

**Data Processing Agreement\Contract Information**

**Shaftesbury Abbey Primary School**

**(V1.02)**

Version: 1.02 Release date: August 2020 Review date: April 2024

Authorised by: dpo@truniton.co.uk

Location: Shared policy please email dpo@turniton.co.uk

**Contents**

* General notes and Information on data sharing agreements
* What is the difference between a controller and a processor?
* When is a contract needed?
* What does the GDPR say about when a contract is needed?
* What is a sub processor and when are they used?
* Why are contracts between data controllers and processors important?
* What responsibilities and liabilities do controllers have when using a processor?
* What is the controller’s liability when it uses a processor?
* What responsibilities and liabilities do processors have in their own right?
* Can a processor be held liable for non-compliance?
* Who is liable if a processor is used?

**Templates**

* Data sharing agreement\contract template

**Further information**

* Contact information
  + School Lead (Data Protection)
  + Data Protection Officer
* Document review information

**General information - Data Sharing Agreements\Contracts**

Any business that is subject to the EU General Data Protection Regulation as a Controller will need to have in place an appropriate contract with any other Controller that it jointly shares data with particularly if that Controller is outside the EU. More importantly any Controller that is subject to GDPR will need to have in place an appropriate Data Processing Agreement with any third party that it shares data with where that third party is a processor as defined under GDPR.

GDPR applies to both Controllers and Processors that are established in the EU (e.g. has EU legal entities) but also to any Controller and Processor not located in the EU where the processing activities are related to either the offering of goods or services to data subjects in the EU irrespective of whether a payment is required or the monitoring of the behaviour of individuals as far as such behaviour takes place within the EU.

Many Processors are offering hosted or cloud services which are not EU located but which clearly cause the Processor to be caught by GDPR. Controllers or Processors not established in the EU but where they are caught by GDPR must designate a representative in writing. That representative must be established in a member state where the data subjects whose data are being processed by the Controller or Processor are located (or where most of them are located).

The appointment of a representative means that all data protection issues from data subjects or data protection authorities will be addressed to that representative but the appointment of the representative does not affect the responsibility and liability of the Controller or Processor under GDPR.

GDPR is quite specific about the duties of the Controller and the Processor and indeed Article 28 (3) of GDPR stipulates that there must be a contract in writing between the Controller and Processor which clearly sets out the subject matter of the processing and its duration as well as the nature and purposes of processing, the types of personal data and any particular special categories of data and the obligations and rights of both parties.

Failure to have in place a suitable Data Processing Agreement is a breach of the law under GDPR and therefore Controllers should be carrying out an audit of their existing contracts with Processors to establish if those contracts already comply with GDPR and in addition putting in place due diligence and procurement requirements in respects of contracts that are going to be entered into to which GDPR will apply.

Articles 28 – 36 set out issues that must be addressed in the Data Protection Agreement which include that:

* The Processor must have adequate information security in place;
* The Processor must not use sub Processors without consent of the Controller;
* The Processor must cooperate with the relevant Data Protection Authorities in the event of an enquiry;
* The Processor must report data breaches to the Controller without delay;
* The Processor may need to appoint a mandatory Data Protection Officer;
* The Processor must keep records of all processing activities;
* The Processor must comply with EU transborder data transfer rules;
* The Processor must help the Controller to comply with data subjects rights;
* The Processor must assist the Data Controller in managing the consequences of data breaches;
* The Processor must delete or return all personal data at the end of the contract at the choice of the Controller; and
* The Processor must inform the Controller if the processing instructions infringe GDPR.

The action for Controllers right now is to ensure that in respect of Data Processing Agreements:

* There are documented instructions for the processing of personal and sensitive data;
* That there is evidence of due diligence by the Controller over the suitability of the Processor in respect of the types of personal data being processed;
* There are suitable confidentiality clauses in the Agreement;
* The Processor has adequate information security in place;
* The contract manages the downline use of sub Processors. The contract puts in place measures for the Processor to help the Controller comply with Data Subject Rights;
* That there are mechanisms to assist in cooperation with the Controller and the relevant Data Protection Authorities;
* That there are processes in place to deal with data incidents and data breach notifications and that there are processes in place to deal with destruction or return of personal data at the end of the Agreement.

In addition to those needs, Processors should anticipate that Controllers will want to revisit not only the mandatory terms under GDPR but also the issues around warranties and indemnities as well as the question of suitable insurance.

Since Controllers and Processors are equally bound to comply with GDPR, in relation to International Data Transfers there will need to be in place suitable solutions in relation to personal data being transferred from the EU or more correctly the European economic area to other jurisdictions. In relation to International Data Transfers privacy shield is an approved solution to the extent that personal data is going from the EEA to the US but where data is being transferred across many borders then other solutions such as the European Commission approved standard contractual clauses or binding corporate rules may be more appropriate. Whilst there are also a number of jurisdictions that have been deemed approved jurisdictions by the EU (such as Argentina, Canada and Israel) there is considerably uncertainty as to the best solution to use given that privacy shield is under regular review by the European Commission as to its robustness as a data transfer solution but equally the standard contractual clauses are currently under review in the European Court of Justice and the European Commission recently announced that it is reviewing all of the countries that have been deemed adequate in the past to ensure that their laws are still fit for purpose in terms of the adequate protection of the rights of individuals.

All of the above raises the bar in relation to the pressures on both a Controller as well as its Processor in relation to any form of data processing whether cloud or otherwise.

Controllers should be putting in place a number of due diligence activities in respect of the Processors that they use which can be summarised as data protection audit, documentation of data processing activities and obviously review.

Data protection audit or assessments via a Controller of a Processor might include:

* Do they process personal data and/or special categories of data (e.g. criminal records, children’s data, health data)
* What are the data flows;
* What is the Processors information securities policies and procedures;
* Has the Processor had a history of breaches (notified or not);
* Has the Processor ever been audited or investigated by a Data Protection Authority (does the data Processor have a Data Protection Officer).

Documented data processing activities should address:

* Data processing mapping for both School\Trust and third-party processing;
* Do the Terms and Conditions of the Processor in any way claim ownership of personal data received from the Controller;
* How are data retention and data destruction practices managed;
* How are the use of sub processors contractually managed.

Review of policies and procedures might require the data Processor to produce:

* Data incident response policy and procedures;
* Data sharing policy and procedures;
* Standard operating procedures for vetting of staff;
* Information security practices;
* Cyber risk assessment and compliance;
* Evidence of training.

Prudent processors must anticipate that their customers as controllers will carry out due diligence and seek to impose new contractual terms and therefore processors should immediately:

* Carry out a GDPR Compliance Assessment;
* Rewrite their Terms of Business as appropriate;
* Audit their sub processors and the contractual terms with them;
* Review their insurance cover;
* Address data transfer solutions;
* Assess their policies and procedures;
* Decide if a mandatory Data Protection Officer is necessary;
* Put in place staff training on policies and procedures; and
* Carry out a genuine assessment as to whether or not they are actually a mere processor or in reality are a joint data controller with their customers.

**Key GDPR provisions**

See Articles 28, 29, 30, 31, 32, 33, 34, 35 and 36 and Recitals 81, 82 and 83.

**What is the difference between a controller and a processor?**

* A controller is a natural or legal person or organisation which determines the purposes and means of processing personal data;
* A processor is a natural or legal person or organisation which processes personal data on behalf of a controller.

If you are not sure whether you are a controller or a processor, please refer to ICO guidance on Data controllers and data processors. Although it is based on the Data Protection Act 1998 (DPA), the parts of the guidance setting out how to determine who is the controller and who is the processor are still relevant under the GDPR.

**When is a contract needed?**

* Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller) it needs to have a written contract in place.
* Similarly, if a processor employs another processor it needs to have a written contract in place with the sub processor.

**What does the GDPR say about when a contract is needed?**

The GDPR states at Article 28.3 that Processing by a processor shall be governed by a contract or other legal act under Union or Member State law, that is binding on the processor with regard to the controller.

This means that you need a written contract every time you employ a processor to process personal data. This includes both:

* When you directly employ a processor; and

* When a processor, with your written authority, employs another processor.

Although the GDPR refers to a contract ‘or other legal act’, in practice, in the UK, contracts are likely to be the appropriate means of complying with Article 28.3.

**Key GDPR provisions**

See Articles 28.3, 28.4 and 28.9 and Recital 81.

**What is a sub processor and when are they used?**

A processor might decide to use another processor to process personal data on its behalf. For shorthand this is sometimes referred to as using a ‘sub-processor’, although this is not a term taken from the GDPR itself. Before employing a sub-processor, the original processor must inform you, as the controller, and obtain your written permission.

**Key GDPR provisions**

See Articles 28.1, 28.2, 28.3 and 28.4 and Recital 81.

**Why are contracts between data controllers and processors important?**

Contracts between controllers and processors:

ensure that they both understand their obligations, responsibilities and liabilities;

* help them to comply with the GDPR;
* help controllers to demonstrate their compliance with the GDPR; and
* may increase data subjects’ confidence in the handling of their personal data.

The GDPR imposes a legal obligation on both parties to formalise their working relationship. Aside from the legal requirements, this makes practical and commercial sense.

By having a contract in place with the required terms:

* you are ensuring that you are complying with the GDPR;
* you are protecting the personal data of customers, staff and others; and
* both parties are clear about their role in respect of the personal data that is being processed and there is evidence of this.

The contract should set out what the processor is expected to do with the data.

Data subjects may be reassured by the fact a formal contract exists between those handling their personal data, setting out their obligations, responsibilities and liabilities. It also indicates to other organisations the professionalism of your business and the standard of your services.

**Key provisions in the GDPR**

See Articles 28.1, 28.2, 28.3, 28.4, 28.9 and 28.10 and Recital 81.

**What responsibilities and liabilities do controllers have when using a processor?**

You have a responsibility to check that your processor is competent to process the personal data in accordance with all the requirements of the GDPR. Your assessment should consider the nature of the processing and the risks to the data subjects. This is because

Article 28.1 says that you must only use a processor that can provide “sufficient guarantees” in terms of its resources and expertise, to implement technical and organisational measures to comply with the GDPR and protect the rights of data subjects.

If you choose a processor which adheres to a code of conduct or a certification scheme that has been approved under Article 40 or 42 of the GDPR (as and when these become available), then this may help to demonstrate your compliance with Article 28.1. Ultimately, however, it is for you to satisfy yourself that the processor provides sufficient guarantees in the context of the processing.

* Controllers must only use processors which are able to guarantee that they will meet the requirements of the GDPR and protect the rights of data subjects.
* Controllers must ensure that they put a contract in place which meets the requirements set out in this guidance.
* They must provide documented instructions for the processor to follow.
* Controllers remain directly liable for compliance with all aspects of the GDPR, and for demonstrating that compliance. If this isn’t achieved, then they may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

Once you have chosen a suitable processor you must put in place a contract which meets all the requirements of Article 28.3, and you must provide it with documented instructions to follow.

**What is the Controller’s liability when it uses a processor?**

As a data controller you are ultimately responsible for ensuring that personal data is processed in accordance with the GDPR. This means that, regardless or your use of a processor, you may be subject to any of the corrective measures and sanctions set out in GDPR. These include orders to bring processing into compliance, claims for compensation from a data subject and administrative fines. Further guidance on sanctions and corrective measures under the GDPR will be issued in due course.

Unless you can prove that you were “not in any way responsible for the event giving rise to the damage”, you will be fully liable for any damage caused by non-compliant processing, regardless of your use of a processor. This ensures that the data subject is properly compensated. You may however be able to claim back all or part of the amount of compensation from your processor, to the extent that it is liable.

**Key GDPR provisions**

See Articles 28, 29, 58, 82, 83 and 84 and Recitals 39, 81, 146, 148, 149, 150 and 152.

**What responsibilities and liabilities do processors have in their own right?**

* A processor must only act on the documented instructions of a controller.
* If a processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a controller and will have the same liability as a controller.
* In addition to its contractual obligations to the controller, under the GDPR a processor also has the following direct responsibilities:
* not to use a sub-processor without the prior written authorisation of the data controller;
* to co-operate with supervisory authorities (such as the ICO);
* to ensure the security of its processing;
* to keep records of processing activities;
* to notify any personal data breaches to the data controller;
* to employ a data protection officer; and
* to appoint (in writing) a representative within the European Union if needed.
* If a processor fails to meet any of these obligations or acts outside or against the instructions of the controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.
* If a processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor’s obligations.

Although a processor may make its own day to day operational decisions, Article 29 provides that it should only process personal data in accordance with your instructions, unless it is required to do so by law. This is also a required contract term under Article 28.3(a).

If a processor acts without your instructions in such a way that it determines the purpose and means of processing, then it will be considered to be a controller and will have the same liability as a controller.

**Can a processor be held liable for non-compliance?**

Under contract law a processor may be directly liable to you for any failure to meet the terms of your agreed contract. This will of course depend upon the exact terms of your contract.

It will be subject to the relevant investigative and corrective powers of a supervisory authority (such as the ICO) under Article 58 of the GDPR and may also be subject to administrative fines or other penalties under Articles 83 and 84.

A processor can also be held liable under Article 82 to pay compensation for the damage caused by processing where:

* it has failed to comply with GDPR provisions specifically relating to processors, or
* where it has acted without the lawful instructions of the controller, or against those instructions.

It will not be liable if it can prove it is not “in any way responsible for the event giving rise to the damage”. Under Article 82.5 it may be able to claim back from you part of the compensation it paid, for your share of liability.

We will provide more guidance on investigative and corrective powers, penalties and damages in due course.

All this provides a very strong reason for you to make sure that your processor is aware of the consequences and penalties which it may be subject to if it fails to comply with the GDPR. The GDPR has real ‘teeth’ in terms of enforcement, which could have serious operational and financial implications for both controllers and processors.

**Who is liable if a processor is used?**

Where a processor uses a sub-processor to carry out processing on its behalf, it must put in place a contract (or another legal act). This should impose on the sub-processor the same legal obligations the processor itself owes to the controller. The sub-processor has the same direct responsibilities and liabilities under the GDPR as the original processor has. If a sub-processor is used and someone makes a claim for compensation then there are potentially three liable parties: you as controller, the original processor, and the sub-processor. Under Article 82.5 each of you may be able to claim against the others for their share of the liability.

**Key GDPR provisions**

See Articles 3, 5, 27, 28, 29, 30, 31, 32, 33.2, 37, 38, 82, 83 and 84 and Recitals 22, 23, 24, 39, 80, 81, 85, 87, 88, 91, 97, 146, 148, 149, 150 and 152.

**Date Sharing Contract – Example Template**

This contract sets out the rules that all companies working for or with the school\trust must follow when using and sharing personal or sensitive information as outlined under the GDPR and general data protection regulations.

Data sharing contract details - **Controller**

|  |  |
| --- | --- |
| Contract agreement details - Controller |  |
| Controller name | Shaftesbury Abbey Primary School |
| Controller address | St James St, Shaftesbury, Dorset |
| Address 2 |  |
| Address 3 |  |
| Post code |  |
| Controller contact name | M.Salisbury |
| Controller contact email address |  |
| Controller contact phone number |  |
| Controller DPO contact name |  |
| Controller DPO email address |  |
| Controller DPO phone number |  |

Data sharing contract details - **Processor**

|  |  |
| --- | --- |
| Contract agreement details - Processor |  |
| Processor name |  |
| Processor address |  |
| Address 2 |  |
| Address 3 |  |
| Post code |  |
| Processor contact name |  |
| Processor contact email address |  |
| Processor contact phone number |  |
| Processor DPO contact name |  |
| Processor DPO email address |  |
| Processor DPO phone number |  |
| ICO reference number |  |

Please complete the following and include as much detail as possible.

**Information on processing and duration of contact.**

|  |  |
| --- | --- |
| Contract agreement processing information |  |
| Duration of contract |  |
| Contract start date |  |
| Contract finish date |  |
| Purpose and nature of processing: | |
| Description of processing activity: | |
| Personal data type and categories of data subject:   * Name: * DOB: * Age: * Gender: * Address: * Phone number: * Email address: * Location data: * Online identifier: * Other unique number: (UPN etc.) * UPN: * SEN:   Other data (please state)  Special category data:   * Racial or ethnic origin * Sexual life * Political opinion * Religious belief * Trade union membership * Physical or mental health or condition * Biometric or genetic data   Other sensitive data (please state) | |

**Contract agreement data retention information (end of contract)**

|  |
| --- |
| Contract data retention information |
| Please state data storage location and data retention information for duration of the contract if relevant and when the contact expires. Please also include any retention periods and data destruction\transfer methods at the end of the contract. |

**Processor responsibilities as part of this agreement\contract**

Please complete the following information and agree to the statements listed. Failure to complete all the information may result in the agreement\contract being rejected or terminated.

|  |  |
| --- | --- |
| Description of responsibility | Yes / No / N/A |
| Processor will only act on the written instructions of the controller. |  |
| Processor will not use a sub-processor without the written authorisation of the controller and under a written contract. |  |
| Processor will co-operate with supervisory authorities (such as the ICO) in accordance with Article 31. |  |
| Processor will ensure the security or its processing in accordance with Article 32. |  |
| Processor will keep records of its processing activities in accordance with Article 30.2. |  |
| Processor will notify of any data breaches to the controller in accordance with Article 33. |  |
| Processor will employ a Data Protection Officer if required in accordance with Article 37 and; and |  |
| Processor will appoint in writing a representative within the European Union if required in accordance with Article 27. |  |
| Processor will delete or return all personal data to the controller as requested at the end of the contract. |  |
| Processor will submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state. |  |
| Processor will assist the controller in obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments. |  |
| Processor must obtain a commitment of confidentiality from anyone it allows to process the data, unless they are already under such a duty of law. |  |
| Processor must inform the controller immediately if it thinks it has been given an instruction which does not comply with the GDPR, or related data protection law. |  |

**A processor should also be aware that:**

|  |  |
| --- | --- |
| Description of responsibility | Please tick (✓) |
| It may be subject to investigation and corrective powers of supervisory authorities such as the ICO) under Article 58 of the GDPR. |  |
| If the Processor fails to meet its obligations, it may be subject to an administrative fine under Article 83 of the GDPR. |  |
| If the processor fails to meet its GDPR obligations it may be subject to a penalty under Article 84 of the GDPR; and |  |
| If the processor fails to meet its GDPR obligations it may have to pay compensations under Article 82 of the GDPR. |  |
| Nothing within the contract relieves the processor of its own direct responsibilities and liabilities under the GDPR. |  |

**Processor agreement\contract sign off**

I\We the Processor agree to the above processor agreement\contract details and responsibilities and adhere to data protection regulations and principles under the GDPR and general data protection regulations.

|  |  |
| --- | --- |
| Sign off – Processor | |
| Name |  |
| Job title |  |
| Signature |  |
| Date |  |

|  |  |
| --- | --- |
| Sign off – Controller | |
| Name |  |
| Job title |  |
| Signature |  |
| Date |  |

**Further information**

# Contact

If you would like to discuss anything in this data sharing agreement\contract, In the first instance please contact the School lead below:

|  |  |  |  |
| --- | --- | --- | --- |
| Position | Name | Email | Phone |
| School lead | **M.Salisbury** | **office@shaftesburyabbey.dorset.sch.uk** | **01747 852620** |
| Data Protection Officer | **DPO** | dpo@turniton.co.uk |  |

**Policy update information (policy number GDPR-108)**

This contract template is reviewed annually and updated in line with data protection legislation.

Contract template review information

|  |  |
| --- | --- |
| Review date | Reviewed by |
| 02-05-2018 | turn IT on |
| 20-08-2018 | turn IT on |
| 01-07-2019 | turn IT on |
|  |  |
|  |  |
|  |  |

Contract template update information

|  |  |  |  |
| --- | --- | --- | --- |
| Review date | Revision | Description on change | By |
| 02-10-2018 | 1.00 | Draft release | turn IT on |
| 20-11-2018 | 1.01 | Full release | turn IT on |
| 01-07-2019 | 1.02 | Revised full release | turn IT on |
|  |  |  |  |
|  |  |  |  |