

Suppliers of systems to schools

What schools need to know regarding suppliers’ compliance

Please complete the information required from page 5

# **Contents**

[**Contents** 1](#_Toc89332260)

[**School supplier compliance** 1](#_Toc89332261)

[**What is Article 30 in the GDPR and why is it so important?** 1](#_Toc89332262)

[**Consequences of non-compliance** 3](#_Toc89332263)

[**What next?** 3](#_Toc89332264)

[**As a supplier to this school/trust, please complete the information below?** 4](#_Toc89332265)

[**Supplier data mapping** 6](#_Toc89332266)

# **[School supplier compliance](#_Contents)**

The General Data Protection Regulation (**GDPR**) came into force on 25 May 2018 and was applied into EU law.

GDPR places on suppliers to schools direct and significant obligations and legal responsibilities. Additionally, data subjects may enforce their rights directly against data processors. Schools are required to include information about their data processing activities in their data audits that, in turn, will require suppliers to provide them with detailed information about how data is processed and their GDPR compliance status.

# **[What is Article 30 in the GDPR and why is it so important?](#_Contents)**

The GDPR is a huge piece of legislation which builds on existing practices and embraces change throughout the mechanisms we use to protect personal data. However, it is Article 30 which epitomises the extent of those changes and how it is necessary to review every part of your data processing and your data protection processes. It is now mandatory to keep written evidence that everything you say you are doing to protect data is in fact true.

A school is entitled to ask for written assurances or even evidence that a supplier, lawfully and securely processing data. Every data controller and processor must keep records of processing activities.

The next page shows the text taken directly from the GDPR Article 30.

**ARTICLE 30**

|  |
| --- |
| Records of processing activities |
|  |
| 1. Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:
 |
| * 1. the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer;
 |
| * 1. the purposes of the processing;
 |
| * 1. a description of the categories of data subjects and of the categories of personal data;
 |
| * 1. the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organisations;
 |
| * 1. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
 |
| * 1. where possible, the envisaged time limits for erasure of the different categories of data;
 |
| * 1. where possible, a general description of the technical and organisational security measures referred to in Article 32(1)
 |
| 1. Each processor and, where applicable, the processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a controller, containing:
 |
| * 1. the name and contact details of the processor or processors and of each controller on behalf of which the processor is acting, and, where applicable, of the controller's or the processor's representative, and the data protection officer;
 |
| * 1. the categories of processing carried out on behalf of each controller;
 |
| * 1. where applicable, transfers of personal data to a third country or an international organisation, including the identification of that third country or international organisation and, in the case of transfers referred to in the second subparagraph of Article 49(1), the documentation of suitable safeguards;
 |
| * 1. where possible, a general description of the technical and organisational security measures referred to in Article 32(1).
 |
| 1. The records referred to in paragraphs 1 and 2 shall be in writing, including in electronic form.
 |
| 1. The controller or the processor and, where applicable, the controller's or the processor's representative, shall make the record available to the supervisory authority on request.
 |
| 1. The obligations referred to in paragraphs 1 and 2 shall not apply to an enterprise or an organisation employing fewer than 250 persons unless the processing it carries out is likely to result in a risk to the rights and freedoms of data subjects, the processing is not occasional, or the processing includes special categories of data as referred to in Article 9(1) or personal data relating to criminal convictions and offences referred to in Article 10.
 |
|   |

# **[Consequences of non-compliance](#_Contents)**

Under the previous legislation, data processors were liable if they failed to comply with their contractual obligations to their controllers. *Everything changed under the GDPR*

Data subjects and data controllers will be able to take action and claim damages where they have ‘suffered material or immaterial damage’ if the processor fails to fulfil their obligations under the GDPR.

As well as data subjects claiming damages from data controllers and data subjects, non-compliant data processors can be investigated, and actions taken by the regulator. These range from access and audit rights, to administrative orders and restrictions on processing of data. Ultimately, there may be financial penalties including fines of up to 4% of annual global turnover for certain breaches.

# **[What next?](#_Contents)**

Schools must greatly increase accountability of their supplier data processors under the GDPR and it means that the school/supplier contract becomes even more important. Suppliers have as much of an interest in making sure obligations are precisely defined because they will become so much more exposed.

This is what needs to done:

* review existing contracts with suppliers;
* review processing activities;
* map how the data is processed and used
* review use of sub-contractors;
* reviewing data export/import arrangements;
* review data security;
* set up compliance accountability procedures;
* conduct risk assessments to establish what form appropriate and organisational technical measures will take.

# [**As a supplier to this school/trust, please complete the information below?**](#_Contents)

1. **A contract**

*Schools, as data controllers, may only appoint data processors that provide sufficient guarantees of their processing meeting the requirements of the GDPR. As a processor, suppliers will be required to process personal data in accordance with the controller's instructions. Thus, a relevant school/supplier contract should be in place that specifies the interest of both controllers and processors, and ensures that obligations are set out in a clear and easy to understand manner. This will usually comprise a Data Processing Agreement.*

Please provide a copy of your Data Processing Agreement

1. **Restrictions on sub-contracting**

*In your role as data processor, do you use sub-contractors to process data? As the lead processor you must ensure that the same contractual obligations you have with the controller in the contract still holds within any sub-processors’ mechanisms.*

*If yes, please state who these are and what data they process.*

1. **Demonstrating compliance**

*Suppliers MUST demonstrate GDPR compliance. Processors are under an obligation to maintain a record of all categories of processing activities.*

*The law says, this does not apply if: the processor has fewer than 250 employees; the processing does not pose a risk to the rights and freedoms of individuals; the processing is not more than occasional and does not include special category data. However, very few suppliers to schools will be able to use this proviso.*

Please confirm that these criteria are met. YES / NO

1. **Security**

*Processors are required to implement appropriate security measures. These measures might include pseudonymisation and encryption. Regular testing of the effectiveness of any security measures is also required where appropriate. Information on Cyber Essentials is available from the UK’s National Cyber Security Centre*

Please confirm that these criteria are met. YES / NO

.

1. **Breach notification**

*The enhanced breach notification requirement apply to both data controllers and data processors.*

Please confirm that you understand what is required of you in the event of a data breach. YES / NO

1. **Data Protection Officers or Lead**

*What are the contact details of your data protection officer or lead?*

1. **Transfers to countries outside of the EEA**

*A data processor relies on its controller’s consent for the use sub-processors. This is especially true, if any of the sub-processing involves data transfers to a third country, which is not in the EEA or enjoys an adequacy decision by the EU.*

Do you process data outside the EEA to a country which does not have an adequacy decision? YES / NO

If YES have you a record of consent?

1. **Codes of Conduct**

*The GDPR refers to approved Codes of Conduct as a means to both impose additional obligations on processors and for them to demonstrate compliance*

Are you a member of an associations or body? YES / NO

If YES which one(s)

Do you regularly refer to their guidance? YES / NO

1. **Retention**

Please say how long personal data is retained.

1. **Data Location**

Please say where data is processed and stored?

1. **Safeguards**

Please List the technical and organisational measures that are in place to limit exposure of the data and reduce impact or likelihood of breach.

# **[Supplier data mapping](#_Contents)**

To demonstrate suppliers’ systems are GDPR compliant, a data mapping exercise should be carried out. In this you will be required to maintain your Records of Processing Activity according to Article 30 of the EU GDPR.

EVERY SCHOOL WHICH USES 3rd PARTIES FOR DATA PROCESSING ARE OBLIGED TO FIND OUT THIS INFORMATION TO COMPLETE THEIR RECORD OF PROCESSING ACTIVITIES. THE SUPPLIER **MUST** PROVIDE PROCESSING INFORMATION.

**Data Fields or Elements – please identify all fields that apply**

|  |  |
| --- | --- |
| Absence information |[ ]  Account details |[ ]
| Activities |[ ]  Address |[ ]
| Admissions data |[ ]  Annual leave records |[ ]
| Appraisal and performance management |[ ]  Associations including trade union memberships |[ ]
| Attainment |[ ]  Attendance |[ ]
| Bank details |[ ]  Behaviour |[ ]
| Biometric |[ ]  Car registration number |[ ]
| Class name |[ ]  Company name and contact details |[ ]
| Complaints record |[ ]  Consent where consent required |[ ]
| Court order affecting pupil |[ ]  CPD training records |[ ]
| Criminal conviction data |[ ]  Date of birth |[ ]
| DBS information |[ ]  Department or faculty |[ ]
| Destination after leaving school/college |[ ]  Dietary information |[ ]
| Disability |[ ]  Disciplinary records |[ ]
| Driving license number |[ ]  EAL information |[ ]
| Education history |[ ]  Electronic signature |[ ]
| Email address |[ ]  Employee work code |[ ]
| Employment history |[ ]  Estranged status |[ ]
| Exclusion |[ ]  External agency involement |[ ]
| EYTS status and date of award |[ ]  Family links |[ ]
| First Aider status and information |[ ]  First generation of family to enter HE |[ ]
| Forename |[ ]  Forename (legal) |[ ]
| Forename (preferred) |[ ]  Forename and surname |[ ]
| FSM information |[ ]  Full name |[ ]
| Gender |[ ]  Gifted and Talented |[ ]
| HLTA status and date of award |[ ]  House Name |[ ]
| Initials |[ ]  Job title |[ ]
| LAC/formerly LAC information |[ ]  Leaving date |[ ]
| Legal name |[ ]  Length of service |[ ]
| Local Authority information |[ ]  Marital status |[ ]
| Medical information |[ ]  Mobile phone number |[ ]
| National Insurance number |[ ]  Nationality, ethnicity, religion |[ ]
| Next of kin |[ ]  NHS Number |[ ]
| Overseas Visitor status |[ ]  Passport number and date of expiry |[ ]
| Photograph/image/voice |[ ]  Pupil Premium information |[ ]
| QTS status and award date |[ ]  Qualifications |[ ]
| Reason for leaving |[ ]  Registration group |[ ]
| Relationship to pupil |[ ]  Safeguarding |[ ]
| Salary and benefits |[ ]  Salutation |[ ]
| School details |[ ]  SEND information |[ ]
| Services Child information |[ ]  Sexuality |[ ]
| Socio-economic information |[ ]  Starting date |[ ]
| Subjects studied |[ ]  Subjects taught |[ ]
| Surname |[ ]  Surname (former) |[ ]
| Surname (legal) |[ ]  Surname (preferred) |[ ]
| Tax code |[ ]  Teacher Reference Number (TRN) |[ ]
| Telephone number |[ ]  Unique Pupil Number (UPN) |[ ]
| Work Experience |[ ]  Working patterns and hours worked |[ ]
| Year group |[ ]  Young carer status |[ ]

**Are there any other fields?**

|  |  |
| --- | --- |
|  |[ ]   |[ ]
|  |[ ]   |[ ]
|  |[ ]   |[ ]

**Thank you for your help. Please return to:**