Preparing for the GDPR:

what nurseries and childcare providers can start doing now

Last issue we gave you a very brief overview on the changes being introduced by the General Data Protection Regulation (GDPR) and promised to give you further guidance.

We asked Philippa Doyle and Chris Hook from Hempsons Solicitors in Newcastle - a firm which specialises in charities and social enterprise, to put together a guide specific to our sector.

The General Data Protection Regulation (GDPR) will apply in the UK from 25 May 2018. Although it is not yet absolutely certain, exactly how the GDPR will be implemented in practice, some things are already clear. Nurseries and childcare providers are well advised to start taking preparatory steps so that they are ready in good time.

Introduction

The General Data Protection Regulation will apply in the UK from 25 May 2018 and will replace the current Data Protection Act 1998. The GDPR will have "direct effect", meaning that it will apply without the need for a specific new Act of Parliament. However, the UK has the option of "derogating" (i.e. adding to or amending) certain provisions of the GDPR. A new Data Protection Bill is currently making its way through Parliament but it is not anticipated that there will be any major changes that will impact on nurseries and childcare providers when it is finalised.

If your setting has already begun looking at what it needs to do, you may have seen that there are still a number of grey areas about how exactly the Government seeks to implement the GDPR in practice. Some of these issues were clarified by the Government's statement of intent[1] published on 7 August 2017. The Department for Digital, Culture, Media & Sport also published a collection of draft guidance documents[2] before introducing the Data Protection Bill in September 2017.

Although Parliament is still considering the final content of the Bill, there are various sensible preparatory steps which your setting can take so that it is ready in good time.

1 Ensure that the board or management committee knows that the law is changing in May

The members of the board or management committee are legally responsible for the management and control of the setting. It is primarily their responsibility to ensure that the setting does whatever it needs to in order to comply with the GDPR. The Information Commissioner's Office (ICO) has published an overview of the GDPR[3], which is a useful starting point.

The ICO has also published on its website various documents intended for specific sectors. The education sector guidance[4] is primarily intended for schools, colleges and universities, but some of it will also be relevant to nursery and childcare providers.

We recommend that nursery and childcare providers consider the ICO's emerging guidance and consider the following plan for ensuring compliance with the GDPR. Formal training may also be required.

2 Identify who will be responsible for reviewing procedures and policies

Currently, the setting will likely also employ someone whose job description includes key responsibilities under the Data Protection Act 1998. However, reviewing policies and procedures and implementing the changes required for the GDPR will likely be a significant task. For that reason, the board or management committee may decide to form a working group or sub-committee, to include manager(s) with an operation role in relation to data protection, to carry out the review and oversee implementation.

The GDPR will require certain organisations to appoint a designated Data Protection Officer to oversee compliance with the GDPR and advise the organisation at a senior level. If the setting falls within the definition of a "public authority" (to be defined) or carries on "large scale" (to be defined) processing of special categories of personal data, it will need to appoint a designated DPO. Pending further guidance from the ICO, the prevailing consensus is that most private and third sector settings will not be required to appoint a Data Protection Officer unless they are part of a large multi-setting provider.

In any event, your setting may find it desirable to appoint a Data Protection Officer or someone to carry out the equivalent responsibilities.

Is there someone suitable within the setting who has the expertise to perform this role? If not, it may be necessary to access training for an existing staff member or appoint someone additional.

If you missed them the first time round, the Welsh Council for Voluntary Action (WCVA) has a series of webinars available for anyone to watch on preparing your organisation for GDPR **#DesktopData.**

Visit: **http://bit.ly/2EtDlpu**

3 Carry out an audit of how your setting uses personal data

The GDPR is concerned with "personal data" and what is called "special categories of personal data" (which is more or less what is currently known as "sensitive personal data" under the Data Protection Act 1998). The GDPR does not affect other types of records or information held by the setting.

The setting should ask itself:

- **What types of personal data does it receive, hold, use or send?** The names and addresses of its children and their parents; the children's entitlement to the 30 hours' free childcare; their medical conditions and GP contact details; their religious beliefs and any dietary requirements; digital images of the children; and so on. The setting will also hold personal data about its staff.
- **Where does the setting get this personal data from?** Usually this will be from the child's parent or guardian, or from the staff member. An important question is: does the setting really need the information it holds? Has it ceased to be required?
- **How is the personal data held or stored?** Is it secure? If it is held electronically, does the setting have the relevant passwords and cyber-security software? If it is held in physical form, how is the personal data kept secure?
- **What does the setting use the personal data for?** The setting will use the children's information for the day-to-day provision of childcare. Much of the parent's information will often be used for the administration of the setting's childcare services e.g. the contractual and payment arrangements. Staff information will be used for HR, payroll and tax functions, for example.
- **Does the setting still need the personal data?** The setting should review its data retention policy to ensure that it ceases to hold the personal data of children, parents and staff after an appropriate period of time, and that such personal data is then safely disposed of. Remember that you willlikely have paper files and IT files.
- **Who does the setting disclose the personal information to?** For different types of personal data this may include staff, parents and other family members; health and social care professionals; HM Revenue & Customs; and so on.
- **How does the setting ensure that the personal data is not disclosed to the wrong person?** For example, if personal data is kept electronically, is access limited to those who need to see it? If it is transported outside the setting, is the laptop or USB-stick password-protected? If it is sent by email, is the email encrypted?

This exercise will assist the setting when it comes to updating its policies and procedures (see opposite). To do this effectively, the setting will also need to consider on what legal basis it holds and processes the personal data.

4 Review the setting's third-party data processing arrangements

Does the setting disclose personal data to a third party so that the third party can process the personal data on behalf of the setting? For example, does the setting have an external HR or payroll provider? If so, the setting will need to have a written data processing agreement containing various mandatory provisions required under the GDPR. The setting should speak with its providers and take legal advice to ensure that a compliant agreement is put in place in good time.

In addition, does your setting process personal data on behalf of another organisation e.g. a "Friends of X Nursery" group? If so, and the setting looks after personal data on behalf of the group, it may be necessary to have a written data processing agreement with the group.

5 Review and update the setting's policies and privacy notices

The setting's existing data protection policies and privacy notices are unlikely to comply with the GDPR in their current form. Having gone through the audit processes above, the setting should consider how its procedures and policies should be updated to ensure compliance. It may be necessary to obtain professional advice from data security professionals and/or specialist legal advice.

References:

1 http://bit.ly/2DHlkDe
2 http://bit.ly/2EiMocY
3 http://bit.ly/2BAtiMx
4 http://bit.ly/2nnmUD4

Philippa Doyle is an associate solicitor at www.hempsons.co.uk in Harrogate. She advises private, public and third sector organisations, particularly in the area of health and social care, on information governance, data protection and regulatory matters.

She can be contacted at **p.doyle@hempsons.co.uk** or **01423 724028.**

Chris Hook is an associate solicitor at www.hempsons.co.uk in Newcastle upon Tyne. He provides specialist legal advice to charities, social enterprises and educational institutions on a wide range of charity, commercial, regulatory and public law matters.

He can be contacted at **c.hook@hempsons.co.uk** or **0191 230 6052.**