GDPR for **Schools**

How GDPR affects the education sector—including checklist and toolkit

This information is meant for educational purposes only and should not be used as or considered a substitute for legal advice. Make sure to seek appropriate counsel for any specific situation

GO2 Consulting Services Ltd
Your reliable, trusted and confidential adviser

Includes:

- How GDPR is affecting the education sector
- The main GDPR challenges for schools
- How to reach compliance —checklist and toolkit

GDPR FOR SCHOOLS

The General Data Protection Regulation, GDPR, came into effect on 25 May 2018. It further protects personal information and strengthens individuals' rights. The regulation also puts more responsibility on organisations, which is why some schools might have to step up their compliance game.

Today, personal data is often treated as a currency, showing how valuable it is to companies and organisations. Yet, individual's rights should always be the number one priority. If you handle data in compliance with the GDPR, you can have a thriving school where students and staff know their data is put to good use, whilst you maintain their privacy.

However, a survey from 2018 showed only 20% of companies believe they are GDPR compliant.* The education sector is vast – the value of the education market in 2015 was calculated to $4.9 trillion globally. Compliance in this sector is vital.

How GDPR is affecting the education sector

The education sector holds and handles a large amount of personal information. The data is often complex and divided into different groups: basic information such as name, contact information and photo identification, and details on grades and medical information. Schools also hold information on their staff, job applicants and other people that might be associated with the school, such as volunteers. It's important to remember that personal data includes both digital and paper-based information.

There is also a type of personal data that the GDPR calls special categories of personal data. It holds information about racial or ethnic origin, religious beliefs, political opinions, biometric data and trade union membership. This data category contains extremely sensitive information, of which the processing is regulated even stricter than for regular personal data. It needs to be correctly protected in order for the data to not fall into the wrong hands.

Since the information they hold is sensitive, it might be very valuable in the wrong hands. Therefore, schools can be targets for security breaches. That makes privacy measures of the utmost importance. Data protection needs to be a part of day-to-day operations, particularly for the senior leadership who decide on new technology and policies. Having a detailed protocol for data processing helps ensure that your data won't be subject to a security breach, whether the leak is caused by an honest mistake or an outside threat.

On a positive note, the trust for public sector is far greater than for commercial counterparts.** Trust has also increased in 2018, and GDPR has likely played a part in that. This means that schools and universities already have a strong starting position. However, there is every reason to further increase trust and work on compliance.

The biggest GDPR challenges for schools

Working with data privacy within the education sector has its challenges. It is vital that you meet the demands of the regulation in order to protect individual's rights, while using data in an effective and responsible manner.

GDPR KNOWLEDGE AND TRAINING

One of the biggest challenges of data privacy in schools it that a variety of staff need to act under the GDPR - the governor, school nurse and teachers, to name a few. Not everyone might possess the right training to do so. Having a well-informed Data Protection Officer can only help so much if the rest of staff – who are the ones that handle the data on a day-to-day basis – lack knowledge on risks and proper data management and recording.

COMPLEX DATA MANAGEMENT

Schools handle large amounts of data, and different roles need to have different data. The school nurse will need a student's medical information, whereas a teacher needs an overview of the student's grades and test results. GDPR means that schools will have to introduce new record keeping that at a first glance might seem like a lot of extra work.

TRANSPARENCY AND TRUST

Not only are schools expected to be compliant, they are also expected to prove that they are. To keep the records and communication transparent means that data processes should adhere to the regulation, but also be easily understood. Both data subjects and the authorities can demand to see what data schools hold and how they manage your data processes. This means that you might have to produce an overview of the information that you have of a certain student, and that this information should be clear and transparent. To prove compliance to authorities, your reports should also be transparent and easy to understand.

According to the 2018 ICO survey, only 18% have a good understanding of how their personal information is used by organisations. Lack of understanding makes it hard for people to trust their data is not mishandled. Communication with your data subjects is crucial.

Compliance for schools

Schools may be faced with fines of up to 20 million euros or 4% of their annual turnover, whichever is greater, if they don't comply with the GDPR. The sum depends on the severity of the violation against the regulation. Also, your reputation might suffer from a security breach or lacking GDPR efforts. Your students should be able to trust you with their personal information, and the incentive has never been bigger.

In order for you to be compliant with the regulation, you need to:

TRAIN AND EDUCATE YOUR STAFF

Your staff needs to understand what the regulation is and what it does. Make sure they understand why your data processes should be managed and registered in a certain way, and why you cannot hold on to the information forever and without just cause. They need to know what a data breach is, and what might cause it.

DELEGATE RESPONSIBILITY TO THE RIGHT PEOPLE

Having someone within the senior leadership team who is responsible for GDPR compliance is vital. Under GDPR, you need to appoint a Data Protection Officer (DPO) if you process or store large amounts of personal information. A DPO is responsible for your data protection strategy to ensure compliance, meaning that this role can make or break your GDPR work. You can have an external DPO, but make sure they know enough about your school to be able to make the correct assessments regarding your compliance

LOOK OVER YOUR THIRD PARTY RELATIONSHIPS

The regulation defines two types of businesses: the controller and the processor. The controller is “the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data”. That means that the school as a whole is the controller. The processor is “a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller”. This can be an external third party. You need to have processing agreements that state that data should be handled in accordance with the regulation.

ESTABLISH THE CORRECT PROCESSING ACTIVITIES

Having the correct activities in place is crucial for your compliance. Article 30 of GDPR states that “each controller and, where applicable, the controller’s representative, shall maintain a record of processing activities under its responsibility”. This is called Records of Processing activities (RoPa). As a controller, you need to make sure that you have records that contain the purposes of processing, a description of the categories of data subjects and personal data, a description of technical and organisational security measures and the categories of recipients that the personal data has or will be disclosed to.

How can GO2 Consulting Services help you?

From data mapping to reporting to the authorities and communicating with students and staff – we understand that GDPR is demanding a great deal of work from you. Privacy professionals who are responsible for their organisations' compliance have a lot on their plate.

Managing your data processing in a digital tool that gathers everything in one place makes your GDPR work manageable and productive. We can save you time and minimise risk by asking the right questions, so you avoid pitfalls and achieve more transparency.

GO2 Consulting Services was formed to help organisations comply with GDPR and protect personal privacy. It was formed by a knowledgeable and experienced DPO, specifically for schools. We believe strongly in building deep understanding of your challenges whilst maintaining the human touch—rather than reliance on a software package. As we already work with a number of schools and other organisations we can not only tailor our offering to your unique situation but we can also share with you experiences of others and also our numerous specialist contacts for complimentary offerings.

Having everything in one place makes it easier to co-operate, and you can see who is responsible for doing what. We can also extract reports to show management and authorities. The investment in time and money when implementing us as your DPO is low. We want you to be in a position to concentrate on providing your children with education rather than having to learn new skills and committing your already stretched, precious resources.

Checklist and toolkit

You need to develop a culture where you have GDPR top of mind and your processes and documentation in compliance with the regulation. But where do you start? This checklist is an overview of the initial project and the following day-to-day work, so you can take those first steps. Before you know it, you will be up and running.

1 EDUCATE YOURSELVES AND YOUR STAFF

Every member of your staff that comes into contact with personal data should know what GDPR is and aims to do. The language of the regulation is likely new to some. It is important to go through the different definitions of roles and responsibilities. Everyone should know what constitutes personal data and the correct handling of it. Make sure you engage many different roles at the school, so that your GDPR work applies to the areas that you are working in. Members of the senior leadership team can be a great help with this, and it is important to listen to their needs and input.

2 START WITH YOUR DATA MAPPING

First, you start by building an overview of where you store and use personal data (digitally and any paper-based storage). Map out where your data comes from and what type of personal information it is.

3 CREATE A DATA ASSET REGISTER

With your new data map, you can create a more detailed register that looks at every individual data asset. Give each data asset a reference number. On every row in your digital tool or spreadsheet you specify data source, data contents and data retention for that particular reference number. What you can learn from this is seeing if you might be storing unnecessary amounts of data. Or perhaps you share data with employees that might not need to be able to view it, making this a crucial step in your GDPR work.

4 DOCUMENT YOUR DATA PROCESSING

You need a good reason to collect and hold personal information, and also to understand how the data is categorised. The Special Category Personal Data holds information on racial or ethnic origin, religious of philosophical beliefs, political opinions, health, trade union membership and criminal offenses. All other data is categorised as personal data. Look at your information and determine whether you are required by law to process the data. If not, you might ask yourself if you need to process the data to effectively run your school. Remember that consent has to be voluntary, and can be revoked by the individual at any point. You also need to create a policy for how long you need to store a specific data asset. Look at why you hold the data, if you are legally obliged to keep it, if you can delete parts of it after a while, and so on. If you cannot justify why you hold the data, you should look into erasing it.

5 LOOK AT POTENTIAL RISKS AND HOW TO ELIMINATE THEM

With the help of your data asset register, you can now identify risks and assess what you need to do to eliminate or reduce areas of risk. Can you for instance see whether you have shared a piece of personal data with a third party or a member of staff? Look at how your GDPR activities adhere to your policies. Are your guidelines and activities sufficiently tailored to your specific needs. Or do you need to revise them? A personal data breach means “a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data” (Article 4). Make sure your staff knows what constitutes a data breach. If they suspect a data breach, they must immediately inform the DPO, who in turn might need to notify the authorities and the affected data subject(s).

6 APPOINT A DPO

As a data controller, your school needs to appoint a named Data Protection Officer to comply with GDPR. A DPO is the point of contact for communications with the authorities and is responsible for ensuring GDPR compliance. They can also help educate and train your staff and conduct internal audits. The DPO can be a member of staff or you can have an external DPO. If you wish, you can cooperate with other schools and share a DPO, but they need to understand your processes to make correct assessments regarding your compliance. They should also be involved from the very start with your GDPR work.

7 COMMUNICATE WITH YOUR DATA SUBJECTS

Be clear about who your data subjects are: students (including ex-students), staff (including former members of staff) and parents/carers. Know what rights they have, and what your plan of action is if a data subject wants to know what data you hold or wants to have their information removed entirely. Make sure to show your compliance in a clear and comprehensible manner. Inform data subjects what information is being collected about them, for what purpose, who they can contact to discuss their data management and so on.

8 MOVE FROM STRATEGY TO DAY-TO-DAY ACTIVITIES

When you have fulfilled the steps up to here, go through your policies to see whether you have all the tools you need to protect your data and manage your data processes. For instance, do you have a policy for how to manage a data breach? You should also check that your staff and different privacy roles have all the tools they need. Perhaps you have done your initial GDPR work in spreadsheets but might need a separate tool built for managing compliance. Your DPO can help ensure that you have the relevant tools and codes of conduct that applies to your particular needs and processes.

If you have any questions, don't hesitate to contact us! We believe that data protection management can be made easier.

*https://gdpr.report/news/2018/09/10/20-of-companies-report-being-gdpr-compliant-post-25th-may-deadline/
**According to a survey from the Information Commissioner's Office

About GO2 Consulting Services Ltd

We are passionate about providing schools with the best support possible in this challenging and often complex subject. As a further sign of our commitment we are proud to say that we are one of the first companies to sign the ICO “pledge” Your Data Matters—we know how important security and compliance are so we lead by example.

Contact Information

Address: 8 Hollingworth Avenue, Sandiacre, Nottingham, NG10 5LY

Telephone: +44 7999 763270

Email: info@go2.consulting

YOUR DATA MATTERS

ico.org.uk/yourdatamatters

GO2 Consulting Services Ltd

Your reliable, trusted and confidential adviser