SCMA BRIEFING SHEET

Preparing for GDPR: 8 Steps to Take Now

Scottish Childminding Association (SCMA) has developed this briefing sheet in response to the main questions we receive through our Helpline (01786 449063), open Monday to Friday, 10am-4pm.

SCMA's Vision Statement:
"Quality childminding...building confident children within a family childcare experience."

General Data Protection Regulation (GDPR) is a new EU directive that aims to make the Data Protection Act more robust and harmonise data privacy laws across Europe. The introduction of GDPR will protect everyone's personal data in a way that is transparent and measurable.

GDPR comes into force on 25 May 2018 and must be adhered to by all organisations – including SCMA and all individual childminding services themselves – that store and collect data.

We understand GDPR may seem daunting as there is a lot of information, and misinformation, out there. The guidance (below) from the Information Commissioner's Office (ICO) makes it relatable to childminders, and aims to help you identify the steps you need to take to make sure you are GDPR compliant.

For childminders already operating best practice when it comes to collecting, storing and handling data, the introduction of GDPR should not involve too many changes.

All childminders who store information about their minded children should be registered with the ICO. Previously only childminders who kept information on electronic devices had to register with the ICO; however due to the introduction of GDPR, all childminders are advised to register to ensure compliance.

SCMA has worked with the ICO Scotland Office to ensure information is available to support childminders in Scotland through the introduction of GDPR.

The Information Commissioner's Office (ICO) states:

"As a childminder you process and hold personal data on the children and families you care for and there are steps you will have to take to ensure your compliance with the new legislation. This includes registering with the Information Commissioner's Office (ICO), the regulator of data protection legislation, which can be completed online at **ico.org.uk**."

1. Know the law has changed. It's not just you who needs to be aware of GDPR and the steps you're taking to comply. Think about how you're going to inform parents and other clients of their rights and how you process both their own and their child's data.

This means you may need to explain that there is new data protection legislation in force which requires some changes in the information you have to provide them with. If they want to know more you can refer them to the ICO's website at **ico.org.uk**.

2. Ensure you have a record of the personal data you hold and why. Consider whether or not you need to hold it. A key principle of both the previous legislation and the GDPR is that you must only hold personal data necessary for the purpose you require it. Once you know what personal data you hold and why, make a record of it. There is guidance on the ICO website to assist you with this.

3. Identify why you have personal data and how you use it. The 'lawful basis' for processing personal data is the reason you are holding it, i.e. for childminders, you are providing a childminding service and under the terms of your registration with the Care Inspectorate you must hold relevant personal information.

4. Under the Data Protection Act there were a range of legal bases for processing personal data and these carry over into the GDPR. You need to know what your legal basis is, as this not only dictates what rights individuals can exercise, but it also needs to be in your data processing notice. The ICO has a self-assessment toolkit to help you identify your lawful basis for processing personal data.

In general, a privacy notice should tell people:

- who you are
- what you are going to do with their information
- who it will be shared with

These are the basics upon which all privacy notices should be built. However, they can also tell people more than this and should do so where you think that not telling people will make your processing of that information unfair. This could be the case if an individual is unlikely to know that you use their information for a particular purpose or where the personal data has been collected by observation or inference from an individual's behaviour.

5. Have a plan in case people ask about their rights regarding the personal information you hold about them. GDPR enhances individual's rights regarding their personal data, mainly making it easier to exercise their rights. Identifying your lawful basis for processing personal data (see Step 3) is important because while some rights can be exercised by everyone others are dependent on your lawful basis. The most commonly exercised right is the Right of Access, known as a Subject Access Request (SAR).

We all have the right to request a copy of our personal data from any business or organisation which is processing it. You can find guidance on SARs on the ICO's website, including a SAR Code of Practice.

6. Ask yourself. Before I collect data, do I clearly tell people why I need it and how I will use it? It was a requirement under the previous legislation to inform individuals how and why you were processing their personal data. This requirement continues under GDPR and requires you to have a data processing notice. The ICO Privacy Notices Code of Practice will help you to write one.

7. Check your security. After you identify where you store personal data, remember to identify how you will keep it safe and secure. GDPR is technology-neutral, therefore it applies to both paper and electronic records. It is important to ensure security, for example if you store your records in paper format, a locked cabinet will be required. If you store records electronically you need to take steps

such as ensuring your anti-virus software is regularly updated and there are user controls to only those that need to access your records can do so. You can find more information about keeping personal data secure on the ICO website at **ico.org.uk**.

8. Develop a process to make sure you know what to do if you breach data protection rules. A data breach is when something happens to personal data which shouldn't. It's not just data being stolen it's also data being lost or destroyed when it shouldn't be. Business owners are responsible for ensuring procedures are in place to both prevent and detect data breaches.

GDPR requires certain breaches to be reported to the ICO within 72 hours of becoming aware of the breach. The ICO website contains guidance on data protection breaches, including when you should report one.

"Don't panic! The ICO is here to help - while data protection legislation can seem daunting there is a wide range of guidance and tools available from the ICO including a section of our website dedicated to micro-businesses, such as childminders."

More Information

The ICO has also produced 'Getting Ready for the new UK Data Protection Law' which sets out eight practical steps for micro-business owners and sole traders, and this may also be useful for childminders.

Find out more about GDPR at **ico.org.uk**.

May 2018