Nottinghamshire County Council

EU General Data Protection Regulation (GDPR) - information for PVI providers in Nottinghamshire

GDPR

This document is intended to provide concise and helpful advice and is not a definitive statement of law. The Information Commissioner's Office website https://ico.org.uk/ contains detailed guidance on all of the matters outlined and will be kept up to date. This is particularly important in the context of the new data protection legislation as new case law and enforcement decisions may change the effect and application of the law.

On May 25th 2018 the Data Protection Act 1998 was replaced by the Data Protection Act 2018. The new Act is based on the EU General Data Protection regulation (GDPR), making changes to the way that organisations should process data. This is new legislation that applies equally across European countries. (In the light of Brexit the GDPR will still apply to UK organisations).

The new legislation ensures that businesses that process personal data do so responsibly. It also provides enhanced legal rights to the data subject (the living individual whom particular personal data is about)-to ensure that they are protected from the mishandling of their data.

Key definitions:

Personal data

Personal data are any data or combination of data that can be linked to an individual which enables them to be identified in some way.

For example, name and personal email address and/or any of the following: telephone numbers, bank account details, payment card details, postal address, marital status and date of birth.

Please note, a title in an email e.g. PersonnelDirector@) is not personal data. However, an email address such as jane.doe@ncc.gov.uk is considered personal data .

Special Category data

Special category data are those which the GDPR defines as more sensitive, requiring more protection and include;

- race;
- ethnic origin;
- politics;
- religion;
- trades union membership;
- genetics;
- biometrics (if used for ID purposes);
- health;
- sex life;
- sexual orientation.

Data Controller

A data controller determines the purposes and means of processing personal data.

Data Processor

The data processor is responsible for processing personal data on behalf of a data controller. There must be a contract between

the two with appropriate data protection provisions.

Data Subject

The data subject is the individual whom particular personal data is about.

Privacy Notice

It is important to be transparent and provide accessible information to individuals about how you will use their personal data. This is a key element of the EU General Data Protection Regulation (GDPR). The most common way to provide this information is in a privacy notice.

What needs to be included in a privacy notice?

- The name of your organisation
- Contact details for the Data Protection Officer.
- The purposes of processing
- Lawful basis for processing
- Who will you share it with
- Details of transfers to third countries or international organisations (if applicable)
- How long data will be kept and what you will do with it after this time
- Rights available to individuals in respect of the processing.
- The right to withdraw consent (if applicable).
- The right to lodge a complaint with a supervisory authority.
- The source of the personal data (if the personal data is not obtained from the individual it relates to).
- The details of whether individuals are under a statutory or contractual obligation to provide the personal data (if applicable, and if the personal data is collected from the individual it relates to).
- The details of the existence of automated decision-making, including profiling (if applicable).

Personal data breach

A breach is when personalised data has been subject to accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed.

What are the lawful bases for processing data?

- Consent
- Contract to which the data subject is party
- Legal obligation
- Vital interests
- Public task
- Legitimate interests

Special category data require additional conditions for processing such as:

- Explicit consent
- Employment, Social Security, Social Protection law
- Vital interests
- Not-for-profit body
- Made public by the data subject
- Legal claims/judicial
- Substantial public interest
- Medicine/Employee capacity, medical diagnosis, health or social care where the processing is carried out under the responsibility of a health professional or a social work professional or another person who in the circumstances owes a duty of confidentiality.

Data Retention Periods

Personal data (bank account, email, and phone numbers) should be destroyed when a child leaves your setting – you no longer have a lawful use for this data

SEND pupil files/ case files should be destroyed at the end of the academic year that the child reaches 25.

Child protection purposes. Records of children who attended your setting, accident and incident records need to be retained until the child reaches the age of 21 or until reaches the age of 24 for child protection records.

Providers are recommended to securely retain 'Parent Declaration Forms' and all other supporting forms. .Forms and evidence should then be destroyed as confidential waste after the period of 6 years after funding period has ended.

It is important to remember that if you have any concerns about a child that come under the child protection, GDPR is not a barrier for sharing information. The safety and welfare of the child always come first.

Records relating to others (employees, volunteers, etc) will have different retention periods.

All documents should be retained securely.

What do settings need to do?

- Give clear notification of each purpose for which they may use data. The GDPR puts more emphasis on making sure that the data subject understands exactly how an organisation will be using their data. This is usually done through a privacy notice.
- Explain the legal basis for processing the data
- Explain data retention periods
- Make people aware who the data protection officer is (if you have one) and that they have the right to complain to the Information Commissioner (ICO) if they think there is a problem with the way the organisation is handling their data.
- GDPR requires information to be provided in concise, easy to understand and clear language.
- Clearly notify the data subject of any other organisations with whom they may need to share their data to deliver the service
- Obtain explicit consent to be able to process user data. Explicit consent is defined as the data subject having to take a positive action such as signing, ticking a box or pressing a submit button with a clear and fair processing statement to acknowledge that they understand and consent to the purposes for which an organisation want to process their data. You must be able demonstrate that consent was given.
- **Consent for the data of children.** If processing the personal data of children the consent must be given by whoever holds parental responsibility for the child. . You will need to be able to evidence your reasonable efforts to verify the consent.
- **It is important that a record of consent is kept clearly stating what the data subject agreed to and what they were told that their data would be used for**
- Allow data subjects to be forgotten. The rights of the data subject are strengthened under GDPR. Individuals have a right to have their personal data erased if there is no legitimate ground for retaining the data; the right to be forgotten requires the setting to delete all traces of the data subject from all systems. This will mean settings will have to assess and amend procedures to ensure they have a clear steps for securely deleting personal data beyond recovery.
- Subject access requests – anyone who has provided data has the right to know what information is being held about them. The GDPR has removed the fee which was in place under the Data Protection Act 1998 for this process. Data controllers will only have one month to respond to a request, which can be extended by a further two months for particularly complex requests.
- The powers of the ICO are being increased significantly. Currently the most the ICO can fine a company for breach is £500,000. Under the GDPR this rises to 20 million euros or 4% of global turnover, whichever is greatest.
- The ICO will require data controllers to report many more breaches than they

are obliged to do at the moment. Organisations will need to maintain a breach register where all breaches are recorded and monitored no matter how trivial. For SERIOUS data breaches, where the breach is likely to result in a 'risk to the rights and freedoms of individuals', the breach must be reported within 72 hours of the organisation becoming aware. Where this is HIGH risk to the rights and freedoms of individuals as a result of the breach the data subjects (person) must be notified of the breach without undue delay

- Currently organisations that process personal data are required to notify the ICO as data controllers. This involves explaining what personal data they collect and what they do with it. They are required to pay the ICO a **notification fee** and this is used to fund most of the ICO's work. When GDPR comes into effect in May 2018 there will no longer be a requirement to notify the ICO in the same way. However, there will be a legal requirement for data controllers to pay the ICO a **data protection fee.** These fees will be used to fund the ICO's data protection work.

Practical Steps

- Ensure that you are registered with the ICO.
- Determine if you need to appoint a Data Protection Officer.
- Audit what information is held. Start by documenting what personal data you hold or collect for any individual, where it came from, what you use it for, who you share it with and how long you need to keep it for. This will include parents, children, staff, volunteers, committee members and other outside providers.
- You should identify the lawful basis for processing information in the GDPR, document it and update your privacy notice to explain it.
- Record what you do with each type of data - this will clarify a set of processes that all staff will need to follow.
- Settings should review their current terms and conditions, privacy and consent notices ensuring that they are written in concise, easy to understand and clear language. Ensure that these explain to your customers what you do with the data they provide.
- Review how you are seeking, obtaining and recording consent. Consent must be given freely, it must be specific and the person giving consent must be clearly informed of how their personal data will be used. It is important that a record of consent is kept listing what the individual agreed to and what they were told the data would be used for.
- Ensure that you clearly notify individuals of any other organisations with whom you may need to share their data with to deliver the service e.g. a third party website. suppliers (again ensure that any external organisations that have access to your data are complying with GDPR and record this).
- Make sure that you have the right procedures in place to detect, report and investigate a personal data breach. The data protection officer will be responsible for maintaining a breach register and liaising with the ICO regarding serious data breaches.
- Settings need to ensure that all staff are made aware of and understand that individuals have the right to access their data records and can have these amended or deleted if requested. This is a good time to ensure you have documented procedures in place to respond if someone asks to have their personal data amended/deleted.
- Ensure that there is a cookies notice on your website which asks for consent for holding and using their data online.
- Ensure you have a privacy notice in place.

Useful linkshttps://ico.org.uk/for-organisations/data-protection-act-2018/

https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf

For Data protection queries please contact https://ico.org.uk/global/contact-us/helpline/

If you are a member of a professional body they will be able to provide you with further information

https://www.ndna.org.uk

https://www.pacey.org.uk/

https://www.pre-school.org.uk/

General Contact information:

Early Childhood Services

Phone: 0115 9772510

Monday to Friday: 9am to 5pm

Email: earlychildhoodservices@nottscc.gov.uk
Website: www.nottinghamshire.gov.uk