ensure that all requests to exercise data protection rights are dealt with in accordance with Article 12.

Position under the GDPR

Subject access requests (Article 15)

Article 15 contains an enhanced right of subject access. Data subjects will be entitled to more information including the legal basis of the processing, the period of data storage, information about data subject rights, details of any transfers outside of the EU and safeguards applied to such transfers, as well as contact details of the data controller’s data protection officer.

Right to object and restrict processing (Article 18)

Article 18 gives data subjects the right to restrict processing. This can be used to:

- pause processing if the data subject says that their personal data is not accurate, until its accuracy is verified;
- prevent the deletion of data that has been processed unlawfully;
- prevent the deletion of data no longer needed by the data controller but needed by the data subject for legal reasons; or
- pause processing if the data subject has objected to it under Article 21(1) while it is verified whether the legitimate grounds of the data controller override those of the data subject.

If processing has been restricted then other than storage, it can only be processed with the consent of the data subject, for legal purposes, the protection of third party rights or reasons of “important public interest”.

Responding to requests to exercise rights (Article 12)

The GDPR introduces general provisions that apply to all attempts to exercise data subject rights.

There is a new duty to help data subjects exercise their rights. No fee can be charged for complying with a request.

The time period for dealing with requests, including subject access requests, has been reduced from 40 days to 1 month. This can be extended by 2 months in some circumstances.

Requests can be refused if they are "manifestly unfounded or excessive".

Responses to subject access requests need to include details of other data protection rights and the ability to complain to the ICO.
Accountability

General Policies and Records

Current position under the DPA and ICO Guidance

There is no general principle of accountability under the DPA. The ICO may request copies of appropriate data protection and information security policies when investigating complaints and may also issue sanctions to data controllers who do not have such policies in place. However, there is no specific requirement for such policies under the DPA. Sanctions are issued on the basis that appropriate technical and organisational measures were not in place in breach of principle 7 (security).

Impact on the health and social care sector

While the principle of accountability is a new concept under data protection law, typically organisations in the health and social care sector already have appropriate systems and controls in place to manage their operational risk. Such systems and controls should be reviewed to ensure they address the principle of accountability in sufficient detail to meet the requirements of the GDPR.

Position under the GDPR

Article 5 introduces a new principle of accountability. Data controllers are responsible for and must be able to demonstrate compliance with the principle of accountability. There are many obligations throughout the GDPR which require documentation to be kept, which will need to be produced to the ICO on request.

Article 24 states that appropriate technological and organisational measures should be in place to ensure that processing is conducted in accordance with the GDPR. Data controllers should be able to demonstrate this and the measures should be reviewed and updated where necessary. The measures in place shall include the implementation of appropriate data protection policies.

Article 30 obliges both data controllers and data processors to maintain records of processing activities. Such records need to include details such as data retention periods, extra EEA transfers of personal data and the recipients of personal data. These need to be made available to the ICO on request.

“There are many obligations throughout the GDPR which require documentation to be kept, which will need to be provided to the ICO on request.”

Practical steps

- Organisations should identify what data they process and the purposes for which the personal data are processed.
- All data protection and data security policies and procedures should be reviewed in light of the new principle of accountability.
Accountability

Data protection by design and by default

Current position under the DPA and ICO Guidance

Principle 7 states that appropriate technical and organisational measures shall be taken to prevent unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The interpretation of this principle states that regard should be had for the state of technological development, the cost of implementing the measures, the nature of the data and the harm which may result. No further details are specified in the DPA.

Position under the GDPR

Article 25 introduces the concepts of data protection by design and by default which are much more specific than the current general obligation to have appropriate security in place under the DPA.

‘Data protection by design’ requires data controllers to implement appropriate technical and organisational measures to protect the rights of the data subject and ensure compliance with the GDPR, having regard to the technology required to meet this obligation and the costs of implementation of the same, the nature, scope and purpose of the processing, as well as the risks posed to the data subject of the processing activities. Pseudonymisation is referred to as a good example of data protection by design (see page 29 for further detail).

‘Data protection by default’ means data controllers must implement appropriate technical and organisational measures to ensure that only personal data that is necessary for processing for a specific purpose is processed. To comply, data controllers should take into account:

- the amount of personal data collected;
- the extent of the processing;
- the period of storage; and
- the accessibility of that data.

Data controllers should ensure that, by default, personal data is not made available or accessible to an indefinite number of individuals.

Impact on the health and social care sector

Most organisations in the health and social care sector already take the security of data very seriously. It is likely that IT systems already operate with privacy in mind e.g. through the use of role-based access controls.

However, there are new rights under the GDPR, such as the right to restrict processing, that it may be difficult for existing systems to comply with. Organisations should consider workarounds and technical solutions.

Practical steps

- All new systems should be commissioned and built using data protection by design and by default. In practice this will mean ensuring that there is the technical functionality to implement the requirements of the GDPR. For example, systems should be capable of searching for and extracting personal data in order to comply with the right of data portability.

- Make sure that your IT and commissioning teams are aware of the requirements of data protection by design and default.
Accountability

Data Protection Impact Assessments

Current position under the DPA and ICO Guidance

There is no legal requirement that data controllers carry out a data protection or privacy impact assessment (PIA). To our knowledge, the ICO is the only data protection authority in Europe that has produced guidance encouraging data controllers to conduct PIAs as a tool to help ensure DPA compliance. Guidance was issued by the ICO in 2007 and subsequently updated in 2014.

Impact on the health and social care sector

Many of our clients have already started to carry out PIAs. However, the mandatory requirement to carry out a PIA in certain circumstances will add an extra compliance step in the process of rolling out new data projects. This will need to be budgeted for both in terms of time and costs. There is a chance that increased communication with the ICO in respect of “high risk” projects could, in turn, bring the ICO’s focus specifically to an organisation’s general data protection compliance.

Position under the GDPR

Article 35 introduces a requirement that PIAs are performed where processing activities present a “high risk” to the rights and freedoms of natural persons.

The GDPR sets out a particular list of activities which will trigger the need to carry out a PIA prior to the processing of that personal data. The list is non-exhaustive and includes:

- activities which are systematic and extensive and which use automated processing of personal data in order to evaluate, analyse or predict behaviour;
- the large scale processing of sensitive personal data; and
- the systematic monitoring of a publicly accessible area on a large scale.

In addition, the ICO is required to establish and make public a list of the types of processing activities which do and do not require a PIA.

The GDPR states that the data controller should seek the advice of the data protection officer when carrying out a PIA. It should also seek the views of data subjects, “where appropriate”.

The PIA should be reviewed whenever there is a change to the risks presented by the processing operations.

If a PIA indicates that the processing would result in a high risk to a data subject, in the absence of steps taken by the data controller to mitigate the risk, prior consultation with its supervisory authority is required before processing begins.

Practical steps

- If you have not done so already, prepare a template PIA and train relevant employees about how and when it should be used.
- If you have not done so already, start carrying out PIAs regarding each new data processing project using service user health data. Ensure that outcomes and compliance steps are documented and actioned.
- Consider whether you carry out activities other than the processing of health data that would require a PIA e.g. through the use of CCTV or health monitoring devices.
- Look out for ICO guidance on when a PIA will or will not be required.
Data Protection Officers

Current position under the DPA and ICO Guidance

Neither the DPA nor any ICO guidance obliges data controllers to appoint a data protection officer. However, in reality most large organisations have a data protection specialist.

Impact on the health and social care sector

Most health and social care organisations will need to have a DPO, either because they are a public body or because their core business requires large scale processing of sensitive personal data.

Most organisations will have a DPA specialist, though this is not true for smaller healthcare organisations such as GP practices. It may be cost effective for those smaller organisations to contract out the role. Public authorities can group together to appoint one DPO between them.

Practical steps

- Review the current job specification of your organisation's DPO and consider whether it is appropriate in light of new requirements specified in the GDPR.
- Consider the practical issues surrounding the DPO appointment (e.g. independence, separate budget, report directly to the board).
- Depending on the size of your organisation, consider whether the DPO is likely to require a support team in order to carry out their role effectively and meet all the obligations of the GDPR.

Position under the GDPR

Article 37 obliges both data controllers and data processors to appoint a DPO in three situations:

- where they are a public body;
- where core activities require regular and systematic monitoring of personal data on a large scale; and
- where core activities involve large scale processing of sensitive personal data.

DPOs must be selected on the basis of professional qualities and expert knowledge of data protection law but do not need to be legally qualified. DPOs can be either an employee or contractor.

DPOs must be informed of all data protection issues within the organisation in a proper and timely manner. DPOs must be provided with the necessary resources to carry out his/her tasks and have access to all personal data and processing operations. They must report directly to the highest level of management.

Data subjects may contact DPOs with regard to all issues related to processing and the exercise of their rights under the GDPR.

The minimum duties of a DPO are set out at Article 39.

The DPO shall be independent from the data controller or data processor that appoints him or her, and specifically must not be instructed on how to carry out the Article 39 tasks. The DPO must report directly to the highest level of management and shall not be dismissed or penalised for performing his/her tasks. This effectively provides the DPO with a special “protected status” within an organisation. It may create challenges for employers if there is a need to take legitimate performance management or other action against a DPO in the context of the employment relationship.

DPOs can carry out other tasks alongside their data protection duties; however, the employer is required to ensure there are no conflicts of interest in the execution of such duties.
Breach Notification

Current position under the DPA and ICO Guidance

With the exception of communication and internet service providers, there is no obligation under the DPA to report breaches of security to the ICO or data subjects, although ICO guidance recommends that “serious” breaches are reported to both the ICO and data subjects.

The ICO considers voluntary notification to be a mitigating factor when considering the level of monetary penalty to be imposed.

Position under the GDPR

Article 33 introduces mandatory data breach reporting. Data controllers will be obliged to report security breaches to the relevant supervisory authority “without undue delay, and where feasible, not later than 72 hours” after it first becomes aware of it. If the notification is made after 72 hours it should be accompanied by reasons for the delay.

However, it is not necessary to notify the breach where it is “unlikely to result in a risk to the rights and freedoms” of data subjects.

Article 34 provides that security breaches must also be notified to a data subject where the breach “is likely to result in a high risk” to the rights and freedoms of data subjects.

However, notification to data subjects is not required if:

- the data controller has implemented appropriate security measures that render the personal data unintelligible to any unauthorised person, such as encryption;
- the data controller has taken subsequent measures to ensure the high risk to data subjects does not materialise; or
- it would involve disproportionate effort, in which case a public communication will suffice.

Impact on the health and social care sector

NHS organisations are already used to reporting data breaches using the reporting tool. It is also common for data subjects to be informed of any breach. The new requirements to notify will therefore have less impact on the NHS than on other sectors.

However, the reporting tool is likely to need adjusting to reflect the requirements of the GDPR. In particular, it appears likely that some incidents involving very small numbers of service users may need to be reported that are not reported under the current system.

It is vital for every organisation to have a data breach response plan in place to enable a quick reaction to identify and contain a breach and notify the ICO, ideally within the 72 hour period.

Practical steps

- Review data breach policies to ensure they deal with informing data subjects.
- Ensure policies enable you to notify the ICO within 72 hours.
Security

Security measures

Current position under the DPA and ICO Guidance

Principle 7 states that appropriate technical and organisational measures shall be taken against unauthorised or unlawful processing of personal data and against accidental loss or destruction of, or damage to, personal data. The interpretation of that principle states that this should have regard to the state of technological development, the cost of implementing the measures, the nature of the data and the harm which may result. No further specifics are given.

ICO guidance has been produced over the years outlining good and bad practice. Undertakings, enforcement notices and monetary penalty notices also give good guidance as to security measures and training that the ICO expects as a minimum standard.

Impact on the health and social care sector

The health and social care sector will generally already have robust security measures in place. Therefore, although the GDPR provides further guidance on what these measures should look like, many organisations will find that they already meet the requirements.

Data processors will now have their own obligations under the GDPR. However in practice they will usually have had such obligations imposed by contract.

Position under the GDPR

Article 5 requires personal data to be processed in a way that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using technical or organisational measures. It applies to both data controllers and data processors.

Article 32 provides greater detail as to what amounts to “appropriate” technical and organisational measures. The GDPR requires data controllers and data processors to balance the changing state of technology, the costs of implementation, the risks presented by the data processing and consequences of breach for data subjects, and implement a level of security appropriate to the risk, including:

- pseudonymisation and encryption of personal data;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services;
- the ability to quickly restore the availability and access to personal data in the event of a physical or technical incident; and
- a process for regularly testing, assessing and evaluating the effectiveness of security measures.

It is also worth remembering that all security measures taken need to comply with the concept of privacy by design and by default, and should be regularly reviewed to ensure that they remain appropriate.

Practical steps

Health and social care organisations (whether a data controller or data processor) should regularly review the security measures in place to ensure that they are appropriate to the nature of the data held and impact on data subjects if a breach were to occur. Particular regard should be had to whether it is appropriate to pseudonymise or encrypt the data. It should also be highlighted that this should not be a one off task – the review process should be carried out regularly to ensure the security measures remain effective and appropriate in light of changing technology.
Security

Anonymous and Pseudonymous Data

Current position under the DPA and ICO Guidance

There is no definition in the DPA of anonymous or pseudonymous data.

In 2012 the ICO produced an anonymisation code of practice which defined anonymised data as:

“Data in a form that does not identify individuals and where identification through its combination with other data is not likely to take place”.

There is no formal recognition of pseudonymous data. However it is commonly referred to as data from which the identity of an individual is removed, but can be recovered.

Position under the GDPR

The GDPR introduces definitions of anonymous and pseudonymous data.

Anonymous data is defined as “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” (Recital 26).

Pseudonymisation means 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 non-attribution to an identified or identifiable natural person (Article 4(5)).

Despite being considered personal data (and therefore generally subject to the GDPR’s personal data requirements), the use of pseudonymisation as a data security method is supported by the GDPR because it is recognised as being able to “reduce the risks to the data subjects concerned”. It is also a recognised process in implementing data protection by design.

There are benefits to organisations utilising pseudonymisation:

- it is a positive factor when determining whether a future data use is compatible with the original use for which the data were gathered (Article 6(4));
- in the event of a data breach affecting pseudonymised data, data subjects may not need to be informed if the “key” that would allow re-identification was not compromised.

Impact on the health and social care sector

It had been hoped that there would be a relaxation of the requirements in respect of pseudonymised data (as indicated by prior GDPR drafts). This has not been realised in the final text.

With the formal recognition of pseudonymisation as a security technique, it seems likely that the ICO could start penalising organisations who suffer a data breach if the data was in fully identifiable rather than pseudonymised form.

Practical steps

- Where possible, personal data that is no longer required for the provision of services, regulatory or legal reasons should be anonymised. This will take it outside the scope of the GDPR and will allow your organisation to use such data as it chooses.
- Where personal data cannot be anonymised, health and social care organisations are advised to apply pseudonymisation as a security measure where possible.
International Transfers

Current position under the DPA and ICO Guidance

Principle 8 states that personal data should not be transferred outside the EEA unless there is adequate data protection.

A transfer is permitted under the DPA if:

- the jurisdiction has been deemed adequate by the European Commission;
- an approved mechanism is used (e.g. model clauses); or
- a derogation applies (e.g. consent of the data subject).

Position under the GDPR

Articles 44 – 50 leave the current position largely unchanged. The following additions should be noted:

- the European Commission can deem a particular sector (e.g. health and social care) in a particular jurisdiction as adequate;
- binding corporate rules are specifically acknowledged;
- there are two new approved mechanisms of transfer – reliance on an approved code of conduct or an approved privacy seal; and
- a new derogation has been inserted which permits a transfer when in the legitimate interests of the data controller and where:
  - the transfer is not repetitive and only concerns a limited number of data subjects; and
  - the controller has assessed the transfer, adduced safeguards and has a compelling legitimate interest that is not outweighed by the interests or rights and freedoms of the data subject.

Impact on the health and social care sector

The changes are unlikely to have a significant impact. This is partly because most health and social care organisations do not transfer data outside the EEA. It is also because the changes to the rules are minimal: they are only likely to have a significant impact on multinational organisations with a number of European establishments.

Practical steps

- Review data flows to ensure that appropriate transfer mechanisms are in place.
Enforcement

Current position under the DPA and ICO Guidance

The DPA empowers the ICO to issue enforcement notices, assessment notices, information notices and determinations. Compulsory audits can only be performed on NHS and other government bodies. The power to issue monetary penalties of up to £500,000 for serious breaches was given in April 2010.

The highest fine to date has been £350,000. The majority of fines in the UK have been for breach of principle 7 (security) but there has been one fine for breach of principle 4 (accuracy) and one for principle 1 (fairness).

Fines can only be imposed against data controllers and not data processors.

There are a limited number of criminal offences under the DPA which can be prosecuted by the ICO through the courts.

An organisation which has an “establishment” in a Member State deals with the supervisory authority of that Member State. Group structures with establishments across Europe therefore have to deal with multiple regulators.

Position under the GDPR

Powers

Article 58 significantly increases the level of fine which can be issued, widens the circumstances in which a fine should be issued and provides supervisory bodies with additional investigative and corrective powers. Fines can be issued against both data controllers and data processors.

Additional powers granted to the ICO will include the ability to:

- carry out audits; and
- issue orders to cease operations, notify data subjects of a breach, rectify, restrict or erase data, suspend or prohibit processing or order suspension of data flows to third countries.

Criminal sanctions

Member States can put in place criminal sanctions for infringements of the GDPR.

Circumstances for a monetary penalty

Fines can be imposed for “any infringement” of the GDPR.

A warning should only replace a fine in the case of a minor infringement or where a fine would be deemed a “disproportionate burden to a natural person”.

The GDPR provides a list of the considerations a supervisory authority shall take into account when assessing the level of fine to be imposed. These include:

- nature, seriousness and length of the infringement;
- nature of the processing and categories of data involved;
- number of data subjects affected and level of damage suffered;
- evidence of intention / negligence;
- mitigation;
- technical and organisation measures implemented by data controller or data processor;
- relevance of previous infringements;
- manner in which the supervisory authority became aware of the infringement(s);
- adherence to approved codes of conduct; and
- other relevant aggravating or mitigating factors.
Enforcement

Level of monetary penalties

When imposing fines supervisory authorities must ensure they are “effective, proportionate and dissuasive”.

The level of fine applicable depends on the Article of the GDPR that has been breached. The fine may be levied by reference to the turnover of an “undertaking”. Full details are set out on page 33.

The GDPR introduces some uncertainty by its use of the word “undertaking”. It is an open-ended concept, which encompasses every entity engaged in an economic activity regardless of the legal status of the entity and the way in which it is financed (European Court of Justice Case C-41/90). If there is a breach of competition law, fines levied on an undertaking are based on its turnover in the relevant market affected by the conduct. If the relevant market is worldwide the fine is based on the worldwide turnover of the undertaking. If the relevant market is smaller (e.g. one country) the fine will be levied by reference to the turnover in that smaller market.

Impact on the health and social care sector

Issues of service user confidentiality are already high up the agenda of most health and social care organisations. The increase in the level of fines will need to be fed into any assessment of risk regarding compliance.

Although the one stop shop mechanism should have had a positive impact for organisations with offices in more than one EU country, the watered down version that appears in the GDPR is likely to disappoint. This is because it looks like supervisory authorities in all relevant Member States will still need to be consulted in the event of a data breach that affects their nationals.

Practical steps

- Start taking all the practical steps in the other sections of this guide to avoid a monetary penalty notice
- Consider whether current insurance covers new liabilities.

One stop shop and responsibility for enforcement

The much publicised “one-stop shop” has survived in a watered-down form in Article 56. For organisations with entities in more than one Member State, the supervisory authority in the Member State of the organisation’s main establishment is deemed competent to take the lead in dealing with any enforcement issues.

The lead supervisory authority will be required to consult with other supervisory authorities whose nationals are affected.

The GDPR also creates a super regulator in the form of the European Data Protection Board (EDPB) (formerly Working Party 29). The EDPB will include the head of each national supervisory authority and the European Data Protection Supervisor. The EDPB will issue guidance, ensure consistent application of the GDPR and be empowered to resolve disputes among the national supervisory authorities.

When imposing fines supervisory authorities must ensure they are “effective, proportionate and dissuasive”. The level of fine applicable depends on the Article of the GDPR that has been breached.
## Enforcement

<table>
<thead>
<tr>
<th>Level</th>
<th>Amount</th>
<th>Relevant articles</th>
</tr>
</thead>
</table>
| 1     | EUR 10,000,000 or in case of an undertaking 2% total worldwide annual turnover in the preceding financial year (whichever is greater) | 8: Child's consent  
11: Processing not requiring identification  
25: Data protection by design and by default  
26: Joint controllers  
27: Representatives of controllers or processors not established in EU  
28-30 & 32: Processing  
31: Co-operation with the supervisory authority  
33: Notification of breaches to supervisory authority  
34: Communication of breaches to data subjects  
35: Data protection impact assessment  
36: Prior consultation  
37-39: DPOs  
41(4): Monitoring approved codes of conduct  
42 & 43: Certification |
| 2     | EUR 20,000,000 or in case of an undertaking 4% total worldwide annual turnover in the preceding financial year (whichever is greater) | 5: Principles for processing personal data  
6: Lawfulness of processing  
7: Conditions for consent  
9: Processing special categories of personal data (i.e. sensitive personal data)  
12-22: Data subject rights to: information, access, rectification, erasure, restriction of processing, data portability, object, profiling  
44-50: Transfers to third countries  
58(1): Requirement to provide access to supervisory authority  
58(2)(f) & 58(2)(i) & 58(2)(j): Orders / limitations on processing (definite or temporary) or the suspension of data flows  
Obligations adopted under Member State law (specific data processing situations) |
Compensation

Compensation for Data Breaches

Current position under the DPA and ICO Guidance

Claims for compensation for data breaches can only be brought against data controllers.

Section 13(1) provides that individuals that suffer material damage as a result of a breach of the DPA are entitled to compensation from the data controller.

Section 13(2) provides that individuals are entitled to compensation for distress arising from breaches of the DPA if the individual also suffers damage as a result of the breach. This had previously been interpreted to mean "material damage", which meant that individuals could only seek compensation for distress arising from data breaches if they had also suffered some financial loss. In 2015, the Court of Appeal in the case of Vidal-Hall v Google recognised that this distinction was somewhat artificial and ruled that individuals are entitled to claim for damages for pure distress caused by breaches of the DPA.

Position under the GDPR

Article 79 provides that data subjects have a right to a judicial remedy against data controllers and data processors.

Article 82 provides that any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation from the data controller or data processor for the damage suffered.

Therefore, damages will be available for pure distress claims arising from breaches of the GDPR and claims can be brought both against data controllers and data processors. A data processor's liability is limited to damage caused by its processing where it has not complied with its specific obligations under the GDPR or acted contrary to the lawful instructions of the data controller.

The burden of proof is on the party that is responsible for the event which has caused the damage.

Where multiple data controllers or data processors are involved in data processing, if any one of them is responsible for any of the damage, then it will be responsible to the data subject for all of the damage. The party which compensates the data subject will have the right to claw back compensation from the other data controllers or data processors for the damage caused by their breach.

Impact on the health and social care

The clarification that compensation is available for both material and immaterial damage simply confirms the law as stated by the Court of Appeal in Vidal-Hall v Google, so the changes will not be a surprise. The fact this is set out clearly in the GDPR may lead to more claims.

Practical steps

- Start taking all the practical steps in the other sections of this guide to help avoid a compensation claim.
Scope

Extra Territorial Effect

Current position under the DPA and ICO Guidance

The DPA has limited territorial scope. It applies to data controllers "established" in the UK. It also applies to data controllers who are processing personal data on equipment in the UK.

Position under the GDPR

Article 3 expands the territorial reach of European data protection legislation. The GDPR will not only apply to data controllers and data processors established in the EU but also to those which:

I. offer goods or services to EU residents (irrespective of whether a fee is charged); or
II. monitor the behaviour of EU residents as far as that behaviour occurs in the EU.

Recital 23 states that when assessing if a non-EU established business is offering goods or services to data subjects in the EU consideration needs to be given to whether the business is:

- offering services in a language or currency of a member state;
- enabling EU residents to place orders in such other language; or
- referencing EU customers in its publications.

This may make it "apparent that the controller envisages offering goods or services" to EU residents, and it is likely to be considered to be subject to the GDPR. Merely having a website which is accessible by EU residents is insufficient.

Monitoring the behaviour of EU residents will include tracking health data of EU residents through wearable devices in order to create profiles or to analyse or predict behaviour (if the behaviour takes place in the EU).

Businesses outside the EU caught by the GDPR will need to appoint a representative established in the EU, who shall act on behalf of the data controller or data processor and act as the point of contact for supervisory authorities.

A representative is not required if the processing is:

- occasional;
- does not include large scale processing of sensitive personal data; and
- is unlikely to result in a risk to the rights and freedoms of data subjects.

The representative may itself also be subject to enforcement action in the event of non-compliance by the data controller.
Scope

Extra Territorial Effect

Impact on the health and social care sector

Organisations established outside of the EU but marketing services to citizens in the EU will need to ensure that they comply with the GDPR obligations. This requirement will extend to UK organisations once the UK has left the EU.

This requirement applies even if no charge is made for the service that is received. The sale of online services appears most likely to be affected as this is most likely to take place across the EU boundary. Some health and social care organisations market their non-NHS services outside of the UK e.g. to the Republic of Ireland. Those organisations will also need to comply.

There is a significant question mark over how this extra territorial extent will be enforced.

“It is unlikely that the widening of the scope of data protection law to cover companies outside the EEA will have a significant effect on the insurance industry outside the EEA.”