GENERAL DATA PROTECTION REGULATION 2016 (GDPR)

IMPLICATIONS FOR SOCIAL CARE EMPLOYERS

Social care organisations hold a significant amount of personal information relating to individuals, whether they be employees, people who need care and support or other customers or suppliers. A proportion of that data is likely to constitute sensitive personal data or "special categories of data" (including for example, medical records, religious beliefs or ethnic origin).

All organisations that process personal data are required to comply with the Data Protection Act 1998 (DPA) and, from 25 May 2018, the General Data Protection Regulation (GDPR). Penalties for failure to comply, including fines, are significant. If GDPR isn't already on your organisation's agenda, now is the time to act.

Get Data Protection Ready

The GDPR extends current requirements set out in the Data Protection Act 1998 and places new obligations on organisations that process personal data and special categories of data. These include, amongst others:

1. more stringent requirements around consent, particularly if special categories of data are involved;
2. the right to be forgotten;
3. taking an approach to projects that promotes privacy and data protection compliance from the start and using privacy impact assessments to identify and reduce risk;
4. a modified subject access request procedure that favours the individual;
5. if there is a breach of GDPR there are new, stricter requirements to notify the Information Commissioner's Office and the affected data subjects; and
6. expanded territorial reach – a non-EU company could be subject to the same sanctions as EU companies.

What are the key implications for organisations in the health and social care sector?

Social care organisations will be affected by the majority of changes introduced by GDPR. The DPA already requires social care employers to be compliant and robust due to the nature of the data frequently being processed. Where this is in place, it will facilitate compliance with GDPR.

Some of the changes that will be introduced by GDPR are advantageous to social care organisations and some will create additional obligations or administrative burden. A few examples are set out below, but the list is by no means exhaustive:

- Subject Access Requests (SAR) – requests from current and former employees, as well as people who need care and support, for sight of all data held about them are relatively common in the social care sector. GDPR removes the £10 fee payable to make a request and decreases the timescales for complying with a request from 42 days to 1 month. Removal of the £10 fee may result in an increase in the number of SARs placed, simply because an administrative obstacle has been removed. Organisations should ensure they have the appropriate policies and procedures in place to collate the relevant data and respond within the new timescales.
- Impact on Children – GDPR requires greater information to be provided to data subjects about the personal data that is being processed. This is particularly challenging if the data subject is a child, in which case it is particularly important to ensure the information is concise, clear and easy to understand. Social care organisations should consider whether it is appropriate to have separate template notices and policies for adults and for children.
- Processing of Personal Data – one of a number of grounds must be met for personal data to be processed by an organisation. "Processing" is widely defined in both the DPA and GDPR and includes simply holding or storing the data. At the point an organisation collects the data, it will be processing it, whether or not

Clarion
Expect More

it is doing anything actively with the data. Under the DPA, many social care organisations rely on the "legitimate business interest" ground. This is no longer an option for public authorities, although it may be possible to argue instead that the processing is necessary for the "performance of a task carried out in the public interest" or, in the case of private care, that the processing is necessary for performance of a contract.

- Data Processor Obligations – unlike the DPA which only places obligations on data controllers, the GDPR applies to both controllers and processors. In the majority of circumstances, social care organisations will be data controller of the personal data they process. The changes introduced by GDPR in this respect may result in data processors (including, for example, commissioning support units, IT and software providers) seeking more detailed data processing agreements to ensure their obligations are clearly defined. It is beneficial from an organisation's perspective to ensure the data processing agreements are clear and detailed so that responsibility and liability is appropriately shared between the parties. The more stringent requirements relating to the processing of special categories of data should also be considered. Helpfully, GDPR introduces express reference to the "provision of health or social care or treatment or the management of health or social care systems and services" as a reason for which special categories of data can be processed.
- Self-governance – data controllers must demonstrate compliance with GDPR by determining and adopting an appropriate and proportionate compliance programme. The programme should be evidenced in writing. This requirement sits alongside the obligations to notify the Information Commissioner's Office and affected data subjects of any breach of GDPR, unless such breach is unlikely to result in a risk for the data subject.
- Data Protection Officer (DPO) – many social care organisations will need to appoint a formal data protection officer (if they don't already have one) on the basis that they are conducting large scale processing of personal data. A formal DPO benefits from enhanced employment rights, but is also beneficial as a point of contact for the organisation in respect of GDPR including, for example, responding to subject access requests.

ICO Enforcement

Under the current legislation, the ICO may levy fines of up to £500,000.

Under GDPR, those fines will increase to a maximum of 20 million Euros or 4% or group worldwide turnover (whichever is greater).

Breaches that are deemed by the ICO to be less serious could incur fines of up to 10 million Euros or 2% of group worldwide turnover. Reputational impact could also be significant.

Next steps...

Social care sector organisations should already be in the process of considering the potential impact of GDPR on their policies, procedures and systems. Budget and resource will need to be allocated to GDPR compliance, bearing in mind that GDPR encourages each organisation to adopt what it considers an appropriate and proportionate response to GDPR compliance, and evidence that response in writing. NHS Digital has issued and updated guidance (available online) around record management and data retention which, where relevant, should be reviewed.

Addressing compliance with GDPR can seem daunting, but it doesn't need to be. Although it potentially requires a significant level of time and resource dedicated to it by the business, it is possible to break down GDPR compliance into bite size chunks on a risk analysis basis.

There is up to date guidance from the Information Commissioner's Office available online. Clarion also have a series of blogs which help to explain the impact of GDPR. If you would like any further information or have any questions about the changes that GDPR will introduce, please contact Clarion's Commercial, IT and Privacy team.

Matthew Hattersley
Partner
Commercial, IT and Privacy Team
matthew.hattersley@clarionsolicitors.com
+44 (0) 113 336 3351

Florence Maxwell
Associate
Commercial, IT and Privacy Team
florence.maxwell@clarionsolicitors.com
+44 (0) 113 336 3420

Clarion
Expect More