TRUEVAULT

The Complete GDPR Guide

2019 Edition

www.truevault.com

Table of Contents

Introduction

In May 2018, the European Union passed the General Data Protection Regulation (GDPR), and it's not a breezy beach read, to say the least. We know first-hand. When we started reading the legislation we couldn't help but wish there was a GDPR cliff notes. A resource that condensed the extraneous details, translated the legalese and simply answered one key question: What does GDPR mean for my business?

After a careful read (and a few rereads) we extracted the essence of the Regulation and summarized it into a user-friendly format. So, if you're thinking about the business impacts of GDPR and want some guidance on the Regulation and have questions about compliance, then you're reading the right book.

This e-book will cover several key topics:

1. What is GDPR?
2. What types of organizations does GDPR apply to?
3. What does GDPR compliance look like?
4. How can my business comply with the law?
5. What happens if we don't comply?

If you have more questions about compliance after reading our e-book, then don't hesitate to reach out to our team at GDPR@truevault.com and say: I loved the e-book, now help me do it.

About TrueVault

TrueVault is the first data security company completely focused on protecting personal data. The company helps businesses manage compliance risk by giving them unprecedented insight into, and control over the personal data they are storing.

As organizations collect and store more data to drive their businesses forward, they are also increasing their risk and liability. TrueVault can remove that liability and ensures compliance with regulations such as HIPAA, GDPR, and the California Consumer Privacy Act (CCPA) while also simplifying tedious tasks like fulfilling Data Subject Requests.

This book was a labor of love and could not have been done without the heavy lifting of Peter Orr with assistance from Sara Kassabian and the TrueVault team. If you enjoy this book and stumble across their path – a high five would be appreciated.

Learn more about TrueVault at www.truevault.com or follow us on Twitter @TrueVault.

CHAPTER 1

What is GDPR?

What is GDPR?

The General Data Protection Regulation (GDPR) is an extensive new law regulating the collection and use of personal data of individuals in the European Union, which came into effect on May 25, 2018.

GDPR replaces the Data Protection Directive of 1995, which was the EU's first legal framework covering data security. In the 20 years since then, the explosion in the use of computers and the internet has contributed to a huge rise in the collection and processing of personal data. Unfortunately, this has also increased the potential for data theft and misuse. GDPR is therefore an attempt to deal with these threats, and update the law for the modern world.

What does GDPR cover?

GDPR is concerned with all kinds of personal data, which is any information relating to an identifiable individual (a data subject). This could for example include names, addresses, contact details, online usernames or demographic information.

Although created by the EU, GDPR applies to any organization (or person) with a European presence, or which deals with the personal data of data subjects within the EU (Article 3). It applies to organizations which act as data controllers and/or data processors:

Data controllers decide the purposes and methods of processing personal data – they coordinate processing.

Data processors are responsible for directly processing personal data based on the instructions of data controllers. This could for example include subcontractors.

There are potentially severe penalties for non-compliance (see below), which means that if your business has any dealings with this sort of data, it is vital for you to understand what GDPR means and what action to take.

Here are the main areas it covers:

The grounds for processing personal data (Article 6)

In order to be lawful, collection and processing of personal data must be justified under one of six possible grounds. For most organizations, the crucial grounds are (i) that the data subject consented to the processing (see below), (ii) that

the processing is necessary to the performance of a contract with the data subject (or to steps requested by them in the lead up to entering such a contract), or (iii) that the processing is necessary for the organization to pursue its legitimate interests. There are stronger requirements covering sensitive information such as a data subject's ethnic origin, religious beliefs or criminal convictions (Articles 9 & 10), as well as processing related to automated decision-making (Article 22).

KEY POINT

A contractual obligation is not enough to satisfy this requirement. Also note that as written, this does not cover the laws of countries outside of the EU.

The type of consent needed to collect personal data (Article 7)

In order to rely on a data subjects' consent to processing (see above), the request for consent must be clear and unambiguous, and it should be clear what their personal data will be used for (e.g. marketing). Consent must be freely given (so avoid making it a requirement of entering a contract unless it is really necessary), and the data subject has the right to withdraw their consent at any time. For children under 16, consent must be given or authorized by a parent or guardian (Article 8).

The manner in which personal data must be processed (Articles 5 & 32)

Data subjects should be informed of what will be done with their data and their rights over the data (Articles 13 and 14). Personal data must be collected and processed in a manner which takes data security seriously, using processes designed with security in mind – this is known as "data protection by design and by default" (Article 25). This includes collecting the minimum information necessary, keeping it for no longer than is necessary, taking steps to keep it accurate and up to date, and protecting it from unauthorized access or accidental loss. It is also important to keep records of the sort of data being kept, the purposes of keeping it and the processes used to keep it secure (Article 30).

The rights of data subjects over their personal data (Articles 15 to 21)

Data subjects have a number of rights regarding their personal data, including the right to access the data, or to have it corrected, deleted or transferred. They also have the right to object to processing in certain situations. You will need to

be prepared to act on these requests in a helpful and timely manner.

The obligations when there has been a data breach (Articles 33 & 34)

If a data breach does occur, data processors are required to notify data controllers, and data controllers must notify the data subjects affected, as soon as possible. In addition, data controllers must, within 72 hours where possible, notify the relevant data protection supervisory body in the EU country in which they have their "main establishment" (for example, the Information Commissioner's Office in the UK).

The relationship between data controllers and data processors (Article 28)

It is the data controller's responsibility to ensure that the data processor can implement sufficient measures to keep the data secure and otherwise comply with GDPR. Data controllers must have a contract with their data processors setting out the types of data being processed and the nature of the processing and requiring (among other things) that processing only be done according to written instructions.

Other miscellaneous requirements

In certain circumstances, data controllers and processors must appoint data protection officers to advise on GDPR and other data protection requirements (Articles 37 to 39). Where proposed processing is high risk, controllers will have to undertake a data protection impact assessment and may need to send details to the supervisory authority (Articles 35 and 36). Personal data can only be sent outside of the EU under certain circumstances, to ensure that it remains safe (Articles 44 to 50).

The penalties for failing to comply (Article 83)

In contrast to the previous regime, GDPR authorizes fines for breaching its provisions which are potentially extremely severe. The maximum fine for more serious breaches is €20,000,000 or 4% of global turnover (whichever is higher), which means that making sure that your business complies with GDPR is a serious matter.

This is the first chapter in our GDPR e-book. In future chapters, we will analyze its requirements and the steps organizations will need to take to avoid breaching them. We will look at who will be affected, and then go into detail about each of the areas above, before concluding with a checklist setting out the responsibilities of data controllers and processors. Our aim is to provide you with enough knowledge and understanding to avoid potential pitfalls and prepare your business for the major changes following GDPR.

If you are concerned about GDPR and want to know what we can do to help you stay compliant, please get in touch.

CHAPTER 2

Do I Need To Be GDPR Compliant?

Do I Need To Be GDPR Compliant?

As explained in the previous chapter, GDPR is a new law regulating the processing (collection and use) of individuals' personal data.

If you are covered by GDPR, then not only will your customers expect you to be compliant, but your business partners may require it as a condition of their contracts. Moreover, the fines for breaching the Regulation are harsh, going up to €20,000,000 or 4% of your global turnover (whichever is higher).

With that in mind, it is vital to know whether you are within its scope.

Data controllers and data processors

To start with, GDPR applies to people and organizations which act as data controllers and data processors:

This will covers any organization which keeps a customer or membership list, or information about its employees. The vast majority of organizations will therefore be affected, as long as they have dealings with the European Union.

Data controllers decide the purposes and methods of processing personal data – they coordinate processing.

Data processors are responsible for directly processing personal data based on the instructions of data controllers. This could for example include subcontractors.

Dealings with the European Union

GDPR was created by the European Union to protect its citizens, and so it only affects organizations with some kind of relationship with the EU or its people. That said, it does not only apply to companies based in an EU country. According to Article 3, you will be affected if you are a data controller or data processor and any of the following apply:

- You are established in the EU (or

somewhere else subject to EU law), or

- You offer goods or services to data subjects in the EU, or
- You monitor the behavior of data subjects in the EU.

Establishment in the European Union

If you are established in the EU, then all processing related to that establishment is covered, even if it takes place elsewhere.

Being established is a broad concept in EU law. It could apply to you if you have (for example) a branch, representative, address or bank account in an EU country. (See the recent Weltimmo case in the European Court of Justice - particularly paragraphs 29 to 33 - regarding the outgoing Data Protection Directive.)

SIDE NOTE

If you are covered by GDPR but you are not established in the EU, you will need to designate a representative within the EU (under Article 27) unless the processing is occasional, does not include a large amount of sensitive information (such as a data subject's ethnic origin, religious beliefs or criminal convictions) and is unlikely to involve a risk to people's rights and freedoms.

Goods and services

If you control or process data relating to people in the EU, in the context of offering them goods and services, then this will be covered by GDPR. This is true even if the goods and services are offered for free.

Note the word offering: it appears that this will only apply where there is some element of targeting your goods at EU countries. Targeting is likely to include providing a version of your website in a local language (which is not your own country's language), allowing purchases in the local currency, or mentioning EU customers or countries on the website. It is possible that merely delivering to EU countries will be enough to count.

Note that the key question is whether your customers (or members, or employees) are in the EU, not whether they are EU citizens. You don't for example need to worry about the nationality of customers based in the US.

Monitoring behaviour

If you control or process data relating to people in the EU, in the context of monitoring their behavior, then this will be covered by GDPR.

A lot of monitoring is done in tandem with the offering and sale of goods and services (see above), such as online vendors using patterns in consumer purchases to offer similar products, or games developers collecting data on player activity. However, monitoring also covers a wider range of activities, including market research and getting feedback. The vast majority of online organizations (commercial or non-commercial) monitor the behavior of visitors to their websites to some extent.

As with the offering of goods and services, there needs to be a certain degree of targeting at people in EU countries. For example, if you merely collect web traffic data without targeting individuals in the EU, this is unlikely to be covered.

What does this mean for American companies?

This all means that GDPR will affect a lot of American companies, whether or not they have any specific presence in the EU.

If you are not established in the EU, but a small proportion of your revenue comes from people in those countries, then you are faced with a choice. You could choose to stop providing (or at least marketing) your goods and services to these people in order to avoid taking the steps necessary for compliance.

However, remember that most of GDPR's rules are good practice in any event. Adhering to them shows to your customers that you take data security seriously, and it puts you in a good position should state or federal government ever decide to enact similar legislation at home.

Cutting yourself off from European markets could ultimately limit your future growth. By contrast, working to make your organization and its products GDPR compliant, whether on your own or with help, is an investment which is likely to pay off in the long run (TrueVault, for instance, offers products that helps your business comply with GDPR).

Some (limited) exemptions

There are very limited categories of processing exempted from GDPR:

- Processing related to activities which are outside of EU law.
- Processing related to law enforcement and immigration control.
- Processing by individuals carrying out purely personal or household activities (such as keeping an address book).

As can be seen, none of these will apply to the vast majority of organizations.

GDPR will apply across the business world,

wherever organizations have an EU presence or deal with the personal data of people in the EU. The sanctions for a data breach will potentially be harsh. We will look at these in detail in the next chapter.

As a result, it is vital to check whether your organization is covered by the new rules, and if so to take all steps necessary to make it compliant. If you need any help bringing your business to GDPR compliance, please get in touch with us, GDPR@truevault.com.

CHAPTER 3

What Are The Penalties For Breaching GDPR?

What are the Penalties for Breaching GDPR?

As previously explained, GDPR is a new law governing the collection and use of personal data. It will affect people or organizations which are established in the European Union or which offer goods or services to or monitor the behavior of people living in the EU. It came into force May 2018.

One of the biggest changes made by GDPR compared to the previous regime is the threat of potentially huge fines for breaches, going up to €20,000,000 or 4% of your global turnover, whichever is higher.

In this article we will go into how GDPR is enforced, the enforcement actions that can be taken if there is a breach and examples of the two levels of breach, along with the maximum fines possible for each.

Supervisory authorities

GDPR is enforced by supervisory authorities, which are established by national governments within the EU (for example, the Information Commissioner's Office in the UK). If your organization processes the data of data subjects in multiple EU countries, then under Article 56 you will primarily deal with the supervisory authority of the EU country where you have your main establishment:

- Your main establishment is usually the place of central administration in the EU.
- However, for data controllers it may be another location if that is where decisions are made on the means and purposes of processing, and if it has the power to have those decisions implemented.
- For data processors, if they have no central administration, then it will be the location where the main processing activities take place.
- If you have no establishment in the EU but have instead designated a representative within the EU (see our article about who GDPR applies to), then presumably this will count as your main establishment.

Note that your main establishment (and so the relevant supervisory authority) may be different for different sets of data. For example, you may deal with customer data in one country, but employee data in another.

Also note that other supervisory authorities will still be entitled to investigate data protection issues relating to their own countries and residents in those countries.

Enforcement

Under Article 58, supervisory authorities have the power to investigate data protection issues. They can order data controllers and processors to give them access to personal data held and generally provide any information necessary to help them investigate. They can also gain access to premises and equipment, according to the normal legal processes (for example by getting warrants).

If they find that there has been or is likely to be a breach, they have the following powers:

- The power to issue warnings if proposed operations are likely to be in breach.
- The power to issue reprimands if past operations were in breach.
- The power to order data controllers and processors to cooperate with data subjects seeking to exercise their rights over their data.
- The power to order data controllers and processors to bring their operations into compliance with the Regulation within a specified time.
- The power to order data controllers to notify data subjects of a personal data breach.
- The power to impose a limitation or ban on processing, temporarily or permanently.
- The power to order the amendment or deletion of personal data.
- The power to order the suspension of data transfers to a non-EU country or international organization.
- The power to impose fines.

As can be seen from the list above, supervisory authorities have a number of alternatives to issuing fines, including giving reprimands and requiring corrective action. In practice, enforcement policies are likely to vary from country to country.

Supervisory authorities are required (by Article 83) to ensure that any fines they do impose are effective, proportionate and dissuasive. They

should take into account a number of factors when setting the level of the fine, including the nature, gravity and duration of the infringement, any action taken to mitigate the damage, cooperation with the supervisory agency, previous infringements and warnings, and adherence to any national codes of conduct or certification procedures.

Maximum fines are set for lower level breaches and higher-level breaches, which will be explained below. If multiple infringements are found connected to the same or linked processes, the fine is still capped at the maximum for the gravest infringement.

Lower level breaches

For lower level breaches, the maximum fine is €10,000,000 or 2% of your global turnover in the previous financial year, whichever is higher. Some of the main types of breach which fall into this category include:

- Failing to keep adequate records of processing activities.
- Failing to cooperate with a supervisory authority.
- Failing to notify data subjects or a supervisory authority of a personal data breach.
- Failing to take steps to get a parent or guardian's consent or authorization to process the personal data of a child under 16.
- Failing to appoint a representative within the EU (if you are not established in an EU country).
- Failing to appoint a data protection officer (where appropriate).
- Failing to carry out a data protection impact assessment or consult with the supervisory authority (where appropriate).
- Data processors acting outside of the scope of documented instructions from data controllers.
- Data controllers engaging data processors without the appropriate safeguards in the contract, or without getting sufficient guarantees that they can and will process the data according to GDPR.

Higher level breaches

For higher level breaches, the maximum fine is €20,000,000 or 4% of your global turnover in the previous financial year, whichever is higher. Some of the main types of breach which fall into this category include:

- Processing personal data without a lawful ground, such as by failing to obtain adequate consent.
- Collecting data beyond the minimum level needed, or keeping it for longer than necessary, for the explicit and legitimate

purposes of the processing.

- Failing to keep adequate records of data protection processes.
- Failing to cooperate with data subjects seeking to exercise their rights over their data.
- Transferring data to a country outside of the EU or to an international organization without the appropriate safeguards.
- Failing to comply with the order of a supervisory authority.

The maximums go to show how high the stakes are for data controllers and processors. In addition, Article 82 also specifically states that data subjects have a right to be compensated by data controllers and processors for damage caused as a result of breaches of GDPR.

It is hard to know how far these astronomical fines will be imposed in practice. Supervisory authorities may well tend to stick to low level fines and their other enforcement powers. However, it is also possible that they will look to make an example of organizations which display serious breaches by imposing punitive fines.

The best way to prevent this happening to your organization is to avoid the kind of situation where any enforcement action is necessary. To do this, you will need to understand the main obligations under GDPR and what you need to do about them. We will start going into depth about these obligations in the next chapter.

CHAPTER 4

What Are The Grounds For Processing Personal Data Under GDPR?

What are the Grounds for Processing Personal Data under GDPR?

As we have seen, GDPR is the new law governing the processing of personal data, which came into force on May 25, 2018. One of its core requirements (in Article 5) is that all personal data must be processed lawfully, fairly and transparently.

In Article 6, it is specified that processing (including collection) is only lawful if one of the following lawful grounds applies:

1. The data subject has given their consent to the processing.
2. The processing is necessary for the performance of a contract you have with the data subject, or to take steps requested by them in the lead up to entering a contract (such as preparing a quote).
3. The processing is necessary to comply with a legal obligation.
4. The processing is necessary to protect the data subject's (or another person's) vital interests.
5. The processing is necessary to perform a task in the public interest or in exercise of official authority.
6. The processing is necessary to protect the organization's (or a third party's) legitimate interests.

For the grounds other than consent, the processing must be necessary for that purpose. This means that if you could reasonably achieve the task (performance of a contract etc) without processing personal data, the lawful ground will not apply.

You should determine what the lawful basis for processing will be ahead of time and notify the data subject of it. When processing data under a different ground from the one for which it was originally collected, you will need to check that the new purpose is compatible with the original purpose (unless the new ground is consent or legal obligation). To do so, you will need to take into account:

1. Any link between the old and new

purposes.
2. The context in which the data was collected, such as the relationship between the parties.
3. The nature of the data.
4. The possible consequences of the further processing for the data subjects.
5. The existence of safeguards to protect the data subjects.

Finally, note that for both special categories of data (along with criminal convictions and offences) and automated decision-making, the requirements are stricter – we will consider these towards the end of this article. First, we will look at the basic grounds in a bit more detail.

The six grounds

Consent

This ground is more complicated than it may sound, as there are various requirements about the quality of the consent. It is certainly not acceptable to assume that by providing their personal data, a data subject has therefore consented to you using it in whatever way you see fit. We will look in detail at the requirements to establish valid consent in the next article.

Performance of a contract or preliminary steps

In order for the second ground to hold, one of the following must apply:

- You have entered into a contract with the data subject. In this case processing is valid if it is that necessary in order to perform this contract.
- The data subject has requested that you take steps (such as providing a quote) prior to entering into such a contract. In this case processing is valid if it is necessary in order to take those steps.

Take care when relying on this ground, as it will only cover types of information and processing which are genuinely necessary for these purposes. For example, say that you require people to provide contact details when they purchase goods or services from you. This is likely to be legitimate to the extent that you may need an address to deliver goods, and you may need to contact them about their order. However, this does not mean that it will be legitimate to use these details for research into your customers' purchasing habits (which will not be necessary to the contract in question).

Legal obligation

It may be that you are required by EU or national law to collect certain data, or process it in a

KEY POINT

A contractual obligation is not enough to satisfy this requirement. Also note that as written, this does not cover the laws of countries outside of the EU.

certain way. If this is the case, then it is lawful to do so under GDPR.

Vital interests

This is an extremely narrow ground which will only cover processing necessary to protect an interest "essential to the life of" the data subject or another person. Examples could include certain crime prevention or humanitarian operations. Note that special categories of data cannot be processed under this ground if the data subject is capable of consent (even if they refuse).

Public interest or official authority

This will cover public authorities (such as the government or emergency services) and organizations to which official tasks are delegated. This processing has to be authorized by EU or national law, so it is not generally available to organizations to argue that they are covered as their activities are "in the public interest". Note that data subjects have the right to object to processing carried out under this ground, under Article 21.

Legitimate interests

This is a potentially quite flexible category, catching a number of processing activities which are not necessary to the performance of a specific contract, but are nonetheless vitally important to running most types of business.

The nature of these legitimate interests is not spelled out in the text of GDPR. However the explanatory notes provide some guidance. A crucial consideration is the reasonable expectations of data subjects when their data is collected. This will be assessed in light of their relationship to the data controller.

The guidance notes also give the following potential legitimate interests which may justify processing:

- Direct marketing.

- The prevention of fraud.
- Ensuring network and data security.
- The administrative transfer of data between organizations within a group.

What is clear from the text is that these legitimate interests only give a lawful ground if they are not overridden by the interests, rights and freedoms of the data subjects. As such, a balancing act must take place.

Also note that data subjects have the right to object to processing under this ground, under Article 21. If they do so, such processing must stop unless the data controller can demonstrate compelling legitimate grounds for the processing which override the data subject's rights. If data subjects object to processing for direct marketing (including profiling for this purpose), then you cannot refuse to stop the processing.

The grounds in practice

The "vital interests" and "official authority" grounds are unlikely to have much impact on the operations of most commercial organizations, most of the time.

Of the other grounds, consent is the broadest, allowing you to catch anything not otherwise covered. You can refer to the next article for details on how to make sure that the consent collected is sufficient to make processing lawful.

However, consent can be refused, or it can be withdrawn at any time. The other grounds can therefore allow you to ensure that you are able to collect and process the data you need in order to perform a contract, comply with any legal obligations, and otherwise pursue your legitimate interests (although remember that data subjects can object to this last type of processing).

To see how this might work in practice, the following is likely to be the best approach when entering into a contract with a client (for example through an online submission form):

- Only require them to supply information that satisfies a non-consent ground (for example, data that will genuinely be necessary for the performance of the contract or for your legitimate interests, or which you are required to collect by law).
- Clearly ask for consent to take any other data and to use the collected data for any other purpose.
- If a customer or other data subject refuses to give this consent, and provides only the information required, you will have to exclude this data from any other types of

processing. To do this, you will probably need to flag the different sets of data according the processing permitted for each.

Special categories of data

In Article 9, there are stricter rules for processing the following special categories of personal data:

- Racial or ethnic origin.
- Sexual orientation.
- Political opinions.
- Religious or philosophical beliefs.
- Trade union membership.
- Genetic data.
- Biometric data.
- Health data.
- Information about a person's sex life.

For these categories, you will still need to have one of the six grounds considered above. However, you will also need one of the following grounds for processing (although there is considerable overlap):

- The data subject has given their explicit consent to the processing.
- The processing is necessary to protect the data subject's (or another person's) vital interests, and the data subject is incapable of giving consent.
- The processing is carried out by a not-for-profit organization, in the course of its legitimate activities and with appropriate safeguards. The processing must only relate to its members or former members, or people regularly in contact with it, and it must not disclose the data externally without consent.
- The processing is of personal data manifestly made public by the data subject.
- The processing is necessary to establish or exercise legal claims or defenses, or is by courts in their judicial capacity.

Alternatively, there are other potential grounds which will first have to be established by specific EU or national laws before they can be relied on:

- The processing is in the field of employment, social security or social protection.
- The processing is necessary for reasons of substantial public interest.
- The processing is necessary for medical purposes.
- The processing is necessary for public health purposes.
- The processing is necessary for archiving purposes.

Of this second category, the most important one for most organizations is likely to be the one covering employment, as governments attempt

to strike a balance between employee rights over their data and the needs of employers to keep full HR records.

If collection and processing of this information is necessary to your organization, it will be important for you to check that one or more of the above grounds applies, as well as one of the original six.

Comparing these to the standard list of six grounds, consent will still justify the processing of special category data (as long as it is explicit), as will a person's vital interests (if the data subject is unable to consent) and most cases of legal obligations and official authority. However, neither the performance of a contract nor an organization's legitimate interests will be enough by itself.

Note that while information about criminal convictions and offenses is not a special category, Article 10 states that it should only be processed under the control of official authority or where specifically authorized by law.

Automated decision-making

In Article 22, there are also stricter rules where decisions are made based solely on automated processing (including profiling). This is only justified under one of the following grounds:

- The processing is necessary to enter into or perform a contract with the data subject.
- The processing is authorized by EU or national law.
- The data subject has given their explicit consent to the processing.

You will need to implement measures to safeguard the data subject's rights, freedoms and legitimate interests. In practice, the biggest difference between these grounds and the standard six grounds is that legitimate interests are not enough to justify this processing.

Note that these decisions may only be based on the special categories of data (above) if the data subject has given explicit consent, or if it is authorized by law and necessary for reasons of substantial public interest.

Conclusion

Getting familiar with the various lawful grounds is a vital part of preparation for, and compliance with, GDPR. You will need to document the grounds under which processing is done (along with the additional grounds for special categories of data) and communicate this to data subjects.

A number of your processing operations are likely to be covered by performance of a contract (or preliminary steps), legal obligations or your legitimate interests. However, outside of these categories you will need to get the consent of data subjects to processing. That is the next area we will cover.

CHAPTER 5

What Are GDPR's Rules On Consent?

What are GDPR's Rules on Consent?

GDPR is the new law governing the processing of personal data. As we looked at previously, the collection and processing of personal data will only be permitted if it is justified under a lawful ground.

KEY POINT

Of the six lawful grounds, the widest-ranging is that the data subject has given their consent to the processing.

However, GDPR has relatively strict requirements to establish that sufficient consent has been given (in Article 7). In this article, we will review the main principles.

Consent must be clear

Your request for consent should be clear, unambiguous and set out in plain language. It should be clearly distinguished from other matters, and data subjects should be given a separate opportunity to consent or refuse consent rather than it being, for example, buried as a clause in a contract. Where appropriate, separate consent should be requested for different processing operations (such as where they are for notably different purposes).

Ticking boxes, choosing settings or clearly indicating consent through statements or conduct will be fine. However, pre-ticked boxes, silence or inactivity cannot be taken as consent.

Consent must be informed

In order for consent to be informed, you must at the time of obtaining consent make sure that data subjects know at least the identity of the data controller (including any third-party data controllers) and the purpose(s) for which the data will be processed (e.g., sending marketing emails or undertaking market research).

Note that there is a general requirement to provide a broader range of information to data

subjects when their data is collected or otherwise received, which applies whether or not you are relying on the consent ground. The items above are the ones specifically indicated in the text of GDPR qualifying consent as being informed. We will look at the broader requirements in the next article.

Data subjects must also be told of their right to withdraw consent (see below).

Consent must be freely given

Consent is unlikely to be seen as freely given where there is a significant power imbalance between parties. GDPR specifically suggests that there is likely to be an imbalance between individuals and public authorities. Similarly, consent to an employer processing their employees' data is unlikely to be considered to be freely given. As a result, it will be better for HR data to be processed under a different ground.

More generally, consent will not be free if the data subject is unable to refuse or withdraw consent without suffering detriment. This would appear to rule out, for example, incentive schemes for giving consent.

GDPR makes clear that consent is unlikely to be free if it is required as a condition of entering a contract. This means that to the extent that collecting and processing the personal data of customers really is vital (whether to performing the contract or to your other operations), it will be better to operate under a different ground.

Consent must be recorded

As with most measures under GDPR, you will need to record the steps you have taken and be able to demonstrate compliance. In practice, this will mean keeping details of exactly what consent has been given with your client records. It also means that you should be very wary of getting consent entirely verbally – instead, make sure that it is backed up in writing.

Consent for children

In Article 8, there are specific requirements for consent to be valid where a service is offered online to an individual under 16 years old (although EU countries may legislate to reduce that age to a minimum of 13). In these cases, consent must be given or authorized by the holder of parental responsibility over the child.

It is your responsibility to take "reasonable steps" to verify that this has happened, given the technology available. You will need to think about children who might use your services and decide the best way to ensure that they get permission before providing their consent.

Withdrawing consent

Data subjects have a right to withdraw their

consent at any time. They should be informed of this right before giving consent, and the withdrawal should be as easy as giving consent.

It is worth giving some thought to what you will need to do if consent is withdrawn. You will need to make a clear note on your client records, and also bring to a halt any processing in progress.

"Explicit" consent

There are three situations in which GDPR states that consent must be "explicit" in order to justify processing. Two were mentioned in the previous article: in the case of special categories of data, and when the processing involves automated decision-making. The third is when the processing involves transfers of data to a country outside of the EU, or to an international organization.

It is unclear how far this goes beyond the normal consent requirements. What is clear is that the requirement to spell out what you will do with the data and to make clear that it is a free choice is heightened in these cases. The general recommendation appears to be to get this kind of consent in writing, with a handwritten signature.

If the requirements for consent appear onerous, always remember that the other lawful grounds are available instead. For some business models, you may not need to rely on consent at all.

By following the guidelines in this and the previous article, you can ensure that you have a lawful ground, and that your processing starts off lawful. However, this is not enough on its own — you will also need to show that the way you go on to process the data satisfies GDPR. That is what we will consider next.

CHAPTER 6

What Are The Rules on Processing Data Under GDPR?

What are the Rules on Processing Data under GDPR?

GDPR is fundamentally a new framework for processing personal data. We have previously looked in detail at the lawful grounds for processing data (including consent). But as well as having a lawful basis, the processing must also be carried out properly and securely.

The Regulation sets out a number of principles governing the collection and use of personal data, following the overall philosophy of "data protection by design and by default". The main principles (in Articles 5 unless otherwise stated) are as follow:

You must keep data subjects informed

GDPR sets out (at Article 13) a number of pieces of information which must be provided to data subjects when their personal data is collected. Note that this applies even if you will not be relying on their consent. The information provided must include:

- The data controller's identity and contact details (as well as those of any data protection officer and/or EU representative).
- The purposes and lawful grounds of the processing (and where legitimate interests are relied upon, what they are).
- Who else (if anyone) the data will be transferred to. If you plan to transfer the data to a non-EU country or an international organization, you must also include the grounds relied upon to justify this (which we will look at in a later article).
- The period for which the data will be stored (or how this period will be determined).
- The data subject's rights to access their data, have it rectified, erased or transferred, or restrict or object to processing (all of which will be considered in the next article).
- The data subject's right to withdraw consent (if consent is relied upon).
- The data subject's right to complain about processing to a supervisory authority (see our article on penalties).

- Whether the data subject is required to provide the information, including if it is a legal or contractual requirement, and any consequences of failing to provide it.
- Whether the data will be used for any automated processing (including profiling) and if so, the logic of the processing and its significance and consequences for the data subject.

You do not need to provide information which the data subject already has. Where you intend to process the data for purposes other than those for which it was originally collected, you must update data subjects with the new purposes, and restate the information listed above.

Clearly, it will be possible to set out most of the above in a standard privacy notice, although some of it will vary with the circumstances of collection. The information must be given in a manner which is clear, concise, intelligible and easily accessible.

Second-hand data

Similar requirements apply if you obtain personal data other than directly from data subjects (under Article 14). In this case, you must usually contact data subjects to provide the above information, as well as:

- The categories of personal data received.
- The source of the data (including if it is from publicly accessible sources).

You must do so within a reasonable period, and in any case by the earliest of (i) your first communication with them, (ii) any further transfer to another party or (iii) a month after receipt of the data.

There are exceptions where the data subject already has the information, where providing the information would be impossible or involve disproportionate effort, and where EU or national law otherwise permits.

You must keep the minimum data necessary

You should collect and keep only the data necessary for the specified purposes of the processing. You will need to think through each piece of data you collect and consider how it contributes to your goals.

There is an overlap between this and the lawful grounds, most of which only justify processing which is necessary (to the performance of a contract, for your legitimate interests etc.). However, this requirement makes clear that even if you have consent to processing, you will still need to think about whether each piece of data collected is necessary for the stated purposes.

You need not be certain that every piece of data will in fact be used, but you should be able to show that there is at least a reasonable chance that they will be necessary. For example, you may only need to collect phone numbers in order to contact clients if there is an issue with their order or account. Although you will not actually use the vast majority of the numbers you collect, it is still likely to be considered necessary data.

You must keep the data accurate

Personal data which you collect, and use should be kept accurate and up to date. This means that you need to take all reasonable steps to correct or delete any inaccurate data.

As we saw above, there is an obligation to inform data subjects of their right to have their data rectified. However, this principle will in some cases go further, requiring a proactive approach to correcting your data. In any case, you should make it easy for them to update their data, and you should process any updates speedily.

The nature of "reasonable steps" will depend on the nature of the processing. If it takes place some time after the data was initially collected, then the risk of inaccuracy increases, and it may be proper to check with data subjects that the information is still correct. This is especially true if the processing will have a significant impact on their freedoms, rights and responsibilities.

> The reasonable steps has not been clearly defined and it would be smart to pay attention to court rulings, lawyers, and thought pieces that come out in the coming months as this gets scoped.

As another example, say that you are an online vendor, and a client with an existing account makes a purchase. It would probably count as a reasonable step (and would certainly be good practice) to remind the client of the delivery address and payment details you have on record and give them an opportunity to amend them before purchase, to avoid problems completing the order.

You must delete data which is no longer needed

As a complement to the principle of keeping no more data than needed, you should also keep data for no longer than necessary for the specified processing purposes.

Again, this will depend on the nature of the processing and your relationship with the data subjects. If they are ongoing clients, then there is unlikely to be an issue with keeping their relevant

KEY POINT

One way to show compliance with this requirement (in appropriate situations) would be to implement a deletion policy for lapsed clients or users. After a set length of time without contact (which will depend on the nature of your relationship and your organization), you could email them to ask if they would like to stay on your records. If you do not get a positive response within a reasonable time, you would then delete their personal data.

details. Do consider whether you actually need to keep, for example, previous addresses and contact details, as they are unlikely to be needed anymore.

There will of course be other legal requirements governing the need to keep certain types of data, for example financial data for tax purposes. These will feed in to how long you need to keep the data for GDPR purposes.

There is an exception to this requirement for archiving in the public interest, for historical or scientific research or statistical purposes. Note that if the data is stripped of identifying information, leaving only non-identifying (e.g. aggregate demographic) data, this is no longer a concern.

You must keep data secure

It is a core requirement of GDPR that you must keep all personal data secure. This includes protecting it against unauthorized and unlawful processing and accidental loss, using "appropriate technical and organizational measures".

What is appropriate will depend on the nature, scope, context and purposes of processing, as well as the costs of implementation and what is in fact possible. Particular thought should be given to the risks should a breach occur. Article 32 spells out a number of possible steps which could be taken to keep data secure:

- Encryption and pseudonymization of data.
- Backing up data, and being able to restore from backup in a timely manner.
- Regular testing, assessment and evaluation

of your processes.

In terms of unauthorized processing, you should consider not just illegal access from outside of your organization, but also rogue employees and agents who may steal, sell or tamper with data to which they have access. To keep these risks to a minimum, you should look to restrict access to personal data to individuals who actually need it, rather than keeping it in a shared space available to all. It may also be wise to put in place measures to record access to and use of data even for authorized individuals.

You must build data protection into your processes

Underlying all of the above is the principle (in Article 25) of "data protection by design and by default". This means that data controllers should design their processes with data protection in mind from the beginning (rather than attempting to bolt it on afterwards).

In practice, this means going through and rewriting your processes (or creating them if they do not yet exist) with principles like data security, data accuracy and data minimization firmly in mind. It also means making sure that these apply by default, rather than requiring specific action in each case.

You must keep records

Finally, a recurring theme throughout GDPR is the importance of keeping records (Article 30). Organizations must generally keep records of the processing activities for which they are responsible, the categories of data subjects involved and the measures taken to demonstrate compliance with the above principles (as well as the other principles discussed in this series). You will need written policies explaining how you implement these principles, and what to do if things go wrong.

Technically, the general obligation to keep records does not apply to organizations which employ fewer than 250 people, unless the processing (i) is more than occasional, (ii) is likely to involve a risk to the rights and freedoms of data subjects or (iii) involves special categories of data or data about criminal offences and convictions (see our article on lawful grounds for processing).

However, the Regulation's other obligations affect everyone, the burden of proof will always be on you to demonstrate compliance, and documentation will often be the only way to do so. Therefore, rather than leaving it and trying to deal with data protection issues only when they become a problem, it is well worth taking the time to get your policies and records in place first.

Now that we have gone through some of the general principles which govern the processing

of personal data, we will look at some specific areas: firstly the rights of data subjects over their data, and secondly the steps which need to be taken if a breach occurs.

CHAPTER 7

What Are The Rights of Data Subjects Under GDPR?

What are the Rights of Data Subjects under GDPR?

GDPR regulates the processing of personal data. One of the ways it does this is by restating and increasing the rights of data subjects, including the rights to access their data, to have it amended or deleted, and to have processing halted.

In this article we will go through these rights, and what you will need to do if they are exercised.

Right to access data (Article 15)

A data subject has the right to request and receive confirmation of whether you hold their personal data. If you do, they have the right to request and receive a copy of the data you hold, as well the following information:

- The purpose(s) of the processing.
- The categories of personal data held.
- Who else (if anyone) the data will be transferred to. If you plan to transfer the data to a non-EU country or an international organization, you must also include the grounds relied upon to justify this (which we will look at in a later article).
- The period for which the data will be stored (or how this period will be determined).
- The data subject's rights to have their data rectified, erased or transferred, or restrict or object to processing.
- The data subject's right to complain about processing to a supervisory authority (see our article on penalties).
- The source of the data (where it was not received from the data subject).
- Whether the data will be used for any automated processing (including profiling) and if so, the logic of the processing and its significance and consequences for the data subject.

As you may have noticed, this list largely replicates the list of information you must provide upon obtaining the data (considered in the previous article). Unless any of this information has changed, it may well be enough to send them a further copy of the original privacy notice along with their data.

The exercise of this right should not be allowed to adversely affect the rights and freedoms of others. In particular, this may mean redacting any personal data of other data subjects which would otherwise be included in the data copy.

Where possible, you should provide data subjects with secure access to their data through a remote self-service system. If you process a large amount of information about the data subject, you are entitled to ask them to be more specific about what they are looking for.

Right to have data transferred (Article 20)

Where the personal data is processed on the ground of consent, and by automated means, the data subject has the following rights (above and beyond the standard right to access):

- The right to receive the data they have provided in a structured, commonly-used and machine readable format.
- The right to transmit this data to another controller without hindrance.
- The right, where technically feasible, to have this data transmitted directly from one controller to the other.

The clearest case where this will be applicable is where the data subject is looking to switch from one service provider to another. This essentially requires the old provider to make the switch as easy as possible for the data subject, including transmitting data directly where appropriate.

This right does not apply to processing necessary to perform a task in the public interest or in exercise of official authority. As with the right of access, it should not be allowed to adversely affect the rights and freedoms of others.

Right to have data rectified (Article 16)

A data subject has the right to have their personal data amended where it is inaccurate or added to where it is incomplete. The Regulation specifically mentions that it should be possible to accept and record a supplementary statement (for example, an explanation that a piece of data you hold does not have the implications it normally would).

As mentioned in the previous article, there is a wider obligation to keep your records accurate and up to date, which may include taking proactive steps even where the data subject has not exercised their right to rectify. In any case, you should make it easy for them to update their data, and you should process any updates speedily.

In some cases it may be appropriate to require evidence before rectifying data. For example, where the data subject does not have the right

to have their data erased on request (see below), they could seek to achieve the same end by providing inaccurate "updated" data. Of course, any such obstacle to the exercise of the right will need to be kept to the minimum necessary to achieve this purpose.

Right to object to processing (Article 21)

A data subject has the right to object to the processing of their personal data, and have it stopped, if it is on the ground of necessity for the data controller's legitimate interests, or necessity for performance of a task in the public interest or in exercise of official authority (see our article on lawful grounds).

This right therefore functions in a similar way to the withdrawal of consent (for processing based on consent). However, in this case the data subject should give a reason for the objection, based on their particular situation.

Also, unlike with the withdrawal of consent, the data controller has an opportunity to dispel the objection by demonstrating compelling grounds for the processing which override the data subject's interests, rights and freedoms.

However, the Regulation explicitly states that there is no defense to an objection to direct marketing. Since this kind of processing will almost inevitably be based on either legitimate interests or consent, data subjects essentially have an absolute right to halt direct marketing.

Right to have data erased – "right to be forgotten" (Article 17)

A data subject has the right to request that you erase some or all of the personal data you hold about them. You are then obliged to do so, but only if one of the following applies:

- The data is no longer needed for the purposes for which it was received or processed.
- The processing was based on consent, and the data subject withdraws that consent.
- The data subject successfully exercises the right to object (see above).
- The data has been unlawfully processed.
- EU or national law requires that the data be erased.
- The data was collected in relation to the offer of services online to a child (that is, in circumstances where consent would require parental consent authorization).

These grounds will cover many circumstances, although notably it will usually not affect data processed as necessary for the performance of a contract with the data subject. In addition, even if one of the above applies, you are not obliged to erase the data if:

- The processing is necessary for exercising freedom of expression or information.
- The processing is necessary for compliance with a legal obligation.
- The processing is necessary to perform a task in the public interest or in exercise of official authority.
- The processing is necessary for medical or public health purposes.
- The processing is necessary for archiving in the public interest, for historical or scientific research or statistical purposes.
- The processing is necessary to establish or exercise legal claims or defenses.

Where the data controller has made the data public and this right applies, they must also take reasonable steps to inform other controllers working on the data that they should likewise delete it.

Right to restrict processing (Article 18)

In certain circumstances, a data subject has another, more short term right to prevent data controllers and processors from processing their personal data (with some exceptions). They have this right where:

- The data subject contests the accuracy of data held, while the data is verified.
- The processing is unlawful, but the data subject does not want the data erased.
- The data controller no longer needs the data, but the data subject needs it in order to establish or exercise legal claims or defences.
- The data subject has exercised the right to object (see above), while it is being determined whether the data controller's legitimate interests override this right.

If any of these apply, then all processing on the data (other than storage) must stop, except to the extent that it further processing is by consent or done in order to establish or exercise legal claims or defenses, to protect the rights of others or for reasons of important public interest. Once a restriction has been put in place, you must let the data subject know before it is lifted.

In most cases, data subjects will prefer to exercise the right to object or the right to be forgotten, with this acting only as a supplement to those rights.

General points

- Where a right is exercised, you should act without undue delay and within a month of the right being exercised. You can extend that by up to two months where necessary, although you will have to let the data subject know that you are doing so within

a month.

- Any communication with data subjects as a result of the exercise of these rights must be clear, concise and intelligible. Where a request is made electronically, information should be provided in the same manner where possible. In other cases, it can be electronic, written or even oral (but only when requested).
- Where the data controller has reasonable doubts about the identity of the individual making the request, they may require further information as proof. Wherever information is requested to be given orally, the data controller must have evidence of the identity of the person asking before providing it.
- Any action should usually be taken free of charge. However, you are entitled either to charge a reasonable fee or refuse to act on a request where it is clearly unfounded or excessive (particularly if it is repetitive). In such a case, the burden will be on you to show that this is the case if, for example, the data subject complains to the supervisory authority.
- If you do not act within the required timescale, whether in error or because you believe the request to be unfounded or excessive, you must explain this to the data subject and let them know of their rights to complain to a supervisory authority or to take the matter to court.
- EU or national law may create further restrictions on the rights of data subjects on a number of public interest grounds.

Clearly, you will need to have policies in place considering how you will deal with any of these requests, to ensure that you are able to do everything required in the appropriate timescales. However, most of these rights are not entirely new, and in many cases, compliance should not be too onerous.

Next, we will look at a situation rather more worrying than receiving a request from a data subject – discovering that the data you hold has been breached. We will look at the obligations GDPR requires of you in these situations.

CHAPTER 8

What Are GDPR's Rules on Data Breaches?

What are GDPR's Rules on Data Breaches?

GDPR's rules on processing personal data are designed to help keep it secure and minimize the risks of data being lost or stolen. However, even with the best security protocols, data breaches do sometimes happen. In these cases, GDPR has rules governing what you need to do next.

Data breaches include any access to, or destruction, loss, alteration or disclosure of personal data which is accidental, unauthorized or otherwise unlawful. In these cases, there are two main duties.

Duty to notify the supervisory authority

As discussed in our article on penalties, supervisory authorities are bodies set up by national governments to monitor and enforce data protection and security. You will usually deal with the supervisory authority of the EU country where you have your main establishment.

KEY POINT

When a data breach occurs, under Article 33 a data processor must inform the data controller without undue delay. The data controller must then report it to the supervisory authority without undue delay, and in any case within 72 hours of becoming aware.

This report must include the following:

- The nature of the breach.
- The categories of personal data, the number of records, and the categories and number of data subjects affected.
- The name and contact details of the data protection officer or other point of contact regarding the breach.
- The likely consequences of the breach.
- The measures taken or proposed to

mitigate the effects of the breach.

Where it is not possible to give all of the information immediately, it can be provided later, after the initial notification of the breach. All of this information must also be documented internally.

There is an exception to this duty where the breach is "unlikely to result in a risk to the rights and freedoms of natural persons". Note that this is a wider category than just the data subjects themselves, as the personal data may also include information on other individuals.

This exception is likely to apply to purely administrative errors which do not lead to unauthorized people getting access to the data, and which can be remedied in a timely fashion: for example, accidental deletion of data which can be restored from backup. Even in these cases the breach should be documented so that you can demonstrate if necessary that you were correct that the duty to notify did not apply.

Duty to notify data subjects

There is a second duty (under Article 34) in cases where a data breach occurs and is likely to cause "a high risk to the rights and freedoms of natural persons". In these circumstances, as well as telling the supervisory authority, the data controller must also without undue delay inform the data subjects whose personal data has been (or may have been) affected.

This report must be in clear and plain language, and include at least the following information:

- The name and contact details of the data protection officer or other point of contact regarding the breach.
- The likely consequences of the breach.
- The measures taken or proposed to mitigate the effects of the breach.

There are a number of exceptions to this duty. The first is where the personal data has been properly protected, particularly through encryption or similar methods (although this is likely to mean that there is not a high risk in the first place). The second is where measures taken after the fact mean that there is no longer a high risk.

The third is where notification would involve disproportionate effort (for example, where contact details of data subjects are not stored). In these cases, a public communication or similar measure must be used to ensure that data subjects are in fact informed of the issue.

Whether there is a high risk is a matter of judgement for data controllers. It is likely to be the case wherever an external party has gained

access to the data (unless it is encrypted or otherwise unintelligible). It is less likely to be the case where the breach is accidental or involves access which is unauthorized only in a technical sense (for example by employees or agents who have not followed procedures, where such access does not appear suspicious).

If in doubt, it should be possible to ask for the supervisory authority's opinion when referring the matter to them. They also have the power to order data controllers to notify data subjects where they have not done so voluntarily.

Duty to mitigate the harm?

Given this, it would be extremely unwise to rely on the lack of a clear duty. You should take all reasonable steps to reduce the harm caused by a breach at the same time as notifying the supervisory authority and the data subjects as required.

The relatively tight timescales and the emphasis on acting in a timely manner emphasize the importance of having workable procedures in place to deal with any data breaches which occur. It also requires good communication between data controllers and data processors. In the next article we will look at this relationship in more detail.

GDPR contains no explicit duty to take steps to mitigate the harm caused by a data breach. However, such a duty is implied throughout the Regulation:

- The requirement to take appropriate measures to ensure data security could be interpreted as including a duty to take steps after a breach.
- Both of the duties to notify discussed above require you to set out the steps taken or proposed to be taken to mitigate the harm caused by breaches.
- Action taken to mitigate the harm is a factor supervisory authority takes into account when deciding whether to impose fines and what the level of fines should be.

CHAPTER 9

What Does GDPR Require in Data Processing Agreements?

What does GDPR Require in Data Processing Agreements?

GDPR regulates the processing of personal data by imposing obligations on two types of organizations - data controllers and data processors. Data controllers set the agenda for processing, while data processors act on the instructions of data controllers.

As well as regulating the activities of each of them (as detailed throughout this series), the Regulation also sets requirements for the relationship between them (in Article 28), including what the processing contract must contain. This article will look at these requirements in detail.

Suitable data processors

Data controllers must only use data processors who can give "sufficient guarantees" that they can and will comply with the requirements of the Regulation and protect the rights of data subjects.

This means being able to show that they have the knowledge, resources and reliability to do so (rather than just being about contractual guarantees). If and when appropriate certification schemes are created, relying on these is likely to be justified.

Processing under authority

Data processors must only ever process data under the data controller's documented instructions, unless required to do otherwise by EU or national law (Article 29). As well as being a violation in itself, straying outside of these instructions may cause them to be redefined as data controllers and therefore subject to additional rules.

Data processing agreements

All processing must be under a contract between controller and processor (or some "other legal act" recognized by EU or national law which binds the processor to the controller's will). There are a number of things which must be contained in this contract:

- The subject matter, duration, nature and purpose of the processing.
- The types of personal data and categories of data subject involved.
- The subject matter, duration, nature and purpose of the processing. The types of personal data and categories of data subject involved.
- A requirement that the processor act only under the controller's documented instructions (unless required by EU or national law).
- A requirement that all people permitted to process the data have committed themselves to confidentiality or are otherwise under an appropriate legal obligation of confidentiality.
- A requirement that the processor take "appropriate technical and organizational measures" to keep the data secure.
- The requirements set out in the next section regarding the processor passing the work on to another processor
- Requirements that the processor (as far as is reasonable) assists the controller to maintain data security, conduct impact assessments, notify supervisory authorities and data subjects of data breaches, and fulfil requests from data subjects exercising their rights over their data.
- A requirement (depending on the controller's preference) that at the end of the contract the processor either deletes the data or returns it to the controller and deletes all copies (unless required by law to keep them).
- A requirement that the processor assist with audits and inspections and provide the controller with the information necessary to show that the processor has complied with its obligations under the Regulation.

Passing to another data processor

A data processor must not pass the work on to another data processor without either (i) getting specific authority from the data controller or (ii) getting general authority from the data controller, informing them of the proposed change and giving them a chance to object. This must be spelled out in their contract with the controller.

Wherever another data processor is engaged in this way, the contract (or other legal act) must impose the same data protection obligations as the first processor's obligations under its contract with the controller. Again, this must also be required by the original processing agreement.

The original processor must remain liable to the data controller for the performance of the

obligations passed on to the new processor. This will be an extra incentive for them to check the fitness of any such new processor.

A major purpose of all of these rules is to prevent data controllers and processors from attempting to avoid responsibility by passing it on to each other. They clearly set out that data processors must work strictly within their instructions and remain liable even if they lawfully pass the work on to another organization. Meanwhile, data controllers must make sure that they only use fit and proper organizations as data processors and use their contracts to bind the processors contractually (as well as under the Regulation itself).

The next article will look at a few remaining obligations under GDPR which have not fit within any of the areas already covered.

CHAPTER 10

What Else Does GDPR Require?

What Else Does GDPR Require?

GDPR is meant to be a complete code for dealing with personal data. As a result, it's a long document filled with numerous requirements.

In this series of articles we have attempted to go through all of the major areas covered by the Regulation. However, there are a few more which did not quite fit into any of the categories discussed so far, and so we will review them here.

Joint controllers (Article 26)

The Regulation provides for the situation where multiple data controllers work together to determine the means and purposes of processing - in this case they are joint controllers. Data subjects may exercise their rights against and in respect of each of them.

Joint controllers should determine between them their respective responsibilities under the Regulation. The "essence" of this arrangement should be made available to data subjects.

Data protection officers (Articles 37 to 39)

In certain cases, data controllers and data processors are required to designate someone with "expert knowledge" of data protection law as a data protection officer. In all other cases, organizations may decide to do so anyway.

A data protection officer must be appointed where:

- The organization is a public authority or body.
- The organization's core activities involve regular, large scale and systematic monitoring of data subjects.
- The organization's core activities involve large scale processing of special categories of data or data relating to criminal convictions and offenses (as defined in Articles 9 and 10 – see our article on lawful grounds).

The data protection officer's job is to be an independent guide to GDPR and other data protection legislation. In particular, they must advise on and monitor the performance of data protection impact assessments (see below). They will also act as the point of contact for the supervisory authority and data subjects regarding data protection issues.

The data protection officer may be an employee or someone working under a service contract. They must report directly to the organization's highest management level and must be someone to whom the organization and its employees will have easy access. The officer may have other duties but these must not cause a conflict of interests.

If an organization appoints a data protection officer, it must also do the following:

- Ensure that they are involved in all data protection issues.
- Support them in their duties and make sure that they have the necessary resources, training and access to data and processes to do their job properly.
- Refrain from instructing them in how to perform their duties (so that they remain independent) and in particular refrain from penalizing or dismissing them for doing so.
- Ensure that they are bound by confidentiality in the performance of their duties.
- Publish their contact details and communicate them to the supervisory authority.

Impact assessments and consultation (Articles 35 and 36)

Supervisory authorities will start drawing up lists of the kinds of processing activities this covers, but the Regulation makes clear that it will include:

KEY POINT

Before starting any processing which is likely to result in a high risk to people's rights and freedoms, you must carry out a data protection impact assessment.

- Processing which is automated and extensive, and which will have legal (or similarly significant) impacts on people's lives.
- Large scale processing of special categories of data or data relating to criminal convictions and offences.
- Systematic and large-scale monitoring of publicly accessible areas.

At minimum, any appointed data protection officer (see above) should be asked to advise on the impact assessment – in most cases, they are

likely to be tasked with drafting it or supervising the drafting. Where appropriate, you should ask for the views of data subjects on the intended processing. The assessment must include:

- A description of the processing.
- Details of the legitimate interest pursued (where appropriate).
- An assessment of how necessary and proportionate the processing is given its purposes.
- An assessment of the rights and freedoms at risk.
- Details of the proposed measures and safeguards to be implemented to address the risks, protect personal data and demonstrate compliance with the Regulation.

Where the assessment finds that the processing would indeed pose a high risk in the absence of measures and safeguards, you must also consult the supervisory authority before starting. You should provide them with the impact assessment as well as details of the means and purposes of the processing, the proposed measures and safeguards to be implemented, the respective responsibilities of data controllers and processors, the contact details of the data protection officer and any other information requested.

If it believes the intended processing will infringe the Regulation, the supervisory authority will provide written advice, and may issue a warning, prohibit the processing or use any of its other powers (see our article on penalties). It should do this within eight weeks (which can be extended by up to six weeks by notice).

Transfers abroad (Articles 44 to 50)

The Regulation imposes specific requirements wherever personal data is to be transferred outside of the EU or to an international organization (even if it is already held outside of the EU). This is to ensure that the data is only sent to places where it is adequately protected.

Such transfers should only take place where at least one of the following applies:

- The EU has decided that the non-EU country, the specific sector of that country or the international organization ensures adequate protection (an "adequacy decision"). This currently covers countries such as the US (under the Privacy Shield framework), Switzerland, New Zealand and Israel.
- The data controller or processor has put in place appropriate safeguards and data subjects have effective legal remedies to uphold their rights. This is a complex

area and the standards are rigorous, so you should consult with lawyers if you are interested in relying on this.

- The data subject has explicitly consented to the transfer after being informed of the possible risks in the absence of an adequacy decision or appropriate safeguards.
- The transfer is necessary for performance of a contract with the data subject or pre-contractual measures requested by the data subject.
- The transfer is necessary for important reasons of public interest.
- The transfer is necessary to establish or exercise legal claims or defenses.
- The transfer is necessary to protect the data subject's (or another person's) vital interests, and the data subject is incapable of giving consent.
- The transfer is from a public register (where permitted under EU or national law).
- The transfer is necessary to protect the organization's legitimate interests, where these are not overridden by the interests, rights and freedoms of the data subjects. However, see further below.

The legitimate interests' ground is further constrained by the following requirements: (i) the transfer must not be repetitive and concern only a limited number of data subjects, (ii) the transferring organization must have assessed the circumstances and put in place suitable safeguards, and (iii) the data controller must inform the supervisory authority and data subjects of the transfer, explaining the compelling legitimate interests in question.

Further information on some of these requirements (explicit consent, performance of a contract, vital interests and legitimate interests) can be found in our article on lawful grounds for processing.

Certification and codes of conduct (Articles 40 to 43)

The Regulation encourages and expects regulatory bodies and other associations to create data protection codes of conduct and certification procedures. Hopefully, these will flesh out some of the vaguer parts of the Regulation, although there is a risk that it will lead to substantial differences in different EU countries.

Once they are in place, certification and adherence to codes will go a good way towards demonstrating compliance with the Regulation, but they will still only act as guides. Attempts to comply with codes only in a technical sense while violating the spirit of the Regulation are unlikely

to endear organizations to supervisory bodies.

Having gone through the miscellaneous provisions above, we have now covered all of GDPR's main requirements.

Glossary

Data breach

Any access to, or destruction, loss, alteration or disclosure of personal data which is accidental, unauthorized or otherwise unlawful.

Data controller

A person or organization which decides on the purposes and methods of processing personal data – they coordinate processing.

Data subject

An identifiable individual about whom personal data is held.

Data processor

A person or organization which processes personal data based on the instructions of data controllers. This could for example include subcontractors.

Establishment in the EU

Having any kind of presence in an EU country such as a branch, representative, address or bank account.

Legitimate interests

Activities of vital importance to the running of a company. Where processing is necessary for your legitimate interests, this can in some cases act as a lawful ground for doing so, but only where they are not overridden by the interests, rights and freedoms of the data subjects.

A crucial consideration is the reasonable expectations of data subjects when their data is collected. This will be assessed in light of their relationship to the data controller. Examples of possible legitimate interests include:

- Direct marketing.
- The prevention of fraud.
- Ensuring network and data security.
- The administrative transfer of data between organizations within a group.

Personal data

Any information relating to a data subject. This could for example include names, addresses, contact details, online usernames or demographic data.

Special categories of personal data

There are stricter rules for processing certain types of sensitive data:

- Racial or ethnic origin
- Sexual orientation
- Political opinions
- Religious or philosophical beliefs
- Trade union membership
- Genetic data

- Biometric data
- Health data
- Information about a person's sex life

Note that while information about criminal convictions and offences is not a special category, it should only be processed under official authority or where specifically authorized by law.

Supervisory Authority

A body established by an EU country to enforce data protection rules. For example, the Information Commissioner's Office in the UK.

Learn more at **www.truevault.com**

or follow **@TrueVault**.