TermsFeed

GDPR

for Business

Table of Contents

Preface

This book was conceived as a tool for those striving for GDPR compliance. While the GDPR is undoubtedly an important and necessary step for the privacy and fairness in our modern age, it has also proven to be a burden on those who desire to abide by these stringent new rules.

The goal of this ebook is to pass on the knowledge, opinions, and interpretations of experts who have been studying and investigating the GDPR since its conception. While we seek the best and most up-to-date interpretations of this new set of laws, it is possible that some of the interpretations and assumptions presented in this ebook are not the same as what was intended by the creators of the GDPR or are no longer the best interpretations in light of new supplements and clarifications released.

While this ebook is undoubtedly full of useful information, examples, guides, and checklists to assist you on your path towards GDPR compliance, we cannot guarantee its accuracy in every aspect, especially as the GDPR continues to change and receive additional clarification. Every attempt was made to call out sections where a clear, general consensus is not currently available or interpretations vary, but our best interpretations are provided with a deep level of understanding in the theory, application, and actual reading of the GDPR.

This ebook, however, should not be considered infallible and is not meant to offer legal advice. It is merely our effort to teach what we have learned from countless hours of research about the GDPR. We recommend you use this ebook as a primer in addition to a full reading of the GDPR to ensure a complete understanding of how the laws affect you and so that you can come to your own conclusions that may or may not be the same as ours.

Best of luck in your endeavors,
Ross Bass

Chapter 1:

What is the GDPR

The **General Data Protection Regulation** (**GDPR**) is a set of privacy laws from the EU that became enforceable on May 25th, 2018 and is perhaps the most important update to privacy law in the 21st century. It has a **global reach** that extends to businesses engaged in collecting or processing the personal information of people within the EU.

One of the major points of interest with this new set of privacy laws is its scope in that it **affects businesses worldwide**, whether or not that business is itself located within the EU.

Image: TermsFeed illustration of man at map showing global privacy laws

Because the GDPR is one of the strongest examples of privacy law in the world, compliance with it means compliance or near-compliance with the majority of other privacy laws currently existing globally.

If your goal is to reach a **global audience**, the GDPR and **CalOPPA** are the golden standards for having both strong and legally compliant policies and procedures.

Even if you are not currently required to comply with the GDPR (if you serve only an American audience, for example), going the extra mile to become compliant now means you will be able to extend your market to the EU whenever that becomes advantageous to you.

It also enhances your credibility to say that you are compliant with the *best and most contemporary* set of privacy laws in the world.

While the GDPR is a sterling example of privacy rights in the modern age and a step forward by holding everyone to the same standards, it can also be a burden to those who need to update and change their procedures in order to become compliant.

Business owners, developers, marketers and companies worldwide will need to familiarize themselves with the GDPR so that they can review and most likely update their current **policies and procedures** in order to meet the new requirements.

While the average internet user might not notice some or any of the changes created by the GDPR, developers will certainly see the differences and it's important to understand the reasons behind the requirements.

As a business owner, you are likely to encounter situations where you need to ensure that you are compliant with the GDPR as you are reaching out to a global audience that could include people located within the EU.

Some of the things you'll need to plan for include (but definitely aren't limited to):

- Getting appropriate **consent** when required
- Allowing for **opt-outs** and **revoking of consent**
- Adequately **disclosing** your privacy practices
- Making it easy for your users to **contact you** to exert their rights under the GDPR

See if you can guess which of the examples below are subject to the GDPR:

An ecommerce store operating in the United States that ships to the European Union	**?**
An app developer with users who reside in the EU	**?**
An online business that does **not** allow EU users to make purchases	**?**
A website that does **not** allow EU visitors to register personal accounts on the site, but serves personalized ads to **all** visitors through Google AdSense (for example)	**?**
A website that markets only to users in the US and blocks IP addresses from outside of North America	**?**

Table 1: Subject to the GDPR - Guess Examples

Let's explore each one in detail with explanations.

Example #1

An ecommerce store operating in the United States that ships to the European Union.

In example #1, it should be fairly obvious that the ecommerce store **would** be subject to the GDPR. In order to serve customers in the EU and ship products to them, the store would need to collect and process the customers' personal information such as names, shipping addresses and payment information at the very least. This would constitute as the handling of personal data of EU residents, so the **store would fall under GDPR jurisdiction**.

Example #2

An app developer with users who reside in the EU.

In example #2, the answer is **a strong "probably."** It is possible that the developer could release an app without collecting or processing any sort of personal information, but this is unlikely. **Be aware that personal data collection and processing is not strictly limited to situations where the data is used for marketing or database building.**

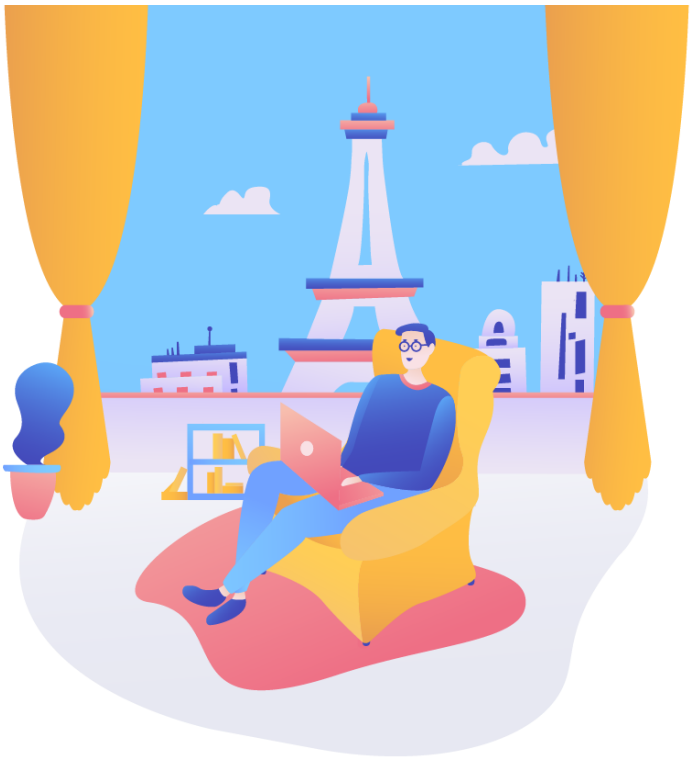


Image:TermsFeed illustration of a man in a chair with Eiffel Tower outside window

The reasons for personal data collecting and processing are immense and include anything from personalized ads and behavioral tracking to social media accounts that include your name and birthday.

Even a simple gaming app might ask for your email address to make an account, track your location, or have you select a username (which could be considered a unique identifier under the GDPR). More often than not, apps process personal information on some level.

Example #3

An online business that does **not** allow EU users to make purchases.

In example #3, the business would **probably not be subject to the GDPR**.

The scope of the GDPR actually makes it somewhat difficult to avoid falling under its jurisdiction, but a business can arrange things in a way to make themselves only available to certain regions.

Image: TermsFeed illustration of man at computer with website blocked in EU

If the business can show that it made an effort to deny access of its products or services to the European market, and in no way marketed to them or attempted to collect or process their data, it should be exempt from GDPR compliance.

Example #4

A website that does **not** allow EU visitors to register personal accounts on the site, but serves personalized ads to **all** visitors.

In example #4, the website is making a similar attempt as the business in example #3, but by serving personalized ads and not blocking traffic from the EU, personal data is likely to be processed. **This is a good example of why it is difficult to avoid the scope of the GDPR**.

Image: TermsFeed illustration of man at computer seeing an internet ad

Even though the website in this case does not allow EU residents to register, these users can still access the website. If while on the website a third-party service collects information about their habits on the web to populate ads on the website, that would be processing the users' information.

It doesn't matter that the website itself is not doing the processing but is using a third-party ad service to do so instead. This indirect method of data processing would still make **the website subject to the GDPR**.

If the website did not have personalized ads or other features that processed personal data (for example, analytics suites for behavioral tracking), or cater to residents of the EU in any way, it *may* escape the jurisdiction of the GDPR.

Example #5

A website that markets only to users in the US and blocks IP addresses from outside of North America.

In example #5, it is more clear that the website is trying to block EU traffic and only cater to the American market.

Image: TermsFeed illustration of man at computer with website blocked in EU

Depending on the methods and effectiveness of blocking visitors from the EU, the website owners should *not* have to comply with the GDPR if they are making no attempt to serve residents of the EU and actually taking steps to make sure that those residents won't be served.

Goals of the GDPR

The GDPR seeks to be an easily understandable, complete, and strong set of privacy laws to protect the privacy of those under its jurisdiction. Some of the core concepts at the heart of the GDPR are **privacy for individuals**, t**ransparency** on the part of businesses and developers, and more **user rights/choices**.

The GDPR aims to give individuals a high level of control over their personal information to ensure it is used safely, appropriately and in ways that people are comfortable with.

Today, possibly more than ever, it's important for individuals to control their personal information across social media, ecommerce, and email. The GDPR strives to both *inform and protect* these individuals while empowering businesses to create strong and secure procedures to ensure that the data they collect and process is handled safely and responsibly in order to limit the chance and threat of data breaches.

Under the GDPR, businesses are required to disclose virtually everything about **what data they collect**, **why** they are collecting it, and **what will be done with** that data. This coincides with

the idea of *transparency* by letting data subjects know exactly what happens with their personal data. This way, the data subjects *can choose* whether or not they agree with or wish to be part of certain data handling processes.

This level of transparency ensures that data controllers are only using data in ways that their users have agreed to. It also holds them accountable for any misuse of personal information outside of the agreed-upon terms.

Gone are the days of collecting, scraping, and buying masses of data for marketing and other purposes. Transparency and user consent are cornerstones of the GDPR than ensure safe and fair usage of personal data.

In addition to requiring developers and businesses to be transparent in their data collection and processing, the GDPR clearly defines **the rights that users have** regarding ownership of their personal information.

For example, individuals have the right to request that a data controller provide them with all of the data that they hold about them, the right to request that processing of their data be ceased, and even the right to request that the data be erased completely if they wish.

User rights such as these ensure that, under the GDPR, individuals essentially own their personal information and it can't be used against their wishes.

As with most sets of laws, the GDPR is a long and sometimes confusing document. However, great care has been given to make the GDPR about as approachable as possible, doing away with much of the cumbersome legalese of other laws.

However, while the GDPR was written to be easy to understand by the average individual, it's still a lot to digest and some concepts can be difficult to understand at first.

This book will not only get you up to speed on the GDPR as a whole, but will specifically cover how it affects business owners and the steps they need to take to become compliant.

Privacy, Transparency and User Rights

These are the cornerstones of the GDPR.

By focusing on the privacy of users, there is less risk to data subjects by minimizing the amount of personal data that is collected, stored, processed, and shared. In fact, the GDPR adopts the concept of "**Privacy by Design**," where businesses are expected to consider privacy at every step of a project. Not just at the end.

By using transparency as the foundation for data controllers and processors who are handling personal data, users can act as the **policing force** that monitors data controllers and ensures

they are handling personal data responsibly. With security measures taken wherever possible, data subjects have much less to worry about when sharing their personal information.

The GDPR also gives the **authorities** better access to data controllers and data processors so that they can keep an eye on things and easily follow up on objections and inquiries from data subjects. The GDPR gives users an arsenal of rights to protect their personal information and ensure that data controllers and processors are handling it properly.

We will cover these rights in detail in Chapter 6 [LINK TO CHAPTER 6], but here's a quick rundown of the eight fundamental rights of data subjects under the GDPR.

Note that **not every business will need to comply with every right**. For example, the right to data portability only applies to data processed based on either consent or a contract, and that's processed using automated means. You can see how this leaves a lot of data that won't have to be made portable.

While these rights exist for users in general, make sure to become familiar with the specifics of each right so you know when and if it's something you must provide to your users.

The Right	What it means
Right to be informed	Users have a right to know all about how you're processing their personal data. This is accomplished by having a thorough Privacy Policy.
Right of access	Users have a right to request information from businesses about their personal data that the business processes.
Right to rectification	Users must be able to correct and update inaccuracies in their personal data.
Right to erasure	Also known as "the right to be forgotten," it means that users have the right to have their personal data erased and cease its processing under certain circumstances.
Right to restriction of processing	Users have the right to limit or postpone the processing of their personal data in some scenarios.
Right to data portability	Users have a right to the personal data that they provide to a controller and can have it transmitted to another controller if they wish in certain circumstances.
Right to object	Users have the right to challenge or object to data processing where they believe it is improper, unlawful, or simply unwanted.

Right to human intervention	Users have the right to not be subject to automated decisions that could be harmful and can request human intervention.

Table 2: GDPR User Rights - What it means

By empowering data subjects with these rights, the GDPR can better ensure that their privacy is protected and their personal information is used fairly.

Of course, all of this is made easier by requiring data controllers and processors to be transparent in their data collection and handling procedures. Essentially, everything that happens with a data subject's information should be declared in one way or another so that the individual knows ***precisely*** what is happening with their information at any given time.

The GDPR and CalOPPA

The GDPR borrows much from the California Online Privacy Protection Act of 2003 (**CalOPPA**). It duplicates and reinforces many of the revolutionary regulations introduced by California's groundbreaking set of privacy laws.

In fact, compliance with the GDPR often means you may also be compliant with CalOPPA. These regulations share a lot in common, including their far reaching jurisdictions that extend worldwide.

Image: TermsFeed illustration of men at desks in the EU and USA

Let's take a brief look at some of the concepts of CalOPPA that the GDPR has adopted.

Global Reach

One of the reasons that the GDPR is such a big deal is because it reaches **far beyond the borders of the European Union**. Instead of regulating the activity of businesses and websites only **operating within** its geographical area, the GDPR regulates *any entity* which collects or processes the personal data of **those within** its geographical area.

This worldwide reach was first implemented by CalOPPA which required any entity that handles personally identifiable information (PII) of **California** residents to have a CalOPPA-compliant Privacy Policy in place (among other requirements).

As most websites receive visitors from the US, and California residents are likely to be included in that traffic, it quickly became clear that ***businesses worldwide needed to take notice of CalOPPA.***

While burdensome to many companies, CalOPPA ensured that the rights and privacy of the residents of California would be respected without geographical loopholes that could jeopardize security.

The GDPR adopted a similar policy, ensuring that individuals located within the EU remain protected *any time* their personal information is collected, processed, or shared.

Privacy Policies

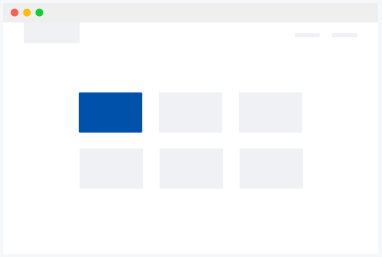
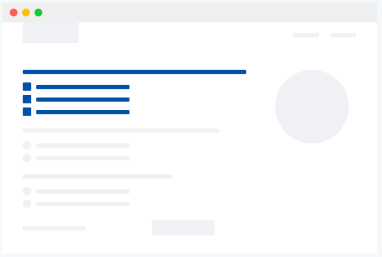
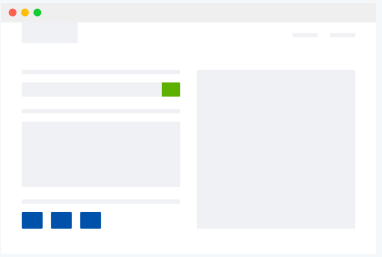
California was the first state in the US to enact a law requiring websites to have a Privacy Policy in place. This requirement applied to any website that collects personally identifiable information from residents of California.

The primary focus of CalOPPA is to encourage **transparency** by setting some standards for Privacy Policies.

Our Privacy Policy Generator makes it easy to create a Privacy Policy for your business. Just follow these steps:

1. At Step 1, **select the Website option or App option or both**.
2. **Answer some questions** about your website or app.
3. Answer some questions **about your business**.
4. **Enter the email address** where you'd like the Privacy Policy delivered and click "Generate."

You'll be able to instantly access and download your new Privacy Policy.

Step 1	Step 2	Step 3
		
Start the Privacy Policy Generator questionnaire	Answers the questions from our Privacy Policy Generator	Integrate the generated Privacy Policy

CalOPPA is less focused on regulating how and why websites collect and process data, and instead focuses more on ensuring that Californians are *informed* about what is happening to their personal information so that they can choose whether or not to give it.

Under CalOPPA, a Privacy Policy must:

- Be **posted conspicuously** on a main page and include the word “privacy”
- Disclose what **categories of personal data** are collected
- Disclose what **categories of third parties** the personal data may be shared with
- Disclose the procedure for **notifying users of changes** to the Privacy Policy
- Include the **date** when the current version of the policy went into effect
- Include the procedure by which users can **review and request updates to** their stored personal information
- Disclose whether Do Not Track requests are honored

You will find many of these requirements in the GDPR, along with some additional, more advanced requirements.

Under the GDPR a Privacy Policy should be **easy to access**, **read**, and **understand**, and should include the following:

- The **identity** of the data controller (and the Data Protection Officer, if applicable)
- **What** personal data is collected
- **How** it is collected
- **Why** it is collected (for what purpose or purposes)
- The **legal basis** for collecting the data
- The **source** of any personal data not collected firsthand
- **How long** data will be retained
- The **rights users have** regarding their personal data
- How to **submit complaints**
- Proof of proper **security** to protect private data
- Disclosure of whether data is stored, shared or processed **outside of the EU**, as well as security measures in place for those circumstances

- Disclosure of if you handle any **special categories** of data, as well as the security measures in place to protect that data
- Disclosure of with whom personal data is shared (**third parties**, partners, etc.)
- **Date** when your Privacy Policy was **last updated**
- Any **consequences** of refusing to provide data (limited site functionality, etc.)
- Disclosure of any **automated decisions or profiling** that may take place

As you can see, the requirements for Privacy Policies under the GDPR focus much more on the content of these policies.

PII and Personal Data

Personally identifiable information or **PII** under CalOPPA can be defined as "*any information which could be used to identify a certain individual or de-anonymize anonymous information*".

That information only theoretically needs to have the potential to identify someone, even if it would be difficult to do so.

For example, a phone number is sometimes used as a unique identifier tied to certain accounts. If that number is also listed in a contact directory or on social media, then you could use that number to discover the name and identity of that individual. Therefore, a phone number is considered PII.

The GDPR defines ***personal data*** in a very similar manner. **Article 4** defines personal data as:

> *"...any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;"*

The GDPR gets a bit more specific and clarifies some uncertainty about what can be considered "*identifiable*."

For example, the predecessor to the GDPR was unclear about whether things like IP addresses or location data were considered personal data. The GDPR makes it clear that they are, in addition to many other things.

Here is a list of some things that qualify as personal data or personal information under the GDPR:

- Email addresses
- Mailing addresses
- Phone numbers
- Physical descriptions
- Demographic information

- Age or date of birth
- Social security numbers
- Driver license numbers
- Names
- IP addresses
- Location data
- Zip codes
- Medical history
- Financial information (such as salary)
- Unique identifiers (student and other ID numbers)
- Religious beliefs
- Political affiliations
- Occupations

This list is by no means exhaustive, but instead contains some common types of information that can be considered personal data under the GDPR.

Cross-Compliance

With the GDPR building upon many of the concepts of CalOPPA, becoming compliant with the GDPR puts you in very good standing under CalOPPA, as well. They share many **similarities**, **requirements**, and **principles**, with only a few things left out of the GDPR.

Unfortunately, the road to compliance from CalOPPA to the GDPR is not as short.

The GDPR builds upon many concepts of CalOPPA and also *evolves* many of them, delving deeper into the processes and procedures of data controllers and data processors. While being compliant with CalOPPA certainly means you are closer to privacy compliance under the GDPR, there are **many more steps** needed to become fully compliant with all aspects of the GDPR.

If you are aiming for compliance with *both CalOPPA and the GDPR*, you should review each set of laws and compare them individually to your operation. Nothing in either set of laws should interfere with the other, though some requirements may be set to a higher standard in one case versus the other. Comply with the **most stringent requirement in situations of overlap** to ensure your methods are adequate or better for both sets of laws.

Below is a chart outlining some common business activities and each law's general requirements so you can see how they differ in a practical way:

Activity	CalOPPA	GDPR
Jurisdiction	Affects any entity that handles personal data of residents of California.	Affects any entity that handles personal data of users in the EU.
Collecting/processing personal data	Practices must be disclosed in the Privacy Policy.	Must have legal basis.

		Practices must be disclosed in the Privacy Policy.
Privacy Policies	Privacy Policies are required and must contain certain information and be easily accessible.	Privacy Policies are required and must disclose additional information and be easy to read and access.
Collecting email addresses from users to create an account with you and sign them up to your marketing emails	No specific requirements.	Must have an additional checkbox or “I Agree” button that users must click to show they are informed that they’ll also be signing up for marketing emails.
Serving personalized ads	Must disclose this in Privacy Policy.	Must get active consent from users.
Using cookies	Must disclose this in Privacy Policy.	Must get consent before cookies can be placed on devices.

Table 3: Cross-compliance - Activity, CalOPPA and the GDPR

Penalties for Failure to Comply With the GDPR

The maximum penalty for breach of privacy laws has been increased under the GDPR to the higher of €20 million or 4% of annual global turnover. A fine of this magnitude would be reserved for only the most egregious breaches of privacy, but goes to show that it is vitally important to understand when it is and is not lawful to process the personal data of residents of the EU.

Article 82 states that individuals who have suffered damages from a breach of the GDPR are entitled to compensation from the data controller and/or data processor. While it does not go into detail about how much compensation could be required or give any examples of such a case, it simply states that this would be handled in court.

Here’s how the GDPR phrases it:

(1) Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.

(2) [1] Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. [2] A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.

(3) A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.

(4) Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.

(5) Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.

(6) Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).

Image: GDPR Info Article 82 - Right to Compensation and Liability

1. *Any person who has suffered material or non-material damage as a result of an infringement of this Regulation shall have the right to receive compensation from the controller or processor for the damage suffered.*
2. *Any controller involved in processing shall be liable for the damage caused by processing which infringes this Regulation. A processor shall be liable for the damage caused by processing only where it has not complied with obligations of this Regulation specifically directed to processors or where it has acted outside or contrary to lawful instructions of the controller.*
3. *A controller or processor shall be exempt from liability under paragraph 2 if it proves that it is not in any way responsible for the event giving rise to the damage.*
4. *Where more than one controller or processor, or both a controller and a processor, are involved in the same processing and where they are, under paragraphs 2 and 3, responsible for any damage caused by processing, each controller or processor shall be held liable for the entire damage in order to ensure effective compensation of the data subject.*

5. *Where a controller or processor has, in accordance with paragraph 4, paid full compensation for the damage suffered, that controller or processor shall be entitled to claim back from the other controllers or processors involved in the same processing that part of the compensation corresponding to their part of responsibility for the damage, in accordance with the conditions set out in paragraph 2.*
6. *Court proceedings for exercising the right to receive compensation shall be brought before the courts competent under the law of the Member State referred to in Article 79(2).*

Chapter 2:

The Pillars of the GDPR

Understanding the pillars of the GDPR can help us **understand and interpret our responsibilities as business owners** to ensure GDPR compliance and strong policies within our organization.

Let's take an in-depth look at these core concepts of the GDPR and how we should navigate them.

Image: TermsFeed illustration of a desk and pillars to represent pillars of GDPR

Pillar 1: Purpose and Proof for Data Handling

Gone are the days when apps and websites can collect any and all information possible from users without the users knowing. The GDPR is doing away with shady data collection practices and leveling the playing field for businesses that respect the privacy and desires of their data subjects.

Under the GDPR, data controllers **must have a legal basis for collecting and processing** the personal information of their users. Without an **adequate reason**, data controllers are not permitted to collect or process personal information. It's as simple as that.

In addition to requiring an adequate purpose for personal data handling, the GDPR also requires **proof** on the part of the data controller to ensure they are acting in accordance to the law.

Data controllers and processors are required to document the data they have **collected**, the data they have **processed**, and the **reason for doing so** so that they can present these records to the proper authorities as proof of their compliance with the GDPR if need be.

This documentation should include the following:

- All **types of personal data** in your possession
- The **reason why** it was collected (including proof of the data subject's consent, if applicable)
- The **lifecycle** of the personal data in your possession (how long will you retain it?)
- Any data processors, third-parties, or other entities with whom you have **shared the data**
- Your **legal basis** for collection and/or processing all data in your possession

See Chapter 5 [LINK TO CHAPTER 5] for more information on "legitimate interests" and when you can use that as your legal basis for data processing.

Collect and Keep Data Only as Needed

A misunderstanding that many business owners have is that once they collect personal data from one of their users, that data then *belongs to them and they can do with it as they wish*. This actually contradicts several sections of the GDPR.

In order to be compliant with the GDPR, you must only collect data with a **sufficient legal basis** to do so, and you should only retain that information for **as long as it is actually needed** for the intended and communicated purpose.

So, having a legal basis to collect personal data from one of your users allows you to obtain that data, but once you are finished using that data to complete the task you had a legal basis for, the data should then be deleted or completely anonymized to remove any connection to the data subject.

Retaining personal information for only a limited time reduces the need for ever growing data storage, encourages efficient use of collected data, and significantly reduces the risk to data subjects in the event of a data breach.

By setting a ***lifespan*** for the personal data that you collect and process, your users are no longer at risk of their data being compromised after the set amount of time when their data is processed.

Pillar 2: Data Security

The GDPR aims to reduce security risks to data subjects by increasing the responsibilities and expectations of data controllers and processors.

Article 32 of the GDPR states that data controllers must have **sufficient security measures in place** appropriate to the sort of personal data they handle and in light of the potential risks involved.

Essentially, this declaration puts the full responsibility of data security on the data controller to ensure that the privacy and personal data of their users are adequately protected by modern measures.

Some recommended and expected measures you should take in order to ensure you have adequate security measures in place to protect your data subjects' personal information include:

- Using SSL encryption
- Applying data anonymization/pseudonymisation
- Erasing nonessential data

Encryption should be used at multiple stages in your processes when possible to ensure that the data is secure, even if it is stolen or you are the victim of a breach.

Image: Small logo for Kruddels DE

A German chat app recently faced a €20,000 fine after a data breach exposed that the company had been storing user passwords in plain text files. This company did everything right in notifying its users and the proper authorities of the breach, and it would seem that the fine came simply as a result of the lack of encryption.

Had the data been properly encrypted, the passwords that were stolen in the breach would have been uninterpretable and useless as a result of encryption. But since this data was stored as plain text without any encryption, it was **left vulnerable** and not compliant with the privacy protection requirements set forth in the GDPR, thus the fine.

Modern day encryption is usually in the form of SSL 256-bit keys that turn easily understandable information such as a text document into an unintelligible jumble of characters that must be unencrypted before it can be understood. 256-bit encryption is virtually uncrackable, meaning even if someone were to steal the content of your encrypted database, the content would be unintelligible without the encryption key to decode it.

Pseudonymisation and Anonymization

Pseudonymisation is a process where data is substituted according to a system so that it is not easily identifiable without knowing the pseudonymization system or by cracking the code.

For example, a very basic form a pseudonymization would be a simple cipher where one letter is replaced with another letter or symbol. This might look something like this:

A=1, B=$, C=F, D=!, E=P, etc.

If you took the word “DAD” and applied the cipher it would become “!1!.” Or if you took the word “CAB” it would become “F1$.”

While this extremely simple version of pseudonymisation is not enough for modern internet security purposes, you can see how even a form as simple as this can make data more difficult to detect and understand. If an unauthorized entity were to take a look at account information in your pseudonymized database, it would be much more secure for the account owner if their name was displayed as “1$P” instead of “ABE.”

However, with access to an entire database worth of information, it would be possible to crack a simple pseudonymization cipher and decode the information within.

Some other weaknesses of pseudonymization are the ability to find patterns. Even if the cipher is not cracked, the name “ABE” would appear as “1$P” in every instance which could give away some information and show a pattern. In some cases, a pseudonymized name or unique identifier would still behave as a unique identifier because it is consistent, even though pseudonymized.

But make no mistake, pseudonymization can be a powerful security measure to use in your projects. While not infallible, and not sufficient for securing your database in and of itself, using any form of pseudonymization is far better than doing nothing at all. Advanced pseudonymization techniques can be much more difficult to crack and offer much higher levels of security.

Article 3 of the GDPR refers to pseudonymization where it mentions using methods of data processing that require “additional information” to be interpreted. Pseudonymization is one such method requiring a cipher to interpret the data.

Anonymization is another method of converting sensitive data into a less interpretable form. It uses a slightly different process to camouflage data, offering some advantages and disadvantages compared to pseudonymization.

Anonymization by definition (**Recital 26**) must alter the data in a way that it is **irreversible**.

Unlike ciphers and other methods used in pseudonymisation which can be cracked and decoded, anonymization is a permanent and irreversible process. In fact, true anonymization completely erases any personal information from an entry to the point that it is no longer identifiable (or useful) to the data controller securing it.

For this reason, there are some methods that can be used to anonymize data without losing all of its value.

One useful way to implement personal data anonymization is to anonymize all unnecessary information after it has been used.

For example, if a user on your website fills out a survey with some information about himself that you will be using to make insights about your business model, you can anonymize that data after you complete the study.

Instead of having a survey that says John Smith likes your new homepage and Jane Doe dislikes your new homepage, you can anonymize the results by simply saying that 50% of your users prefer your new homepage. This result is free of any identifying information.

The trick to using anonymization for data security is to **remove any information that can be used to link to an individual while still retaining useful information** for your analytics. This isn’t always obvious or easy, and you should think back to how the GDPR defines personal data to determine what can be considered identifying information.

Pillar 3: User Rights

User rights create a balance between the data subjects and data controllers. This balance of power makes the relationship between data subjects and data controllers a give and take rather than the data controller holding all of the cards.

These rights are discussed thoroughly in Chapter 6.

Pillar 4: Transparency

The final pillar of the GDPR is **transparency** on the part of data controllers and data processors.

Privacy Policies are perhaps the most crucial component of transparency. The GDPR has strong guidelines for what should be disclosed to data subjects, and a strong Privacy Policy is an effective way for data controllers to communicate a vast amount of information to their users.

Transparency is also a good way to build a relationship with your users as well as improve your reputation. Keeping your data subjects informed shows that you want what's best for them and lets them know what you are doing to protect their personal information and privacy.

Chapter 3:

Data Controllers vs. Data Processors

A crucial aspect of the GDPR is the **difference between a data controller and a data processor**. Luckily, the distinction is fairly easy to understand and remember.

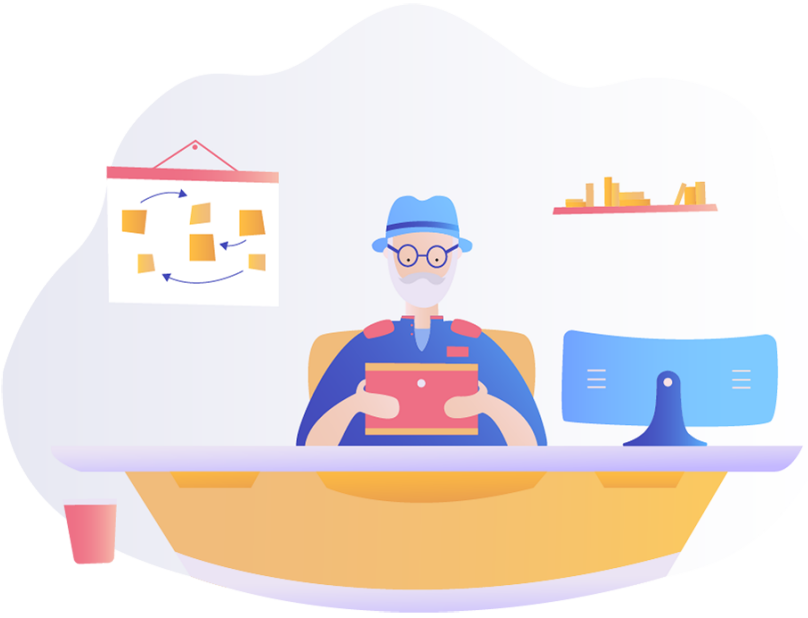


Image: TermsFeed illustration of a man reading at a desk version 1, the Data Controller

Basically, **a data controller** is the one who decides what data is collected and how that data will be processed. Data controllers usually collect the data for purposes they decide and manage, and are responsible for ensuring that it is handled properly. Data controllers are often also data processors, but can also use a separate data processor.

Image: TermsFeed illustration of a man reading at a desk version 2, the Data Processor

A data processor takes information that has been collected by a data controller and then uses it to complete a task or tasks on behalf of the data controller. The data processor must obey the data controller and only process data in the ways that they have been instructed. Data controllers are similar to managers who guide and oversee the work of data processors.

Imagine an ecommerce website that utilizes a third-party payment processor.

When a user decides to make a purchase from the website, the website handles the majority of the transaction but hands of the *payment information to the third-party processor*. The ecommerce website is the controller in this scenario because it facilitates the sale between the buyer and decides what is done with the customer's data.

The ecommerce website doesn't actually process the payment data though. Instead, the third-party payment processor handles the actual data processing at the direction of the data controller.

In the above example, the ecommerce website manages the transaction and collects the payment information from the data subject. It then transfers that information to the third-party payment processor with instructions on what to do with that data.

The payment processor only acts *according to the instructions of the website* with the data provided to it. In this scenario and example relationship, the **ecommerce website is the data controller** and the third-party **payment processor is the data processor**.

By and large, both data controllers and data processors must abide by many of the same rules. They are required to handle personal data a certain way, have adequate safeguards in place to protect that data, and must respect the rights and privacy of their data subjects.

However, there are some crucial scenarios where it is necessary to distinguish between the two as the **rules and regulations can vary according to your role**.

In this chapter, we will discuss how the GDPR regulates these two categories of data handlers so you ***understand your responsibilities*** as a data controller and/or processor.

In order to really drive home the difference between data controllers and data processors, and to help you determine which one you are, let's explore a few examples.

The Dynamic Between a Data Controller and Data Processor

Some businesses take on the role of **both** data controller and processor by handling all of their data processing needs internally.

For example, consider a website that prompts you to create an account by providing your email address in order to send you updates or a newsletter. If the website handles its own email list **and** does not utilize a third-party service to handle the list or send out updates and its newsletter, then the website would be **both** the data controller and the data processor.

This is because the website decides what is to be done with the email address data **and processes** it to send out updates and its newsletter.

The Data Controller

If, on the other hand, the website in the above example used a third-party service (like MailChimp) to handle the distribution of its newsletter to the email list, the website would be the data controller and the third-party service would be the data processor. The data controller decides what is to be done with the data it provides to the processor.

In this example, the website would inform the distributor of what it wants done with the email list (such as sending out a monthly newsletter) and the distributor would carry out that task. You can see how the website is "controlling" the email list while the distributor is simply "processing" the information.

The Data Processor

The distributor in the above examples would be the data processor as it **does not decide** what to do with the email addresses **but simply carries out the tasks requested** by the data controller (the website).

Under the GDPR, data processors are ONLY to process data in response to *orders and directions from the data controller*. A data processor **may not** process that data for any additional purposes beyond what was requested by the data controller.

Being Both a Data Processor and Data Controller

Data processors can also be data controllers and *almost always will be*.

Consider a data processing company that handles email newsletter processing for other companies. While the company is a data processor in the relationship between itself and its clients, *it is a data controller in other relationships and with other data*.

The data processing company will be data controller when it comes to things like:

- Contact and billing information it collects from its clients
- Its own employee documentation like information found on employee applications and in payroll databases

While data processing requirements will apply to the processor in its relationship with its clients, it will also need to take steps to comply with data controller requirements in regard to other data it chooses to collect.

Example #1: Social Media Website That is Both a Data Controller and Data Processor

Consider a social media platform where users are able to create an account by providing information about themselves. This information would likely include things like name, age, city of residence, workplace, etc. which would constitute personal information under the protection of the GDPR.

As such, the social media website collecting this information would be designated as the data controller regarding that data.

Imagine that a feature of this social media website is sending email updates regarding information about the website as well as notifications regarding user interactions through the

social media platform. The website automatically forwards these messages and notifications to the email associated with that account.

By processing the information regarding the account and the associated email address, the website would *also qualify as a data processor*.

In this example, the social media website would be considered **both** the data controller and data processor because it **collects** personal information **and dictates** what tasks it will be used for, in addition to carrying out those tasks itself. It both controls and processes the data.

Example #2: Ecommerce Website that is a Data Controller but not a Data Processor

Consider an ecommerce website started by an individual or small team seeking to sell a product. That product could be anything from t-shirts to software. In order to sell the product online, a small website is created in order to showcase and advertise the product. Potential buyers who visit the page can learn more about the product, see images, videos and reviews, or place an order.

The website itself, however, is not capable of processing payments. Instead, prospective customers pay via a third-party payment processor. In this scenario, the website is the data controller but **not** the data processor.

The website is the data controller because it dictates what is to be done with the personal data of its customer (payment is requested). The third-party, however, is the one actually processing the payment on behalf of the website and would be the data processor in this relationship.

Example #3: Email Marketing Service that is a Data Processor but not a Data Controller

Consider a company that assists in the creation and delivery of email marketing content and newsletters.

For example, a store hires this company to create and distribute an email advertising a new product to a list of interested customers. The email marketing service receives the email addresses for the recipients from the store along with information and assets about the product to be advertised. The marketing service then crafts an email and sends it to those email addresses as dictated by the store.

The email marketing service in this relationship would be the data processor while the store who hired the marketing service is the data controller. Here, the store collects the email addresses of the recipients, then provides that information to the email marketing service in order for them to complete a task as directed.

Since the email marketing service receives the email addresses for the sole purpose of distributing the advertisement and will not process the data for any other reasons, they are simply acting on behalf of the data controller as the data processor.

Remember, the email marketing service also acts as a data controller in other capacities, such as when handling the data of its own clients, but in this specific scenario they would be acting as the data processor when sending these emails at the direction of another company.

Here are some telltale signs that an entity **is a data controller**:

- It **dictates what data** is collected
- It **dictates why and how** data is to be processed
- It **takes possession** of the data **first**

Data processors are given data that is:

- To be **processed by them** but **provided by another** entity
- Provided only for use in a specific task
- Only to be processed **at the direction of the data controller**

Data Controller Responsibilities

Data controllers are responsible for everything from notifying data subjects of their practices, collecting data, keeping that data secure, and even determining how qualified the data processors they select are.

The data controller is responsible for the personal data it manages at virtually every point in the life cycle of that data, meaning *the majority of responsibilities revolve around the controller*.

Here is a list of responsibilities for **data controllers** as described by the GDPR:

- Must be able to **prove compliance** with the GDPR
- Is responsible for **ensuring lawful data processing**
- Should only handle and share **necessary** personal data
- Should only share personal data with **reputable** entities
- Must **have appropriate security measures** in place to protect the personal data of its users, and these measure should predate the collection of that data
- Have an appointed EU representative if located outside of the EU and involved in sufficient data processing
- Must only appoint **processors who can prove compliance** with the GDPR and agree to an adequate data processing agreement
- Must **report any security breaches** as soon as possible
- Must **keep adequate records** for proof of compliance with the GDPR if it has over 250 employees or processes personal data that is sensitive or on a large scale
- May be required to **appoint a Data Protection Officer** depending on the type and quantity of personal data that it processes or monitors

In many ways, the GDPR's primary focus is on data controllers.

The regulation seeks to ensure that data controllers responsibly handle personal data in order to protect the rights and privacy of the users. By enforcing the rules above, data controllers must be responsible and transparent in their usage of personal data to reduce risks and potential mishandling.

Data Processor Responsibilities

While data processors incur fewer responsibilities in their role, these responsibilities are no less important. Failure to follow the correct procedures can result in serious risks to data subjects and hefty fines for data processors as well as their data controllers in some cases.

Here is a list of responsibilities for **data processors** as described by the GDPR:

- Must **keep adequate records** for proof of compliance with the GDPR if it has over 250 employees or handles personal data that is sensitive or on a large scale
- May only process data in the manner **dictated by** the data controller
- Must have **adequate security measures** in place that predate the receiving of personal data for processing
- Must **obtain consent** from the data controller **to employ sub-processors**
- Must **agree to** an adequate data processing agreement
- May need to appoint an EU representative and/or DPO
- Shall return or delete the personal data at the end of the contract
- Must **report security breaches** as soon as possible

Again, while data controllers carry more responsibilities as the entities that decide what to do with the personal data that they manage, non-compliance on the behalf of a data processor can create just as dire of a situation that could put the rights and privacy of data subjects at risk.

The GDPR assigns several obligations to **both** data controllers and data processors in order to ensure that all parties involved in handling personal information do so safely and responsibly.

Recordkeeping Obligations

In order to be able to prove compliance with the GDPR, and for the safety of data subjects, ***both*** *data controllers and data processors have certain record keeping requirements* as mentioned above. The specifics of these requirements are different for data controllers and data processors, though they also share some aspects.

The recordkeeping obligations for ***data controllers*** under the GDPR can be boiled down to the following:

- Have on record the name and **contact information** for any controllers, joint controllers, representatives, or Data Protection Officers

- Have in your records the **reasons for processing** the personal data that you possess
- Describe in your records the **categories of data subjects** and personal data that you handle
- Include in your records the **categories of recipients with whom you share** or disclose the personal data that you possess, especially international entities
- Keep records of the international recipients of personal data and any applicable documentation about the relevant security measures in place for those **transfers**
- Have in your records the **procedure for deleting** personal data that is no longer needed and the estimated **life cycle** of different types of data
- Describe in your records the **security measures** that you have in place to protect the personal data that you possess

The recordkeeping obligations for ***data processors*** under the GDPR are as follows:

- Keep on record the name and **contact information** for any processors, joint processors, sub-processors, representatives or Data Protection Officers involved, as well as the data controller on whose behalf you are acting
- Have on record the **categories of data processing** that you handle on behalf of the data controller
- Keep records of the international recipients of personal data and any applicable documentation about the relevant security measures in place for those **transfers**
- Describe in your records the **security measures** that you have in place to protect the personal data that you possess

While these obligations of both data controllers and data processors are similar in many aspects, the role of data processor is only to act on behalf of the data controller. Therefore, more of the responsibility and decision-making falls on the controller.

Article 30 of the GDPR states that these records should be kept in written form (which **can be digital**) and the data controllers, data processors, or their representatives must be able to make these records available to the proper authority upon request.

An Exception

Article 30 also includes an exception for organizations of less than 250 employees. It states that organizations of **less than 250 employees** are not obligated to keep records as described above **unless** one of the following is true:

- The processing is likely to put **user rights or freedoms at risk**
- Processing takes place **more than occasionally**
- **Special categories of data** with additional protections are processed

This exception applies to *both* data controllers and data processors and is intended to limit the burden on small companies and small-scale operations that may not have the resources to maintain such detailed records.

Processing that takes place “more than occasionally” is fairly clear, but what does “occasionally” mean in this context?

It's easy to see that something that happens daily or very often would be "more than occasionally," such as a forum like Reddit where users tend to visit daily or even many times per day to interact with the site and submit comments and posts.

"Occasional" processing typically means if something is processed in a one-off way, or is *done rarely*.

An example of this may be a tax website that collects user information but only uses it once a year to submit tax returns for the individual, and only uses email addresses to confirm the returns have been submitted. In a case like this, the tax company may be exempt from needing to keep records.

However, if the tax company sends marketing emails consistently throughout the year, this changes things and the processing will be considered "more than occasionally" done. In this case, records will need to be kept.

Ask yourself how often you use the data you have on hand to determine if it's just occasional (rarely or only once), or more than occasional (regularly or somewhat consistently).

Chapter 4:

EU Representatives and Data Protection Officers

Depending on your data processing and collection methods as well as your geographical location and the location of your audience, you may be required to appoint **an EU representative or Data Protection Officer**.

While both of these roles are intended to improve compliance with and enforcement of the GDPR, they do so in **different ways** by serving **different purposes** for **different reasons**.

In this chapter, we will explore the *specific requirements and obligations* for these two roles to help you determine if you need to appoint an EU representative, a Data Protection Officer, both, or neither.

Image: TermsFeed illustration of EU Representative

The purpose of an **EU representative** is to ensure that companies outside of the EU have a local contact for matters concerning the GDPR. This is to *ease the burden of communications across continents* and time zones, expediting and guaranteeing communications between foreign entities and supervisory authorities within the EU.

Image: TermsFeed illustration of DPO Data Protection Officer

The purpose of a **Data Protection Officer** (or DPO) is to have an expert within your organization that is *knowledgeable about and responsible for compliance* with the GDPR.

DPOs are required for companies who process certain types or amounts of data. By appointing a Data Protection Officer, it becomes less likely that personal data will be mishandled or the laws of the GDPR will be broken.

When an EU Rep and DPO are Required

It is very possible that your company could require **both an EU member state representative and a Data Protection Officer**.

For this to happen, your company would need to:

- Be located outside of the EU, **and**
- Process or monitor a large amount of personal data or special kinds of data on a regular basis

Let's review the requirements for each to see if you need to appoint either or both.

When an EU Member State Representative is Required

An **EU representative is required** in the following circumstances:

- When a data controller or a data processor is located outside of the EU, **and**
- That data controller or data processor regularly collects or processes the personal data of residents of the EU, **or**
- That data controller or data processor processes special categories of data on a large scale, **or**
- That data controller or data processor processes personal data related to criminal histories

If these conditions are met, then an EU member state representative must be appointed within one of the countries where the data controller or data processor has users.

When a Data Protection Officer is Required

A **Data Protection Officer is required** in the following circumstances:

- When a **public authority** processes personal data
- When a data controller or data processor regularly or systematically **monitors personal information on a large scale**
- When a data controller or data processor **handles special categories of personal information on a large scale**
- When a data controller or data processor handles personal information relating to **criminal history**

If any of these conditions are met, a Data Protection Officer must be appointed.

Could One Person Do Both Roles?

While these two positions are different and distinct, they do share many similarities between them. Considerations for special categories of data and criminal histories are given in both cases, as well as distinctions between occasional versus regular, and large scale versus small scale data processing.

While the purpose of these two roles is different, and you could very well be required to have both, it might be theoretically possible that one person could fill both roles. But it isn't recommended and won't be practical in most cases.

Article 37 tells us that a Data Protection Officer may have other duties in addition to his or her role as a DPO. This could potentially mean that a single individual could serve as both an EU member state representative and Data Protection Officer. While theoretically this could be done, such an individual would need to be a resident of the EU while your company or organization would be located outside of the EU (or else you wouldn't need an EU rep).

This could create a contradiction for the requirement that a Data Protection Officer have easy access to the company for which they work, however. After all, it would be probably difficult for a DPO to ensure the organization they work for is complying with the GDPR when they're far away and in another country.

While there is no actual mention of this being possible or forbidden under the GDPR, it probably would not be recommended or logistically feasible in most cases, though theoretically it could be possible.

EU Representatives

Article 27 of the GDPR: *Representatives of controllers or processors not established in the Union*, covers the basics of when companies outside of the EU are required to appoint a member state representative.

For starters, the individual **must be located within the EU** and serves as a liaison for your company and the authorities of the GDPR. This is intended to improve and expedite communications which will result in less of a burden for both the authorities and affected data subjects.

If either of these parties have questions or concerns about your policies or compliance with the GDPR, they can contact a local representative rather than a company in another country or timezone. This will cut down on potentially costly communication delays and reduce lost or overlooked inquiries.

Let's look at some specifics from the GDPR to nail down **why and when** some businesses may need to appoint an EU representative.

Article 27: Representatives of Controllers or Processors Not Established in the Union

Article 27 makes up the core of the regulations pertaining to EU member state representatives in the GDPR.

Another important section is **Article 3**, which covers the territorial scope of the regulation. Article 3 states that companies both within and outside of the EU that handle the personal information of residents of the EU must be fully compliant with the GDPR.

This is very clear and is important when considering Article 27 which refers to Article 3. This reference reconfirms that data controllers and data processors who are not located within the EU are required to designate a representative who is located there.

Section 2: Exceptions

Section 2 of Article 27 describes the scenarios in which a representative is NOT needed:

2. The obligation laid down in paragraph 1 of this Article shall not apply to:

(a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or

(b) a public authority or body.

Image: GDPR Info: Article 27 Section 2 - Representatives of controllers or processors not established in the Union

> *The obligation laid down in paragraph 1 of this Article shall not apply to:*
>
> *a) processing which is occasional, does not include, on a large scale, processing of special categories of data as referred to in Article 9(1) or processing of personal data relating to criminal convictions and offences referred to in Article 10, and is unlikely to result in a risk to the rights and freedoms of natural persons, taking into account the nature, context, scope and purposes of the processing; or*
> *b) a public authority or body.*

Point (a) is a lot of information to take in at once, so let's break it down.

Data controllers and data processors located outside of the EU do NOT need to appoint a representative inside the EU if they:

- Only process data **occasionally**,
- Do not process **special categories of data on a large scale**. These special categories of data include:
  - Race
  - Ethnicity
  - Political opinions
  - Religion
  - Philosophical beliefs
  - Trade union membership
  - Genetic data
  - Biometric data
  - Health data
  - Sexual orientation
  - Sexual activity
- Do not process personal information that is related to **criminal history**, **or**
- If they only process data that comes with **limited risk potential** in the event of a data breach

In order to comply with the GDPR from outside of the EU, these are the requirements that will determine if you need to designate an EU representative or not.

The terms “occasionally” and “large scale” are admittedly vague, and we hope to receive more clarification on these entries in the near future to specify at what point data processing becomes more than “occasional” or the distinction between “large” and “small” scale.

For now, it’s best to rely on common sense and err on the safe side if you are truly uncertain by appointing an EU representative, just in case.

Section 3: Relation of EU Rep’s Residence to Your Business Dealings

Section 3 states that your EU representative **must reside within one of the EU member states from where your company collects personal information**. That is, your representative should be located in an **area you are targeting**, not just within the broad confines of the EU.

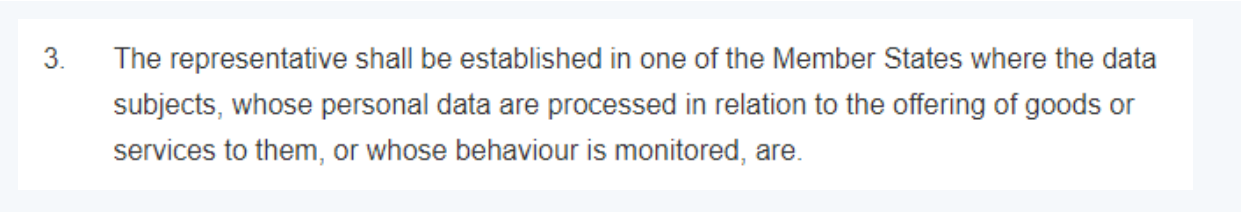

3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.

Image: GDPR Info: Article 27 Section 3 - Representatives of controllers or processors not established in the Union

> *3. The representative shall be established in one of the Member States where the data subjects, whose personal data are processed in relation to the offering of goods or services to them, or whose behaviour is monitored, are.*

After all, the purpose of appointing an EU representative is to make it easy for your data subjects and their supervisory authorities to contact you. Having your representative on the opposite side of the EU from the majority of your customers would not be convenient or wise.

Say, for example, that you process the personal information of citizens of the UK, France, and Italy. In that case, your EU representative should be located in *one of those three countries*.

If your representative was located instead in Germany, that would not be compliant because although Germany is a part of the EU, that is not one of the countries in which your data subjects reside.

Section 4: Communications

Section 4 explains that your designated EU representative should be included as a contact for supervisory authorities and users. This is so that the rep can be contacted with questions or concerns about your data processing procedures or compliance with the GDPR.

4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purposes of ensuring compliance with this Regulation.

Image: GDPR Info: Article 27 Section 4 - Representatives of controllers or processors not established in the Union

> *4. The representative shall be mandated by the controller or processor to be addressed in addition to or instead of the controller or the processor by, in particular, supervisory authorities and data subjects, on all issues related to processing, for the purpose of ensuring compliance with this Regulation.*

This is one of the major reasons for having an EU rep, as your local representative will be a much more convenient point of contact for your data subjects and the authorities located in the Union.

Article 35: Data Protection Impact Assessment

Article 35 is another relevant section of the GDPR that describes the main functions of EU representatives. In it, data protection impact assessments are discussed, and it mentions that in some situations data controllers should call on their EU representatives for input.

9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.

Image: GDPR Info: Article 35 Section 9 - Data protection impact assessment

> *9. Where appropriate, the controller shall seek the views of data subjects or their representatives on the intended processing, without prejudice to the protection of commercial or public interests or the security of processing operations.*

This is important because it not only gives additional responsibility to EU reps, but it also highlights another purpose for designating an EU member state representative: *having someone in your organization who is familiar with the laws, culture and pulse of a country that may be very different from your own*.

Having someone located in a foreign market could provide valuable insight into how that society is similar to your own or how it might be very different.

This knowledge could be vital to foreign companies that are unfamiliar with social norms in a region that they are targeting. Language barriers, translations, differences in daily life, or even opinions on personal privacy could vary wildly between countries. This could lead to embarrassing mistakes, poor business decisions, or potentially failure to comply with the GDPR despite the best intentions.

Your EU member state representative is not only a convenient point of contact for your company in foreign markets, but a knowledgeable expert of that market that you can consult with.

As explained in Article 27 and further detailed in Article 35 of the GDPR, your EU member state representative is an appointed local contact within your foreign market.

This individual serves as an intermediary for supervisory authorities, your company, and your users. This individual is meant to ease communications between your company located outside of the Union and those you interact with within the Union.

While it may seem burdensome to keep a designated representative in the EU, the reasons for having one are certainly reasonable. This representative will also provide your company with valuable information about the local market. In addition, a local contact could be vital for time-sensitive matters that otherwise could cost your company valuable time, money, or reputation.

You may encounter aspects of the duties of Data Protection Officers that seem very similar to those of EU member state representatives, but remember that these are entirely separate entities with their own conditions and duties.

Data Protection Officers

The core guidelines and requirements for Data Protection Officers are presented in Articles 37, 38 and 39 of the GDPR.

Article 37: Designation of the Data Protection Officer

Article 37 begins with an explanation of when a Data Protection Officer is required. The circumstances for needing to appoint a Data Protection Officer are as follows:

1. The controller and the processor shall designate a data protection officer in any case where:

   (a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;

   (b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or

   (c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.

Image: GDPR Info: Article 37 Section 1 - Designation of the Data Protection Officer

> 1. *The controller and the processor shall designate a data protection officer in any case where:*
>   a) *the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;*
>   b) *the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or*
>   c) *the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 or personal data relating to criminal convictions and offences referred to in Article 10.*

It may be noteworthy that point (a) of Section 1 of Article 37 is the opposite of point (b) of Section 2 of Article 27.

That is, Data Protection Officers **ARE** required by public authorities who process personal data, but EU member state representatives are **NOT** required for public authorities. This won't apply to most businesses, but is one of many *important distinctions* between EU reps and DPOs.

Article 37 goes on to say that multiple entities or branches of a single company are permitted to share one Data Protection Officer *as long as that individual has sufficient access to each unit*. In addition, it states that Data Protection Officers should be selected based on their qualifications and expertise about privacy law and the GDPR.

Data Protection Officers are allowed to have other roles within a company, but there should not be any conflict of interest in these roles and the individual is responsible for carrying out the tasks of a DPO in addition to any other duties.

Similar to EU representatives, the contact information for your Data Protection Officer should be published and accessible to both your users and the proper GDPR authorities in the event of questions or concerns regarding your compliance with the GDPR.

A Data Protection Officer is an expert in this area, making them the natural contact point for such inquiries.

Article 38: Position of the Data Protection Officer

Article 38 discusses the responsibilities of data controllers regarding their Data Protection Officers:

1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which relate to the protection of personal data.
2. The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.
3. [1] The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. [2] He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. [3] The data protection officer shall directly report to the highest management level of the controller or the processor.
4. Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.
5. The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.
6. [1] The data protection officer may fulfil other tasks and duties. [2] The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.

Image: GDPR Info: Article 38 - Position of the Data Protection Officer

> *1. The controller and the processor shall ensure that the data protection officer is involved, properly and in a timely manner, in all issues which*

> *relate to the protection of personal data.*
> 2. *The controller and processor shall support the data protection officer in performing the tasks referred to in Article 39 by providing resources necessary to carry out those tasks and access to personal data and processing operations, and to maintain his or her expert knowledge.*
> 3. *The controller and processor shall ensure that the data protection officer does not receive any instructions regarding the exercise of those tasks. He or she shall not be dismissed or penalised by the controller or the processor for performing his tasks. The data protection officer shall directly report to the highest management level of the controller or the processor.*
> 4. *Data subjects may contact the data protection officer with regard to all issues related to processing of their personal data and to the exercise of their rights under this Regulation.*
> 5. *The data protection officer shall be bound by secrecy or confidentiality concerning the performance of his or her tasks, in accordance with Union or Member State law.*
> 6. *The data protection officer may fulfil other tasks and duties. The controller or processor shall ensure that any such tasks and duties do not result in a conflict of interests.*

Let's explore what you need to do to ensure that your DPO can fulfill their duties unhindered.

Essentially, this all boils down to the Data Protection Officer being able to ***independently*** *carry out their duties without interference or oversight* by the company. This is not to say that the company should not interact with the Data Protection Officer, but that potential conflicts of interest may present themselves and the company should not pressure or otherwise control the duties of the DPO.

This independence is to prevent companies from forcing their DPO to hide or ignore policy breaches for fear of penalties and other legal repercussions. The job of a Data Protection Officer is to ensure that his or her company is acting in accordance with the GDPR, and any efforts to hinder these duties are in direct violation of the law.

Article 39: Tasks of the Data Protection Officer

Article 39 covers the responsibilities of a Data Protection Officer:

1. The data protection officer shall have at least the following tasks:

   (a) to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;

   (b) to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;

   (c) to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;

   (d) to cooperate with the supervisory authority;

   (e) to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter.

2. The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.

Image: GDPR Info: Article 39 - Tasks of the Data Protection Officer

1. *The data protection officer shall have at least the following tasks:*
   a. *to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions;*
   b. *to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits;*
   c. *to provide advice where requested as regards the data protection impact assessment and monitor its performance pursuant to Article 35;*
   d. *to cooperate with the supervisory authority;*
   e. *to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in*

> *Article 36, and to consult, where appropriate, with regard to any other matter.*
> 2. *The data protection officer shall in the performance of his or her tasks have due regard to the risk associated with processing operations, taking into account the nature, scope, context and purposes of processing.*

As you can see, the role of the Data Protection Officer includes being an **expert** on the GDPR. This individual can be a valuable asset by reviewing and monitoring all facets of your operation to ensure that your activities are compliant.

The DPO also serves as the **liaison** between your organization and the supervisory authorities to answer questions and help smooth over any concerns that may arise. The DPO will be a good source of information for any questions you may have about your data handling procedures and it would be wise to consult them about new ideas pertaining to personal data collection and processing as he or she is sure to have valuable insight.

While there are many similarities between what is required of Data Protection Officers and EU member state representatives, there are also some important differences, primarily *the purpose* for each position.

Data Protection Officers are intended to be experts in privacy law and responsible for ensuring that the company is following proper and compliance procedures.

EU representatives, on the other hand, are merely representatives of and points of contact for the company.

It's worth considering appointing people to these roles even if you do not currently meet the requirements to need them.

If you are not in the European market now but are planning to expand there in the future, why not appoint someone to be a Data Protection Officer and start learning about the GDPR?

Or, if you have contacts in the EU but your current data processing does not require an EU rep, consider bringing up that this position may be necessary in the future and start building a relationship with someone willing to fill it when that happens.

While you obviously need to meet the requirements for your current situation, going above and beyond basic compliance or planning for the future can only help you succeed and be prepared to continue your success as you expand into new markets and opportunities.

Chapter 5:

Choosing the Right Legal Basis

The GDPR goes into great detail about when and how personal information can be collected and processed. Gone are the days where massive swathes of information could be collected, shared, and used for any number of reasons. The GDPR defines what is a lawful basis for collecting and processing personal data. Anything outside of that is not compliant.

Essentially, there must be a *lawful reason* to handle personal data in any way.

Image: TermsFeed Illustration: Cannot Decide, Choosing Legal Basis

Article 6 of the GDPR gives the conditions for when it is legally permissible to process data. By requiring businesses to meet one of these conditions before processing personal information, the GDPR ensures that there is a justifiable reason whenever personal data is handled.

A quick list of other stipulations is as follows:

- The data collected or processed must be **proportional** to the task at hand
- The **reason why** data is being collected or processed must be **disclosed**
- Only data **needed** to complete a task should be collected or processed
- The collected data must only be held for **as long as needed**

In the eyes of the GDPR, a legal basis is a **justifiable reason why** a data controller is collecting or processing the data of an individual.

Examples include to complete tasks which the individual has signed up for, for marketing purposes to which the individual has given consent, or for legitimate interests that benefit both the data controller and data subject.

Let's take a look at some of the major entries in the GDPR that cover legal bases and lawfulness of data processing.

Article 6: Lawfulness of Processing

Article 6 is perhaps the most important section of the GDPR covering lawful bases for the collection and processing of personal data.

In it we are given the requirements for lawful data processing, informed that Member States may introduce stricter requirements, informed of the authorities in such cases, and given guidelines for when data may be processed for additional purposes than those originally consented to.

Let's dive deeper into each of these sections.

Section 1: Requirements for Lawful Processing

Section 1 of Article 6 lays out the possible circumstances for when it is lawful to process personal data.

These circumstances are:

a. When **consent** has been given by the data subject for a specific purpose
b. When processing is necessary to perform or prepare for a **contract** with the data subject
c. When there is a **legal obligation**
d. When **protecting the vital interests** of the data subject or someone else
e. For the **public interest** or when exercising **official authority**
f. To carry out **legitimate interests** of the data controller or a third party where these interests do not infringe on the rights, freedoms, or interests of the data subject

If none of these conditions are met, data is **not to be processed** under the GDPR. Period.

Point (a) is pretty straightforward:

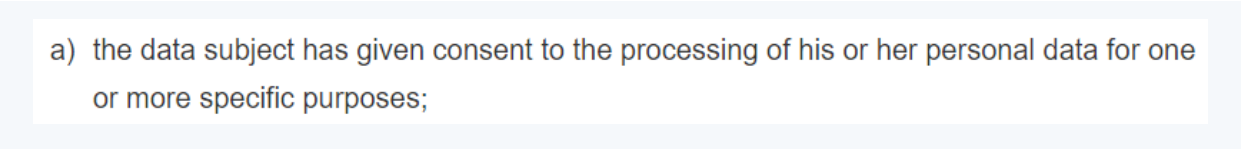

a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

Image: GDPR Info: Article 6 Section 1a - Lawfulness of Processing

> *a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;*

For example, if a data subject consented to giving their email address to join a newsletter, the data controller has the right to use that email address to send the newsletter. The data controller obtained consent to do something specific, then followed through with that activity.

Point (b) refers to situations similar to point (a), but in these cases data processing is often implied and consent may not be specifically needed.

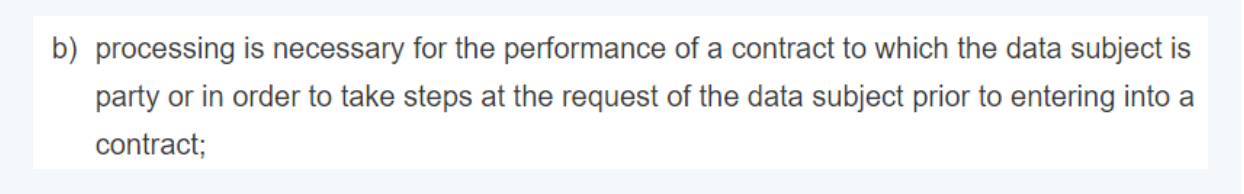

b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

Image: GDPR Info: Article 6 Section 1b - Lawfulness of Processing

> *b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;*

For example, if an individual gives their phone number to the website of an attorney to be contacted about a potential case, the attorney has a right to use that phone number and contact the individual as it is implied that this was the reason why the individual gave out their phone number.

Point (c) refers to situations where the data controller is legally obligated to provide certain information.

> c) processing is necessary for compliance with a legal obligation to which the controller is subject;

Image: GDPR Info: Article 6 Section 1c - Lawfulness of Processing

> *c) processing is necessary for compliance with a legal obligation to which the controller is subject;*

For example, if a company is subpoenaed to provide documentation about an event, this could include information regarding an individual involved in the event and the data controller may be legally obligated by the court to process such data as it is relevant and necessary for the case.

There are, of course, requirements for when a legal obligation could require data processing and situations where the data subject's rights and freedoms would not permit such processing, but that topic would require extensive explanation that you likely will never need to worry about.

Point (d) may refer to situations such as data breaches or suspected fraud.

> d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

Image: GDPR Info: Article 6 Section 1d - Lawfulness of Processing

> *d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;*

For example, if a company discovers suspicious behavior on a customer's account, it may be in the vital interest of that individual to take action to protect their account, personal information, privacy or finances.

Data processing may be required to suspend the account, temporarily change a compromised password, and/or contact the customer about the situation. This would be permissible in the vital interest of that data subject.

Section (e) may refer to situations such as investigating a crime where it is in the public interest or by official authority that data be processed to track down a suspected culprit.

> e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

Image: GDPR Info: Article 6 Section 1e - Lawfulness of Processing

> *e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;*

For example, if an email is distributed which contains a phishing scam to steal private information from its recipients, it would be in the public interest to track down the sender of the email and determine their identity in order to stop the email from being further distributed or for stolen information to be unlawfully used.

Point (f) refers to "legitimate interests" which may be one of the more confusing and misunderstood aspects of the GDPR. It also tends to be the go-to legal basis that many businesses use.

> f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Image: GDPR Info: Article 6 Section 1f - Lawfulness of Processing

> *f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.*

Essentially, this point is intended to cover unforeseen and unregulated instances where the data controller has a **compelling reason** to process data that is not covered by the previous points.

This is counterbalanced by the inclusion that the data controller's legitimate interests must be weighed against the **rights**, **freedoms**, **and interests of the data subject** to avoid taking advantage of this legal basis.

For example, a company claiming "legitimate interest" as a lawful basis for sending advertisements to a former customer without first obtaining consent would not be a strong case,

as the former customer has rights to privacy and may or may not be interested in receiving those ads. The legitimate interest of the company to engage in marketing doesn't override the individual's rights to not be bombarded with ads.

However, an app developer contacting current users to inform them of an update to the app that solves a newly discovered security issue would be a strong case, as a potential security flaw would be of interest to both the app developer and the user. Being required to obtain consent first would likely do more harm than good in such a case where time could be of the essence.

Let's take a better look at this last legal basis.

Legitimate Interest as a Legal Basis

One of the legal bases for which a business can collect and process the personal information of their data subjects is for the legitimate interest of the business and/or the data subject. If that sentence was confusing, it's because the term "legitimate interest" under the GDPR is one of the most uncertain and controversial concepts in the regulation.

Determining what constitutes a legitimate interest for a business compared to the legitimate interests of their data subjects can sometimes be a complex question.

This section will explore the main areas of the GDPR that deal with legitimate interests in a way that could be relevant to business owners.

Article 6 Section 1(f) (shown earlier) is the first major usage of the term "legitimate interest."

Here we see the term "legitimate interests" used when referring to a legal basis that data controllers can use to **justify the processing** of personal information. While at first glance this may not seem too complicated, try considering *exactly* what is meant by this clause.

What qualifies as a legitimate interest? Updates to policies? Marketing new products? Sales? Where do we draw the line between legitimate interests of the business versus the interests of their customers/data subjects?

In order to answer these questions, let's look at other usages of the term to find more evidence so we can achieve a more complete understanding of what is intended by the term "legitimate interest."

Recital 47: Overriding Legitimate Interest

Recital 47 starts by saying that:

> *"The legitimate interests of a controller… may provide a legal basis for processing, provided that the interests or the fundamental rights and freedoms of the data subject are not overriding, taking into consideration the reasonable expectations of data subjects based on their relationship with the controller."*

This may seem straightforward on the surface, but once again, where do we draw the line?

What happens when the company's definition of "legitimate interest" varies from the definition of one of their data subjects? Who is right?

In the usage in Recital 47, we might interpret that the "legitimate interests of a controller" means "the reasons a business might want to process a data subject's personal data." This could range anywhere from notifying users about a data breach to marketing a new product. Both of those things would certainly be of legitimate interest to the business owner.

This is where the counterbalance of Recital 47 comes in:

> *"At any rate the existence of a legitimate interest would need careful assessment including whether a data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could in particular override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing."*

Rectial 47 clarifies that just because the business has a legitimate interest in doing something, this must also be **fair and reasonable** to the data subjects involved. That is to say, data subjects have certain rights of their own that must be respected and considered when processing their personal information without their consent.

For example, a business sending an email out of the blue to its users to notify them about an update to their app that fixes a security flaw would be of interest to both the user and the business. This would likely constitute a justifiable reason to invoke the "legitimate interest" clause as a legal basis to contact users without their pre-approval.

On the other hand, a business sending an unwarranted email to its users promoting another brand may not be in the interest of the data subjects. If they did not give prior consent for the use of their contact information in that manner, and if the business does so under the guise of

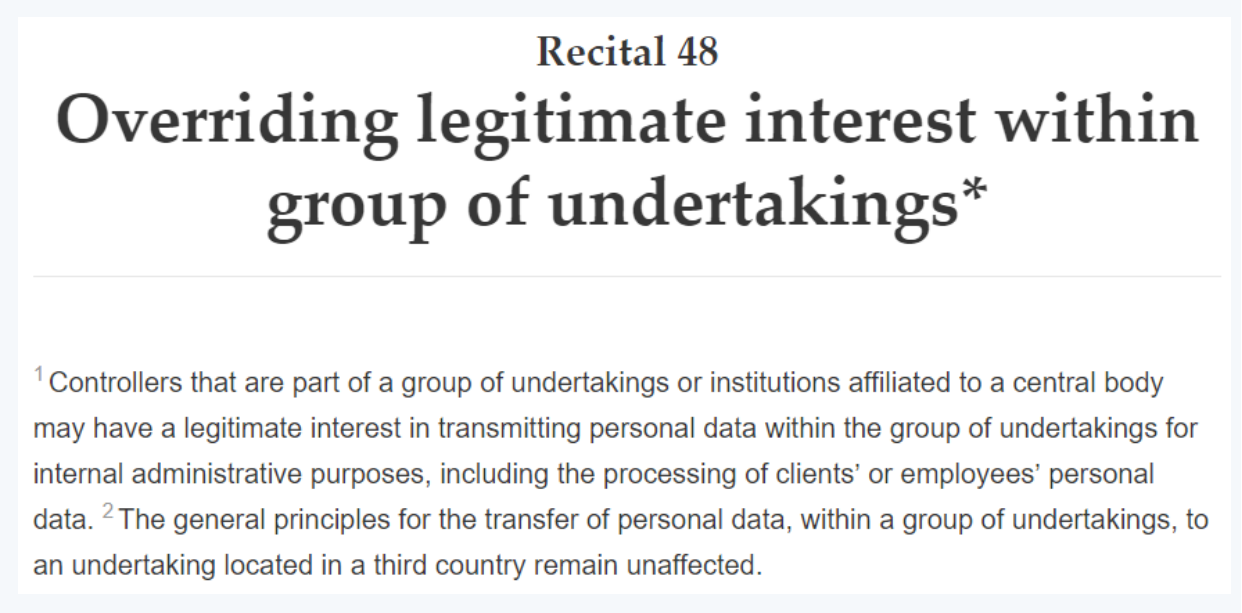
"legitimate interest," it is likely that the data subject could see it as spam and invoke their right to object because the business did not take the rights and interests into account.

The GDPR gives data subjects the *right to object* for this very reason, to ensure that businesses are not taking advantage of the "legitimate interest" clause to process personal data without consent. The right to object is discussed in Recital 69 which we will cover shortly.

Recital 48: Overriding Legitimate Interest Within Group of Undertakings

Recital 48 of the GDPR clarifies that data controllers may consider transferring data within their organization a legitimate interest.

That is, a branch of a company may transfer data to another branch or central administration in order to complete agreed upon tasks. This may seem obvious, but it is helpful as evidence of what is and is not considered legitimate interest under the GDPR.



Recital 48

Overriding legitimate interest within group of undertakings*

[1] Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. [2] The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.

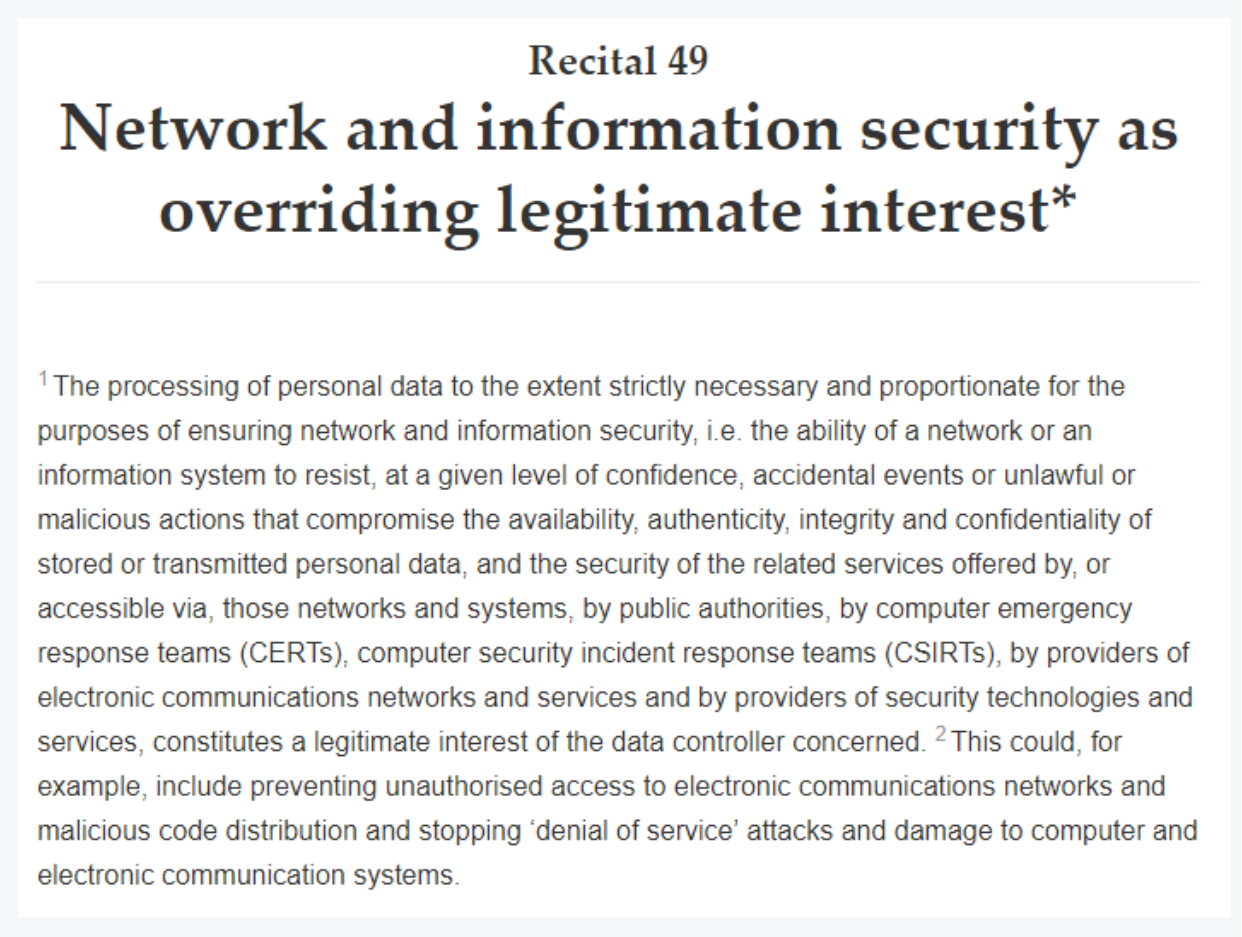
Image: GDPR Info: Recital 48 - Overriding Legitimate Interest Within Group of Undertakings

> ***Recital 48. Overriding legitimate interest within group of undertakings****
>
> *Controllers that are part of a group of undertakings or institutions affiliated to a central body may have a legitimate interest in transmitting personal data within the group of undertakings for internal administrative purposes, including the processing of clients' or employees' personal data. The general principles for the transfer of personal data, within a group of undertakings, to an undertaking located in a third country remain unaffected.*

Recital 49: Network and Information Security as Overriding Legitimate Interest

Recital 49 of the GDPR makes it clear that instances of security and fraud prevention should be considered legitimate interests for data controllers.

We can assume things like notifying users of new updates with **security fixes**, **warning users about fraud attempts**, or **verifying the identity** of users to prevent security breaches would all likely be strong cases for invoking legitimate interest as a legal basis in order to process personal data without consent. After all, these scenarios should be in the interest of the data subjects in order to protect their rights and privacy.


Recital 49

Network and information security as overriding legitimate interest*

[1] The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence, accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. [2] This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.

Image: GDPR Info: Recital 49 - Network and Information Security as Overriding Legitimate Interest

> ***Recital 49. Network and information security as overriding legitimate interest****
>
> *The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security, i.e. the ability of a network or an information system to resist, at a given level of confidence,*

> *accidental events or unlawful or malicious actions that compromise the availability, authenticity, integrity and confidentiality of stored or transmitted personal data, and the security of the related services offered by, or accessible via, those networks and systems, by public authorities, by computer emergency response teams (CERTs), computer security incident response teams (CSIRTs), by providers of electronic communications networks and services and by providers of security technologies and services, constitutes a legitimate interest of the data controller concerned. This could, for example, include preventing unauthorised access to electronic communications networks and malicious code distribution and stopping 'denial of service' attacks and damage to computer and electronic communication systems.*

Article 13: Information to be Provided Where Personal Data are Collected from the Data Subject

Article 13 gives guidelines for what must be shared with data subjects upon the collection and processing of their personal data.

In Section 1(d), it refers to Article 6, saying that the data subject must be informed where processing is based on the legitimate interests of the controller:

(1) Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:

a) the identity and the contact details of the controller and, where applicable, of the controller's representative;

b) the contact details of the data protection officer, where applicable;

c) the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;

d) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

e) the recipients or categories of recipients of the personal data, if any;

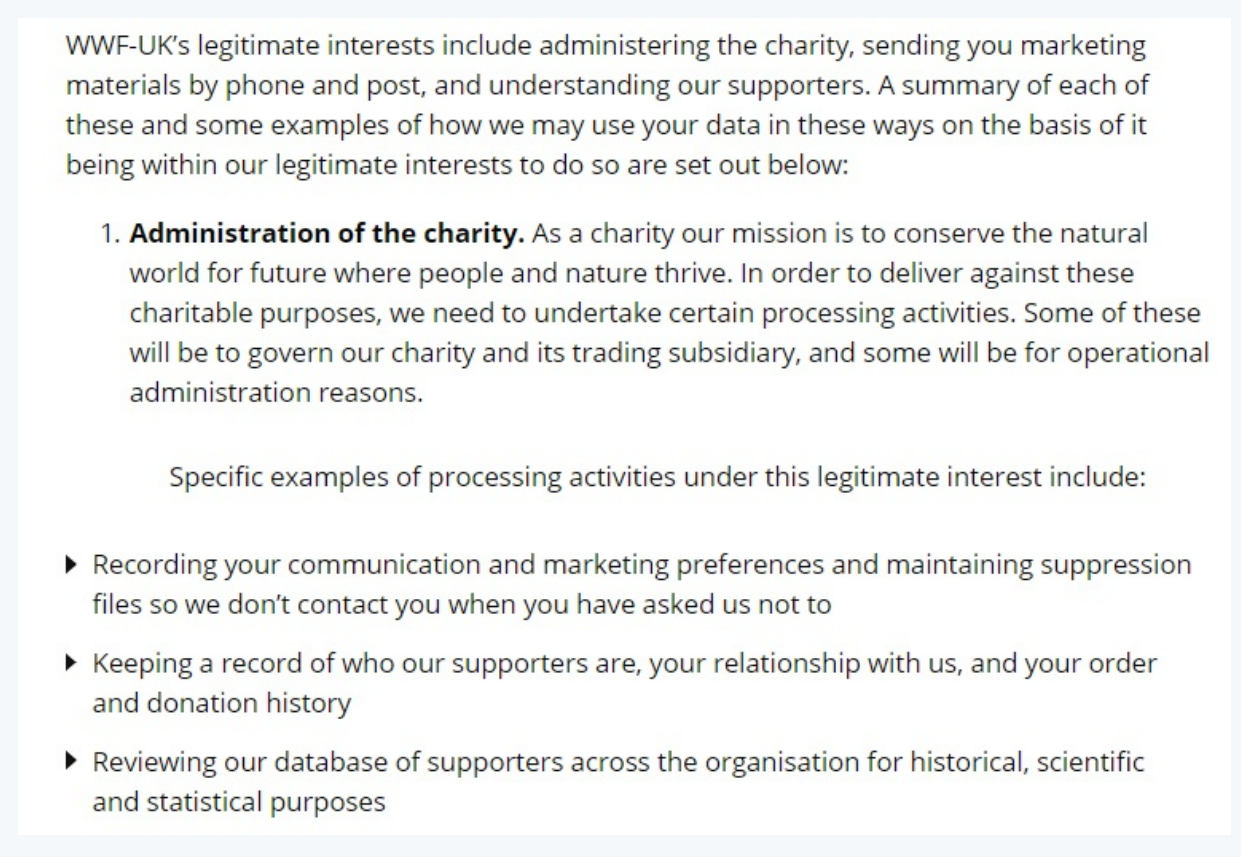
f) where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

Image: GDPR Info: Article 6 Section 1 - Information to be Provided Where Personal Data are Collected From the Data Subject

1. *Where personal data relating to a data subject are collected from the data subject, the controller shall, at the time when personal data are obtained, provide the data subject with all of the following information:*
    a. *the identity and the contact details of the controller and, where applicable, of the controller's representative;*
    b. *the contact details of the data protection officer, where applicable;*
    c. *the purposes of the processing for which the personal data are intended as well as the legal basis for the processing;*
    d. *where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;*
    e. *the recipients or categories of recipients of the personal data, if any;*
    f. *where applicable, the fact that the controller intends to transfer personal data to a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in Article 46 or 47, or the second subparagraph of Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.*

Essentially, this means that if data is being processed on the grounds of legitimate interests, this must be disclosed to the data subject.

This can be done through a **Privacy Policy clause**, like this one:



WWF-UK's legitimate interests include administering the charity, sending you marketing materials by phone and post, and understanding our supporters. A summary of each of these and some examples of how we may use your data in these ways on the basis of it being within our legitimate interests to do so are set out below:

1. **Administration of the charity.** As a charity our mission is to conserve the natural world for future where people and nature thrive. In order to deliver against these charitable purposes, we need to undertake certain processing activities. Some of these will be to govern our charity and its trading subsidiary, and some will be for operational administration reasons.

Specific examples of processing activities under this legitimate interest include:

- Recording your communication and marketing preferences and maintaining suppression files so we don't contact you when you have asked us not to
- Keeping a record of who our supporters are, your relationship with us, and your order and donation history
- Reviewing our database of supporters across the organisation for historical, scientific and statistical purposes

Image: WWF UK Privacy Policy: Legitimate Interests clause

> *WWF-UK's legitimate interests include administering the charity, sending you marketing materials by phone and post, and understanding our supporters. A summary of each of these and some examples of how we may use your data in these ways on the basis of it being within our legitimate interests to do so are set out below:*
>
> *1. **Administration of the charity.** As a charity our mission is to conserve the natural world for future where people and nature thrive. In order to deliver against these charitable purposes, we need to undertake certain processing activities. Some of these will be to govern our charity and its trading subsidiary, and some will be for operational administration reasons.*
>
> *Specific examples of processing activities under this legitimate interest include:*
>
> - *Recording your communication and marketing preferences and maintaining suppression files so we don't contact you when you have asked us not to*
> - *Keeping a record of who our supporters are, your relationship with us, and your order and donation history*

- *Reviewing our database of supporters across the organisation for historical, scientific and statistical purposes*

Article 14: Information to be Provided Where Personal Data Have Not Been Obtained From the Data Subject

Article 14 of the GDPR similarly states that data subjects should be informed if their personal data is being processed on the grounds of legitimate interests when their data is processed without being collected directly from the data subjects.

This ensures that data subjects retain the right to challenge unfair data processing *no matter how* their data was obtained.

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

(a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

(b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

Image: GDPR Info: Article 6 Section 1 - Information to be Provided Where Personal Data Have Not Been Obtained From the Data Subject

2. In addition to the information referred to in paragraph 1, the controller shall provide the data subject with the following information necessary to ensure fair and transparent processing in respect of the data subject:

a) the period for which the personal data will be stored, or if that is not possible, the criteria used to determine that period;

b) where the processing is based on point (f) of Article 6(1), the legitimate interests pursued by the controller or by a third party;

Article 14 also states that data subjects should be informed how legitimate interests justify any further processing of their personal data.

Data Controller Interests Versus Data Subject Interests

The conclusion we can draw is that if a data controller has a **good and compelling reason** (a legitimate interest), they may process data without another legal basis *so long as* it does not infringe on the rights, freedoms, or interests of the data subject.

The GDPR states that you must consider the legitimate interests *of the individual* before processing their data. You must weigh their rights, freedoms, and interests against your reason for processing their data and be able to prove that it is fair and proportional.

If you have any doubt, you are better off asking for consent or using another legal basis from Article 6.

Chapter 6:

User Rights Under the GDPR

While the majority of the GDPR lays out the rules and guidelines for those who wish to collect or process the personal data of residents of the EU, Chapter 3 focuses on the rights of those data subjects whose personal information is being handled.

By clearly spelling out the rights of data subjects and how these rights affect data handlers, the GDPR creates a **system of checks and balances** to ensure that data subjects have forms of recourse in the event that their personal information is abused or mishandled.

Image: TermsFeed illustration of a man giving a presentation

By informing both data subjects and data controllers/processors of these rights, all parties involved are made aware of how personal data should be handled so that they can keep an eye out for accidental or purposeful mishandling.

For example, the *right to rectification* gives data subjects the right to review and correct their personal data in the event that it is incorrect or changes. The GDPR has rules in place requiring data controllers to have a procedure for making these corrections, and gives the data subjects the right to have those corrections made.

By including this right into the data subject-data controllers relationship, there is rarely a need for intervention from an authority and the data subjects themselves are able to **police their own data**.

Without these rights, it would be nearly impossible for the authoritative body to monitor all data handling in the EU.

The right to rectification is just one of the **eight fundamental rights of the GDPR** which empower data subjects to have their personal information used only how they wish within the confines of the law.

Let's take a look at these rights and how they protect the privacy of data subjects.

The Eight Data Subject Rights of the GDPR

The eight fundamental rights of data subjects under the GDPR can be found in Articles 15 through 22. These rights can be summarized as follows:

1. The right to **be informed**
2. The right of **access** by the data subject
3. The right to **rectification**
4. The right to **erasure** (commonly referred to as "the right to be forgotten")
5. The right to **restriction of processing**
6. The right to **data portability**
7. The right to **object**
8. The right to **human intervention**

You may be able to infer what some of these rights entail in part or in whole, but let's discuss each one so that we have a complete understanding of what they entail.

The Right to Access

Article 15 of the GDPR describes the right of access by the data subject.

This right allows individuals to know if a data controller or processor possesses personal information about them and if that information is being processed.

The individual also has the right to request access to that information as well as answers to any of the following questions:

- What is the **purpose** for processing my data?
- What **categories** of my personal data are being processed?
- With whom has my personal information been **shared** (or with whom will it be shared in the future)?
- **How long** will my information be kept?
- Can my information be **updated**, **restricted**, or **erased**?
- Can the processing of my data be **objected to**?
- Who is the supervisory authority if I need to **lodge a complaint**?
- What is the **source** for personal data not directly collected from me?
- Is my data used for **automated decision-making**?
- **What effect** might automated decisions have on me?

Article 15 also states that data subjects may request **a copy of their personal data** from the data controller. It goes on to say that data subjects should be informed of the safeguards in place if their personal data is transferred out of the country.

To summarize, the right to access gives data subjects the right to know if and what information about them is being stored or processed, why it is being processed, with whom it is being shared, and how long it will be kept.

The Right to Rectification

Article 16 of the GDPR covers the right of rectification, which in essence says that data controllers **must correct**, **update** or **complete personal data that is inaccurate or incomplete** at the request of the data subject.

This goes along with the right of access in Article 15, where data subjects can request a copy of their personal data, know if it is being processed, and know if it can be updated. This way data subjects can check their personal data to ensure that it is accurate, complete, and up to date, and request corrections if it is not.

The Right to Erasure

Commonly known as “the right to be forgotten,” **Article 17** of the GDPR covers the right to erasure. This right gives data subjects the power to request that their personal information be deleted without undue delay under any of the following circumstances:

- The data is **no longer needed** to complete the task for which it was collected
- **Consent is withdrawn** and there is no other legal basis for processing the data
- The data subject **objects**, as per the right below
- The data has been **unlawfully processed**

There are a few exceptions to this rule (such as in order to defend against legal claims), but in most cases data subjects have “the right to be forgotten” if they no longer wish to have their personal data used by an organization.

The data controller must make a *reasonable effort* to erase all data that they possess including what has been shared with other entities and cease all processing of that data.

The Right to Restriction of Processing

Article 18 lays out the rules for restricting processing in cases where the data subjects wishes to enforce control over their personal information without enacting the right to erasure.

Data subjects may enforce this right in any of the following situations:

- When a data subject **contests the accuracy** of their personal information
- When personal data has been **unlawfully processed**
- When the controller **no longer needs** the data but the data subject does not want it deleted for legal reasons
- When the **right to object** has been used

Data subjects may restrict the processing of their personal information to only operations for which they have given express consent or for legal reasons, and the data controller must inform the data subjects before the restriction is lifted.

The right to restriction allows data subjects to *control their data even if they do not wish for their data to be erased*.

This can be crucial for legal claims that require evidence, though the data subject no longer wants his or her data processed for other reasons. It is also important in situations where

objections or investigations take place and a temporary pause is to be put on the data to prevent further processing.

Notification Obligations

Article 19 discusses the notification obligations of data controllers in the event that a data subject enacts the right to rectification, erasure, or restriction as described in Articles 16, 17, and 18. The data controller is required to notify the third parties with whom the data has been shared so that the third parties may also rectify, erase, or restrict the use of that data.

This ensures that a data subject's personal information can be corrected, erased, or restricted by all parties that possess it, not just the data controller.

Otherwise the data controller would simply delete the data it possesses and the third party processor would continue to use it.

Article 19 goes on to say that data subjects have the right to request to know the recipients of their personal data so that they can ensure all copies of their personal information are rectified, erased, or restricted as per the data controller's notification obligation.

The Right to Data Portability

Article 20 of the GDPR covers the right to data portability. This right only applies to data that's processed based on **either consent or a contract**, **and** that's **processed using automated means**.

In such a case, this right gives data subjects the ability to request a copy of their personal data in a structured, commonly used and machine-readable format. When technically feasible, the data subjects can request the information be transmitted to a different business for processing.

The Right to Object

Article 21 of the GDPR gives data subjects the right to object to the processing of their personal data if they believe that there is not a legal basis for doing so as described in Article 6 of the GDPR.

Let's take a look at that section:

1. [1] The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. [2] The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.
2. Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.
3. Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes.
4. At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.
5. In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.
6. Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.

Image: GDPR Info: Article 21 - Right to Object

1. *The data subject shall have the right to object, on grounds relating to his or her particular situation, at any time to processing of personal data concerning him or her which is based on point (e) or (f) of Article 6(1), including profiling based on those provisions. The controller shall no longer process the personal data unless the controller demonstrates compelling legitimate grounds for the processing which override the interests, rights and freedoms of the data subject or for the establishment, exercise or defence of legal claims.*
2. *Where personal data are processed for direct marketing purposes, the data subject shall have the right to object at any time to processing of personal data concerning him or her for such marketing, which includes profiling to the extent that it is related to such direct marketing.*
3. *Where the data subject objects to processing for direct marketing purposes,*

> *the personal data shall no longer be processed for such purposes.*
> 4. *At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information.*
> 5. *In the context of the use of information society services, and notwithstanding Directive 2002/58/EC, the data subject may exercise his or her right to object by automated means using technical specifications.*
> 6. *Where personal data are processed for scientific or historical research purposes or statistical purposes pursuant to Article 89(1), the data subject, on grounds relating to his or her particular situation, shall have the right to object to processing of personal data concerning him or her, unless the processing is necessary for the performance of a task carried out for reasons of public interest.*

In the event that a data subject challenges a data controller's legal basis, *any processing of their data should be postponed* until the data controller can prove its legal basis for doing so.

Under Article 21, data subjects also have the right to object to **direct marketing**, including more general forms of targeting such as demographic profiling. If a data subject objects to direct marketing, any processing of their personal data for such reasons must cease.

Recital 69 gives individuals the right to object to or challenge when a business invokes legitimate interest as a legal basis for processing their personal information. If an individual feels that the business' legitimate interests interfered with their own rights or interests, then that individual may challenge the decision.

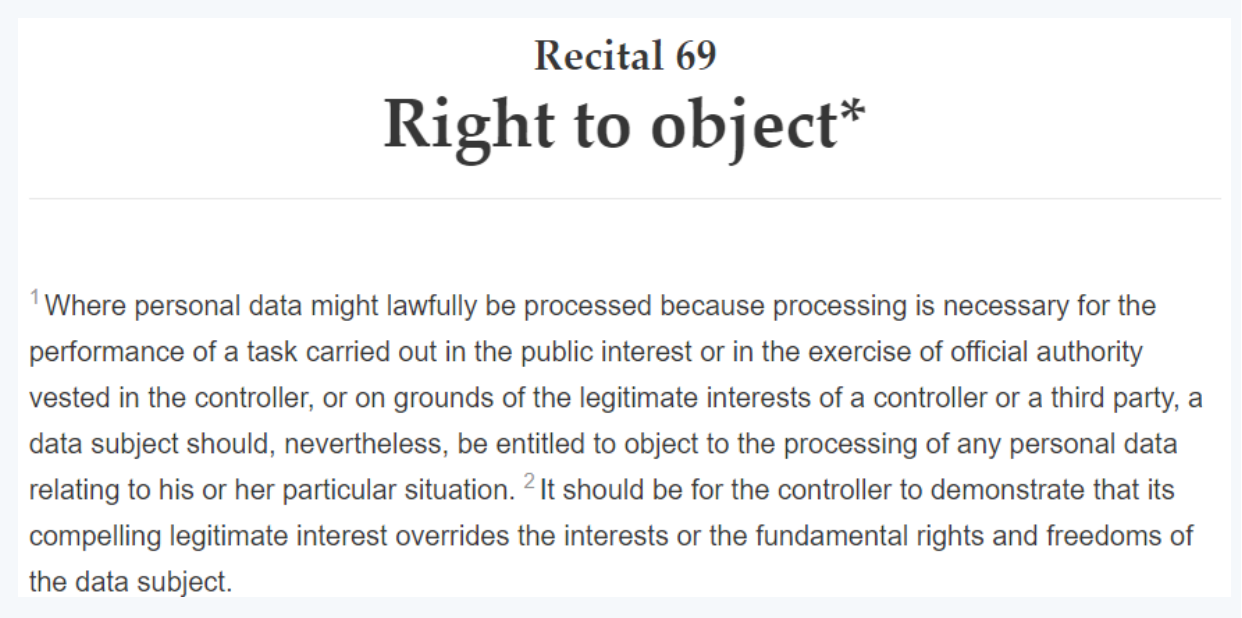


Image: GDPR Info: Recital 69 - Right to Object

> ***Recital 69. Right to object****
>
> *Where personal data might lawfully be processed because processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller, or on grounds of the legitimate interests of a controller or a third party, a data subject should, nevertheless, be entitled to object to the processing of any personal data relating to his or her particular situation. It should be for the controller to demonstrate that its compelling legitimate interest overrides the interests or the fundamental rights and freedoms of the data subject.*

For example, if a website collects shipping addresses for delivering products purchased online, then the company sends advertisements to those same addresses without obtaining consent to do so, some of the recipients may see this as undesirable junk mail.

Those data subjects would have the right to challenge the website's decision to use their shipping information in this manner without permission. If it was found that the website was indeed infringing on the rights of their data subjects, the data controller would likely be penalized.

Recital 69 also stipulates that it is the responsibility of the data controller to prove that its legitimate interests are compelling and override the rights, freedoms, and interests of the data subjects who challenged them. Such a situation could quickly turn into a costly burden, which is why understanding the law regarding legitimate interests is so important.

The Right to Human Intervention

Article 22 of the GDPR discusses user rights in the event of automated decisions. Here is the exact language of Section 1 of Article 22:

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

Image: GDPR Info: Article 22 Section 1 - Automated Individual Decision-making Including Profiling

> 1. *The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.*

This right protects data subjects from poor decisions that human intervention might prevent but automated processes do not.

Note that Section 1 of Article 22 does not apply in cases where:

- **Express consent is given** for the automated processes
- Automated processes are **necessary to complete a contract** between the data subject and the data controller
- Another relevant and adequate law from the Union or a Member State **allows it**

The above exceptions are still subject to human intervention and the data subject can object if they do not agree with how their data is being processed.

The data controller is still responsible for having suitable safeguards in place to protect the rights and privacy of data subjects, and these data subjects should, at the very least, be able to express their concerns and obtain human intervention on the part of the data controller.

Data Controller Obligations

While all of these rights should be reviewed and understood by *both* data controllers and data processors to ensure a complete understanding of the GDPR, some of the user rights are targeted primarily at controllers while others are meant for processors. Most *of the responsibility falls on data controllers* as they decide what is done with the data and who has access to it.

Let's take a look at which rights pertain more directly to the data controller and why:

The Right to Access

The right of access gives users the right to find out if a data controller or processor possesses or is processing their personal data. This includes knowing what information is possessed, why it is being processed, and who is processing it.

While **Article 15** of the GDPR specifically mentions both data controllers and data processors, the fact that a data controller must notify inquiring users of who their data has been shared with makes the **data controller the obvious choice** when invoking the right of access.

The right of access pertains more to data controllers as they are the *ones who possess that data*.

Data processors only possess this data for a limited time until the task they were recruited for is completed. As the probable collector of the data, the data controller is the one who is more likely to have to deal with data access requests and inform users what is being done with their data and send copies of that data if requested.

Data controllers must answer all of the questions in Article 15 if requested by a data subject, while only some of these questions are usually answerable by data processors.

The Right to Rectification

This right applies **more often to data controllers**.

This is because any corrections requested by a data subject would first be corrected in the records of the data controller who is utilizing and potentially sharing that data before ensuring that it is corrected elsewhere along the path of distribution.

Since the data processor only processes the data it is provided with from the data controller, it is usually the responsibility of the data controller to **ensure that the data it possesses is accurate** and up to date.

Most rectification requests will be sent to the data controller and corrected in the controller's database.

The Right to Erasure

The right to erasure is usually targeted at the **data controller** for the simple reason that it requires the erasure of said data *at every level*. That is, after the request has been made by the data subject, the data controller is responsible for seeing that all parties with whom the data has been shared also erased their copies of the data in question.

The request will usually be sent to the data controller who is then responsible for notifying any data processors it employs to also erase any copies of that data that have been shared with them.

For this reason, it makes sense for individuals to simply *invoke this right to the data controller* and have the controller notify the processors it's affiliated with and direct them to delete the data.

Data Processor Obligations

While data controllers are largely responsible for ensuring that personal data is handled properly by all parties involved, some of the user rights are intended particularly for the data processor or affect both data controllers and data processors equally.

These are:

The Right to Erasure

While the request to invoke the right of erasure is usually handled between the data subject and data controller, data processors must also be aware of this right and have a procedure in place for how to handle it.

The request may come from the data controller or the data subject directly, but in either case the data processor has the obligation to erase the data in question when applicable.

The Right to Restriction of Processing

The right to restrict processing can be invoked for *either* a data controller or data processor. If the request goes to the data controller, the data controller is obligated to notify any data processors it employs about the request for a data processing restriction.

But keep in mind that since either the data controller or data processor may be responsible for the action that led to a request for data restriction, either could be the recipient of the request directly from the data subject and may be the only party affected.

The Right to Rectification

Again, while this request will usually be made to data controllers, data processors should also have a procedure in place so that they can make corrections and updates to the information they possess and process about a data subject.

Continuing to process inaccurate or incomplete data after the right to data rectification has been invoked could potentially land the data processor and data controller in hot water.

User Rights Summaries

1. The **right of access** gives data subjects the right to know if their personal information has been collected and is being processed, as well as what information, why and by whom.
2. The **right to rectification** gives data subjects the right to have their personal information corrected and updated in the records of data controllers and processors.
3. The **right to erasure** gives data subjects the right to have their personal information deleted from the records of data controllers and processors.
4. The **right to restriction of processing** gives data subjects the right to pause, postpone, and limit the processing of their personal information.
5. The **right to notification** gives data subjects the right of having data controllers and data processors notify other data processors of requests made for rectification, erasure, and restriction of their data to ensure all parties are informed of the data subject's will.
6. The **right to data portability** ensures that the data subject retains ownership of their personal data and can request copies and transfers of their data to do with as they please.
7. The **right to object** gives data subjects the right to object to data collection and processing activities that they feel infringes on their rights or is not compliant with the GDPR in order to protect their privacy and interests.
8. The **right to human intervention** ensures that data subjects will not face the consequences of automated decisions without their consent, and grants the ability to request human intervention.

Remember that some of these rights only apply in *specific circumstances* and may come with *exceptions*. Become familiar with the details of each, when each applies and how to facilitate each right.

Chapter 7:

How the GDPR Affects Your Online Business/Online Presence

So far we've looked at the substance of the GDPR and how it applies in theory. Now we'll look in detail at how the law applies to online businesses, and consider the **practical steps** you can take to ensure you're compliant.

Firstly a reminder - with a few exceptions (such as the requirement to keep data processing records) the GDPR doesn't discriminate in terms of company size. It applies to everyone from huge multinational conglomerates like Google, all the way down to lone bloggers who aren't even pursuing a profit.

Image: TermsFeed illustration of a man on a computer and a man with EU flag spying in window

The GDPR doesn't care who you are. Its focus is on what you're **doing**.

Business websites and apps can process a lot of personal data, and sometimes they do so without even really thinking about the implications.

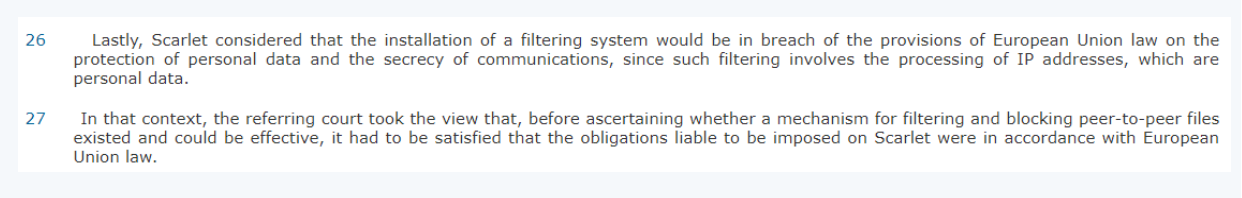
Let's consider the ways in which a website or app might be collecting personal data:

- Analytics
- Cookies
- Checkout pages
- Contact forms

The GDPR refers specifically to "online identifiers" as an example of personal data. We have to look to the EU's guidance and case law for an understanding of the implications of this.

For example, one such online identifier is the **IP address**. There are two cases from the EU's Court of Justice that confirms that an IP address falls under the scope of EU privacy law.

The first case was Scarlet Extended. Here's an excerpt of what the Court said:



26 Lastly, Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of IP addresses, which are personal data.

27 In that context, the referring court took the view that, before ascertaining whether a mechanism for filtering and blocking peer-to-peer files existed and could be effective, it had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with European Union law.

Image: InfoCuria: Scarlet Extended Judgment document sections 26 and 27

> *26 Lastly, Scarlet considered that the installation of a filtering system would be in breach of the provisions of European Union law on the protection of personal data and the secrecy of communications, since such filtering involves the processing of **IP addresses, which are personal data**.*
>
> *27 In that context, the referring court took the view that, before ascertaining whether a mechanism for filtering and blocking peer-to-peer files existed and could be effective, it had to be satisfied that the obligations liable to be imposed on Scarlet were in accordance with European Union law.*

The second was Breyer v Germany, in which the Court said that the definition of personal information can extend to include even **dynamic IP addresses**.

The principles of the GDPR need to permeate through every stage of your online business. This sounds like a lot of work. It might be - but you may find you're already applying a lot of what the GDPR requires. And once you've done the required work, you'll be left with a **safer**, **cleaner** and **more transparent** set of practices. This is a good thing in itself.

Data Protection By Design and By Default

A key concept in the GDPR is set out at **Article 25** - "*data protection by design and by default*."

Data protection by design means creating systems in such a way that builds on the principles of the GDPR. This includes ensuring any areas where personal data is processed are adequate and secure.

Data protection by default means minimizing the amount of personal data that is processed and always choosing the least intrusive methods. Where there is a choice between processing a little bit of personal data or a lot of personal data, the default setting should be the lowest.

Here are some examples provided by the European Commission:

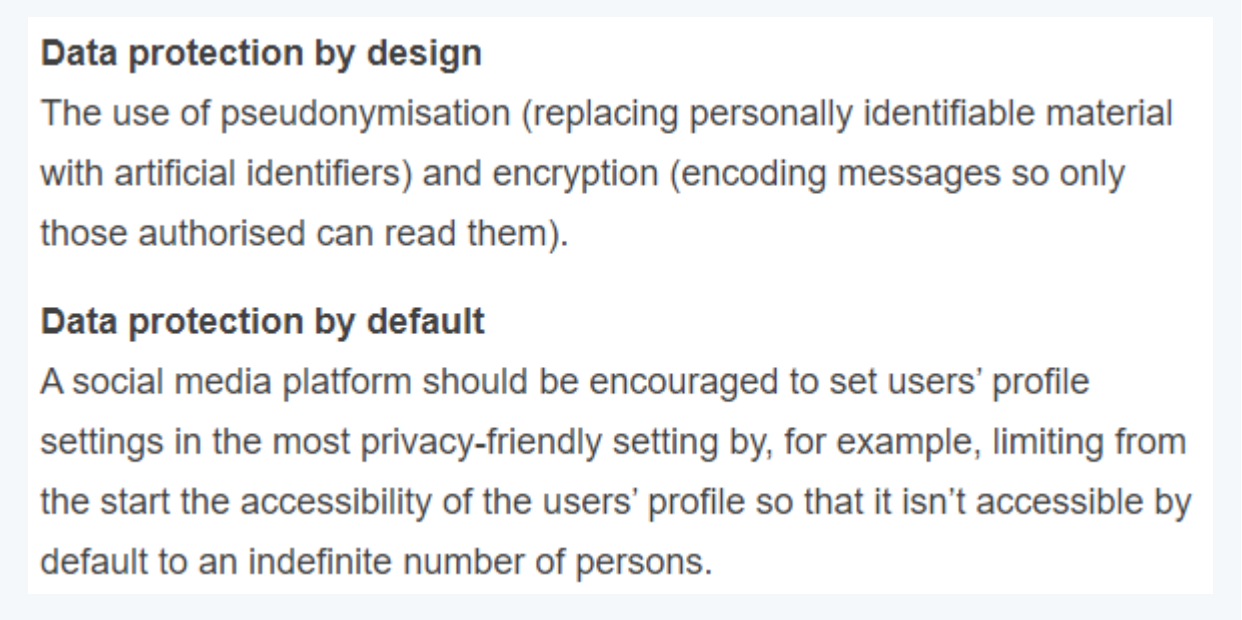


Image: European Commission: Definitions of Data protection by design and by default

> ***Data protection by design***
> *The use of pseudonymisation (replacing personally identifiable material with artificial identifiers) and encryption (encoding messages so only those authorised can read them).*
>
> ***Data protection by default***
> *A social media platform should be encouraged to set users' profile settings in the most privacy-friendly setting by, for example, limiting from the start the accessibility of the users' profile so that it isn't accessible by default to an indefinite number of persons.*

These principles are dealt with throughout this book. We're now going to take a look at how they apply to a specific aspect of online business.

Legitimate Purposes for Data Collection

Under Article 5 (1)(b) of the GDPR, and as discussed in Chapter 5 [LINK TO CHAPTER 5], personal data can only be collected for "*specified, explicit and legitimate purposes.*" This means that data controllers must only collect personal data, by whatever means, when they have a **good reason** for doing so.

How is this relevant to online businesses? By way of example, let's imagine a scenario where a website might infringe this principle.

A form captures email addresses in order to sign users up to a mailing list:

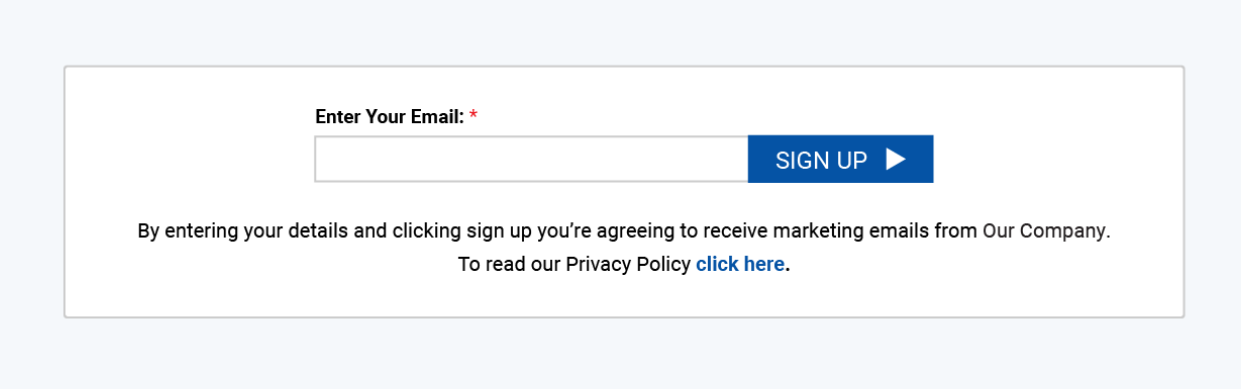


Image: Generic email sign-up form

The form is GDPR-compliant in that it makes the **purposes** of collecting the personal data clear: to receive marketing emails.

In its Privacy Policy, the data controller can explain to its users **how long** it will retain their email address data, and how users can withdraw **consent** or request the data **deletion**. It makes no mention of any other use of the email addresses except for its own marketing purposes.

Now imagine the company starts sharing these email addresses with third parties so the third parties could start sending marketing emails to the individuals. This would be a problem.

The users **didn't consent** to this, nor were they **informed** about it. This is processing personal data in a way that is not consistent with the purposes for which it has been collected.

The data controller would need to change the text in the box above to say something like "*...you're agreeing to receive marketing emails from OKA and third parties that OKA selects.*"

It would also need to update its Privacy Policy to include a clause that lets users know that email addresses may be shared with third parties, and for the purpose of marketing.

Minimize Data Collection

Your website is likely to collect a lot of information from users in a number of different ways. Some ways are more overt like with an email address sign-up form, but some may be less detectable, if detectable at all.

For example, referral data (or “referrer data”) is collected in logs and provides information about how a user arrived at the site. This type of log data might show, for example, the details of the site from which a user clicked through. This can be helpful in, for example, determining the effectiveness of affiliate marketing campaigns, personalized advertising campaigns and even analytics purposes.

In addition to requiring that personal data is only collected in connection with a specified purpose, at Article 5 (1)(c) the GDPR requires that any personal data processed is “***relevant*** *and* ***limited*** *to what is* ***necessary***” for fulfilling those purposes.

Your business will need to consider the principle of **data minimization** when determining how your business website collects data. And remember that any data about a person’s web browsing activity can be personal data insofar as it relates indirectly to an identifiable person.

There are many people who would guard their web browser history more closely than their credit card information. The fact that referrer data only provides information about the previous website a user visited does not negate the requirement to treat this information as personal data. This could be very private information.

In light of this, it’s clear why certain web browsers, such as Firefox, provide the option to prevent the sending of referral information by disabling the Referer header in an HTTP request.

Anonymization of Data

Where personal data, such as IP addresses, is collected in log files, this data should be **anonymized** whenever possible. One personal data is anonymized, and any identifiers have been **irreversibly erased** (*not* simply masked) it’s no longer capable of leading to the identification of an individual. It is therefore no longer personal data, and the GDPR doesn’t apply to it.

This is confirmed by guidance from the UK’s Data Protection Authority, the Information Commissioner’s Office (ICO) (at page 6 of the linked PDF):

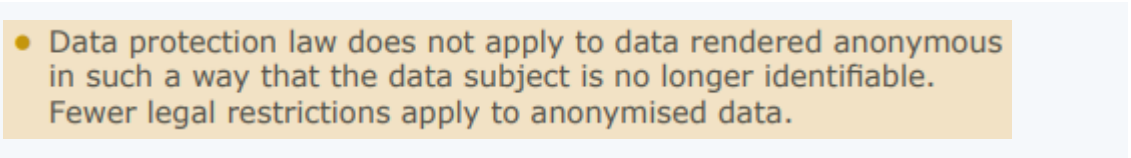


Image: ICO Anonymisation: Managing Data Protection Risk Code of Practice - Data protection law does not apply to data rendered anonymous

> - *Data protection law does not apply to data rendered anonymous in such a way that the data subject is no longer identifiable. Fewer legal restrictions apply to anonymised data.*

The Article 29 Working Party, however, does note that anonymized data is still covered by certain privacy law such as the ePrivacy Directive.

It is clear that it's in a data controller's interests to ensure that personal data is anonymized.

Let's look at how the identifier most commonly found in log files, an IP address, can be anonymized. A common suggestion, that comes both from the ICO and from IntArea, is to **remove certain octets** of an IP address to render it anonymous.

This is the strategy employed by Google Analytics in order to anonymize IP addresses:

> When a customer of Analytics requests IP address anonymization, Analytics anonymizes the address as soon as technically feasible at the earliest possible stage of the collection network. The IP anonymization feature in Analytics sets the last octet of IPv4 user IP addresses and the last 80 bits of IPv6 addresses to zeros in memory shortly after being sent to the Analytics Collection Network. The full IP address is never written to disk in this case.

Image: Google Analytics Help: IP Anonymization summary

> *When a customer of Analytics requests IP address anonymization, Analytics anonymizes the address as soon as technically feasible at the earliest possible stage of the collection network. The IP anonymization feature in Analytics sets **the last octet of IPv4 user IP addresses and the last 80 bits of IPv6 addresses to zeros** in memory shortly after being sent to the Analytics Collection Network. The full IP address is never written to disk in this case.*

As noted, this occurs before the IP address is ever recorded:

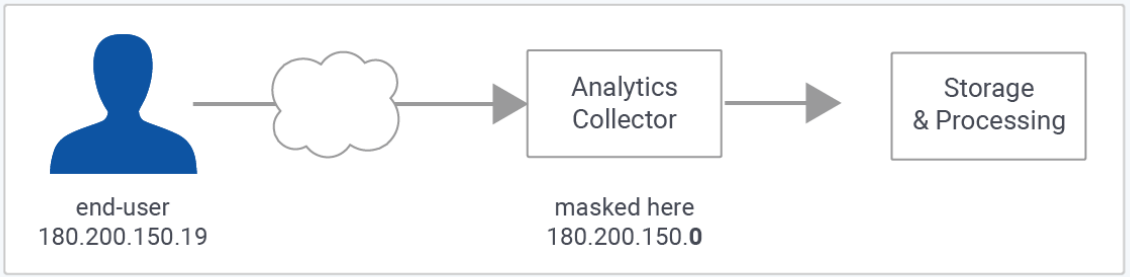


Image: Generic Google Analytics: IP Anonymization flow diagram

IntArea actually advocates going further than this, suggesting that the **last two octets** of an IPv4 address are removed. This would turn "12.214.31.144," in Google's example, into "12.214.0.0."

Pseudonymization or Encryption of Data

If log files can't be anonymized and must contain personal data, any identifiers within the files should be **pseudonymized or encrypted**. Remember that this extends to dynamic IP addresses. There may be a good reason for retaining personal data in logs, but it must be treated carefully.

Image: Logo of Aol.

Pseudonymized or encrypted personal data in log files is still subject to all the safeguards of the GDPR. Don't be like AOL. In 2006, AOL released a database of search logs attributable to 650,000 users. AOL had taken certain measures to pseudonymize the data by replacing each user's login with a numerical code. This was not enough to prevent some of the users being personally identified when the data was made public.

The act of de-identification, whether by pseudonymization or any method of encryption, requires balancing the **usability and accessibility** of the data against the level of security. If personal data must be retained logs, it should remain accessible in case it is subject to a rights request from the user.

Here's an example.

A website logs data about a user's activities. This includes data about the occasions on which that user accessed the site and records of form entries. The personal data needs to be **secure** enough to limit the amount of damage that would be caused in the event of a security breach. But it would also need to be **accessible** enough to allow a staff member (with the appropriate access permissions) to retrieve the data and present it to the user in the event of a subject access request.

Equally, if personal data is retained in log files, it must be because there is some **operational reason** for it to remain accessible. Where log data is pseudonymized or encrypted and can be decrypted via a key, this key must be kept **securely** and in a **separate location** from the pseudonymized or encrypted log data. Companies must only allow very privileged access to anything that enables the interpretation of personal data stored in log files.

Think of pseudonymization or encryption techniques as a lock on the front door. The lock can be extremely effective. But if the key is left under the mat, it won't be hard for someone to break in.

It should be clear that, for this reason among many others, the collection of personal data in the log files should be **kept to a minimum**.

Storage Limitation and Log Files

At Article 5 (1)(e), the GDPR states that personal data must not be stored for a period longer than is necessary. This is known as the principle of **storage limitation.**

How long is it really **necessary** for you to store log data? IntArea suggests that IP addresses in server logs are erased after **three days**. Unless they really need to be kept for longer, there's no downside to pruning log files regularly:

- It means there is less data sitting around, thus reducing the **risk** of a harmful breach.
- It saves **storage** space. Log files can get bloated quickly.
- There will be no requirement to **provide** this information to a user in the result of a subject access request, or find it and **delete** it in the result of an erasure request, etc.

A utility such as logrotate can help you manage your log files. It can be used to automatically delete log files and "**shred**" them by overwriting them a specified number of times. This should ensure that log files are not readable post-deletion.

Centralized Management and Storage of Data

In the context of the GDPR, there are two good reasons to have a centralized system for managing and storage of log data:

1. It allows for more efficient **detection** and **analysis** of security issues
2. It helps with the **facilitation** of data subject rights requests

The National Institute of Standards and Technology (NIST) produced some guidance on log management that advocates implementing a centralized system. Bear in mind that this guidance is quite old, having been written in 2006, but it provides some valuable insight into the principles of log management.

The importance of the effective management and accessibility of log files is highlighted by this story of a Facebook user who submitted a subject access request. Facebook was unable to facilitate the request to provide sensitive log data to an individual user because of the way in which the data is indexed and stored in its logs. This led to the user lodging a complaint with Ireland's Data Protection Authority.

Doing the necessary work to ensure that logs are **well-indexed** and **centrally accessible** (in a secure way, by people with appropriate clearance) could prevent serious problems in the long term.

Lawful Basis for Processing Data

As mentioned in other chapters, all processing of personal data must take place under one of the six lawful bases. Let's consider how the lawful bases might apply to the processing of IP addresses in logs. Remember that this needs to be considered even if IP addresses are pseudonymized or encrypted.

Under certain conditions, it is possible to process someone's personal data where you have a **legitimate interest** in doing so. This is established in Article 6 (1)(f). Where there is a legitimate interest in processing someone's personal data in a particular way, there is no need to request the person's **consent**.

A Legitimate Interests Assessment is required to establish legitimate interests as a lawful basis for processing. The ICO suggests a particular format for this assessment known as the "three-part test":

1. The purpose test (identify the legitimate interest);
2. The necessity test (consider if the processing is necessary); and
3. The balancing test (consider the individual's interests).

Let's apply this to the storing of IP addresses for security reasons.

The Purpose Test

Can there be a legitimate reason why a developer or web admin might need to log IP addresses? One potential reason is for **security purposes**, e.g. in order to detect and guard against denial of service (DoS) attacks.

In the case of Breyer v Germany the EU's Court of Justice decided that the storing of IP addresses for security purposes can, in theory, constitute a **legitimate interest**.

This is also reflected in Recital 49 of the GDPR, which states that:

> "*The processing of personal data to the extent strictly necessary and proportionate for the purposes of ensuring network and information security* [...] *constitutes a legitimate interest* [...]"

So, storing IP addresses for security reasons **passes the purpose test**.

The Necessity Test

"Necessity" is defined in quite a broad way by the ICO in this instance. Here are some of the questions that the ICO suggests considering:

- Will the processing actually help you achieve your purpose?
- Is the processing proportionate to that purpose, or could it be seen as using a sledgehammer to crack a nut?
- Can you achieve your purpose without processing the data, or by processing less data?
- Can you achieve your purpose by processing the data in another more obvious or less intrusive way?

There could be various **technical justifications** for logging IP addresses for security purposes. If a website is being repeatedly spammed in a DoS attack, an examination of the logs could help identify the origin of the attack.

If it's possible to meet the security needs of a website or app in a way that does *not* involve processing personal data, then this will almost always be preferable, unless it involves a disproportionate amount of extra effort.

Assuming there is no viable alternative, processing IP addresses for security reasons **passes the necessity test**.

The Balancing Test

Finally, the balancing test requires consideration of the following according to the ICO:

- the **nature of the personal data** you want to process;
- the **reasonable expectations** of the individual; and
- the **likely impact** of the processing on the individual and whether any safeguards can be put in place to mitigate negative impacts.

This is a matter of balancing the **risks** and the **privacy rights** of the individual against the **legitimacy** and **necessity** of the processing of their personal data.

While it is technically feasible to identify someone even from a dynamic IP address, this is fairly **low-risk** personal data.

But the **context is important**. A list of IP addresses that have accessed a dating app or adult website is **more sensitive** than a list of IP addresses that have accessed an online grocery store.

As long as IP addresses are **pseudonymized** or **encrypted** then it's most likely that this act of processing personal data **passes the balancing test**.

If you can pass all three tests, this means it's not normally necessary to ask for permission (consent), or wait until someone's life depends on it (vital interests), in order to be allowed to collect and store IP addresses for security purposes.

Bear in mind if you wish to rely on legitimate interests, you'll need to conduct this assessment and relate it to your own specific data processing requirements.

Working with Third Parties

Businesses rarely build absolutely everything in their websites from the ground up. They will almost always use some **third parties** throughout the development, maintenance and distribution processes of their sites.

Compliance with the GDPR is a requirement both when:

- Integrating third-party services **into a project** - for example, running analytics software on a website, or
- Integrating a project **into third-party services** - for example, distributing an app through a mobile marketplace

Software or service providers who process personal data for, or on behalf of, their customers will want those customers to comply with privacy law. These third parties will often specify this in their Terms and Conditions. Sometimes they also make **specific demands** about ***how*** their customers comply with privacy law.

In this section, we're looking at these requirements. The key takeaway from this section is that developers must be careful to **read the Terms & Conditions** of any third party companies they use. These Terms & Conditions can have specific instructions about the privacy practices of developers in building their website, app or other software.

Using third-party services also has other legal implications that are discussed more generally throughout this book.

Google EU User Consent Policy

Google products are practically ubiquitous across the web, and many developers use them in producing websites and apps. We're going to look at the specific requirements of some of these products below. But first, it's worth noting that Google has a blanket EU User Consent Policy that applies across many of its products.

Let's take a look at what Google's EU User Consent Policy requires:

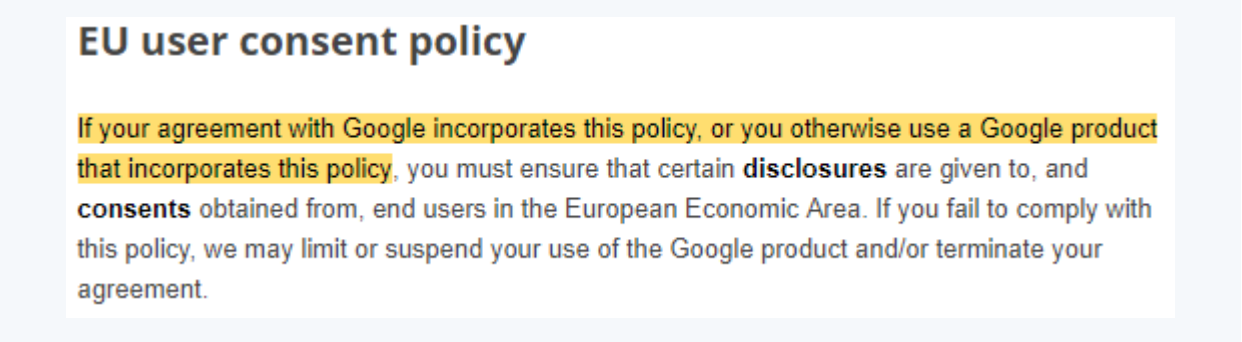


Image: Google EU User Consent Policy: Intro section

> ***EU user consent policy***
>
> ***If your agreement with Google incorporates this policy, or you otherwise use a Google product that incorporates this policy****, you must ensure that certain* ***disclosures*** *are given to, and* ***consents*** *obtained from, end users in the European Economic Area. If you fail to comply with this policy, we may limit or suspend your use of the Google product and/or terminate your agreement.*

First Google says that its EU User Consent Policy is **incorporated** into policies for other products. Google has a bewildering number of policies across its services, and many of them point to other policies or sets of policies that must also be obeyed.

For example, the EU User Consent Policy is incorporated into the policy of any product involving personalized advertising, such as Google Ads:

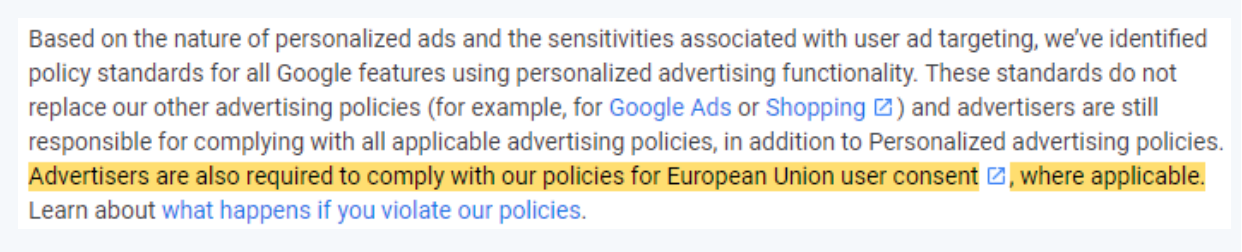
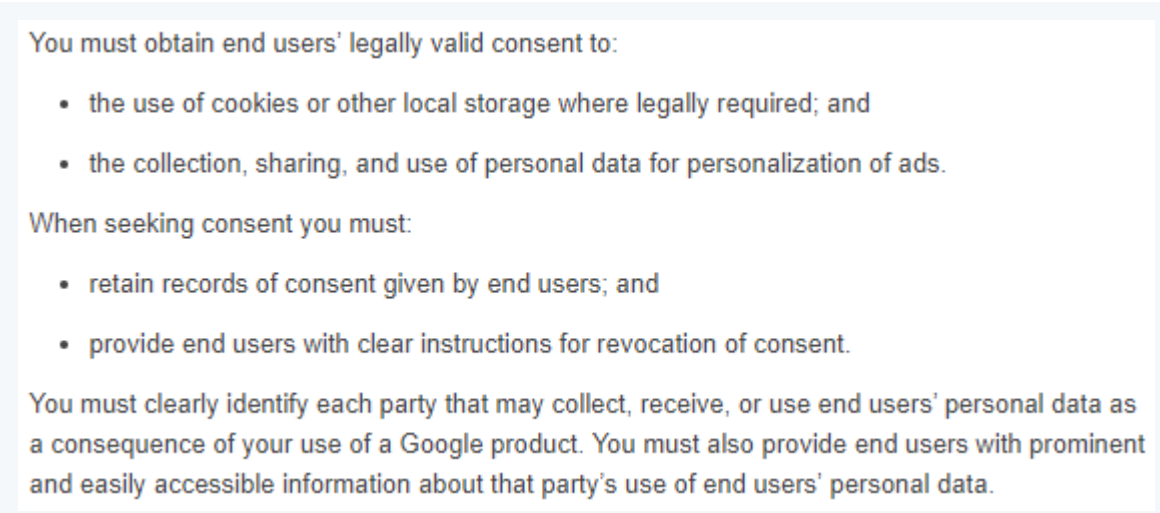


Image: Google Personalized Advertising Policies Help: EU User Consent Policy section

> *Based on the nature of personalized ads and the sensitivities associated with user ad targeting, we've identified policy standards for all Google features using personalized advertising functionality. These standards do not replace our other advertising policies (for example, for Google Ads or Shopping) and advertisers are still responsible for complying with all applicable advertising policies, in addition to Personalized advertising policies.* ***Advertisers are also required to comply with our policies for European Union user consent, where applicable****. Learn about what happens if you violate our policies.*

Google also explains (broadly) ***how*** its customers must obey EU law:



You must obtain end users' legally valid consent to:

- the use of cookies or other local storage where legally required; and
- the collection, sharing, and use of personal data for personalization of ads.

When seeking consent you must:

- retain records of consent given by end users; and
- provide end users with clear instructions for revocation of consent.

You must clearly identify each party that may collect, receive, or use end users' personal data as a consequence of your use of a Google product. You must also provide end users with prominent and easily accessible information about that party's use of end users' personal data.

Image: Google EU User Consent Policy: Consent requirements

> *You must obtain end users' legally valid consent to:*
>
> - *the use of cookies or other local storage where legally required; and*
> - *the collection, sharing, and use of personal data for personalization of ads.*
>
> *When seeking consent you must:*
>
> - *retain records of consent given by end users; and*
> - *provide end users with clear instructions for revocation of consent.*
>
> *You must clearly identify each party that may collect, receive, or use end users' personal data as a consequence of your use of a Google product. You must also provide end users with prominent and easily accessible information about that party's use of end users' personal data.*

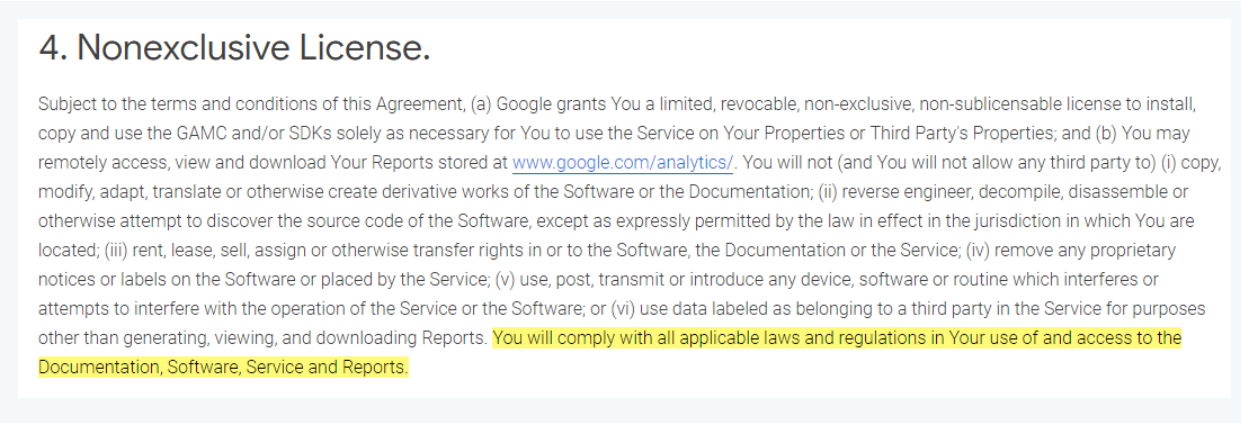
We can read the section as a requirement to comply with the GDPR's conditions around **consent**, which are set out mainly in Article 7, and the requirement to provide **transparent information**, as set out mainly in Article 12.

Analytics

There are significant privacy implications inherent in using an **analytics** suite. The data gathered by analytics software can potentially be used to build a picture of a person's online habits. The ICO has published guidance which demonstrates that the use of web analytics falls firmly within the scope of the GDPR (at page 20 of linked PDF):

- Some types of big data analytics, such as profiling, can have intrusive **effects** on individuals.
- Organisations need to consider whether the use of personal data in big data applications is within people's reasonable **expectations**.
- The complexity of the methods of big data analysis, such as machine learning, can make it difficult for organisations to be **transparent** about the processing of personal data.

Google Analytics makes clear in its Terms of Service that legal compliance is a prerequisite of being granted a license for the use of its software:



4. Nonexclusive License.

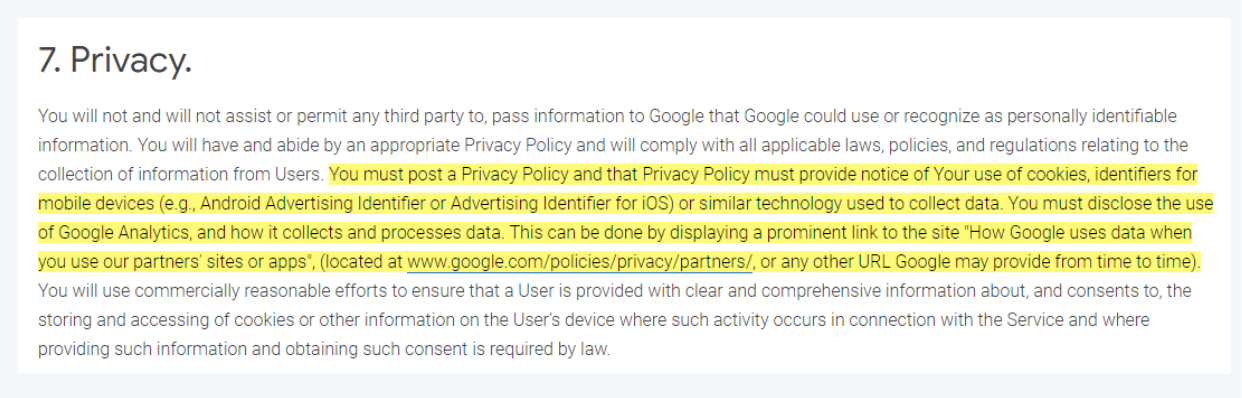
Subject to the terms and conditions of this Agreement, (a) Google grants You a limited, revocable, non-exclusive, non-sublicensable license to install, copy and use the GAMC and/or SDKs solely as necessary for You to use the Service on Your Properties or Third Party's Properties; and (b) You may remotely access, view and download Your Reports stored at www.google.com/analytics/. You will not (and You will not allow any third party to) (i) copy, modify, adapt, translate or otherwise create derivative works of the Software or the Documentation; (ii) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software, except as expressly permitted by the law in effect in the jurisdiction in which You are located; (iii) rent, lease, sell, assign or otherwise transfer rights in or to the Software, the Documentation or the Service; (iv) remove any proprietary notices or labels on the Software or placed by the Service; (v) use, post, transmit or introduce any device, software or routine which interferes or attempts to interfere with the operation of the Service or the Software; or (vi) use data labeled as belonging to a third party in the Service for purposes other than generating, viewing, and downloading Reports. You will comply with all applicable laws and regulations in Your use of and access to the Documentation, Software, Service and Reports.

Image: Google Analytics Terms of Service: Nonexclusive License clause

> ***4. Nonexclusive License.***
>
> *Subject to the terms and conditions of this Agreement, (a) Google grants You a limited, revocable, non-exclusive, non-sublicensable license to install, copy and use the GAMC and/or SKDs solely as necessary for You to use the Service on Your Properties or Third Party's Properties; and (b) You may remotely access, view and download Your Reports stored at www.google.com/analytics/. You will not (and You will not allow any third party to) (i) copy, modify, adapt, translate or otherwise create derivative works of the Software or the Documentation; (ii) reverse engineer, decompile, disassemble or otherwise attempt to discover the source code of the Software, except as expressly permitted by the law in effect in the jurisdiction in which You are located; (iii) rent, lease, sell, assign or otherwise transfer rights in or to the Software, the Documentation or the Service; (iv) remove any proprietary notices or labels on the Software or placed by the Service; (v) use,*

> *post, transmit or introduce any device, software or routine which interferes or attempts to interfere with the operation of the Service or the Software; or (vi) use data labeled as belonging to a third party in the Service for purposes other than generating, viewing, and downloading Reports.* ***You will comply with all applicable laws and regulations in Your use of and access to the Documentation, Software, Service and Reports.***

Google Analytics also requires its customers have a Privacy Policy that includes reference to its service, and that explains how Google Analytics processes personal data:



7. Privacy.

You will not and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information. You will have and abide by an appropriate Privacy Policy and will comply with all applicable laws, policies, and regulations relating to the collection of information from Users. You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses data when you use our partners' sites or apps", (located at www.google.com/policies/privacy/partners/, or any other URL Google may provide from time to time). You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.

Image: Google Analytics Terms of Service: Privacy clause

> ***7. Privacy.***
>
> *You will not and will not assist or permit any third party to, pass information to Google that Google could use or recognize as personally identifiable information. You will have and abide by an appropriate Privacy Policy and will comply with all applicable laws, policies, and regulations relating to the collection of information from Users.* ***You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies, identifiers for mobile devices (e.g., Android Advertising Identifier or Advertising Identifier for iOS) or similar technology used to collect data. You must disclose the use of Google Analytics, and how it collects and processes data. This can be done by displaying a prominent link to the site "How Google uses data when you use our partners' sites or apps", (located at www.google.com/policies/privacy/partners/ , or any other URL Google may provide from time to time).*** *You will use commercially reasonable efforts to ensure that a User is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the User's device where such activity occurs in connection with the Service and where providing such information and obtaining such consent is required by law.*

And take a look at the last few lines of that section, which require Google Analytics users to provide **information** about cookies, and gain **consent** for use of cookies, where required to do so by law.

EU law **does** require this in respect of the types of cookies set by Google Analytics. The ePrivacy Directive is more relevant here than the GDPR, but the GDPR requires compliance with the ePrivacy Directive.

Like many things, cookie consent is not explained clearly or explicitly in the GDPR, but here it is confirmed by the ICO:

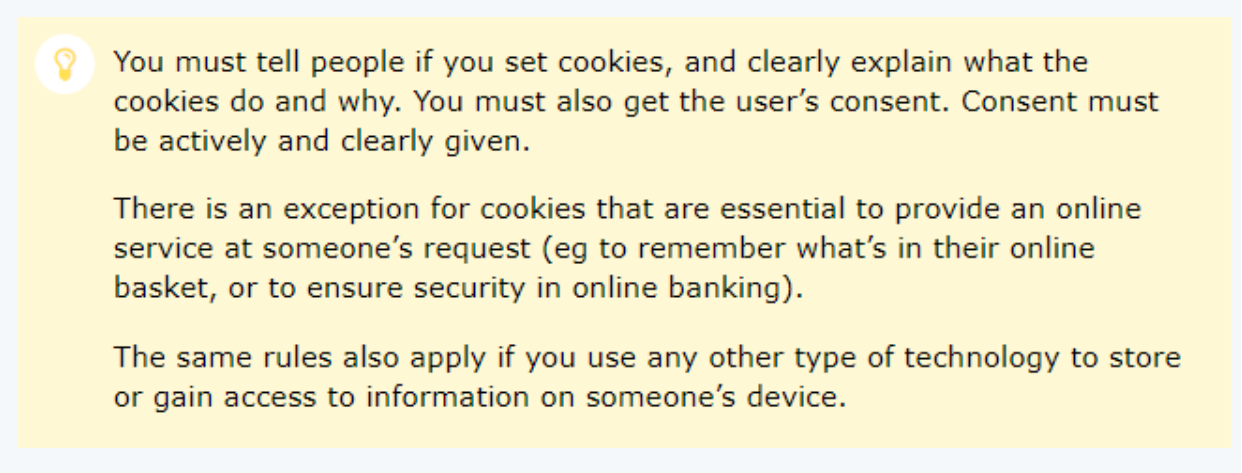


Image: ICO Guide to PECR: Cookies tip

> *You must tell people if you set cookies, and clearly explain what the cookies do and why. You must also get the user's consent. Consent must be actively and clearly given.*
>
> *There is an exception for cookies that are essential to provide an online service at someone's request (eg to remember what's in their online basket, or to ensure security in online banking).*
>
> *The same rules also apply if you use any other type of technology to store or gain access to information on someone's device.*

So, as you can see, using Google Analytics requires **compliance with the GDPR**.

App Development Platforms

Where developers build an app using a third party platform, they'll have to abide by certain legal requirements set out by the provider. This will inevitably include compliance with any relevant privacy laws. Google Firebase is a commonly used app development platform for developing **mobile apps** for Android and iOS.

Like many other platforms, Google requires Firebase customers to agree to a **Data Processing Agreement** as part of its Terms. Here's an excerpt from the Firebase Data Processing and Security Terms:

12.2 Google's Processing Records. Customer acknowledges that Google is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Google is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly Customer will, where requested, provide such information to Google via the Admin Console or other means provided by Google, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.

Image. Firebase Data Processing and Security Terms: Google's Processing Records clause

> *12.2 Google's Processing Records. Customer acknowledges that Google is required under the GDPR to: (a) collect and maintain records of certain information, including the name and contact details of each processor and/or controller on behalf of which Google is acting and, where applicable, of such processor's or controller's local representative and data protection officer; and (b) make such information available to the supervisory authorities. Accordingly Customer will, where requested, provide such information to Google via the Admin Console or other means provided by Google, and will use the Admin Console or such other means to ensure that all information provided is kept accurate and up-to-date.*

This clause makes reference to a data processor's obligations under Article 28 to **keep records** of processing activities and provide them to a Data Protection Authority when required.

The Data Processing Agreement also acknowledges that in certain contexts, Google **or** the developer might be either the data **processor** or data **controller**.

Whilst the Data Processing Agreement does make provision for either party to act as the data controller, this role will generally be fulfilled by a developer who creates an app in Firebase. This is explained in another document - Privacy and Security in Firebase:

Firebase is GDPR-ready

On May 25th, 2018, the EU General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive. Google is committed to helping our customers succeed under the GDPR, whether they are large software companies or independent developers.

The GDPR imposes obligations on data controllers and data processors. Firebase customers typically act as the "data controller" for any personal data about their end-users they provide to Google in connection with their use of Firebase, and Google is, generally, a "data processor".

This means that data is under the customer's control. Controllers are responsible for obligations like fulfilling an individual's rights with respect to their personal data.

If you're a customer, and would like to understand your responsibilities as a data controller, you should familiarize yourself with the provisions of the GDPR, and check on your compliance plans.

Image: Firebase Privacy and Security: GDPR-ready intro

> ***Data Protection***
>
> ***Firebase is GDPR-ready***
>
> *On May 25th, 2018, the EU General Data Protection Regulation (GDPR) replaces the 1995 EU Data Protection Directive. Google is committed to helping our customers succeed under the GDPR, whether they are large software companies or independent developers.*
>
> *The GDPR imposes obligations on data controllers and data processors. Firebase customers typically act as the "data controller" for any personal data about their end-users they provide to Google in connection with their use of Firebase, and Google is, generally, a "data processor".*
>
> *This means that data is under the customer's control. Controllers are responsible for obligations like fulfilling an individual's rights with respect to their personal data.*
>
> *If you're a customer, and would like to understand your responsibilities as a data controller, you should familiarize yourself with the provisions of the GDPR, and check on your compliance plans.*

Like some other Google services, Firebase requires any company with an **EU Representative** or **Data Protection Officer** (DPO) to register them with Google. This should be done in the Privacy Settings of the Firebase Console.

App Distribution Platforms

There's really no way around it - for a mobile app to have any significant reach, it will have to be hosted in either Apple or Google's marketplace platforms. This requires jumping through quite a few hoops.

For example, Google Play Store effectively requires GDPR compliance. Here's a section from the Google Play Developer Distribution Agreement:

> 4.8 You agree that if You make Your Products available through Google Play, You will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and You agree to provide legally adequate privacy notice and protection for those users. Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so. If Your Product stores personal or sensitive information provided by users, You agree to do so securely and only for as long as it is needed. However, if the user has opted into a separate agreement with You that allows You or Your Product to store or use personal or sensitive information directly related to Your Product (not including other products or applications), then the terms of that separate agreement will govern Your use of such information. If the user provides Your Product with Google Account information, Your Product may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given You permission to do so.

Image: Google Play Developer Distribution Agreement: Clause about protecting data and limiting data use

> *4.8 You agree that if You make Your Products available through Google Play, You will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords, or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and You agree to provide legally adequate privacy notice and protection for those users. Further, Your Product may only use that information for the limited purposes for which the user has given You permission to do so. If Your Product stores personal or sensitive information provided by users, You agree to do so securely and only for as long as it is needed. However, if the user has opted into a separate agreement with You that allows You or Your Product to store or use personal or sensitive information directly related to Your Product (not including other products or applications), then the terms of that separate agreement will govern Your use of such information. If the user provides Your Product with Google Account information, Your Product may only use that information to access the user's Google Account when, and for the limited purposes for which, the user has given You permission to do so.*

Here's another crucial section of this agreement:

8.2 Notwithstanding Section 8.1, in no event will Google maintain on any portion of Google Play (including, without limitation, the part of Google Play where previously purchased or downloaded applications are stored on behalf of users) any Product that You have removed from Google Play and provided written notice to Google that such removal was due to (a) an allegation of infringement, or actual infringement, of any third party Intellectual Property Right; (b) an allegation of, or actual violation of, third party rights; or (c) an allegation or determination that such Product does not comply with applicable law (collectively "**Legal Takedowns**"). If a Product is removed from Google Play due to a Legal Takedown and an end user purchased such Product within a year (or a longer period as local consumer law mandates) before the date of takedown, at Google's request, You agree to refund to the end user all amounts paid by such end user for such Product.

Image: Google Play Developer Distribution Agreement: Clause about app take-downs and refunds

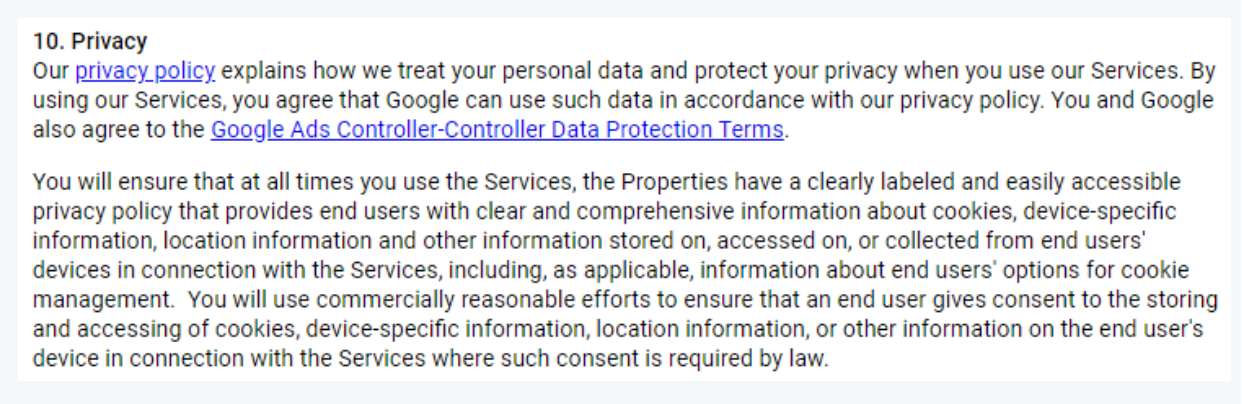
> *8.2 Notwithstanding Section 8.1, in no event will Google maintain on any portion of Google Play (including, without limitation, the part of Google Play where previously purchased or downloaded applications are stored on behalf of users) any Product that You have removed from Google Play and provided written notice to Google that such removal was due to (a) an allegation of infringement, or actual infringement, of any third party Intellectual Property Right; (b) an allegation of, or actual violation of, third party rights; or (c) an allegation or determination that such Product does not comply with applicable law (collectively **"Legal Takedowns"**). If a Product is removed from Google Play due to a Legal Takedown and an end user purchased such Product within a year (or a longer period as local consumer law mandates) before the date of takedown, at Google's request, You agree to refund to the end user all amounts paid by such end user for such Product.*

Google can take down an app from the Play Store where there has been even an **allegation** that it's legally non-compliant. The owner must then **refund** anyone who purchased the app in the past year. This could be a critical blow for any app developer and is yet another reason to ensure you can demonstrate GDPR-compliance.

Advertising Tools

Because they use potentially intrusive methods and technologies, such as cookies and remarketing, **advertising tools** like Google Ads, Google AdMob and MoPub require their users to be compliant with privacy laws.

For example, Google AdSense provides the Terms of Service for both Google AdMob (used by mobile app publishers to run ads on a mobile app) and AdSense (used by web publishers). The AdSense Terms of Use effectively requires developers to maintain GDPR compliance:



10. Privacy

Our privacy policy explains how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policy. You and Google also agree to the Google Ads Controller-Controller Data Protection Terms.

You will ensure that at all times you use the Services, the Properties have a clearly labeled and easily accessible privacy policy that provides end users with clear and comprehensive information about cookies, device-specific information, location information and other information stored on, accessed on, or collected from end users' devices in connection with the Services, including, as applicable, information about end users' options for cookie management. You will use commercially reasonable efforts to ensure that an end user gives consent to the storing and accessing of cookies, device-specific information, location information, or other information on the end user's device in connection with the Services where such consent is required by law.

Image: Google AdSense Terms of Service: Privacy clause

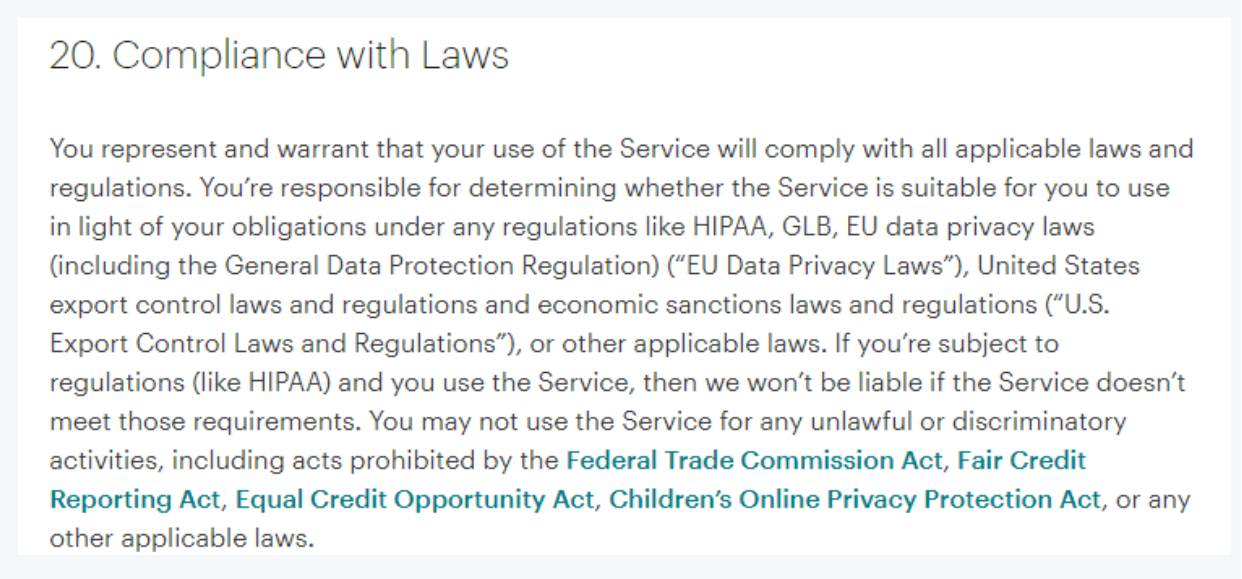
> ***10. Privacy***
> *Our privacy policy explains how we treat your personal data and protect your privacy when you use our Services. By using our Services, you agree that Google can use such data in accordance with our privacy policy. You and Google also agree to the Google Ads Controller-Controller Data Protection Terms.*
>
> *You will ensure that at all times you use the Services, the Properties have a clearly labeled and easily accessible privacy policy that provides end users with clear and comprehensive information about cookies, device-specific information, location information and other information stored on, accessed on, or collected from end users' devices in connection with the Services, including, as applicable, information about end users' options for cookie management. You will use commercially reasonable efforts to ensure that an end user gives consent to the storing and accessing of cookies, device-specific information, location information, or other information on the end user's device in connection with the Services where such consent is required by law.*

Here the developer must obtain **consent** to collect various types of personal data such as cookie data, where required to do so by law. As we've seen above, **this is necessary** under the GDPR.

Email Marketing Services

Using third-party email marketing services like MailChimp is a good way to help ensure GDPR-compliance. Because many businesses see privacy and anti-spam legislation as such a minefield, companies such as MailChimp depend on being able to offer legally compliant marketing services.

This is not to say, however, that outsourcing email campaigns excuses a business from complying with the GDPR. This is made clear by MailChimp in its terms:



20. Compliance with Laws

You represent and warrant that your use of the Service will comply with all applicable laws and regulations. You're responsible for determining whether the Service is suitable for you to use in light of your obligations under any regulations like HIPAA, GLB, EU data privacy laws (including the General Data Protection Regulation) ("EU Data Privacy Laws"), United States export control laws and regulations and economic sanctions laws and regulations ("U.S. Export Control Laws and Regulations"), or other applicable laws. If you're subject to regulations (like HIPAA) and you use the Service, then we won't be liable if the Service doesn't meet those requirements. You may not use the Service for any unlawful or discriminatory activities, including acts prohibited by the **Federal Trade Commission Act, Fair Credit Reporting Act, Equal Credit Opportunity Act, Children's Online Privacy Protection Act**, or any other applicable laws.

Image: MailChimp Terms of Use: Excerpt of Compliance with Laws clause

> ***20. Compliance with Laws***
>
> *You represent and warrant that your use of the Service will comply with all applicable laws and regulations. You're responsible for determining whether the Service is suitable for you to use in light of your obligations under any regulations like HIPAA, GLB, EU data privacy laws (including the General Data Protection Regulation) ("EU Data Privacy Laws"), United States export control laws and regulations and economic sanctions laws and regulations ("U.S. Export Control Laws and Regulations"), or other applicable laws. If you're subject to regulations (like HIPAA) and you use the Service, then we won't be liable if the Service doesn't meet those requirements. You may not use the Service for any unlawful or discriminatory activities, including acts prohibited by the Federal Trade Commission Act, Fair Credit Reporting Act, Equal Credit Opportunity Act, Children's Online Privacy Protection Act, or other laws that apply to commerce.*

MailChimp's terms also include some clauses that are required in a Data Processing Agreement:

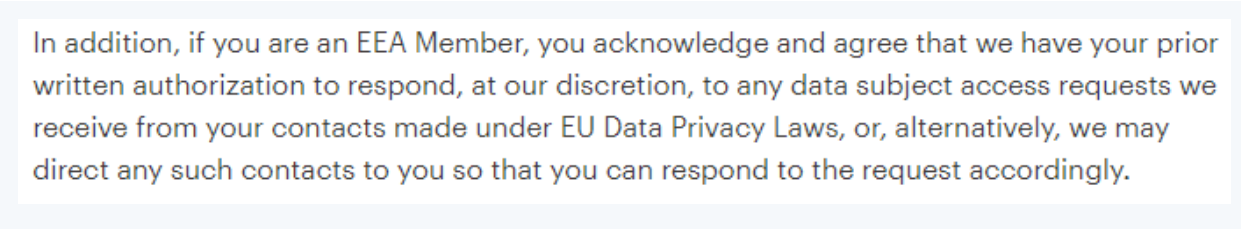

In addition, if you are an EEA Member, you acknowledge and agree that we have your prior written authorization to respond, at our discretion, to any data subject access requests we receive from your contacts made under EU Data Privacy Laws, or, alternatively, we may direct any such contacts to you so that you can respond to the request accordingly.

Image: MailChimp Terms of Use: Excerpt of Compliance with Laws clause - EEA Members

> *In addition, if you are an EEA Member, you acknowledge and agree that we have your prior written authorization to respond, at our discretion, to any data subject access requests we receive from your contacts made under EU Data Privacy Laws, or, alternatively, we may direct any such contacts to you so that you can respond to the request accordingly.*

By agreeing to this clause, a business is authorizing MailChimp to provide its customers with any personal data it holds about them on receipt of a subject access request. This is unusual for a data processor, which would normally supply the information to the data controller to provide to the customer directly. There's no need for the business to worry about this, of course, so long as it's operating in a **transparent** and **GDPR-compliant** way.

Lead Generation

Lead generation and inbound marketing services, such as Hubspot and CrazyEgg, also require their users to abide by privacy law.

Hubspot specifies that its customers must obtain **consent** for processing under the GDPR in its Terms of Service:

For customers that are located in the European Union or the European Economic Area, the Standard Contractual Clauses adopted by the European Commission, attached to the Data Processing Agreement, with HubSpot, Inc., which provide adequate safeguards with respect to the personal data processed by us under this Agreement and pursuant to the provisions of our Data Processing Agreement apply. You acknowledge in all cases that HubSpot acts as the data processor of Customer Data and you are the data controller of Customer Data under applicable data protection regulations in the European Union and European Economic Area. Customer will obtain and maintain any required consents necessary to permit the processing of Customer Data under this Agreement. If you are subject to the GDPR you understand that if you give an integration provider access to your HubSpot account, you serve as the data controller of such information and the integration provider serves as the data processor for the purposes of those data laws and regulations that apply to you. In no case are such integration providers our sub-processors.

Image: Hubspot Customer Terms of Service: EU Data Processing Clause - GDPR consent section

> *For customers that are located in the European Union or the European Economic Area, the Standard Contractual Clauses adopted by the European Commission, attached to the Data Processing Agreement, with HubSpot, Inc., which provide adequate safeguards with respect to the personal data processed by us under this Agreement and pursuant to the provisions of our Data Processing Agreement apply. You acknowledge in all cases that HubSpot acts as the data processor of Customer Data and you are the data controller of Customer Data under applicable data protection regulations in the European Union and European Economic Area.* ***Customer will obtain and maintain any required consents necessary to permit the processing of Customer Data under this Agreement. If you are subject to the GDPR you understand that if you give an integration provider access to your HubSpot account, you serve as the data controller of such information*** *and the integration provider serves as the data processor for the purposes of those data laws and regulations that apply to you. In no case are such integration providers our sub-processors.*

You can see that Hubspot also uses its terms to navigate the complicated relationship between itself, its customers, and providers for whom it provides CRM integration such as Salesforce.

An understanding of the relevant GDPR provisions is **essential** in order to meaningfully agree to these sorts of terms.

Enterprise Mobility Management

Android is a common choice of platform for businesses that wish to develop custom software or hardware to be used as part of their operations.

Android Enterprise supports developers using Android in the workplace, specifically in the context of **enterprise mobility management** (EMM). Developers might use Android Enterprise resources in the development of employee-owned devices to be used by employees at work (BYOD), or company-owned devices to be used by staff.

Pitney Bowes is an example of a company that uses Android Enterprise resources to develop its own devices - a range of office equipment.

In the EMM context, Android Enterprise provides application programming interfaces (APIs) such as Managed Google Play:

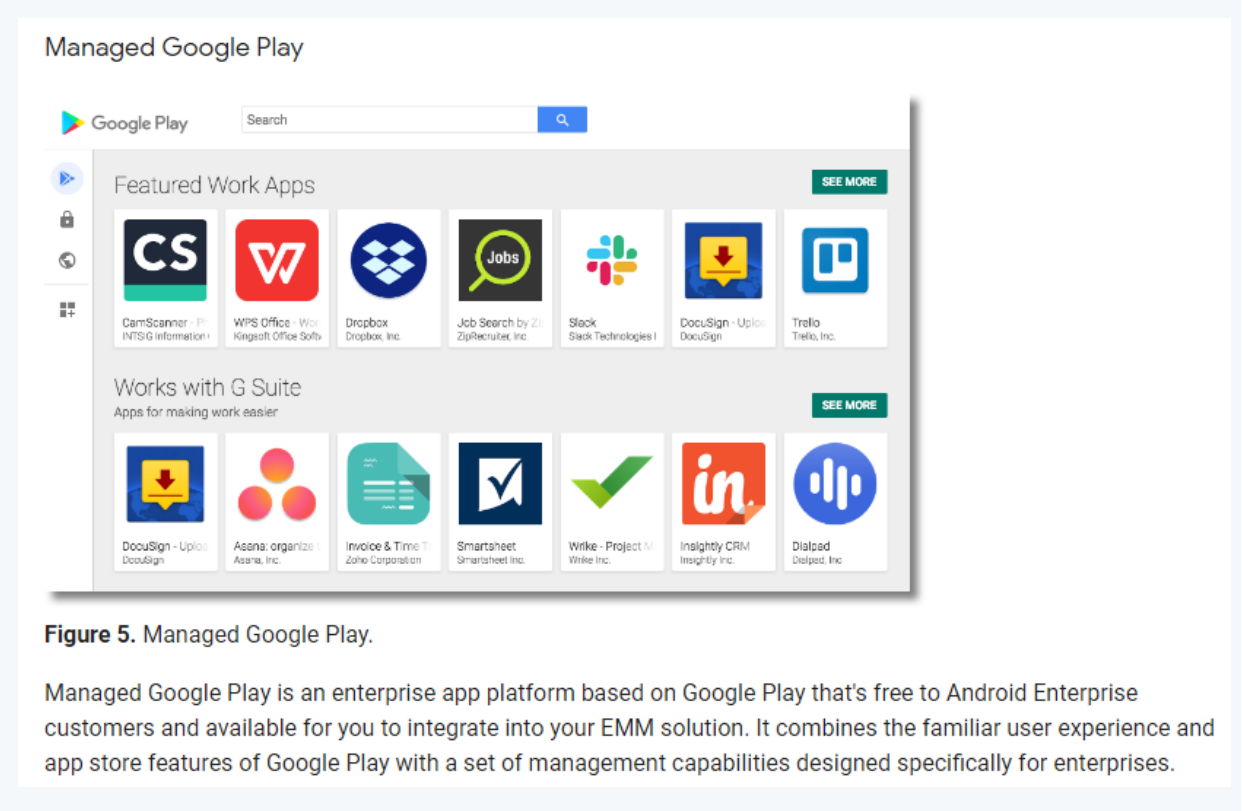
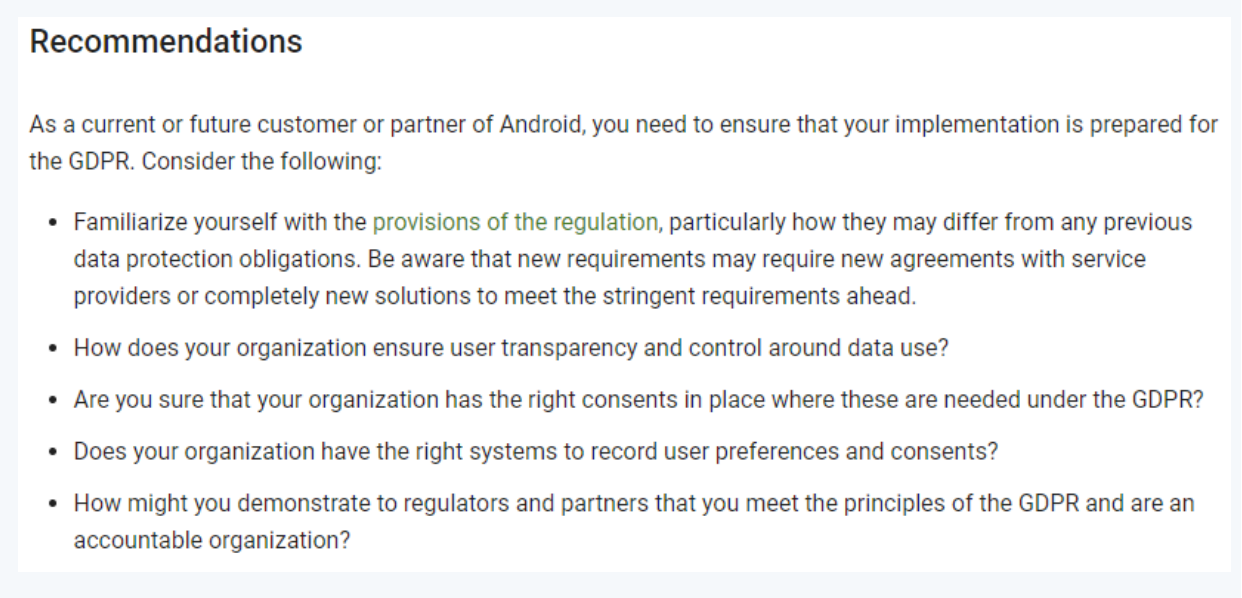


Image: Android Enterprise Overview: Managed Google Play screenshot

Complying with the GDPR is required in order to use Android Enterprise. Google sets out some recommendations on **how to comply with the GDPR** when using the service:



Recommendations

As a current or future customer or partner of Android, you need to ensure that your implementation is prepared for the GDPR. Consider the following:

- Familiarize yourself with the provisions of the regulation, particularly how they may differ from any previous data protection obligations. Be aware that new requirements may require new agreements with service providers or completely new solutions to meet the stringent requirements ahead.
- How does your organization ensure user transparency and control around data use?
- Are you sure that your organization has the right consents in place where these are needed under the GDPR?
- Does your organization have the right systems to record user preferences and consents?
- How might you demonstrate to regulators and partners that you meet the principles of the GDPR and are an accountable organization?

Image: Android Enterprise: Recommendations for GDPR compliance

> ***Recommendations***
>
> *As a current or future customer or partner of Android, you need to ensure that your implementation is prepared for the GDPR. Consider the following:*
>
> - *Familiarize yourself with the provisions of the regulation, particularly how they may differ from any previous data protection obligations. Be aware that new requirements may require new agreements with service providers or completely new solutions to meet the stringent requirements ahead.*
> - *How does your organization ensure user transparency and control around data use?*
> - *Are you sure that your organization has the right consents in place where these are needed under the GDPR?*
> - *Does your organization have the right systems to record user preferences and consents?*
> - *How might you demonstrate to regulators and partners that you meet the principles of the GDPR and are an accountable organization?*

Mobile devices typically process a lot of personal data. Developing a device that uses Android as its OS will require careful consideration of the associated privacy implications.

Even devices running “stock” Android collect personal data. Google states that the Android OS itself, “*in so far as it is executed exclusively within the mobile device,*” does **not** send personal data to Google. However, several apps which come in the “factory” (default) version of Android **do**.

In respect of some of these apps, Google is the data **controller**:

- Google Play Services

- Google apps on Android (e.g. Google Chrome, Google Search)
- Zero-touch enrollment (for corporate-owned devices)

For others, Google is the data **processor**:

- Managed Google Play
- Android Management API
- Zero-touch reseller

This is relevant to developers in several ways.

A **data controller** that has developed an EMM device using Android Enterprise will need to be explicit in its Privacy Policy about the relationship between its data subjects (e.g. its employees) and Google.

Google is acting as a **data processor** in some respects, and so it is also necessary for a company using Android Enterprise to have a Data Processing Agreement in place with Google. The Android Enterprise Data Processing and Security Terms takes care of this.

Note that under Article 28 (1), the data controller is obliged to ensure that any data processors it contracts are compliant with the GDPR. There are **no exceptions** to this, even where Google is the data processor. This will require a thorough reading of this Data Processing Agreement, as the buck stops with the data controller in the event of a data breach.

Voice Activation

Many opportunities are emerging for developers to integrate their software with **voice-activated services** like Google Assistant, Apple's Siri, or Amazon Alexa.

Through Actions on Google, developers can have their Android app interact with Google Assistant. By publishing an Action through Actions on Google, developers can enable their users to "talk" to their app or device via Google Assistant.

Here are some examples of apps that have published Actions for Google Assistant via Actions on Google:

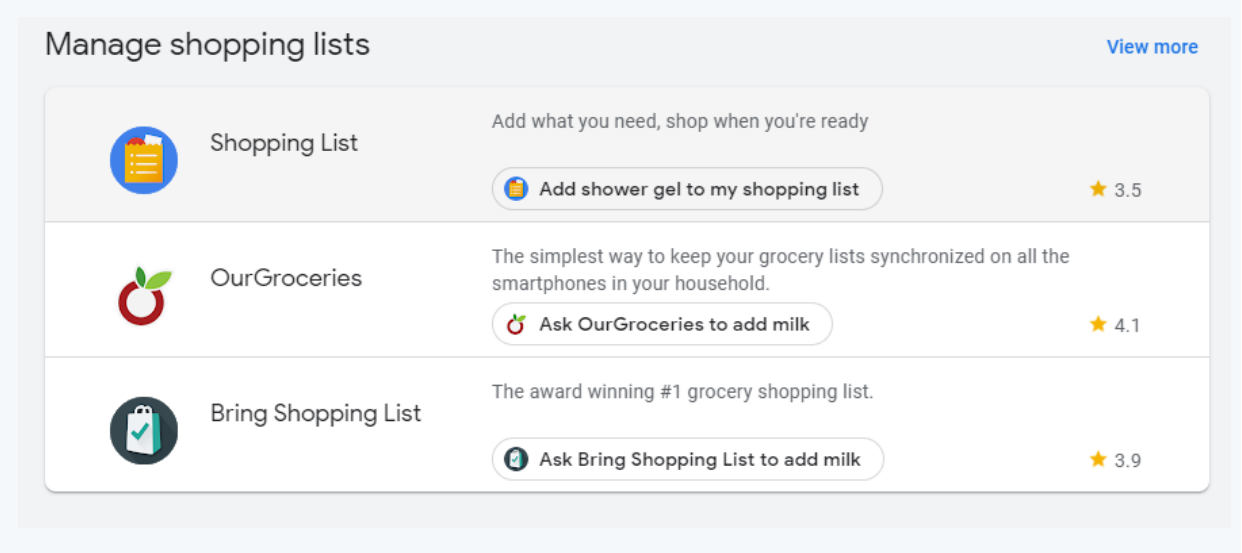


Image: Screenshot of shopping list apps on Google Play

There are a number of privacy considerations inherent to voice-command apps and devices. So it's not surprising that Google requires developers to have a Privacy Policy before publishing an Action:

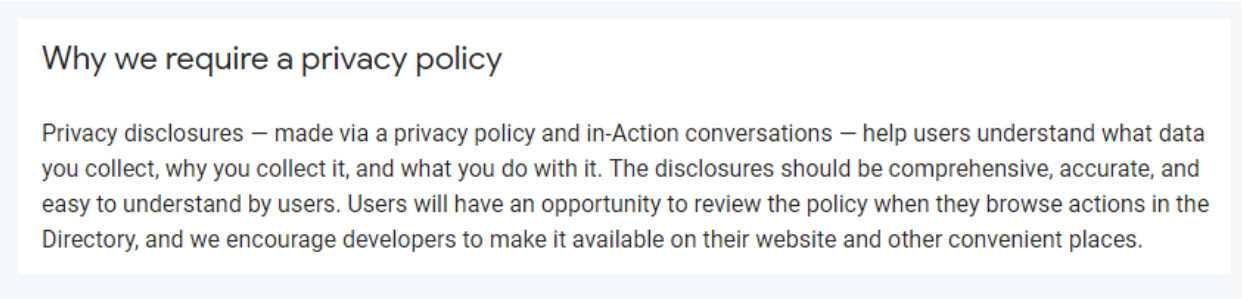


Image: Actions on Google Privacy Policy Guidance: Why we require a Privacy Policy section

> ***Why we require a privacy policy***
>
> *Privacy disclosures — made via a privacy policy and in-Action conversations — help users understand what data you collect, why you collect it, and what you do with it. The disclosures should be comprehensive, accurate, and easy to understand by users. Users will have an opportunity to review the policy when they browse actions in the Directory, and we encourage developers to make it available on their website and other convenient places.*

Actions on Google expects developers' Privacy Policies to, at a minimum, address these three questions:

- **What information do you collect?**

  In your policy you should disclose all the information your Action collects. This includes information that you may collect automatically, such as server and HTTP logs, data transmitted by the Actions on Google API to you, and usage information. This also includes information that you get from the user, either directly or via the permissions API. You should also disclose whether you collect any persistent identifiers (like the Google ID).

- **How do you use the information?**

  In your policy, you should disclose how you use the information you collect. For example, you may use the information to provide certains services to users, to recognize them the next time they use your Action, or to send them promotional emails.

- **What information do you share?**

  In your policy, you should disclose the circumstances when you share information. For example, you may share information with third parties as part of the service (like a restaurant reservation Action), with other users (like a social network or forum), with marketing partners, or with service providers that assist with your service (like hosting companies or technology platforms).

Image: Actions on Google Privacy Policy Guidance: What information to include in Privacy Policy

- ***What information do you collect?***

  In your policy you should disclose all the information your Action collects. This includes information that you may collect automatically, such as server and HTTP logs, data transmitted by the Actions on Google API to you, and usage information. This also includes information that you get from the user, either directly or via the permissions API. You should also disclose whether you collect any persistent identifiers (like the Google ID).

- ***How do you use the information?***

  In your policy, you should disclose how you use the information you collect. For example, you may use the information to provide certain services to users, to recognize them the next time they use your Action, or to send them promotional emails.

- ***What information do you share?***

  In your policy, you should disclose the circumstances when you share information. For example, you may share information with third parties as part of the service (like a restaurant reservation Action), with other users (like a social network or forum), with marketing partners, or with service providers that assist with your service (like hosting companies or technology platforms).

Google doesn't specifically refer to the GDPR in its Actions on Google Privacy Policy guidance. But Google is asking developers to provide very similar information as that which is required under Article 13 of the GDPR.

First Steps to GDPR Compliance

Now that you are up to speed on the core concepts and major changes brought about by the GDPR, what's the next step? The answer to this question isn't the same for everyone, but let's take a look at what you might do next in your journey to GDPR compliance.

Under the GDPR, you are required to have a legal basis for collecting and processing the personal information of your data subjects. You should determine which legal basis you will use when collecting and processing personal information, and be prepared to defend this decision if it is challenged.

New Projects

If you are a new company or starting a new project with GDPR compliance as one of your goals, you have a fresh slate and can hit the ground running with a good understanding of these new regulations.

Are you the data controller or data processor?

One of the first items you must address is determining whether you are the data controller, data processor, or both.

Simply put, the data controller is the one who determines how personal data is collected, why it is collected, and what is done with it afterwards. The data processor simply uses data to complete a task dictated by the data controller. In many cases, the data controller is also the data processor, collecting personal data for certain purposes and then also processing it to achieve those tasks.

You may wish to review Chapter 3 [LINK TO CHAPTER 3] of this ebook, as well as reread Article 24: *Responsibility of the controller* and Article 28: *Processor* to help you answer this question.

Privacy by Design

Privacy by Design is a concept that the GDPR has adopted as a requirement to ensure that data handlers consider the privacy and security of their data subjects every step of the way. In

essence, privacy by design expects developers to have security baked into their projects before those projects even begin.

In the earliest stages of conception and planning, the GDPR expects developers to be mindful of how their systems and processes are designed to protect against data breaches, ensure that personal data is only collected and kept as needed, and is processed securely and lawfully so that there is no risk to their data subjects.

The alternative to this concept is developers creating an app or website and then tacking on security measures at the end of the project. This is not only inefficient, but often results in vulnerabilities or oversights that can be exploited intentionally or may fail on their own, putting the privacy of data subjects at risk.

Here are some things to keep in mind when beginning a new project with privacy by design:

- Use **pseudonymization where reasonable** to add an extra layer of security and privacy
- Give access to the personal information you control **only to those who need it**, and only the information they need to fulfill their tasks (including third-parties and data processors)
- Include all necessary declarations, rights, and options for your data subjects in your **Privacy Policy** so they can make informed decisions
- **Use encryption** to protect data when transferred or otherwise vulnerable
- Make use of sufficiently strong **passwords** (never use default passwords or simple ones such as “1234”)
- Ensure internal employees and outside consultants are **properly trained in your security procedures** and their responsibilities under the GDPR
- **Have a contract in place** for data processors and third-party vendors you use so everyone understands their roles and expectations
- **Have a plan** for data breaches, subject access requests, and other security scenarios
- Ensure all of your software, firmware, and hardware have **modern security measures** (security suites, OS updates, firewalls, spam blockers, etc.)

By being mindful of these key areas of your development and considering security in other aspects of your project and business as a whole, you can minimize risk to yourself and your data subjects.

The Benefits of Starting Fresh

New projects and startups have the distinct advantage of prior knowledge about the GDPR before they even begin. As opposed to long-running companies who may now need to make drastic changes to their operations in order to comply with the GDPR, you can start off on the right foot with a strong foundation and guidelines to help you toward success.

With that foundation in place, it's up to you to decide the best course to take for your project.

What data will you collect and process? What legal basis will you use to do so? When will you ask for consent?

A good place to start is **drafting a Privacy Policy** which you can then use along with the GDPR as an outline for your operations. This will help you see where your strongpoints are, where you may need to make more efforts towards compliance and make it clear what your actual procedures are.

Updating Current Projects

Updating current projects in response to the GDPR can be more complicated as the rules you started the project with now vary from the rules you must abide by under the GDPR.

While no two projects are the same, there are some steps that should be taken when converting a current project to meet GDPR requirements.

Purge Non-Essential Data

As mentioned in the last chapter, retaining unneeded personal data goes against GDPR compliance and opens you and your users to unnecessary risk. One of the first steps that should be taken when converting a project to GDPR compliance is to **delete or anonymize any information that is no longer needed**.

Purging your systems and databases of extraneous personal information is not only required under the GDPR, but makes setting up adequate security measures much more manageable.

Instead of needing to create or modify security measures to protect the information you are retaining, you can instead focus on developing security measures for the data you collect moving forward, and need not worry about the collection methods and security measures you began the project with as the old data has been erased or converted.

Deduplicate Data

A related step you should take is deduplicating personal data that is redundant and not needed in more than one location. This not only allows you to focus your security efforts in one area, but *reduces the risk of oversights* where copies or backups of your database may be left vulnerable.

While not explicitly called out in the GDPR, redundant information goes against the security pillar of the GDPR where data should only be collected, processed, and retained as needed.

Duplicate data could be seen as "not needed" and therefore it should not be retained.

Deduplication might also come into play if you are developing multiple iterations of the same project (for example, a GDPR-compliant and not GDPR-compliant version). While retaining a backup of your database may be necessary at some points in the process, your old version of the project should be cleansed of personal data once you transition to the new version. Allowing an old version of an app or website to exist with sensitive data attached is an unnecessary risk.

Limit Data Access

One of the ways that duplicate data can put you and your data subjects at risk has to do with access.

Say you are creating a new GDPR-compliant version of you website and you still have the old website as a backup and for reference. You might update who has access to the new website's database according to GDPR guidelines (third-parties, current and former employees, etc.). If you do not also update access to the old website, former employees and third-parties you no longer work with may be able to access your database. This could put the personal data you control at risk.

By removing duplicate data and *properly limiting access to the data* you control, you can ensure that only those with authorization to do so can access your database.

The GDPR states that only those necessary should have access to the personal data in your database. Without limiting access to the personal data that you control, you make yourself vulnerable in two ways.

First, more people than necessary can access and potentially mishandle the personal information under your protection. **Secondly**, in the event of mishandling or a data breach, it is much more difficult to determine who is responsible.

Limiting who has access to your database reduces the avenues for mishandling and also make it easier to determine the points where mishandling may have occurred to pinpoint issues and remedy any vulnerabilities.

Section 4 of Article 6 notes some factors that should be weighed in situations where you have data you've collected for one purpose and wish to process it in a different way, and:

- You don't have consent to do so, **or**
- The data isn't being processed according to a Union or Member State law

These factors include the following:

- **Links** between the original purpose for which the personal data was collected and the purposes of the further processing,
- The **context** that the personal data was collected under, particularly looking at the relationship between the data subjects and the collector,
- **What kind** of personal data is it, and in particular whether it's special categories of personal data or personal data related to criminal convictions and offences,
- Any **possible consequences** the data subjects may endure because of the further processing, and
- Whether **appropriate safeguards exist** to protect the data, such as encryption or pseudonymisation

Basically, if you wish to use data beyond what you've collected it for and made clear to your users was your purpose for collecting it, you'll need compelling reasons and you can't put your users at risk for having their data compromised or abused.

Your Privacy Policy

Review your current Privacy Policy and see if it includes everything it needs to be up to date and accurate. Also be sure that your Privacy Policy is written in a way that it is easily understandable to your average user.

Consider the examples below:

Example #1:

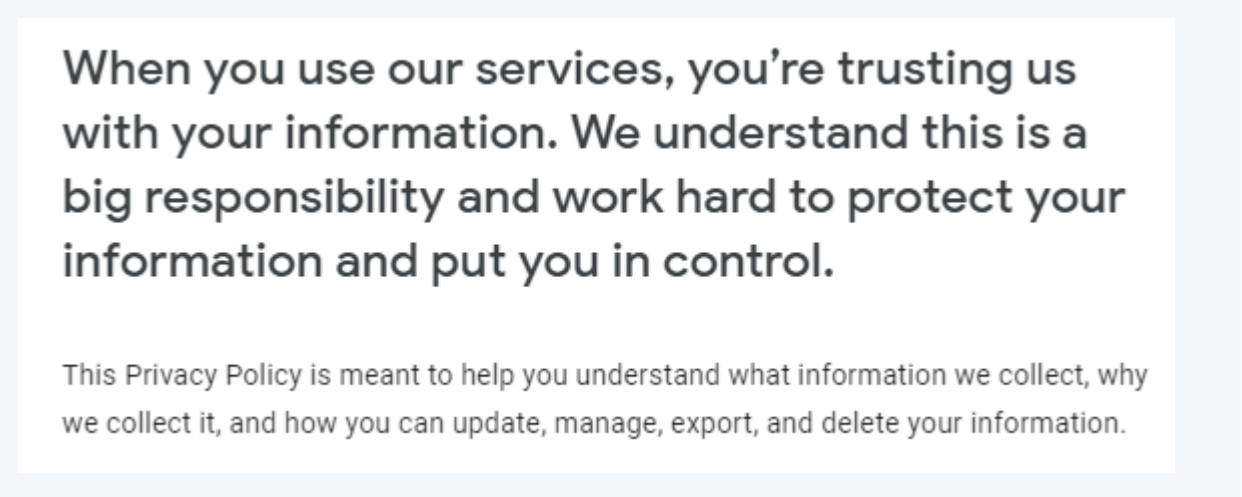


Image: Google Privacy Policy intro

Example #2:

1. Scope of this Privacy Policy

Lyft ("Lyft," "we," "our," and/or "us") values the privacy of individuals who use our application, websites, and related services (collectively, the "Lyft Platform "). This privacy policy (the "Privacy Policy") explains how we collect, use, and share information from Lyft users ("Users"), comprised of both Lyft riders ("Riders") and Lyft drivers (including Driver applicants) ("Drivers"). Beyond the Privacy Policy, your use of Lyft is also subject to our Terms of Service (www.lyft.com/terms).

Image: Lyft Privacy Policy: Scope of Privacy Policy clause

As you can see, the verbiage in example #1 is much more casual and conversational, while the verbiage in example #2 is full of cumbersome legalese. If your Privacy Policy reads more like example #2, you should rewrite it in **more natural language** so your users can easily digest the information you disclose there.

Consent Checkboxes

Affirmative consent is one of the most noticeable changes brought about by the GDPR, one that you have almost certainly encountered by now.

Many privacy laws prior to the GDPR required consent for certain data collection and processing activities, but this was rarely spelled out specifically.

App and website users would be considered to be agreeing to legal agreements by default if they chose to use the service, whether or not they even read the policies that they were agreeing to. While this became an acceptable practice for several years, the GDPR saw this as a *serious fault*.

The GDPR clarified that *active* consent must be given along with other stipulations for fair and legal data collection and processing. Active consent requires the user to *interact in some way* (typically by **checking a box** or **clicking a button** that reads “I Accept” or something equally clear) in order to ensure that they agree to the policies of that app or website.

While users may still often choose to not read the policies they are agreeing to, they are at least required to confirm their consent and cannot simply be found to be in an agreement unknowingly.

The GDPR calls for “affirmative consent” in a number of situations and specifies that *passive consent is no longer sufficient*.

Checkboxes used to obtain affirmative consent must not be checked by default, as the user must be required to take an action to give their consent. This eliminates the chance of a user not noticing a passive popup and being unaware that they have consented to something.

Here are some locations where placing a checkbox to obtain consent is a good idea:

- A **popup for new visitors** asking for their consent to collect and process their data according to your Privacy Policy (which you should include a link to). You may also ask them to agree to your Terms & Conditions and Cookie Policy in this popup.
- Any **processing activity** that requires consent should have its own separate checkbox. You should specify when a processing activity is mandatory or where lack of consent may affect the functionality of your app or website (location services, for example).
    - If you are a data controller who relies on legitimate interest for certain processes, or a data processor, you may want to disclose that.
- **Pages** where the user fills out personal information, such as when creating an account.
- **Forms** for entering a contest or sweepstakes, you may also include the conditions for entry.
- The **payment screen** where users provide payment and shipping information.

These locations are just some common examples of where developers should include a checkbox for affirmative consent under the GDPR.

The GDPR also gives data subjects the **right to revoke their consent at any time**. It is best practice to notify users at the time of consent that this is an option and where they can do it (usually in settings or in their profile).

When consent is not needed because legitimate interest is used as the legal basis, this should be disclosed and users should be notified of their right to object as per Article 21 of the GDPR.

Below are some examples of consent checkboxes:

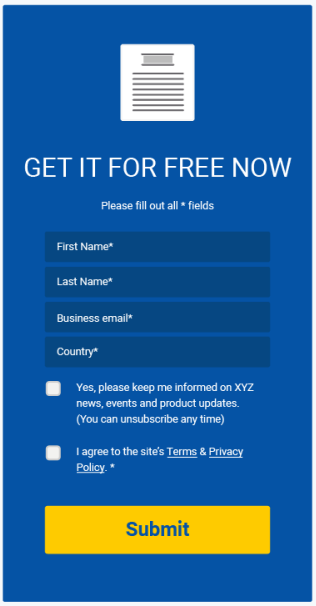


Image: Generic example: Free content form with checkbox to agree

While these examples are from mobile apps, the same concept applies whether it's an app or a website requesting consent.

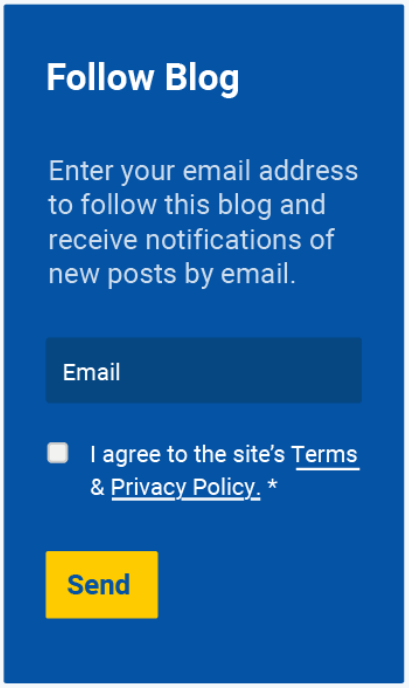


Image: Generic blog email sign-up form with checkbox to agree

The old way of obtaining consent prior to the GDPR often included a popup that stated that by using the website, you agree to their Privacy Policy and Terms & Conditions. This sort of **passive consent is no longer permissible** under the GDPR. The GDPR requires affirmative, active consent. This can be in the form of a checkbox or button that must be clicked to give consent.

Example #1:

Image: Generic browsewrap example of by using this website you agree to terms statement

Example #2:

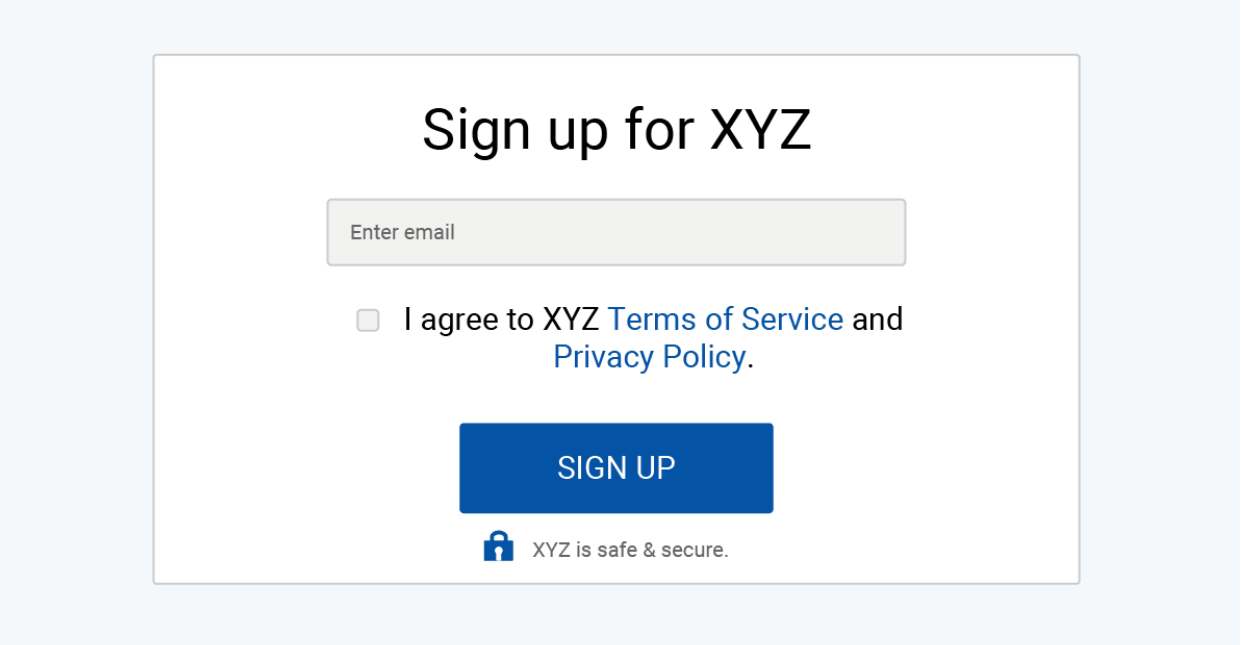


Image: Generic example: Email sign-up form with checkbox to agree

Example #3:

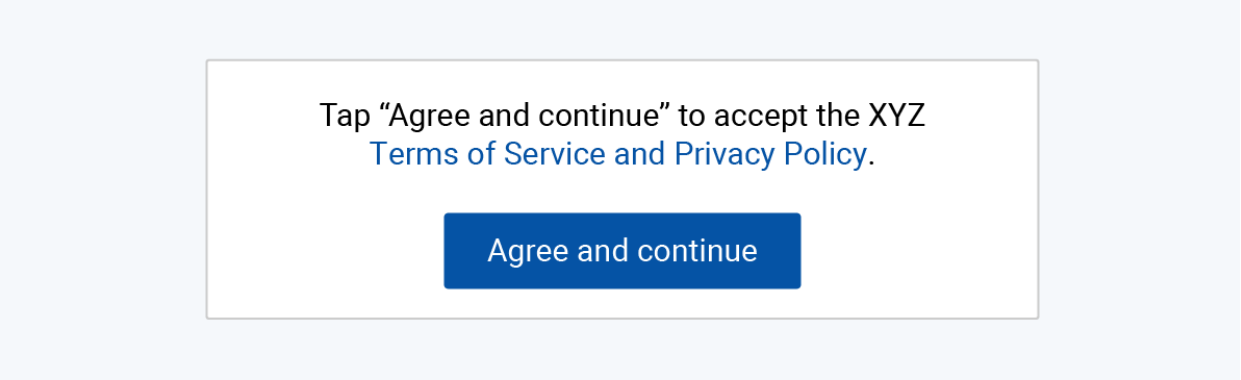


Image: Generic App: Tap Agree and continue button - example

Example #1 is the old way of obtaining passive consent. This method is no longer viable under the GDPR.

Example #2 and #3 are the new way of obtaining active consent. Note that in example #2, the checkbox **must not be pre-checked**, requiring the user to click the box to give their consent.

Other Responsibilities

Chapter 3 [LINK TO CHAPTER 3] includes lists of responsibilities for both data controllers and data processors. By this point you should know which one you are, so you should review your responsibilities to ensure you are meeting all of these expectations.

Once again, it would be impossible and redundant for this ebook to cover every aspect of the GDPR as it continues to grow, change, and receive clarifications. The purpose of this ebook is not to replace the need to read the GDPR, but instead to help you understand it by providing examples and breakdowns of the information it provides. It is your responsibility as a data handler to read the entirety of the GDPR and keep up to date with the laws therein as they evolve, change and become more defined through real-life applications.

Note from the Editors

With more and more privacy laws popping up all the time and existing privacy laws being modernized and updated all around the world, it can seem daunting to keep up with what it takes to stay compliant.

We created this ebook to help you navigate the groundbreaking GDPR a little bit easier and take some of the stress and mystery out of compliance. We hope it helped explain some of the philosophy behind the law, demystified some of its requirements and provided you with some practical steps you can take to meet its mandates.

At the time of writing this, the GDPR is the most strict global privacy law in existence. Moving forward, privacy laws around the world will likely be modeled after the GDPR. This means that if you understand the GDPR and become compliant with it, you'll be in a really good position to comply with other global privacy laws, both now and in the future.

Thank you for trusting us to provide you with informative, useful content and guidance. We hope this and our other resources will help your business, blog or website stay compliant and thrive.


TermsFeed