The General Data Protection Regulation
Information for Providers

Introduction:

We have put together some information we hope will help you have a better understanding of how the General Data Protection Regulation (GDPR) will impact on settings.

Please note this does not constitute legal advice, so any changes to your current processes and forms should be reviewed with your legal team or advisors.

1. What is it?

GDPR stands for General Data Protection Regulation and comes into effect on 25th May 2018.

2. GDPR - Key Principles:

The right to be informed - Parents and staff need to be informed of what data you are collecting, what you are going to do with it and who it is shared with.

The right of access - Parents and staff can request access to their own data at any time. If requested, you must be able to provide all the information you hold on them.

Kent County Council
kent.gov.uk

The right to rectification - Personal data must be rectified if it is incorrect or incomplete.

The right to be forgotten - Individuals can request the deletion of their data where there is no compelling reason for its continued use. As a nursery there are certain guidelines on how long you should keep certain records for, and if this is requested you will need to seek advice from the Information Commissioner's Office and/or Ofsted.

The right to restrict processing - Parents and staff can object to the processing of their data. If this is requested, you cannot use the individual's information in reports, or for communications.

The right to object - Parents and staff can object to their data being used for certain activities like marketing or research. The objection must relate to their specific situation.

3. What is changing?

The existing Data Protection Act became law in 1998. The GDPR combines legislation from across the EU and will create one regulation that protects the data of everyone in Europe (Brexit will not have an impact on GDPR).

Whilst there are legal changes under the GDPR, if you have rigorous policies and processes in place currently under the Data Protection Act, then you are in a good position already, and should find it relatively straightforward to plan for, and demonstrate, GDPR compliance.

4. What do I need to do?

It is important to have a clear and detailed understanding of what information you hold in your setting, what it is used for, how it is stored, and who it is shared with.

You should consider both software systems and paper files. This mapping will help you identify any particular risks that need further follow-up.

The GDPR is only concerned with **Personally Identifiable Information.** This is anything that can be used to identify a specific person.

You should not only think about the data you hold on children and parents, but also your staff members and other contacts. Things like name, date of birth, bank details, and photos all count as personally identifiable information.

We have drafted a simple data mapping tool that might help you, please click **here** to view.

Also think about who in your setting has access to personally identifiable information and make sure they are aware that the rules are going to be changing.

Limiting the amount of people that can access this data will help reduce risk and make it easier to make sure the requirements are being followed.

You may or may not need to make changes to your current processes, but you need to understand your responsibilities over the data you hold on children, parents and staff members. You must be able to evidence that you are managing all the data you hold.

For example, but not exhaustive:

•Permission forms
•Parent / child documentation
•Privacy notices
•Confidentiality policy
•Complaints procedures
•Induction training
• Website and marketing information

All data processing must be appropriate. You must only record and process the data that you need to manage and maintain your setting.

It is worth thinking whether you are able to remove some of the personal information and leave only what is absolutely necessary to minimise risk.

5. Gaining Consent:

For providers, the best course of action is to ask parents to tick a box or sign a form (or both) to confirm they give their consent.

You may already use registration forms for new parents. If so you can include your privacy notice and include a tick box at the bottom. A signature or tick box (or both) is acceptable.

The new regulations also call for a 'concise, transparent, intelligible and easily accessible' Privacy Notice. It needs to be clear what data you are collecting, how you will use it, and who it will be shared with.

It is important to note to comply with the EYFS and Ofsted registered early years settings have to collect, process and store personal data.

The GDPR states that personal data should be 'Processed fairly and lawfully' and 'Collected for specified and legitimate purposes'. These legal obligations override the GDPR and therefore you do not need consent to collect certain data from your parents or children.

For example, child and parent details must be kept and recorded for two years. Accident reports must be kept for twenty one years and three months and staff records must be kept for seven years. It is still good practice to get agreement and consent.

6. Retention Schedules:

They should be reviewed to ensure they are up to date and fit for purpose and they are applied to your different sets of information?

Please click **here** to view the Information Management Toolkit for Early Years. Please note this document currently refers to statutory provisions within the 2014 EYFS and is being updated.

7. Privacy Management:

Under the GDPR privacy notices need to be clearer about the lawful basis for information sharing, and the reasons for holding information, and who you share it with and why.

The privacy notice is now on KELSI, please click **here** to view. There are other examples that can be located on the internet.

8. Contracts:

Suppliers may already be getting in touch with you about the GDPR. However, you need to collate a full list of contracts you manage and contact those suppliers to update the terms of the contract to reflect GDPR compliance, to receive and collate signed agreements to these changes, and to ask them for further details about how they can or will demonstrate GDPR compliance.

These responses can be used to identify any risky contracts from a GDPR perspective.

9. Information Security & Information Sharing Process:

As well as an overarching information governance and data protection policy, you will need to ensure you have clearly defined processes in place for how staff/committee members use personal data.

These should govern when information is taken away from the setting and where and how information is displayed, used and stored within the setting e.g. locked cabinets, wall displays of emergency contact or allergy information, and how technology can support data security e.g. do all staff have an encrypted memory stick, are your laptops encrypted?

You should have an information sharing log to record any information sharing that takes place outside of the main documented processes and agreements. This is important both for transparency purposes, but also in the event of any challenge around information sharing, it enables efficient follow-up.

You will need to update your procedures for dealing with a request for access to personal information (Subject Access Request (SAR) to reflect the changes under GDPR in respect of the timescale for compliance (now 1 month and no longer 40 calendar days) and the fact that you can no longer charge for a SAR (currently under DPA can charge £10) unless the request is manifestly unfounded or excessive.

At any point a parent can make a request relating to their data and you will need to provide a response (within 1 month). You can refuse a request if you have a lawful obligation to retain data (from Ofsted or a requirement of the EYFS) but must inform the individual of the reasons why you are refusing and have a clear process in place. This does not prevent individuals making a complaint.

It is unlikely that you will be faced with many of these requests, but it is important to understand these rights and have the ability to act on them if necessary.

10. What if there's a breach?

You must have procedures in place in case of a data breach. You must report a breach to the ICO within 72 hours of the incident.

It is good practice to also inform the individual whose data has been breached.

The ICO may want to investigate the breach, in which case you need to demonstrate that you have investigated how it happened and review your procedures to stop it happening again.

The ICO has the right to fine organisations that do not comply with GDPR an amount up to £20 million, or 4% of global turnover (whichever is greater).

11. Data Protection Lead:

Although not a requirement, it is a good idea to have a data protection lead. They are responsible for understanding the rules and ensuring you are compliant.

……and finally:

The changes can feel very scary and overwhelming. This is a good opportunity to review and update your current procedures and to see what information you hold. It is important to consider to only collect what you need and to use it for what it was intended.

For more information please click **here.**