Data Controllers and Data Processors

The Data Controller

Any organisation that handles personal data and decides how and why the data is used is classed as a **'data controller'**. Under the General Data Protection Regulation (GDPR), a data 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".* They control the data but don't necessarily store or process it, although they are responsible for how it's used, stored and deleted.

We are a data controller where we decide:

- to collect the personal data and has the legal basis for doing so;
- which items of personal data to collect;
- to modify the data;
- the purpose or purposes the data are to be used for;
- whether to share the data, and if so, with whom;
- the retention period for the data.

A data controller is a central figure when it comes to protecting the rights of the data subject and has certain obligations under the GDPR:

- maintain records of processing activity (ROPA)
- provide information to individuals about, for example, who the organisation is and what personal information it holds and what is done with the information
- comply with the GDPR regarding the fair and lawful processing of personal data for specific and legitimate purposes
- implement technical and organizational measures to protect personal data against accidental loss/destruction, unauthorized access or other unlawful processing.
- enter into written agreements with processors that require them to
    - (a) act only on your instructions, and;
    - (b) comply with the same security obligations as are imposed on you under GDPR.

There may be situations, however, where a data controller needs to use an external service to process the data further. The data controller is not handing 'control' to another organisation; the data controller remains in control by instructing the purpose and ends to which that organisation can process the data. The organisation that processes the data on behalf of the controller is known as the **'data processor'**

The Data Processor

Under the GDPR, a data processor, is a *"natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller"*

An organisation may be a data processor if it's instructed by a data controller to carry out some of the following tasks:

- implement IT systems or other methods to collect personal data;
- use certain tools or techniques to collect personal data;
- install the security surrounding the personal data;
- store, delete, dispose of and retrieve the personal data;
- transfer the personal data from one organization to another

This could include something as simple as storing the data on a third party's server (such as with a cloud service), but also includes for example payroll companies, accountants and market research businesses. A good way to think of a data processor is as a specialised technical partner, appointed to carry out specific tasks to accomplish the goals set by the data controller

It is important to point out that the data processor does not control the data and cannot change the purpose or use of the particular set of data. The data processor is limited to processing the data according to the instructions and purpose given by the data controller. The data processor can however decide the means by which it process the data (for example the technical framework)

The Data Processor: Enhanced obligations under GDPR

Where previously, data processors could avoid legal liability, under the GDPR, processors have many more obligations. The most significant are that they are now required to:

- maintain a record of all processing operations under their responsibility
- be responsible for implementing appropriate security measures
- inform the data controller(s) immediately of any data breach
- hold status as joint controller for any data processing they carry out beyond the scope of the controller's instructions
- appoint a Data Protection Officer, if their business processes 'big data' or sensitive data

Given the heavy fines that can be imposed for breaches of the new GDPR, processors will need to familiarise themselves with the new rules.

Why is the distinction important?

In a perfect world, the data controller and data processor would clearly understand their roles and the communication between them would be seamless. Unfortunately, the real world is far from perfect and therefore GDPR establishes a framework and roles in case problems arise.

A common example where knowing one's role is crucial is in the event of a data breach. In such a case, where there is a controller/processor relationship between organisations to

which the breach applies, each must understand their individual responsibilities, and be able work together on management, containment and resolution.

It is vitally important to make sure there is a clear and specific data processing agreement before handing over the processing to a third party. It is important to for the organisation to understand its level of involvement in regards to the particular data it's handling.

A common recommendation is to provide a specific data protection clause in a contract between a controller and processor, preferably in the form of a supplemental agreement. Appendix A provides an example of a supplemental agreement.

Can an Organisation be both controller and processor?

It is perfectly possible for two separate organisations to be data processors of the same data. In the example of market research companies, one may run the analytics whereas the other stores the data – both are data processors of the data.

Similarly, the same organisation can be both a data controller and data processor. Article 26 of the GDPR states *"where two or more controllers jointly determine the purposes and means of processing, they shall be joint controllers".*

Taking the example one step further, if our analytics provider runs a customer's data through its systems, the provider will be the processor of that data. However, the analytics provider may hold any number of other data sets, perhaps which it uses in its analytics tools. If the analytics provider is entitled to determine the way in which that other data is used, it will be the controller of that data.

The key distinction is to determine the degree of independence that each party has in determining how and in what manner the data is processed, as well as the degree of control over the content of personal data

If you have any questions regarding working with data processors, then please get in touch with Michele Sarginson, the Authority's Data Development Manager and DPO. Telephone 01629 816278, email michele.sarginson@peakdistrict.gov.uk.

Appendix A: supplemental agreement for data processors

This supplementary agreement ("Agreement") is between:

1. The Peak District National Park Authority ("the Data Controller")

2. …….. ("the Data Processor")

1. BACKGROUND

a. The Agreement is supplemental to any other separate agreement entered into between the parties and introduces further contractual provisions to ensure the protection and security of data passed from the Data Controller to the Data Processor for processing.

b. Article 24 of General Data Protection Regulation place certain obligations on a Data Controller to ensure that any Data Processor it engages provides sufficient guarantees to safeguard the security of the data that it is processing on its behalf.

c. This agreement sets out the obligations in relation to the processing of data under the Contract. If there is a conflict between the provisions of the Contract and this Agreement, the provisions of this Agreement shall prevail.

2. DEFINITIONS

Regulation: means the General Data Protection Regulation 2016

Contract: means the agreement between the parties for the provision of the service

Data: means the information provided to [the organisation] for the stated purpose as defined on the order form

Data Controller: means a person who (either alone or jointly in common with other persons) determines the purposes for which and the manner in which any personal data are, or are to be processed and is defined in Article 4(7) of the Regulation.

Data Processor: means any person (other than an employee of the data controller) who processes the data on behalf of the data controller and is defined in Article 4(8) of the Regulation

ICO: means the Information Commissioners Office

Personal data: means any information relating to an identified or identifiable natural individual and is defined in Article 4(1) of the Regulation, and which is processed by the data processor on behalf of the data controller in accordance with this Agreement.

Processing: is defined in Article 4(2) of the Regulation as any operation or set of operations which performed on personal data or sets of personal data, whether or not by automated means, such as:

a) collecting, recording, organisation, structuring, storage
b) adaptation or alteration
c) retrieval, consultation, use
d) disclosure by transmission
e) dissemination or otherwise making available
f) alignment or combination
g) restriction, erasure or destruction

SIRO: means Senior Information Risk Owner

3. OBLIGATIONS

a. The Data Processor is to carry out services as described in the order form and process personal data only on the express instructions of the Data Controller and designated contacts at the Data Controller. Instructions may be specific or of a general nature as set out in the Contract, or as otherwise notified by the Data Controller to the Data Processor during the term of the Contract.

b. Where the Data Processor processes personal data on behalf of the Data Controller it shall;

i. Implement appropriate technical and organisational measures and take all reasonable steps necessary to protect the personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, alteration or disclosure, and promptly supply the details of such measures as requested by the Data Controller;

ii. At all times ensure material compliance with the Regulation and not provide the service in such a way as to cause the Data Controller to materially breach any of its applicable obligations under the Regulation

iii. Agree to comply with any reasonable measures required by the Data Controller to ensure that its obligations under this Agreement are satisfactorily performed in accordance with all applicable legislation in force during the lifetime of the Contract and best practice guidance issued by the ICO

iv. Ensure the confidentiality of the data and not copy, disclose or process it in any way without the express authority of the Data Controller including by the use of a sub-contractor to deliver any part of the service.

v. Notify the Data Controller within 2 business days if it receives any complaint, notice or communication from any third party in connection with the service provided and will provide the Data Controller with full co-operation and assistance in dealing with such complaint, notice or communication.

vi. Notify the Data Controller within 1 business days if it is made aware of any data loss or breach of security which may affect the Data Controller. **If equipment containing the data has been lost or stolen the Data Processor will notify the Data Controller's SIRO.**

vii. Will not transfer or process data to any third party or outside of the United Kingdom without the prior consent of the Data Controller, and where the Data Controller consent to a transfer, to comply with the obligations set out in Chapter V of the Regulation with due regard to the provision of adequate levels of protection or appropriate safeguards

c. The Data Processor shall ensure that any of its employees, agents or sub-contractors or professional advisers who have access to the data under the Contract are made aware of and act in accordance with the obligations in regards to the security and protection of the data.

4. LIABILITY/INDEMNITY

a. The Data Processor agrees to indemnify the Data Controller against all costs, claims, losses, damages or expenses incurred by the Data Controller as result of the Data Processor's failure to comply with its obligations under this Agreement and the Regulation.

5. WARRANTIES

a. Each party warrants to the other that it is authorised to enter into this Agreement

b. The Data Processor warrants that it will process the personal data materially in compliance with all applicable laws, enactments, regulations, orders, standards and other similar instruments.

c. The Data Processor warrants that it will not authorise any third party or sub-contractor to process the data save for as granted in this Agreement.

6. RIGHTS OF DATA CONTROLLER

The Data Controller reserves the right upon giving reasonable notice and within normal business hours to carry out compliance and information security audits of the data processor in order to satisfy itself that the Data Processor is adhering to the terms of this Agreement. Where a sub-contractor is used, the Data Processor agrees that the Data Controller may also, upon giving reasonable notice and within normal business hours, carry out compliance and information security audits and checks of the sub-contractor to ensure adherence to the terms of this Agreement.

7. RIGHTS OF DATA PROCESSOR

a. The Data Processor will not be restricted by this Agreement in its use of any data which is in the public domain or in its possession prior to commencement of the Contract.

8. INTELLECTUAL PROPERTY RIGHTS

a. The Data Processor agrees and acknowledges that any Intellectual Property Rights in the data belongs to the Data Controller and that the Data Processor does not acquire any rights, title or interest in such data, save as granted under this Agreement.

b. The Data Controller hereby grants the Data Processor a royalty free non-assignable licence to process the data under this Agreement. For the avoidance of doubt this licence shall terminate automatically on termination of the Contract.

9. TERM

a. This Agreement shall commence on acceptance and signing of the Contract.

b. The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of data and data storage devices upon completion of overwriting or destruction of any devices used during the term of the Agreement.

10. TERMINATION

a. Termination of this Agreement will complete on both termination of the Contract in accordance with the termination terms set out in the contract and the successful transfer of all data back to the Data Controller (or a third party nominated in writing by the Data Controller). All data transfers must be made by secure means, and must only be made with the prior consent of the Data Controller.

b. Promptly on termination of the Contract and the completion of successful data transfer back to the Data Controller (or a third party nominated in writing by the Data Controller), the Data Processor will delete all data and any copies of the data in its possession to current CESG standards as by the National Cyber Security Centre

c. The Data Controller shall provide written confirmation of satisfactory transfer to the Data Processor as soon as possible, along with instructions for destruction of any data remaining in the Data Processor's possession.

d. The Data Processor shall provide the Data Controller with copies of all relevant overwriting verification reports and/or certificates of secure destruction of data and data storage devices upon completion of overwriting or destruction of any devices or media containing the Data Controller's data at the time that the contract is terminated.

e. Notwithstanding termination the provisions of clause 3 shall survive the termination of this Agreement and shall continue in full force and effect until all Data are returned to the Data Controller (or a third party nominated in writing by the Data Controller) and all overwriting verification reports and/or certificates of secure destruction of data have been provided to the Data Controller to its reasonable satisfaction.

11. JURISDICTION

This Agreement will be governed by and construed in accordance with the laws of England and Wales and the parties shall submit to the exclusive jurisdiction of the Courts of England and Wales