Irish National Teachers' Organisation
Cumann Múinteoirí Éireann
150

General data protection regulation

INTO question and answer guide

"Everyone has the right to the protection of personal data" – European Commission
The General Data Protection Regulation (GDPR) came into force from 25 May 2018. The new law, which seeks to make the EU 'fit for the digital age', governs how we all must collect and process the personal information we hold. The INTO's legal team provides you with this timely update as you return to school.

1 What is GDPR?

General Data Protection Regulation (GDPR) is an EU-wide piece of legislation which forms part of the data protection regime in the UK together with the new Data Protection Act 2018 (DPA2018). The main provisions apply from 25th May 2018.

GDPR enhances the individual's data privacy and data rights and builds on the obligations and responsibilities of data controllers.

Prior to the commencement of GDPR, EU Member States had the opportunity to legislate for GPDR at a national level. GDPR is the law and supercedes any national legislation.

2 When did GDPR commence?

GDPR commenced across EU Member States, including Northern Ireland, on 25 May 2018. Since that date, GDPR is the law in all EU Member States.

3 Who does GDPR affect?

GDPR affects all data subjects. An individual under GDPR is known as the 'data subject'; that is, they are the subject of the data collected about them by the organisation. In schools, a data subject is a pupil; a parent/guardian; a teacher; a school secretary; any employee of the school. All data subjects had certain rights protected under the previous data protection legislation. GDPR enhances and builds on these rights.

4 What are GDPR principles?

Schools shall be responsible for, and must be able to, demonstrate compliance with GDPR principles. The principles are:

- Fair, transparent and lawful processing: the data subject should know the type of data collected and the reason the school collects that data.
- Purpose limitation: schools should only collect data for a specific purpose and keep only for as long as necessary.
- Minimisation of processing: schools must only process data that is needed to achieve its processing purpose.
- Data accuracy: schools must take every reasonable step to ensure the data they process is accurate and complete.
- Storage limitation: schools should hold data in a form that identifies a data subject for as short a time as possible.
- Integrity and confidentiality: schools must process data securely to safeguard against unauthorised/ unlawful processing, accidental loss, destruction or damage.

5 What are data subject rights?

Data protection legislation/GDPR, sets out the rights of data subjects including:

- The right of access:
  – *Accessing one's own data can be done via a Subject Access Request (SAR). This means that a data subject can request a copy of all his/her data (or their own child) free of charge and this must be provided within 30 calendar days.*
- The right to rectification:
  – *This right means that a data subject can ask the data controller to rectify the data the controller holds e.g. if a data subject's phone number changes.*
- The right to be forgotten/right to erasure:
  – *This means that a data subject can apply to a data controller to erase all the data which the controller holds on that data subject. This is not an absolute right and is qualified in certain circumstances e.g. where data is being held for a statutory purpose or in line with legislation, for example, the register..*
- The right to restrict processing:
  – *This means that, in certain circumstances, a data subject can apply to a data controller to restrict the processing of his/her data.*
- The right to data portability:
  – *Data portability, in simple terms, means that a data subject can apply to have all of his/her data held with one data*

controller copied and passed to a new data controller.

- The right to object to certain processing:
  – *Save for compelling legitimate reasons, this right means that a data subject can object to the processing of his/her data based on his/her particular situation or state of mind.*

6 What is personal data?

Personal data is any information relating to an identified or identifiable living person ('data subject'). An identifiable living person is one who can be identified, directly or indirectly, e.g. by reference to a name, an identification number, location, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that living person/data subject.

7 What are special categories of personal data?

Special categories of personal data have additional legal responsibilities, which you should discuss with the board of governors, and they include:

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

8 Why do we collect data? Are we entitled to collect data?

Yes, schools are entitled to collect personal data about pupils through the enrolment process and/or through expressions of interest in relation to enrolment. This is legitimate for the purposes of providing education services to pupils. Additional information may be collected from third parties, including former schools and through school activities and interaction(s) during the course of the pupil's time at school.

Schools also collect personal data about parents and guardians through the enrolment process or expressions of interest for enrolment. Additional personal data may be collected through interactions during the course of the pupil's time at school.

In addition, schools are also places of employment and so personal data is collected by the school in relation to all employees, including teachers, prior to and during the course of their employment at the school.

> Schools are entitled to collect personal data about pupils through the enrolment process and/or through expressions of interest in relation to enrolment

9 What is data processing?

Processing is the legal term used to describe various acts including the collection, recording, organisation, structuring, storage, alteration, use of, retrieval, disclosure or transmission of information/data.

10 What are processing grounds?

A processing ground is the legal reason for which data is collected, processed and retained – in other words, the legal reason why we are allowed to collect, process and retain certain data. Schools collect and process personal data about teachers, other employees, volunteers, pupils, parents/guardians for a variety of legitimate purposes and are entitled to rely on a number of legal grounds to do so. Schools require this data to perform the duties and responsibilities of the school and to comply with legal and statutory obligations.

In addition, schools require this personal data to pursue the legitimate interests of the school and any dealings it may have with relevant third parties, for example, the Department of Education. The legitimate interests upon which schools rely are the effective operation and management of the school, managing the education and welfare needs of pupils; the employment of teachers and other members of staff; the management of volunteers and other approved school-related matters. Schools, generally but not exclusively, process personal data on the basis of the following lawful purposes:

a. Legal obligation
Schools process personal data to comply with legal and statutory obligations.

b. Legitimate interests
Schools may also process personal data in order to:

- enable pupils to develop to their full potential and meet the educational, social, physical and emotional requirements;
- employ members of staff;
- enable parents/guardians to be contacted in the case of emergency, school closures;
- inform parents/guardians of their child's educational progress;
- secure and benefit from the support and services of relevant third parties.

Further information about the lawful processing conditions of personal data is contained in Article 6 of GDPR.

11 What is consent?

The processing of some pupils' personal data requires consent. For example, the school needs to be sure that parents have consented to allowing photographs of their child to be taken by the school, which may be displayed on the school's website or on social media platforms or in the print media. Consent can be withdrawn at any time by contacting the school.
Please note: consent regarding data under GDPR is different to consent received from parents for the purposes of allowing their child attend, for example, a school trip/tour. That type of consent must still be sought in the usual way by the school, in line with advice from the school patron and/or insurer(s).

12 What is a data controller?

A data controller determines what data the organisation/school needs to collected, how it will be stored and for how long. The data controller in schools is the board of governors.
Data controllers are required to store data which they process confidentially and securely. If a security or data breach arises, a data controller, by law, must report the breach to the Information Commissioner within 72 hours. This is not optional, but a legal requirement.

In schools, it is advisable to create a culture of awareness and support about GDPR and data privacy

In schools, it is advisable to create a culture of awareness and support about GDPR and data privacy. It is vital that all colleagues feel that they can immediately report to the principal/management if they are concerned that they may have inadvertently caused a data breach at the earliest opportunity. The concern can then be reported to the Information Commissioner.
GDPR compliance at school involves looking at – or auditing – the data that is collected in the school. In other words, what data is collected by the school, how and why it is collected, retained, updated, stored, and/or accessed in respect of pupils, employees and third parties.
It is vital to foster a conversation about data privacy awareness among staff. Whilst there is an onus on the board of governors as data controller, there is an onus on all individuals who handle the data of others to be prudent in that regard. Having a discussion about the types of data processed in the school and the importance of reporting any breach in a prompt manner in a supportive culture is advised. This may involve a discussion amongst staff around the need to make some changes in how the school processes (collects, retains, stores and interacts with) the data collected.

13 What is a data processor?

A data processor processes data on behalf of the data controller, for example, a service provider to the data controller, i.e. the board of governors. A good example of a data processor for schools would be a third party service provider of IT services.
It is important to ensure that within the agreement or contract a school has in place between the data controller (board of governors) and a third party service provider that the following is clarified:

a. The personal data are processed only on documented instructions from the controller, including with regard to transfers of personal data to a third country or an international organisation.
b. The confidentiality and security of the data being processed is ensured by the third party service provider.
c. The third party service provider gives an undertaking to the data controller that they respect and are compliant with the data subjects' rights.
d. The third party service provider can engage subcontractors with the data controller's approval.
e. Where necessary/appropriate, that the third party service provider will delete or return the data to the data controller at the end of the provision of services arrangement unless European Union or Member State law requires the continued storage of that data.
f. The processor makes available to the controller all information necessary to demonstrate compliance with the obligations under European Union or Member State law.

Regarding the engagement of third party data processors/service providers by a board of governors, members are advised to continue to consult with their relevant management bodies for advice.

14 What is data retention?

Data retention means holding on to data relating to a data subject. A school should only retain personal data for as long as it is necessary to fulfil the purposes the information was collected for, including any legal, accounting or reporting requirements. Some data is required to be retained indefinitely, because of legal requirements, e.g. the register data. The retention period(s) of other types of data collected by the school is a matter for each individual board of governors to decide.
Members are advised to continue to consult with their relevant management bodies and school insurers for advice in this regard.

15 Does my school need a Data Protection Policy?

Yes, all organisations that process data require a data protection policy. If your school already has a data protection

A school should only retain personal data for as long as it is necessary to fulfil the purposes the information was collected for

policy, that's great. However, you should check to make sure that the legislation referred to in the policy is GDPR and the Data Protection Act 2018, and not the previous legislation. If GDPR and the Data Protection Act 2018 is not reflected in your school Data Protection Policy, the policy will need to be reviewed. It is anticipated that most schools will need to update their Data Protection Policy and, in this regard, please refer to the INTO website where further advice and resources are available.

Some key elements of your school's Data Protection Policy should include:

- The purpose of the policy.
- The data controller's commitment to data protection principles/rights under GDPR and the Data Protection Act, 2018.
- The name of the data controller (i.e. the BOG).
- The lawful basis of the processing of data.
- Details of when consent is required and that it can be withdrawn.
- The categories/types of pupil data collected, processed, retained, shared by the school.
- The categories/types of BOG data processed, retained, shared by the school.
- Data security measures taken.
- CCTV, including purpose and use of CCTV data in the school.
- Rights of data subjects and how to access them.
- Contact details for the Data Protection Commission.
- All other policies which may interlink: e.g. Child Protection Policy; Anti-Bullying Policy; Code of Behaviour/ Discipline; CCTV Policy; ICT Policy; Acceptable Use Policy etc.

16 What is a Subject Access Request?

A Subject Access Request (or SAR) is exactly the same as a Data Access Request, in that a data subject can apply to a data controller to be given a copy of any information on record relating to the data subject, which is kept on computer or in a structured manual filing system operated by the data controller.

In schools, teachers can make a SAR to the data controller, board of governers as their employer, in relation to their own data only. Parents/guardians can make a SAR to the data controller, board of management, on behalf of their own child.

Under GDPR, a SAR can be done by writing to the data controller/board of government requesting copy of the personal data held in relation to the data subject. A SAR must be complied with within 30 calendar days, whether it arises during a school closure or not. Failure to comply within this timeframe may be reported to the Information Commissioner. Crucially, GDPR provides that copy of the data is provided to the data subject free of charge.

17 Does my school use CCTV?

If your school uses CCTV, data subjects should be informed through visible and clearly legible notices inside and outside the school. While it is a good idea to have a CCTV policy, at the very least, use of CCTV in the school must be noted within the school Data Protection Policy. In addition, please note that it is advisable to specify the basis – or purpose for the use of CCTV. Is it for security purposes only? Is it for health and safety purposes also? Whatever the purpose, it must be specified in your policy.

Please note that if CCTV is used for health and safety purposes – i.e. for investigations into bullying etc, data subjects would be entitled to seek a copy of a recording should they wish to. Should any SAR be made in relation to CCTV, please note that, before release, the recording must be redacted/pixelated so that the only visible person is the relevant data subject. Pixilation is a process which may incur fees, so it is a good idea to have a discussion about this with the board of management. In addition, it is a good idea to note the duration period of a CCTV recording in the school policy – i.e. whether it lasts for 25/28/30 days etc., before restarting.

18 What is a website privacy notice?

If your school website collects, processes and retains personal data, you need a privacy policy that informs users about this. The purpose of the privacy notice is to inform the users of your website about how their data is collected, processed and retained (if it is retained). This will differ from school to school, depending on the nature and construction of the school website. Schools can verify with the relevant service provider whether the school website collects, processes and retains personal data.

19 What is a data breach?

A data breach is where, accidentally, inadvertently or unlawfully, personal data are destroyed, lost, disclosed or accessed, transmitted, stored or otherwise processed. Schools, as data controllers, are required to store data which they process confidentially and securely. If a data breach does happen or you have concern that it may have happened, you must report your concern to your principal/the board of governors immediately. The relevant data subject must also be informed. The reason for the immediate requirement of reporting is that the data controller, by law, must report the breach to the Information Commissioner within 72 hours. This timeframe is not optional, but a legal requirement.

20 What is a joint controller?

Where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers.

Contact information Information: Commissioner's Office
14 Cromac Place
Belfast
BT7 2JB
Tel: 028 9027 8757
or 0303 123 1114
Email: ni@ico.org.uk

If GDPR and the Data Protection Act 2018 is not reflected in your school Data Protection Policy, the policy will need to be reviewed.

21 Do schools require a Data Protection Officer (DPO)?

Currently, schools are not required to appoint a DPO. EA is prepared to assume the specific role of Data Protection Officer (DPO) for all schools in Northern Ireland with the principal in each school as the key point of contact. The creation of a DPO role creates specific legal obligations on the Data Controller, including the provision of relevant training and specific resources. In this regard, it is advised that schools do not create a DPO role, unless further directed.

22 Fines, data breaches, liability and compensation

Under GDPR, fines for data breaches can be imposed by the Information Commissioner. In certain circumstances, where a data subject's rights have been breached, a data subject can seek to claim compensation. Such circumstances will be context/case specific. For the most part, the spirit of the legislation suggests that large fines will only be applied to large companies and corporations.

23 INTO supports/ resources/templates

- The INTO released a Data Privacy Statement for schools on 25 May, 2018 – 'GDPR Day'. This Data Privacy Statement is an amendable Word document which sets out the various key considerations for the collection of pupil data in schools www.into.ie/ROI/NewsEvents/LatestNews **NB:** All template documents must be approved by the school board of governors prior to use/circulation.
- In Northern Ireland the Education Authority have resources and templates on their website.
- www.eani.org.uk
- www.eani.org.uk/about-us/ea-think-data-online-resource-hub/
- Information Commissioner's Office also have available information on GDPR on their website. www.ico.org.uk

24 Can I contact the INTO if I have a further query about any of these matters?

Of course, members are most welcome to raise any further queries with the INTO by telephone or email.
Tel: 02890381455
Email: infoni@into.ie and ensure you include your INTO membership number or teacher number in any correspondence.

The INTO has taken every care to ensure the accuracy of the content of this guide. However, it not intended as exhaustive information or legal advice. It is important for each school's board of governors to ratify its own policy and procedure in line with GDPR, taking any advice as required.

Summary Points for Schools

1

GDPR affects all data subjects. An individual under GDPR is known as the 'data subject'; that is, they are the subject of the data collected about them by the organisation. In schools, a data subject is a pupil; a parent/guardian; a teacher; a school secretary – any employee of the school.

2

Under data protection legislation/GDPR, when an individual gives their data to an organisation or a body, there is a legal obligation on that organisation or individual to keep that data safe, secure and private/confidential, in line with the data subject's rights.

3

Schools collect and process personal data about teachers, other employees, volunteers, pupils, parents/guardians for a variety of legitimate purposes and are entitled to rely on a number of legal grounds to do so. Schools require this data to perform the duties and responsibilities of the school and to comply with legal and statutory obligations.

4

Schools are entitled to collect personal information about pupils through the enrolment process and/or through expressions of interest in relation to enrolment. This is legitimate for the purposes of providing education services to pupils.

5

Personal data is any information relating to an identified or identifiable living person ('data subject'). An identifiable natural person is one who can be identified, directly or indirectly.

6

Schools are also places of employment and so personal data is collected by the school in relation to all employees, including teachers, prior to and during the course of, their employment at the school.

7

Processing is the legal term used to describe various acts including – the collection, recording, organisation, structuring, storage, alteration, use of, retrieval, disclosure or transmission of information/data.

8

The legitimate interests upon which schools rely are the effective operation and management of the school, managing the education and welfare needs of pupils; the employment of teachers and other members of staff; the management of volunteers and other approved school-related matters.

9

It is vital to foster a conversation about data privacy awareness among staff. Whilst there is an onus on the board of governors as data controller, there is an onus on all individuals who handle the data of others to be prudent in that regard.

10

The processing of some pupils' personal data requires consent. For example, the school needs to be sure that parents have consented to allowing photographs of their child to be taken by the school, which may be displayed on the school's website or on social media platforms or in the print media. Consent can be withdrawn at any time by contacting the school.

11

A data controller determines what data the organisation/school needs to collect, why that data is needed, how it will be collected, how it will be stored and for how long. The data controller in schools is the board of governors.

12

In schools, it is advisable to create a culture of awareness and support about GDPR and data privacy. It is vital that all colleagues feel that they can immediately report to the principal/management if they are concerned that they may have inadvertently caused a data breach at the earliest opportunity. The concern can then be reported to the Information Commissioner.

GDPR

13

If a security or data breach arises, a data controller, by law, must report the breach to the Information Commissioner within 72 hours. This is not optional, but a legal requirement.

14

Schools should review the types of data collected, processed and stored by your school as this will inform its Data Protection Policy. The school can identify, perhaps as a whole staff exercise, the types of data collected and processed by the school by completing the Information Asset Register (IAR).

15

If GDPR and the Data Protection Act 2018 is not reflected in your school Data Protection Policy, the policy will need to be reviewed. It is anticipated that most schools will need to update their Data Protection Policy and, in this regard, please refer to the EA website where further advice and resources are available.

16

A Subject Access Request (or SAR) is exactly the same as a Data Access Request, in that a data subject can apply to a data controller to be given a copy of any information on record relating to the data subject, which is kept on computer or in a structured manual filing system operated by the data controller.

17

A SAR must be complied with within 30 calendar days, whether it arises during a school closure or not.

18

A school should only retain personal information for as long as it is necessary to fulfil the purposes for which the information was collected. Some data is required to be retained indefinitely, because of legal requirements e.g. the register. The retention period(s) of other types of data collected by the school, is a matter for each individual board of governors to decide.

19

If your school uses CCTV it is a good idea to have a CCTV policy. Data subjects should be informed of the use of CCTV through legible notices.

20

If your school website collects, processes and retains personal data, you need a privacy policy that informs users about this.

21

Currently, schools are not required to appoint a DPO.

22

INTO members are most welcome to raise any further queries with INTO by telephone or email.

Tel: 02890381455

Email: infoni@into.ie

and ensure you include your INTO membership number or teacher number in any correspondence.

into
Irish National Teachers' Organisation
Cumann Múinteoirí Éireann
150

GDPR checklist for schools

- Has your school a Data Protection Policy?
- Is the school's Data Protection Policy in line with GDPR?
- Has the school reviewed your school's practice in processing data?
- What type of data does your school collect?
- Why is the school holding data?
- How did the school obtain it?
- For what purpose did the school originally gather data?
- Does the school check data for accuracy?
- How long will the data be retained by the school?
- How secure are the data?
- Does the school ever share data with third parties?
- What is the basis for the school sharing data?
- Is there a clear procedure to follow in the event of a data breach?
- Is there a clear procedure for responding to Subject Access Requests?
- Is there a process for data subjects to invoke other GDPR rights?
- What steps has the school taken to familiarise staff with GDPR principles and its Data Protection Policy?
- Where is your school's Data Protection Policy displayed or available?