2019

GDPR obligations for data Processors

IN 10 MINUTES

www.datastreams.io
contactus@datastreams.io

GDPR obligations for data Processors in 10 minutes.

INTRO The European Union (EU) General Data Protection Regulation (GDPR) brings big changes for data processors and data controllers. Implementing these changes in time is crucial to avoid monetary fines and reputational damage. The first step towards ensuring you are in compliance with the GDPR, is knowing what will change for you as an organisation.

In this whitepaper, we discuss the most important changes the GDPR brings for the data processors. Not sure whether you are a controller or a processor? We'll help you figure that out first.

Processors vs Controllers

To help you quickly work out which parts of the GDPR apply to you in terms of how you collect and/or process personal (& sensitive) data, we need to establish whether you are a data processor or a data controller. GDPR article (art.) 4 defines data controllers and processors as:

CONTROLLER Means 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; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law.

PROCESSOR A natural, or legal person, public authority, agency of other body which processes personal data on behalf of the data controller.

In short; if you make decisions about what data is collected or why data is processed, you are a data controller. If you process data on behalf of somebody else, you are a data processor. Note that the data processor might make **technical** decisions about the data like how it is stored, the security measures taken and the methods of collecting personal data. Only the data controller, however, can determine the purpose of data processing, the legal basis for processing and by what means the data is processed. As a rule of thumb, if you decide about the **why** and **how** of the processing activity, you are considered a data controller.

It is possible for two organisations to be processors of the same data, such as one company running analytics while the other stores it. It is also possible you are both a controller and a processor of different datasets or data activities. Figuring out which of the two you are for which specific activities and what other organisations are concerned with the data you work with, are important first steps to realising your responsibilities.

Data Processors

The GDPR Is long and complex. It can be easy to miss the most important obligations and requirements buried within the regulation, which overflows with information. Our Data Protection Officer (DPO) has combed through the most relevant chapters, articles and recitals of the GDPR for organisations and has relayed to us the most important things you, as a data processor, should know. To equip you with the information you need, we answer four key questions you might have about the GDPR.

To help you even further, we provide an overview of the most important points of the GDPR. Relevant article (art.) numbers are referred to in brackets, so you can easily find them if you want to read more.

What makes the GDPR so special?

Before we start getting into the details of the GDPR, we need to clarify what makes the GDPR so special compared to the previous EU 'Data Protection Directive'. The unique nature of the GDPR is due to two very significant changes:

01 The GDPR places for the first time, direct statutory obligations on data processors. Previously under the EU Data Protection Directive, these only applied to data controllers.

02 The GDPR is a regulation, rather than a directive. Hence it applies in the same way, across all EU member states.

Perhaps the most significant change for data processors, is that under the GDPR they will be subject to compliance obligations and risk serious penalties if they do not comply. Where before any contact with the Data Protection Authorities was limited to data controllers, data processors will now be held accountable for non-compliant processing. Furthermore, working with compliant processors will be even more important for controllers. Good reasons to start working on compliance immediately. The second change might prove beneficial, as it means that obligations for processors will be clear and consistent across countries. With these important changes out of the way, let's get into some pressing questions you might have.

Which data subject rights does a data controller need to respect?

While data processors are generally less affected by the rights of the subject than data controllers, it is still important to be aware of changes in these rights when processing data. Usually, the responsibility for respecting these rights will lie largely with the data controller, however, data processors will be expected to assist the controller in fulfilling their obligations. To this end, let's look at the (improved) data subject rights relevant for data processors.

The data processor may be called to assist the data controller in fulfilling its obligations to respond to these requests from data subjects:

01 Provide a copy of the personal data undergoing processing on request by the data subject.

```
Right of access by the data subject [art. 15].
```

02 Rectify inaccurate personal data without undue delay upon request from data subject.

```
Right to rectification [art. 16].
```

03 Restrict processing where any of the given criteria within the GDPR applies (e.g. unlawful processing).

```
Right to restriction of processing [art. 18].
```

04 No longer process data, where a data subject objects to the processing of their personal data (especially direct marketing), unless they can demonstrate compelling legitimate grounds for processing. Controllers must communicate this right to data subjects at the time of first communication with the data subject, at the latest.

```
Right to object [art. 21].
```

In short:

CHAPTER	ARTICLE	RECITAL
3 Rights of the data subjects	15, 16, 18, 21	63, 64, 65, 67, 69, 70

What key areas do data processors need to focus on?

Many overviews of the GDPR are very extensive, including aspects of the regulation that might not be relevant for you as a data processor. There are, however, plenty of important changes you might need to implement as a data processor. Here is an overview.

When working on behalf of a data controller, data processors:

01 Should provide sufficient guarantees to controllers that appropriate technical and organisational measures for GDPR compliance are implemented and ensure a level of security appropriate to the risk.

- This includes: pseudonymising/ encryption, maintaining confidentiality, restoration of access following physical/technical incidents and regular testing of measures.

`[art. 28 + 32].`

02 Shall not process personal data except on instructions from the data controller.

`[art. 32].`

03 Should ensure any natural person acting under their authority does not process data except on the data controller's instructions.

`[art. 29].`

04 Shall not engage with another processor without prior written authorisation from the data controller. Data controller shall have a right to object to any changes regarding data sub-processors.

`[art. 28].`

- The data sub-processor will be subject to the same contractual data protection obligations as between the first data processor and data controller. The initial data processor is liable to the data controller for performance of the data sub-processor's obligations.

05 should enter into written contract with the data controller to specify processing activities and duration. An example is entering into a "Data Processing Agreement" (DPA). This obligation also applies to any data sub-processors.

`[art. 28].`

06 Should designate a DPO where obligatory under the GDPR, publish the DPO's contact details and communicate them to the supervisory body.

`[art. 37].`

- The organisation should ensure the DPO is involved in all issues relating to the protection of personal data, should provide the necessary resources for the performance of DPO tasks and should ensure DPO tasks and duties do not cause a conflict of interest.

`[art. 38].`

07 Should maintain written records of processing activities, which must contain the information specified within the GDPR and must be made available to the supervisory authorities.

`[art. 30].`

- Does not apply if fewer than 250 persons employed (unless risk to rights and freedoms of data subjects, or special categories of data processed).

08 Must inform supervisory bodies without undue delay (within 72hrs) of becoming aware of any personal data breach.

`[art. 33].`

- Notification should contain information specified within the GDPR and the controller to document any breaches, including its effects and remedial action taken.

09 Must comply with conditions laid down within the GDPR to ensure personal data is adequately protected when transferred to a third country.

`[art. 44 - 49].`

In short:

CHAPTER	ARTICLE	RECITAL
4 Controller and Processor	27, 28, 29, 30, 31, 32, 33, 37, 38	13, 80, 81, 82, 83, 85, 86, 87, 88, 97
5 Transfers of personal data to third countries or international organisations	44, 45, 46, 47, 48, 49	101, 102, 103, 104, 105, 106, 107, 108, 109, 110, 111, 112, 113, 114, 115

What happens if data processors don't meet these obligations?

You might already have heard about the risks of non-compliance. Indeed, the GDPR brings big financial fines for organisations unable or unwilling to comply. A big change compared to the EU Data Protection directive, is that this time, processors can also be held accountable. As such, it's important to know the risks of non-compliance. We've summarised them below.

The results of non-compliance include that:

01 Every data subject has the right to lodge a complaint with a supervisory authority.

`[art. 77].`

02 Each data subject has the right to effective judicial remedy where they consider that their rights under the GDPR have been infringed through the processing of their personal data.

`[art. 79].`

03 Any person who has suffered material or non-material damage as a result of an infringement of the GDPR shall have the right to receive compensation for the damage suffered.

`[art. 82].`

04 A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller. Processors are exempt if it is proven they are in no way responsible for the event giving rise to the damage.

`[art. 82].`

05 Depending on severity of the infringement, fines of up to €20,000,000 or up to 4% of global turnover can be given to non-compliant organisations.

`[art. 83].`

Turning legislation into action

Now that we've helped you understand the legislative requirements and obligations a bit better, it's time to start thinking about the practical next steps. While you can immediately start taking some of the key actions we have discussed, you might require specialised solutions for other actions.

At Datastreams we have developed our software solutions with the GDPR in mind. Our Privacy & Compliance solution ensures consent is collected in a GDPR compliant way, while our Datastreams Platform empowers you to get control of your data infrastructure; mapping, governing and distributing your data streams in an easy and comprehensive manner. Want to find our more? Visit us at www.datastreams.io.

www.datastreams.io
contactus@datastreams.io