2019

GDPR obligations for data Controllers

IN 10 MINUTES

www.datastreams.io
contactus@datastreams.io

GDPR obligations for data Controllers 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 controller. 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 Controllers

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 controller, should know. We discuss these based on six typical GDPR related questions.

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.

These changes can be good for you as a data controller. They mean that your processors will also have incentives to become GDPR compliant and that the rules regarding data processing will be clear across all EU member states.

Which principles must be upheld by data controllers?

The GDPR is built on several important principles that need to be upheld by data controllers. Before getting into specifics, it is important to understand the principles of data protection, lawful processing and consent. We discuss the most important obligations stemming from these principles below.

Under the requirements and obligations within the GDPR, the data controller:

01 Is accountable for compliance with data protection principles. E.g.

- Lawfulness, fairness and transparency
- Accuracy
- Purpose limitation
- Storage limitation
- Data minimisation
- Integrity and confidentiality

`[art. 5].`

02 Must carry out lawful processing by virtue of at least one of the conditions laid out in the GDPR. Possible conditions are:

- Consent
- Vital interests
- Contractual
- Public task
- Legal obligation
- Legitimate interests

`[art. 6].`

NOTE The conditions for lawful processing are stricter where sensitive data like genetic data or data revealing ethnic origin are concerned [art. 9]. Be sure to check what data you process and whether this activity is subject to the rules for sensitive data.

03 Needs to demonstrate data subject's consent to processing their personal data, if consent is the legal basis for processing.

- Requests for consent to be presented in a manner clearly distinguishable from other matters and in an intelligible and easily accessible form.
- Consent may be withdrawn by data subjects at any time.

NOTE To be valid, consent must be obtained through a freely given, specific, informed and unambiguous (in some cases explicit) indication of the data subject's wishes.

`[recital 32].`

04 Must make reasonable efforts to verify parental consent.

`[art. 8].`

In short:

CHAPTER	ARTICLE	RECITAL
2 Principles	5, 6, 7, 8, 9	32, 33, 38, 39 40, 41, 42, 43, 44, 45, 46, 47, 48, 49, 50, 51, 52, 53, 54, 55, 56

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

The improved rights of the data subjects are a crucial part of the GDPR. Understanding the rights your data subjects have with regards to your data, is crucial in ensuring you can provide your customers with the service and information they are legally entitled to. Let's take a look at the (improved) data subject rights and how to deal with them.

With respect to data subject rights, the data controller needs to:

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 Erase personal data without undue delay either when data subject requests so, or where obligatory (e.g. the data subject withdraws consent) and inform other controllers involved in processing of the request, subject to certain exceptions within the GDPR.

`Right to erasure ('right to be forgotten')[art. 17].`

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

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

05 Provide data subject with their personal data in a structured, commonly used, machine-readable format where processing is carried out by automated means, upon request.

`Right to data portability [art. 20].`

06 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].`

07 Honour the data subject's right to withdraw consent at any time.

`Right to withdraw [art. 7].`

08 implement suitable measures to safeguard the data subject's rights and freedoms and legitimate interests where automated individual decision making is necessary for the performance of a contract between controller and data subject and/or is based on the data subject's explicit consent.

`Rights relating to automated individual decision-making [art. 22].`

In short:

CHAPTER	ARTICLE	RECITAL
2 Principles	7	32
3 Rights of the data subjects	15, 16, 17, 18, 20, 21, 22	63, 64, 65, 66, 67, 68, 69, 70, 71, 72

How should a data controller inform and communicate with data subjects?

The GDPR doesn't only give data subjects more control over with happens with their data, but also ensures they are informed correctly of any data processing and collection activities. This means that you need to communicate certain information about your activities to your data subjects in a GDPR compliant way. We have summarised the most important points below.

In terms of communicating with data subjects, the data controller needs to:

01 Ensure information/communications are concise, transparent, intelligible and in an easily accessible form (especially when specifically addressing a child).

`[art. 12].`

02 Provide requested information by data subjects without undue delay (within 1 month) of receipt of request .

`[art. 12].`

03 provide certain information when personal data is (and when it is not) collected from data subjects. Information that must be provided includes:

- Controller's identity & contact details
- Data Protection Officer contact details
- Purposes & legal basis for processing
- Recipients of the personal data
- The period that the data will be stored
- Information on data subject rights

`[art. 13 - 14].`

04 communicate any rectification or erasure of personal data and any restriction of processing to each recipient to whom personal data has been disclosed.

`[art. 19].`

05 Communicate any personal data breach to the data subject without undue delay.

`[art. 34].`

In short:

CHAPTER	ARTICLE	RECITAL
3 Rights of the data subjects	12, 13, 14, 19	58, 59, 60, 61, 62
4 Controller and Processor	34	86

What key areas do data controllers need to focus on?

With all the possible areas of change, identifying the key areas where change is most needed can be difficult. For this reason, we have provided you with a list of actions you may need to undertake in your organisation to comply with the GDPR.

Key actions data controllers need to take are:

01 implement appropriate technical and organisational measures to ensure and demonstrate processing is in line with the GDPR regulation and ensure a level of security appropriate to the risk. They should also obtain sufficient guarantees (via a written contract) that their processors do so as well.

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

[art. 24 - 32 - 28].

02 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].

03 Follow the principles of data protection by design and default; meaning that both in the planning and implementation of processing activities, data protection principles and appropriate safeguards are addressed and implemented.

[art. 25].

04 when not established in the EU, designate in writing a representative established in one of the Member States where data subjects being monitored are based, unless processing is occasional or controller is a public authority or body.

[art. 27].

05 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).

06 Enter into a written contract with processors to specify processing activities and duration. In addition, ensure compliance with specific GDPR obligations (e.g. agreeing that the processor may only act on documented instructions from the controller when processing personal data).

[art. 28].

07 Apportion respective responsibilities for compliance between themselves and another joint controller and make their arrangements known to data subjects

`[art. 26].`

- They should also ensure any natural person acting under their authority does not process personal data except on the controller's instructions.

`[art. 32].`

08 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 carry out a Data Protection Impact Assessment (DPIA) prior to carrying out potentially high-risk processing, and seek the advice of its DPO while doing so

`[art. 35].`

- In the absence of measures taken to mitigate the risk, the data controller should consult supervisory authorities prior to processing data that a DPIA has indicated is high risk.

`[art. 36].`

10 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	24, 25, 26, 27, 28, 30, 31, 32, 33, 34, 35, 36, 37, 38	13, 39, 74, 75, 76, 77, 78, 79, 80, 81, 82, 83, 85, 86, 87, 88, 89, 90, 91, 92, 93, 94, 95, 96, 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 controllers 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 to comply. Additionally, data subjects are entitled to compensation in some cases of infringement. We've summarised the most important results of non-compliance 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 Any controller involved in processing shall be liable for the damage caused by processing which infringes the GDPR.

`[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].`

In short:

CHAPTER	ARTICLE	RECITAL
8 Remedies, liabilities and penalties	77, 79, 82, 83	141, 145, 146, 147, 148, 150, 151

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