TermsFeed

GDPR Compliance for Developers

Preface

We created this book to help developers who are in the process of complying with the GDPR. We believe developers are at the cornerstone of GDPR compliance because the GDPR was created with online privacy at its center, and developers are the architects of our online landscape.

This book will help you understand the inherent goals of the GDPR in a way that will make your compliance journey more intuitive and almost a second nature. We break down the specific requirements of the GDPR and offer practical steps and solutions for compliance. Case studies and examples help to demonstrate the GDPR's principles in relatable, real-world ways.

Whether you're just starting out with compliance or are looking for a solution to a specific problem that you're facing further into your compliance journey, this book will hold the answers and guidance that you need.

Please note that we have captured the details, requirements and interpretations of the GDPR as it stands at the time of writing. This doesn't mean that the information is guaranteed to be without errors or omissions as the GDPR and all laws are living documents. For the most up to date information, please check out our database of current articles addressing the GDPR.

This book is not intended to be legal advice, nor does it create an attorney-client relationship between us and you. While we've done our best to be as accurate as possible and not leave anything out, we acknowledge that laws are always changing, especially in the field of global privacy. Thus, the content may not be 100% accurate at all times. We encourage you to use this book as a starting point for clarity and guidance, and we hope it brings you both.

Best wishes, from our team to yours.

The Table of Contents:

Chapter 1:

Why the GDPR Affects Developers

The EU General Data Protection Regulation (GDPR) has had a substantial impact around the world.

Marketers have been hurriedly spamming their EU subscribers to ensure that they have legally-valid **consent**. Businesses running **targeted ads** in the EU have had to jump through a series of regulatory hoops. Some companies have even made their websites **inaccessible to EU visitors** out of fear that they might violate the law.

And **within the EU** itself, the GDPR has affected just about everyone.

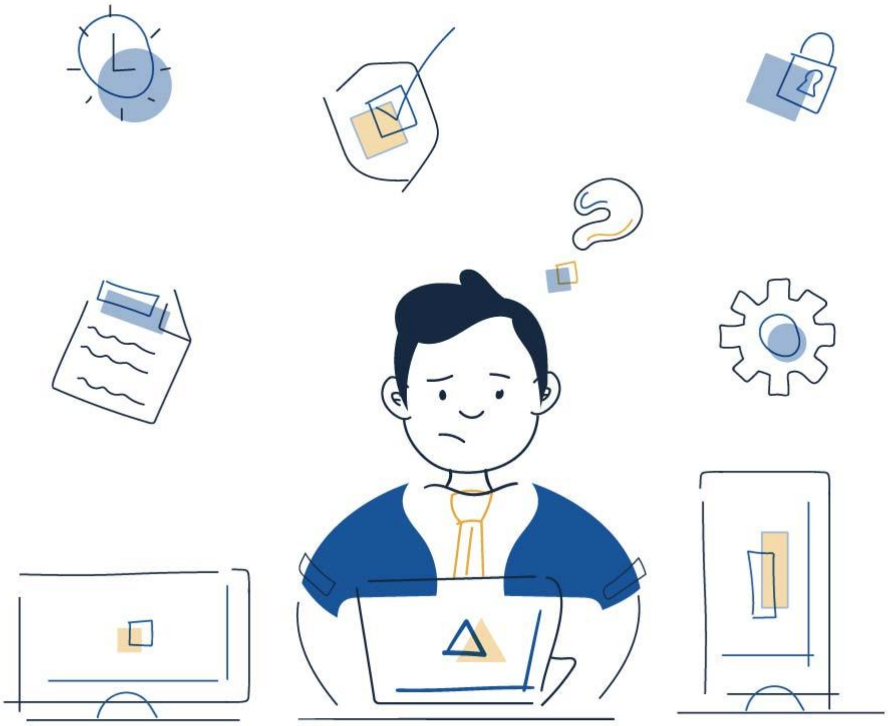


Illustration: Why the GDPR Affects Developers

School teachers have been herded into classrooms and subjected to mandatory **GDPR training sessions**. Doctors' offices have appointed **Data Protection Officers** to oversee the handling of medical records. Even the local priest has lost sleep, worrying about how to **anonymize** the church choir sign-up sheet.

Every web developer should be aware of how the GDPR affects them. After all, if it weren't for the ubiquity of technology in modern life, there would be no need for such privacy laws.

Billions of people have an **online identity**, whether they know it or not. People transmit their private information over the web on a daily basis. They've invited intrusive **data-processing devices** into their homes.

At its heart, the GDPR is about **security** and **control**. It should make cybercrime a much less worthwhile endeavor. It aims to reduce the exploitation of people's online presence. And it ensures that individuals can maintain ownership of their **personal data**.

These are all admirable goals. And for the most part, it's **developers** that will actually make this stuff happen.

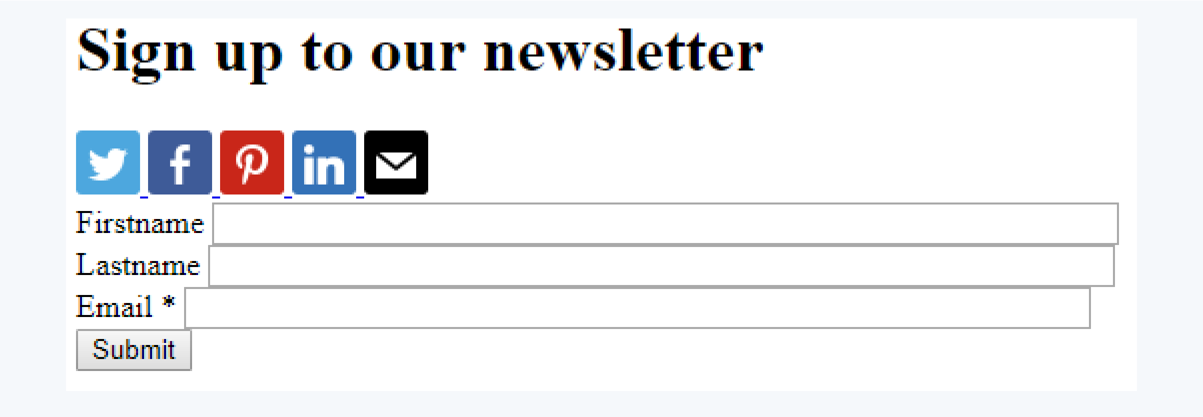
Developers at the Heart of GDPR Implementation

Let's consider a few examples of how crucial developers are to the implementation of this law.

Consent is a big deal under the GDPR. It's important that you ask a person whether you have their permission to send them direct marketing. And the ***way*** you ask them is also important.

With this in mind, many companies have been looking at the way they ask for consent. In many cases, their long-established methods are not compliant with the new law.

Here's a real example, taken from an archived version of Adoption UK's website back in 2015.



Sign up to our newsletter

Firstname

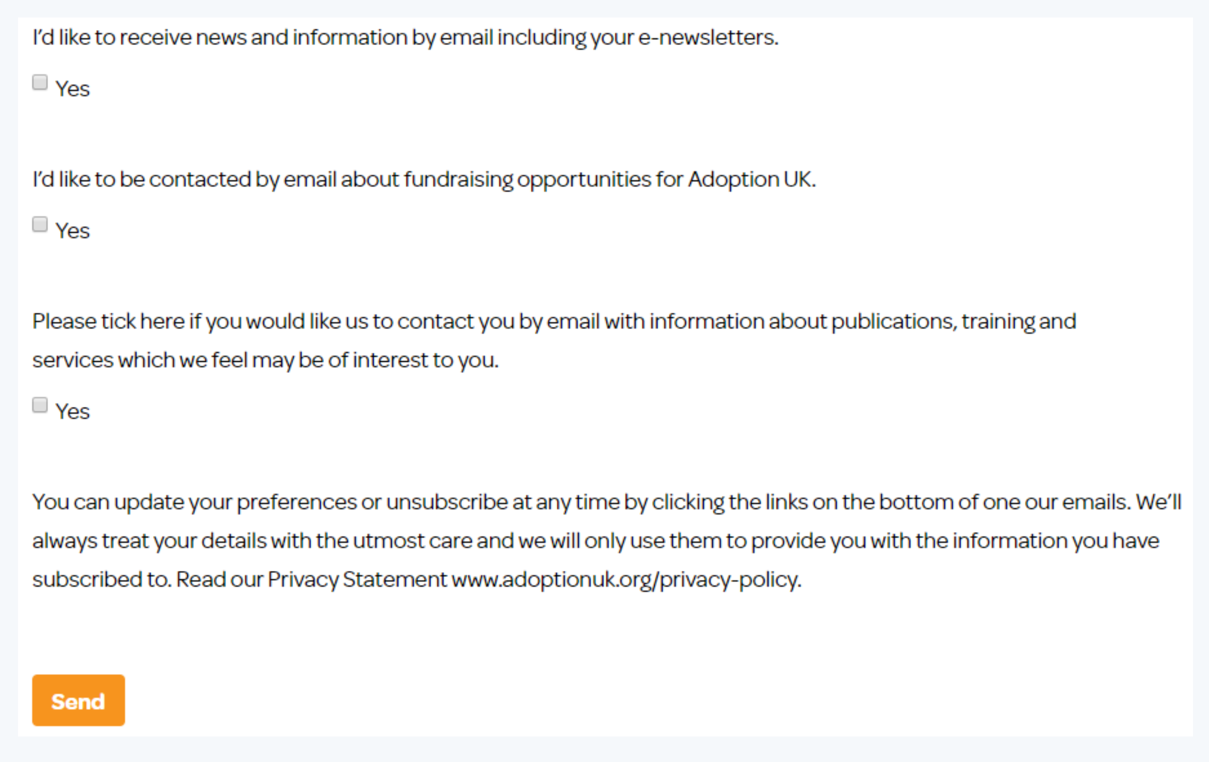
Lastname

Email *

Submit

Image: Adoption UK newsletter sign-up form

Something like this would **not be sufficient** under the GDPR's requirements. Fortunately, Adoption UK's more current newsletter consent request looks much better now:



I'd like to receive news and information by email including your e-newsletters.

□ Yes

I'd like to be contacted by email about fundraising opportunities for Adoption UK.

□ Yes

Please tick here if you would like us to contact you by email with information about publications, training and services which we feel may be of interest to you.

□ Yes

You can update your preferences or unsubscribe at any time by clicking the links on the bottom of one our emails. We'll always treat your details with the utmost care and we will only use them to provide you with the information you have subscribed to. Read our Privacy Statement www.adoptionuk.org/privacy-policy.

Send

Image: Adoption UK newsletter sign-up form checkboxes

You can see the difference between these two methods.

The latter one allows the user to make **real decisions** about what correspondence they receive. They are invited to read the charity's Privacy Policy and told how to **withdraw consent** (by unsubscribing). A front-end developer made this happen.

There may be many people in a company who can spot areas where their data processing practices fall short of the law's requirements. But this is not enough. Developers are required to actually bring these changes about.

There are countless other examples where a developer would be required to put GDPR-mandated changes into practice.

For instance, if an app publisher decides to integrate new **account controls** into its software, so as to allow users to **directly access** their personal data - it's a developer that will have to create this function.

Or perhaps an instant messaging software company decides to employ a higher standard of **encryption**, to ensure compliance with the GDPR's enhanced **security requirements**. Who do you think would be called upon to implement this measure? You guessed it - developers.

This is a **huge opportunity**, but it's also a **big responsibility**. Privacy law is expanding, and the GDPR is the latest clear indication of this. It's incumbent on developers to cultivate an **in-depth understanding** of **data protection** and **information security**.

Developers on the Frontline of Enhancing Data Protection

High profile security incidents occur all the time. Every week we hear of another **data breach** where account credentials, payment card numbers or passport details are compromised. This can be devastating for a business and its customers. Developers play a crucial role in preventing these occurrences.

In the first eight months of the GDPR, there were nearly 60,000 data breaches reported. But a 2019 study revealed that GDPR-compliant companies are **significantly less likely** to suffer a data breach. This survey took place before the GDPR had been in force for even one year.

There are many possible reasons for this, including:

- The GDPR demands that personal data is processed **securely**, and subject to **technical measures** such as anonymization, pseudonymization, and encryption. Data in these forms is far less likely to be useful to hackers.
- Personal data is only to be **stored** for as long as it's **needed**. Less personal data in storage automatically means less risk.
- Because of the **controls** that individuals can exercise over their personal data, **transparency** is required at every stage of processing. Personal data must be well-organized and accessible to those who require access.

These are just three examples of how the GDPR can improve a company's data protection practices, and **developers are crucial in each case**.

When ensuring that personal data is stored securely, a developer must choose a method that is **GDPR-compliant, genuinely secure, and also functional** according to the needs of the business.

To fulfill the GDPR's principle of storage limitation, **a developer must implement a system that automatically deletes unneeded personal data.** For example, by using logrotate to remove expired log files.

And in order to facilitate users' requests for **access**, **rectification** or **erasure**, developers must create and maintain secure and orderly databases. These databases should be easily accessible to those with permission, but they must remain impenetrable to those without it.

The GDPR: An Opportunity for Developers

This book is very much focused on the GDPR law that developers must know about, rather than the **technical aspects** of development. Whilst the book won't shy away from the technical implications of following the law, it isn't about coding.

Here are some of the things you'll be learning about:

- What the GDPR says, and why it's important
- Some of the myths and half-truths surrounding the GDPR
- How the GDPR relates to developers
- The practical steps developers can take to fulfill the GDPR's requirements
- How you can turn this new challenge into an opportunity

The law is coming down hard on companies who do not treat their customers' personal data with respect. Those who fail to realize this are liable to be **left behind**. But opportunities await those who understand the law and can thrive in this new culture.

Chapter 2:

What is the GDPR?

For all its insistence that businesses use “clear and plain language” when communicating with their customers, the GDPR is **long**, **obscure** and frankly **bewildering** in places. The GDPR can be a fantastic opportunity for developers, but only if they truly understand it.

It is possible to distill the rules and principles of the GDPR down into a comprehensible form. But a lot of **misunderstandings** and **myths** are circulating about it. Quite frankly, these misconceptions are causing people to break the law.

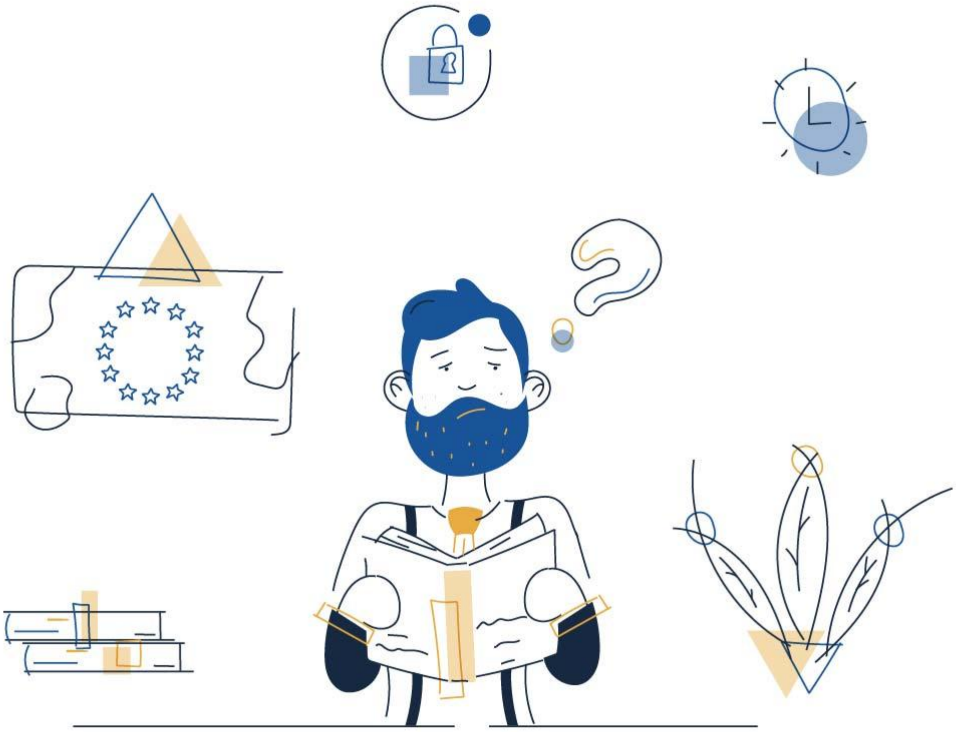


Illustration: Developer thinks what is the GDPR?

Before honing in on how the regulation applies to developers, we’re going to get familiar with the basics.

Why the GDPR Exists

The GDPR was passed in April 2016 and took effect in May 2018. It replaced the "**Data Protection Directive**" which had been in place since 1995. Despite the monumental changes in the world of information technology in the two decades between the passing of the two laws, they are actually pretty similar in many respects.

The GDPR sets **rules** regarding the **automated** or semi-automated **processing of personal data**.

The main objectives of the GDPR are:

- To **protect people's rights** in relation to their personal data
- To make sure that personal data is **processed in a consistent way** across the whole of the EU

What is Personal Data?

The term personal data is similar to what is called personal information, or personally identifying information (PII) in other jurisdictions.

The GDPR gives a very broad definition of personal data, and it's also interpreted very broadly by institutions and courts within the EU.

Personal data is sometimes defined as information that identifies a person. This is actually too narrow a definition.

Personal data is best thought of as any information that might reveal something about a specific person.

A person's name and address are amongst the most obvious examples of personal data. On their own, a name or an address don't reveal much. But combine them, and you know where a person lives.

The principle extends to more obscure types of information.

For instance, take an **IP address.** This has been held by the EU Court of Justice to constitute **personal data**. An IP address on its own means very little. But it could, in theory, reveal a lot about a person, if linked to their **name** and **browsing history**.

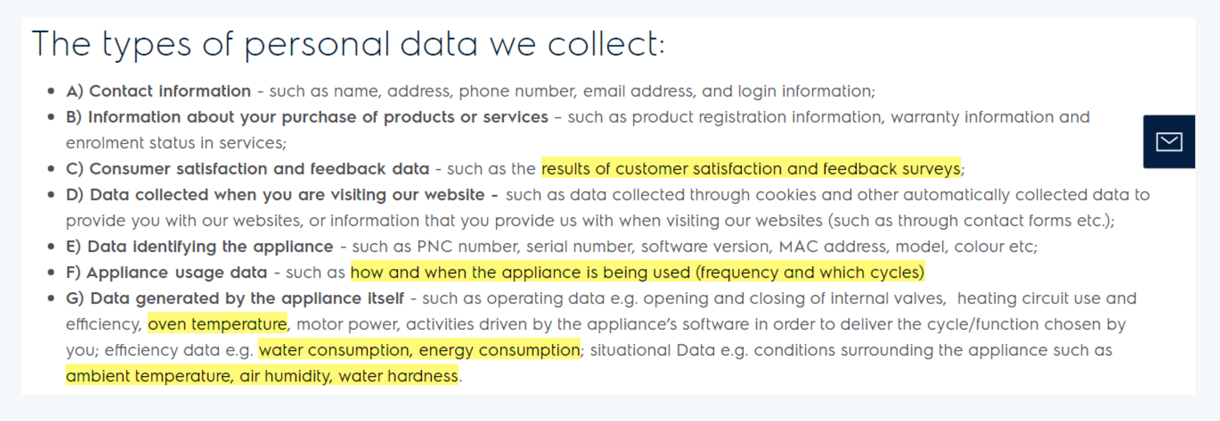
Think about all the information people offer up about themselves online. Web developers and administrators can potentially handle a lot of personal data.

A notorious example is **cookie data**. Cookies can track users across multiple websites and monitor how they behave online.

The sort of information collected by cookies is unlikely to reveal the identity of an individual in itself. But if it *were* linked up with other information it could reveal a great deal about a person's personality, interests, and activities.

This extensive definition of personal data is particularly important given the increasing use of connected "smart home" devices.

Take a look at how Electrolux defines "personal data" in its Privacy Policy. Some of the more obscure examples are highlighted:



The types of personal data we collect:

- **A) Contact information** - such as name, address, phone number, email address, and login information;
- **B) Information about your purchase of products or services** – such as product registration information, warranty information and enrolment status in services;
- **C) Consumer satisfaction and feedback data** - such as the results of customer satisfaction and feedback surveys;
- **D) Data collected when you are visiting our website -** such as data collected through cookies and other automatically collected data to provide you with our websites, or information that you provide us with when visiting our websites (such as through contact forms etc.);
- **E) Data identifying the appliance** - such as PNC number, serial number, software version, MAC address, model, colour etc;
- **F) Appliance usage data** - such as how and when the appliance is being used (frequency and which cycles)
- **G) Data generated by the appliance itself** - such as operating data e.g. opening and closing of internal valves, heating circuit use and efficiency, oven temperature, motor power, activities driven by the appliance's software in order to deliver the cycle/function chosen by you; efficiency data e.g. water consumption, energy consumption; situational Data e.g. conditions surrounding the appliance such as ambient temperature, air humidity, water hardness.

Image: Electrolux Data Privacy Statement: The types of personal data we collect clause

It may seem ridiculous at first to consider that personal data could include information about when a person's **washing machine** is being used, or data about a person's **oven temperature** and **air humidity**.

But given the amount of information that people are beginning to share about their private lives, isn't it sensible to treat these ostensibly banal details with sensitivity?

Territorial Scope

One of the reasons that the GDPR is such a big deal is because of its broad territorial scope, i.e. the large region it covers.

The focus is on the **individuals** whose personal data is being protected by the law. This means people within the EU. Or more accurately, the **European Economic Area (EEA)**.

The GDPR law isn't restricted to citizens or even residents. Being situated within the EU at a given moment is, nominally, enough to be covered by it.

So, **companies from outside the EU still need to comply with the GDPR law, so long as they're processing the personal data of people in the EU**. But there are limits on this rule, and you're unlikely to fall within the scope of the GDPR "by accident."

You need to be doing at least one of the following two things **in order to be subject to the GDPR:**

1. **Offering goods and services** to people in the EU, or
2. **Monitoring the behavior** of people in the EU

Some other things **could** be relevant in determining whether you're subject to the GDPR:

- Whether your website or app uses a language spoken in the EU
- Whether you sell goods using an EU currency (remember that the euro is not the only EU currency)
- Whether you mention **EU users** in your policies or publicity

Certain things are *not* relevant:

- The **size** of your company
- Whether you are **pursuing a profit**
- Whether you are a **charity**

The GDPR also applies to a **lone developer** with a one-page website as much as it applies to **Google**. It even applies to people running a Facebook Page, due to the way that Facebook uses cookies.

Monitoring behavior has the potential to bring a large number of developers and businesses under the scope of the GDPR. It applies to **behavioral advertising** and the use of **tracking cookies**.

Principles of the GDPR

The GDPR gives a set of **principles** which guide all processing of personal data.

Processing personal data means **collecting** it, **storing** it, **sharing** it or otherwise **using** it in some way.

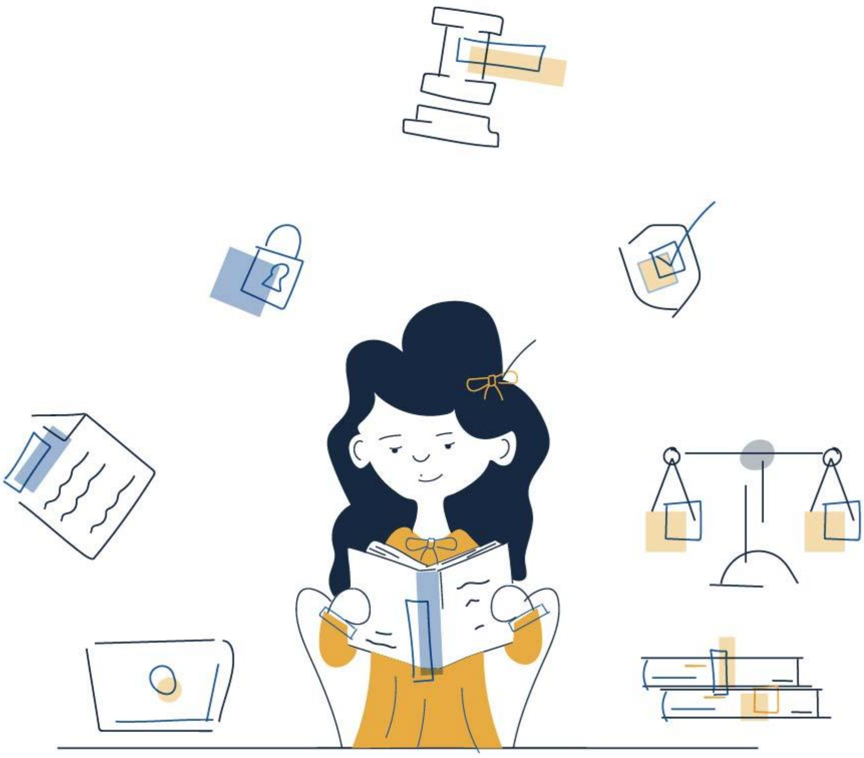


Illustration: The developer reads about the principles of the GDPR

The application of these principles is, in a sense, the whole purpose of this book. If you follow them in the right way, you'll be GDPR-compliant. So, we'll be returning to each of them in detail.

Lawfulness, Fairness, and Transparency

The first of the principles, "**lawfulness, fairness, and transparency**," looks a lot like three principles in one.

Processing personal data "**lawfully**" means doing so in compliance with the GDPR and other laws. But it also has a more specific definition. It means only processing personal data under one of the GDPR's legal bases.

The legal bases represent a set of **good, lawful reasons** for processing personal data. You can't process personal data unless you have a good, lawful reason (a legal basis) for doing so.

The legal bases are:

a) **Consent**. You can process someone's personal data if they've given you their permission to do so. This permission must be freely given, specific, informed and unambiguous. It must be given via a clear and affirmative action, and easy to withdraw. We'll be looking at consent in detail later.

b) **Contract**. You can process someone's personal data if it's **necessary** to do so in order to fulfill or enter into a contract with them.

   For example, if you ask a home insurance company for a quote, they can lawfully process personal data about you and your home.

c) **Legal obligation**. You can process someone's personal data if you're required to do so by law.

   For example, banks are legally required to store some personal data for a long time. And employers are legally required to share their employees' personal data with tax authorities.

d) **Vital interest**. You can process someone's personal data if you need to do so in order to protect someone's life. This generally applies as the last resort.

   For example, if someone is seriously injured and unconscious, it's legal for a doctor to access their medical records.

e) **Public interest**. You can process someone's personal data if you're exercising official authority, or you're performing a task in the public interest set out in law. This mostly covers public bodies or privatized industries.

f) **Legitimate interest**. You can process someone's personal data if it has a minimal impact on them, and you're pursuing a legitimate and ethical purpose that **benefits** you or a third party. We'll be looking at legitimate interests in detail later.

Lawfulness also means obeying other EU laws such as the **ePrivacy Directive**. This is an older privacy law that has very important rules that developers must know about regarding the use of cookies and other technologies.

Processing personal data **fairly** means doing so in a way that people would **reasonably expect**. It means not using people's personal data for unethical purposes, even if it might be technically legal to do so. It also means not deceiving people into giving up their personal data.

Transparency is a really important part of GDPR-compliance. One important step towards achieving transparency is writing a Privacy Policy.

Purpose Limitation

The second of the GDPR's principles is known as **purpose limitation**.

With very limited exceptions, you must only process personal data in relation to a **specific purpose**. You must always be **clear** and **honest** with people about your **reasons** for processing their personal data.

If you *do* need to process data for a purpose other than the one for which you originally collected it, you must go about this in the proper way. The conditions for "**further processing**" are addressed at Recital 50.

Here's an example of what *not to do.*

A travel company has a "comments" section underneath each of their blog posts. Commenting requires visitors to **register** with an email address for **verification purposes**.

A registered user leaves a comment under an article about Japan. The company then uses that person's email address to send them **marketing information** about Japanese vacation packages.

This is a violation of the principle of purpose limitation. The person was told that their email address was required for verification. It should not have been used for any other purpose.

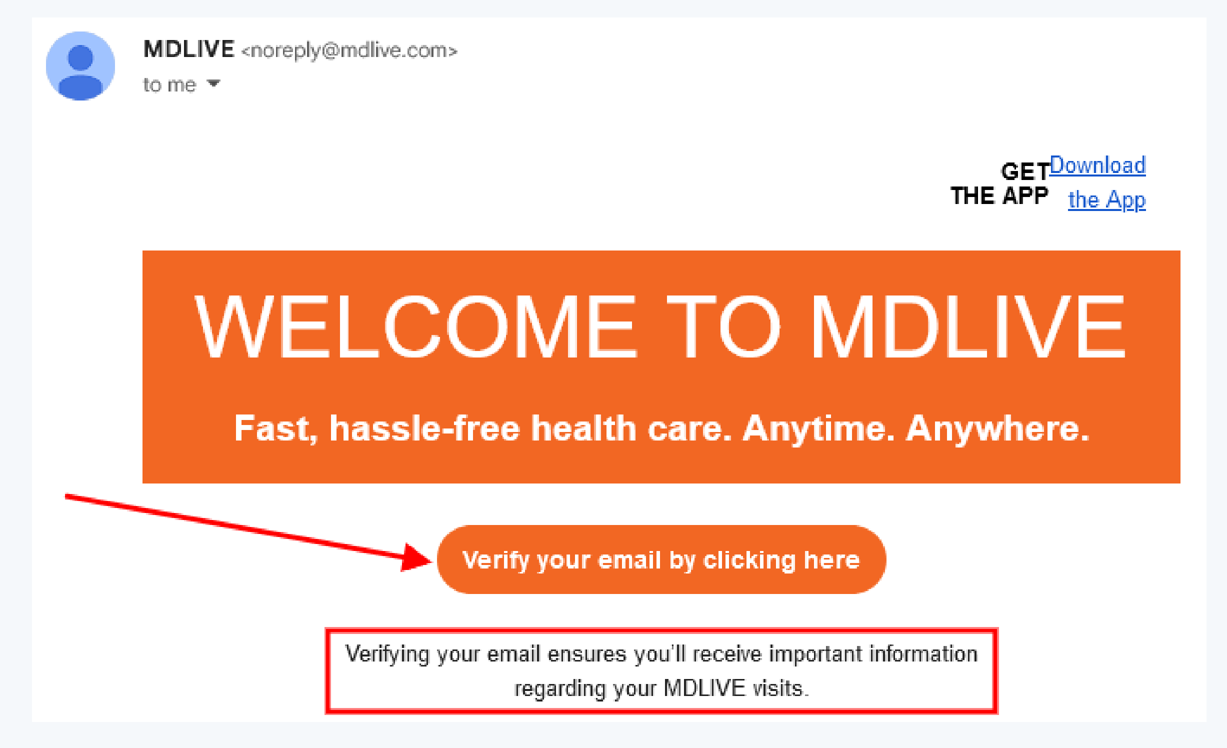
Data Minimization

The principle of **data minimization** requires that you do not process personal data that you don't need. All the personal data you process should be **relevant to your purposes**.

Here's an example of how a developer might help with the fulfillment of this requirement.

Using a **double opt-in** for direct email marketing is considered good practice under the GDPR. Where a person signs up to receive marketing communication, a double opt-in means sending a **validation** email to **verify their identity**.

Here's an example of how this can look:



MDLIVE <noreply@mdlive.com>

to me

GET THE APP
Download the App
WELCOME TO MDLIVE
Fast, hassle-free health care. Anytime. Anywhere.
Verify your email by clicking here

Verifying your email ensures you'll receive important information regarding your MDLIVE visits.

Image: MDLive verification email screenshot

If a person doesn't respond to this email verification email, their details should be **automatically removed** from a company's records within a **predetermined period** (say, seven days).

Accuracy

The principle of **accuracy** means maintaining **correct** and (in some cases) **up-to-date records**. It also means allowing people to request their personal data is rectified if they believe it to be inaccurate.

Storing inaccurate personal data can sometimes have **disastrous consequences**. For example, in 2012, insurance company Prudential was fined £50,000 by the UK's Data Protection Authority, the Information Commissioner's Office (ICO), after **inaccurate records** led to a customer's money being transferred into the wrong account.

Storage Limitation

The principle of **storage limitation** states that **you shouldn't keep personal data for longer than you need it**.

There will be some rare instances where personal data might be kept **indefinitely**. For example, the GDPR allows this in some cases related to research.

However, in almost every case, you must have a **predetermined deletion point** for each type of personal data you collect.

For example, **server logs** should be purged of personal data regularly (if they need to contain any in the first place), **unused accounts** should be deleted, and **cookies** should have the shortest practical lifespan.

Integrity and Confidentiality

The principle of **integrity and confidentiality** is sometimes called the principle of **security**. Developers play a **crucial role** in ensuring that personal data is processed securely.

Part of your fulfillment of this principle might involve certifying to a particular ISO (International Organization for Standardization) standard. This will certainly be a step in the right direction, but will not be sufficient in itself. Some of the technical and security measures discussed in this book are not covered by the ISO standards.

Part of what's required under this principle is organizational in nature: ensuring that your organization has (or, if you're a lone developer, *you* have) **suitable procedures for identifying and dealing with security threats**.

You must know what personal data is flowing throughout your systems, and you must be able to suitably restrict access to personal data records.

Accountability

The principle of **accountability** sits separately from the other principles in the text of the GDPR. It requires that you **comply** with the other GDPR principles, and that you can **demonstrate your compliance**.

There are many ways you can hold yourself or your organization accountable under the GDPR:

- Conducting a data audit
- Keeping accurate records
- Appointing a Data Protection Officer, if required

We will cover these issues and many more throughout this book.

Data Subject Rights

One of the ways that the GDPR achieves its aim of protecting people's personal data is by empowering them to protect it for themselves.

The data subject rights are a way for individuals to exercise control over their personal data:

1. **The right to be informed:** Individuals must receive clear and comprehensive information about the ways in which their personal data will be processed.
2. **The right of access:** Individuals can receive information about any of their personal data that a person or organization is processing.
3. **The right of rectification:** Inaccurate personal data relating to an individual must be corrected at their request.
4. **The right to erasure** (also known as **the right to be forgotten**)**:** Individuals can request that their personal data is erased.
5. **The right to restrict processing:** Individuals may restrict the ways in which their personal data is processed.
6. **The right to data portability:** Individuals can receive a copy of their personal data so as to transfer it to another organization.
7. **The right to object:** Individuals may object to their personal data being processed.
8. Rights related to **automated decision-making and profiling:** Where important decisions are made by automated means, individuals have the right to human intervention.

There are **many exceptions** to the rights above, and some only apply where the processing takes place under particular legal bases.

We'll be looking in more detail at some of these rights and how they apply to developers in a later chapter.

The GDPR and Other Privacy Laws

The GDPR is probably the most **comprehensive** data protection law in the world. But it's not the only one. There are many others, including:

- The Colorado Privacy Act (CPA)
- The Virginia Consumer Data Protection Act (VCDPA)

- The California Online Privacy Protection Act (CalOPPA)
- The California Consumer Privacy Act (CCPA) and its amendments known as the California Privacy Rights Act (CPRA).
- Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- The Enhancing Privacy Protection Act (Privacy Act) in Australia
- Several Southeast Asian countries

Illustration: The developer juggles with GDPR and other privacy laws

Let's take a look at some of the major similarities and differences between the CCPA (CPRA) and the GDPR, followed by CalOPPA.

The GDPR and the CCPA (CPRA)

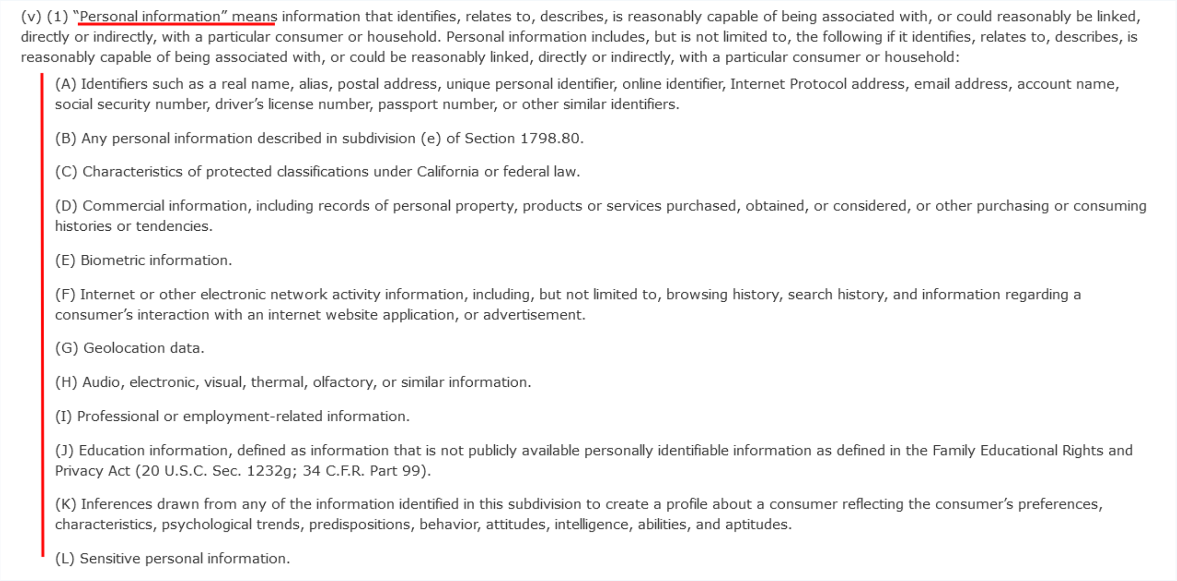
Definition of Personal Information

The CCPA (CPRA) defines "personal information" as the following:

> *"Information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not*

> *limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household."*

It gives a list of specific types of information that fall under its scope:



(v) (1) "Personal information" means information that identifies, relates to, describes, is reasonably capable of being associated with, or could reasonably be linked, directly or indirectly, with a particular consumer or household. Personal information includes, but is not limited to, the following if it identifies, relates to, describes, is reasonably capable of being associated with, or could be reasonably linked, directly or indirectly, with a particular consumer or household:

(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.

(B) Any personal information described in subdivision (e) of Section 1798.80.

(C) Characteristics of protected classifications under California or federal law.

(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.

(E) Biometric information.

(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.

(G) Geolocation data.

(H) Audio, electronic, visual, thermal, olfactory, or similar information.

(I) Professional or employment-related information.

(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).

(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.

(L) Sensitive personal information.

Image: CCPA full text: Definition of Personal Information updated for 2023

Here it is from the text of the law:

> *(A) Identifiers such as a real name, alias, postal address, unique personal identifier, online identifier, Internet Protocol address, email address, account name, social security number, driver's license number, passport number, or other similar identifiers.*
> *(B) Any personal information described in subdivision (e) of Section 1798.80.*
> *(C) Characteristics of protected classifications under California or federal law.*
> *(D) Commercial information, including records of personal property, products or services purchased, obtained, or considered, or other purchasing or consuming histories or tendencies.*
> *(E) Biometric information.*
> *(F) Internet or other electronic network activity information, including, but not limited to, browsing history, search history, and information regarding a consumer's interaction with an internet website application, or advertisement.*
> *(G) Geolocation data.*
> *(H) Audio, electronic, visual, thermal, olfactory, or similar information.*
> *(I) Professional or employment-related information.*

> *(J) Education information, defined as information that is not publicly available personally identifiable information as defined in the Family Educational Rights and Privacy Act (20 U.S.C. Sec. 1232g; 34 C.F.R. Part 99).*
> *(K) Inferences drawn from any of the information identified in this subdivision to create a profile about a consumer reflecting the consumer's preferences, characteristics, psychological trends, predispositions, behavior, attitudes, intelligence, abilities, and aptitudes.*
> *(L) Sensitive personal information*

Scope

The CCPA (CPRA) will apply to a business that operates for a profit, that does business in California, and additionally meets even just one of the following requirements:

- Has a gross annual revenue of more than $25 million,
- Buys, receives or sells the personal information of at least 100,000 (100,000 or more) California residents or households, **or**
- Makes at least half (50% or more) of its annual revenue from sharing or selling the personal information of California residents

Privacy Policy Requirements

The CCPA (CPRA) requires a number of specific things for your Privacy Policy.

Your Privacy Policy must contain the following information:

- The rights granted under the CCPA (CPRA)
- A link to a "Do Not Sell My Personal Information" page
- The categories of personal information you've collected over the past 12 months
- The categories of sources where you obtain personal information
- Why you collect personal information
- How long you keep or plan to keep personal information
- The categories of personal data you've sold over the past 12 months
- The categories of personal information you've disclosed for business purposes over the past 12 months

Your Privacy Policy must be updated every 12 months to ensure it's current.

In addition, you must post a "conspicuous" link to your Privacy Policy on your website's front page (such as in the website footer).

The GDPR and CalOPPA

Definition of Personal Data

As we've seen, **the GDPR's definition of "personal data" is extremely broad**. In CalOPPA, the definition of personal data (which it calls "personally identifying information") is somewhat narrower.

CalOPPA lists the following as constituting personal data:

- A person's full name
- A physical address, which includes a street name and the name of a city or town
- An email address
- A phone number
- A social security number
- Any other identifier could lead to a specific individual being contacted
- Data collected by a website or app, such as cookies, but *only if* they are stored in a personally identifiable form alongside one the identifiers listed above

All of these examples, and much more besides (as noted earlier in this chapter), are also personal data under the GDPR.

Scope

The scope of the GDPR, meaning **who** and **what** it applies to, is also very broad, covering "automated" or "semi-automated" processing of personal data, except in the context of "**purely personal or household activities**."

This means that you don't have to worry about encrypting your mobile phone's contact list or anonymizing your kids' school reports. But you should assume that anything outside of the domestic context is covered.

CalOPPA only applies to:

> *"An operator of a commercial Web site or online service that collects personally identifiable information through the Internet about individual consumers residing in California who use or visit its commercial Web site or online service."*

This includes **apps**, as confirmed when the California Attorney General brought a case against Delta Airlines for failing to provide a Privacy Policy with its mobile app.

CalOPPA and the GDPR apply similarly in terms of territorial scope. Both should be read as applying to businesses that are **operating within**, but **based outside of**, their respective territories.

Any commercial website that collects personal data about **California residents** is covered by CalOPPA. The location of the owner of that website is not a relevant consideration.

Privacy Policy Requirements

CalOPPA imposes only two obligations:

1. Write a **Privacy Policy**, and
2. Display a **conspicuous link** to it on your website

The GDPR imposes a **huge range** of obligations. One of these is to write a Privacy Policy.

Both laws also provide specific rules about what a Privacy Policy must contain. The table below broadly sets out what's required under each law.

Privacy Policy must disclose:	**GDPR**	**CCPA (CPRA)**	**CalOPPA**
The categories of personal data processed	Yes	Yes	Yes, but specifically only personal data collected through the website or app
The categories of third-party recipients of the personal data	Yes	Yes	Yes
The existence of the data subject rights, and a method by which an individual might exercise those rights	Yes	Yes	If the commercial website operator provides a method by which users can access and make changes to their personal data, they must disclose this. Other rights do not apply
The process by which changes to the Privacy	This is not explicit in the	No	Yes

Policy will be communicated	GDPR, but would be good practice		
The effective date of the Privacy Policy	This is not explicit in the GDPR, but would be good practice	No	Yes
Whether the website respects browsers' "Do Not Track" (DNT) signals	No	Yes	Yes, if users are tracked
Whether third parties can collect individuals' personal data over time and across other websites (e.g. via a retargeting campaign)	Yes, in that you must disclose the purposes for which personal data is processed	Yes	Yes
The purposes for which personal data is processed	Yes	Yes	No
Whether the personal data will be subject to any international transfers, and if so what safeguards will be applied	Yes	No	No
How long personal data is stored	Yes	Yes	No
Any third-party sources of personal data	Yes	Yes	No
Contact details of the data controller, plus its Data Protection Officer and EU Representative, if applicable.	Yes	N/A	N/A
The legal basis on which personal data is processed	Yes	N/A	N/A

Table 1: Privacy Policy Disclosure Requirements - GDPR, CCPA (CPRA) and CalOPPA

Keep in mind that under the GDPR, there may also be **additional information** required in some circumstances.

As you can see from this table, the Privacy Policy requirements under the GDPR are much more extensive than those under the CCPA (CPRA) and CalOPPA.

If you're compliant with the GDPR, you're likely to be very close to compliance with other privacy laws, too, including the CCPA (CPRA) and CalOPPA.

Key Takeaways from This Chapter

In this chapter, we've explored the basics of the GDPR, including:

- The objectives of the GDPR
- Who the GDPR applies to
- The principles of data processing
- The data subject rights

In the next chapter, we're going to look at an important concept from the GDPR, and how this applies to developers: **data controllers** and **data processors**.

Chapter 3:

Data Controllers and Data Processors

The GDPR categorizes people and organizations on the basis of their **relationship to personal data**. These different categories confer very different **roles and responsibilities**. It's possible to be in one category in some respects, and a different category in others.

It's crucially important to understand which category you as a developer (or your company) occupy.

When processing personal data, you'll be doing so either as a data controller or a data processor.

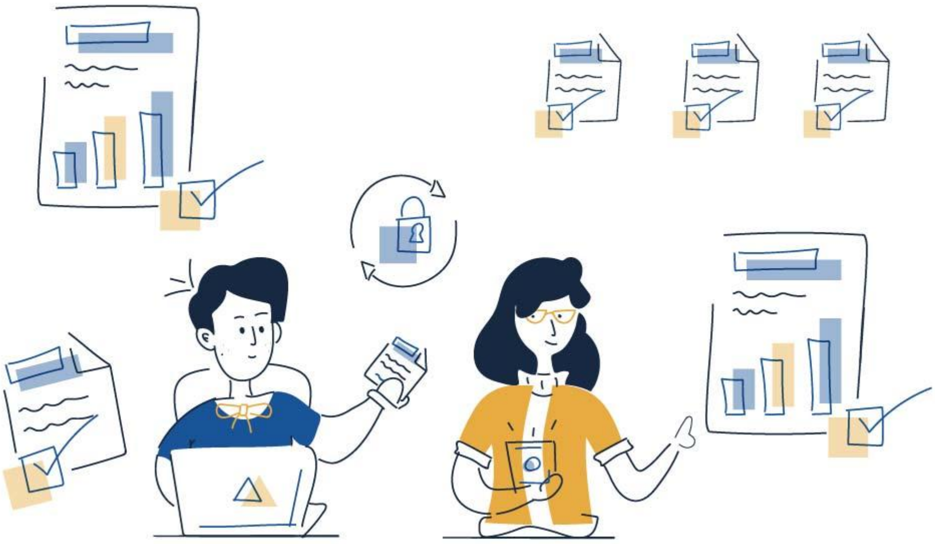


Illustration: Data Controllers and Data Processors

In this chapter, you'll be figuring out which of these two roles you fall into, and what this means for your data protection practices.

People and Organizations According to the GDPR

No matter who you are, you'll feature in the GDPR in at least one role. We're going to focus on data controllers and data processors in this chapter, but let's take this opportunity to define some other terms as well.

Here are the four major players that feature throughout the text of the GDPR:

1. **Data controller** - A person or organization that "*determines the purposes and means*" of processing personal data. A data controller can be an individual, private company, public body or even a government - all that matters is that it has decided how and why personal data will be processed.
2. **Data processor** - An organization that "*processes data on behalf of a data controller*." A data processor is processing personal data because it has been asked to do so by a data controller. It must follow the data controller's instructions.
3. **Data subject** - An individual; an ordinary person, with rights and interests, to whom personal data relates. A data subject is a "natural person," not a "legal person." Legal persons can include companies and other organizations, who cannot own personal data.
4. **Supervisory authority** - An independent public body set up in each EU country to enforce the GDPR. Also known as a Data Protection Authority.

Try not to think of your role in the GDPR as defined by **what you are**. It is better determined by **what you are doing** with personal data, at any given moment.

Differences Between GDPR Data Controllers and Data Processors

A **data controller** can be thought of as the "**data boss**." A data controller takes the **decision** to process someone's personal data, in connection with a specific **purpose**. It also decides **how** this processing should occur.

A **data processor** is more like the data controller's **employee**. A data processor processes personal data in order to **fulfill the data controller's purposes**. Even if it has devised the method of processing that data, it **can't** be said to determine **how** personal data is processed in any given instance.

The following types of business will normally be acting as **data controllers**:

- Ecommerce stores
- Social media networks
- Insurance companies

The following types of business will normally be acting as **data processors**:

- Analytics providers
- Email marketing services
- Payroll companies

Case Study

Let's put this in context. We'll see how a company can **be a data controller *and* a data processor**, and **work with data processors and other data controllers**, all depending on the context.

BigPrint is a printing company. It has a mailing list. It **collects** email addresses via a web form and **shares** these with email marketing company Mailchimp. Mailchimp sends emails on BigPrint's **behalf**.

Image: Intuit Mailchimp logo - small

BigPrint is the **data controller** in this respect. Mailchimp is the data processor.

- BigPrint **collects** the personal data
- BigPrint **shares** the personal data with MailChimp
- BigPrint **decides** how often direct marketing emails are sent
- Mailchimp sends the emails using personal data **provided** by BigPrint

BigPrint also runs **analytics** on its website using Google Analytics. It uses Google Analytics to gain insights about **web traffic** and **user behavior** on its site.

Image: Google Analytics logo - small

BigPrint is also the **data controller** in this respect. Google Analytics is the data processor.

- Google collects the personal data

However:

- BigPrint **determines** how and why the personal data is processed
- BigPrint **tells** Google what personal data to collect
- BigPrint can **access and modify** the personal data

BigPrint receives an order from a client, a local art collector. The art collector is running an exhibition and wants BigPrint to print the invitations. The art collector **shares** the invitees' names and addresses with BigPrint.

BigPrint is the **data processor** in this respect. The art collector is the data controller.

- The art collector **collects** the personal data
- The art collector **determines** how and why the personal data is processed
- The art collector **shares** the personal data with BigPrint
- BigPrint **processes** the personal data by producing the invitations

The art collector **makes a payment** on BigPrint's website using PayPal.

Image: PayPal logo - small

PayPal is the **data controller** in this respect. BigPrint is **also** a **data controller**, but not in this context. The art collector is the data subject.

- PayPal **determines** what personal data is required to process the payment
- PayPal **collects** the personal data (credit card information or login data)
- PayPal **contacts** the acquiring bank to obtain the art collector's payment
- PayPal **stores** the personal data and is responsible for protecting it

Are You a GDPR Data Controller or a Data Processor?

We've seen that it is possible to be a data controller in some contexts and a data processor in others. However, there are **different roles and responsibilities** for each, and it's important to determine the **primary role** of your company.

Below is a table containing some questions about your **relationship to personal data** and data subjects. This should help you determine which category you fall into.

	Data controller	**Data processor**
Did you take the **initial decision** to collect the personal data?	Yes	No
Did you **decide** which **types** of personal data to collect?	Yes	No
Did you **decide** the **purpose** for which the personal data will be processed?	Yes	No
Did you **determine** the **legal basis** for processing?	Yes	No
Are you **responsible** for **telling** data subjects about the processing?	Yes	No
Are you **responsible** for receiving and coordinating **data subject rights** requests?	Yes	No
Are you **responsible** for **earning consent** for the processing where applicable?	Yes	No

Table 2: Questions about your relationship to personal data - GDPR Data Controller or Data Processor

You may not know which of these apply you do yet. You can refer back to this section as you learn more about the GDPR.

Shared Responsibilities

There are a number of roles and responsibilities that both data processors and data controllers have in common.

For example, **both** data controllers and data processors must:

- Understand the GDPR
- Appoint a Data Protection Officer and/or an EU Representative if required (we'll be looking at this in detail later)
- Store and otherwise process personal data **securely**
- Only **transfer** personal data out of the EU with appropriate **safeguards** in place
- Make sure that there is a **written contract** in place whenever they are working together

Data Processing Records

Both data controller and data processors are also responsible for **keeping extensive records** of their **data processing activities**, but **only if** at least **one** the following applies:

- They are a company with **over 250 employees**
- The processing is **not occasional**
- The processing is could be **high risk**
- The processing involves "**special category**" (sensitive) personal data, or **criminal conviction** data. Special category data includes information about people's:
    - Race
    - Political views
    - Religion or beliefs
    - Sex life
    - Genetic, biometric or health data
    - Union membership

Where these records ***are*** required, **both a** data controller and data processor must provide:

- Their company's **name** and **contact details**, and those of its **Data Protection Officer** and/or **EU Representative** (if it has either)
- Details of any safeguards that are in place for **international transfers** of personal data
- A description of the technical **security measures** it has in place

For a **data controller**, these records must also contain information about:

- The **purposes** of the data processing
- The types of **data subjects** and **personal data** it processes
- The types of **third parties** it will share personal data with
- **Storage periods** for different types of personal data

For a **data processor**, these records must also contain information about:

- The **name and contact details** of each **data controller** it is working with
- The types of **data processing** it carries out for each data controller

Data Processing Agreement

It's absolutely crucial that all arrangements between a data controller and a data processor take place under a Data Processing Agreement. This is a **legally binding contract**.

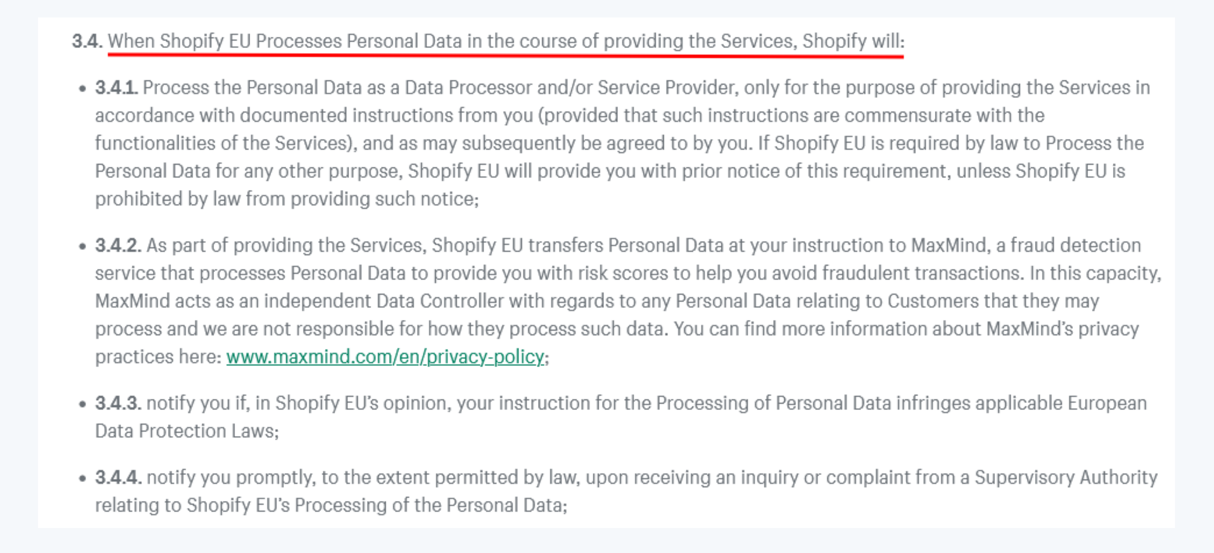
The GDPR has very specific requirements for what this agreement must contain. The requirements for Data Processing Agreements are mostly contained in Article 28.

A Data Processing Agreement must contain details of:

- The **subject matter**, **duration**, **nature**, and **purpose** of the processing
- The categories of **personal data** that will be processed, and the categories of **data subject**
- The data controller's obligations
- The data processor's obligations

Image: Shopify logo - small

Here's an excerpt from Shopify's DPA. Here Shopify sets out some of its obligations as data processor:



3.4. When Shopify EU Processes Personal Data in the course of providing the Services, Shopify will:

- **3.4.1.** Process the Personal Data as a Data Processor and/or Service Provider, only for the purpose of providing the Services in accordance with documented instructions from you (provided that such instructions are commensurate with the functionalities of the Services), and as may subsequently be agreed to by you. If Shopify EU is required by law to Process the Personal Data for any other purpose, Shopify EU will provide you with prior notice of this requirement, unless Shopify EU is prohibited by law from providing such notice;
- **3.4.2.** As part of providing the Services, Shopify EU transfers Personal Data at your instruction to MaxMind, a fraud detection service that processes Personal Data to provide you with risk scores to help you avoid fraudulent transactions. In this capacity, MaxMind acts as an independent Data Controller with regards to any Personal Data relating to Customers that they may process and we are not responsible for how they process such data. You can find more information about MaxMind's privacy practices here: www.maxmind.com/en/privacy-policy;
- **3.4.3.** notify you if, in Shopify EU's opinion, your instruction for the Processing of Personal Data infringes applicable European Data Protection Laws;
- **3.4.4.** notify you promptly, to the extent permitted by law, upon receiving an inquiry or complaint from a Supervisory Authority relating to Shopify EU's Processing of the Personal Data;

Image: Shopify Data Processing Addendum: Section 3 4 excerpt

Shopify is a large data processor, and so requires its clients to agree to this contract when they sign up to use its services. However, there are two things to note about this:

1. Not **all** data processors will have a standard Data Processing Agreement. If you're a data controller engaging a data processor, you may be required to produce one yourself.
2. Even where a standard Data Processing Agreement is offered by a data processor, the data controller **must *still* ensure** that the contract is valid and the data processor **is GDPR-compliant**.

Where a data processor subcontracts some data processing out to another processor (known as a **subprocessor**), they will also need a similar written contract in place for this arrangement.

GDPR Responsibilities of Data Controllers

Data controllers have a **direct relationship** with data subjects, and they have a **direct interest** in the end result of the data processing.

A developer may **create an application or website** that collects personal data. They will be the data controller if they (or their company) has also decided **why** this personal data should be collected.

A data controller must comply with the GDPR in full. There are some things that are particularly important for a data controller:

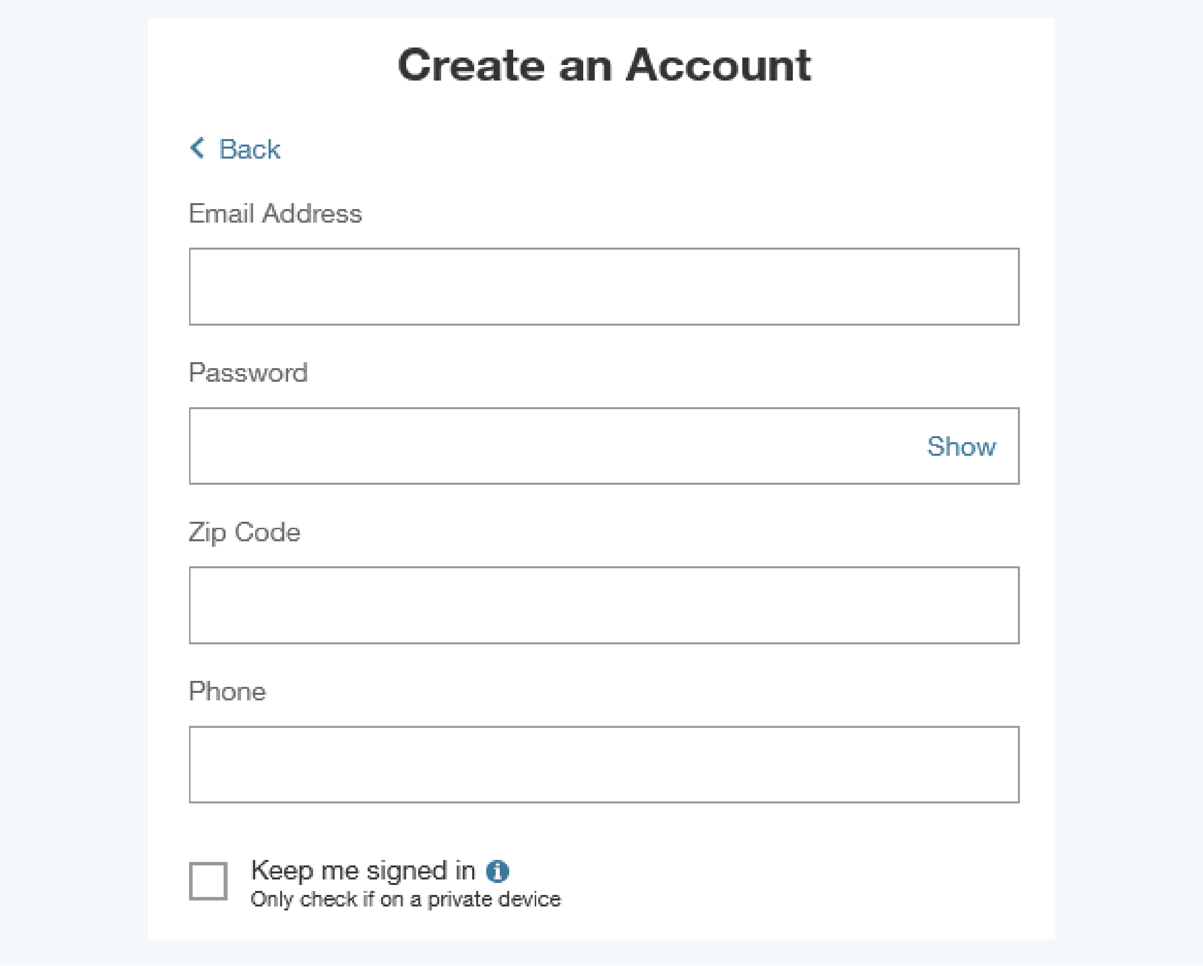
- Following the **principles** of the GDPR. These must also be followed by data processors, but most of the actual implementation of these principles is the responsibility of the data controller.
- Creating a **Privacy Policy** to be read by data subjects.
- Dealing with **data subject rights** requests directly with the data subject. The processor may be required to help access or modify data.
- **Choosing data processors** carefully and subject to due diligence.
- Carrying out a **Data Protection Impact Assessment** when required.
- Notifying the Data Protection Authority, and in some cases the data subjects, if a **data breach** has occurred.
- Paying a **fee** to a Data Protection Authority where applicable.

We'll be looking at many of these responsibilities in detail throughout this book.

Developer Case Study

Here's an example of how a **developer** might act as a **data controller**.

NewsBash has developed a news feed app, which asks users to **create an account**. The app asks for a first name, last name, and email address. If a **user** (data subject) creates an account, the app can remember the user's preferences, and the user can log in across multiple devices.



Create an Account

‹ Back

Email Address

Password

Show

Zip Code

Phone

□ Keep me signed in ⓘ
Only check if on a private device

Image: Create Account form example

As the developer, NewsBash is **controlling all the personal data** in this scenario. It has decided how and why the personal data is collected. It is a **data controller**.

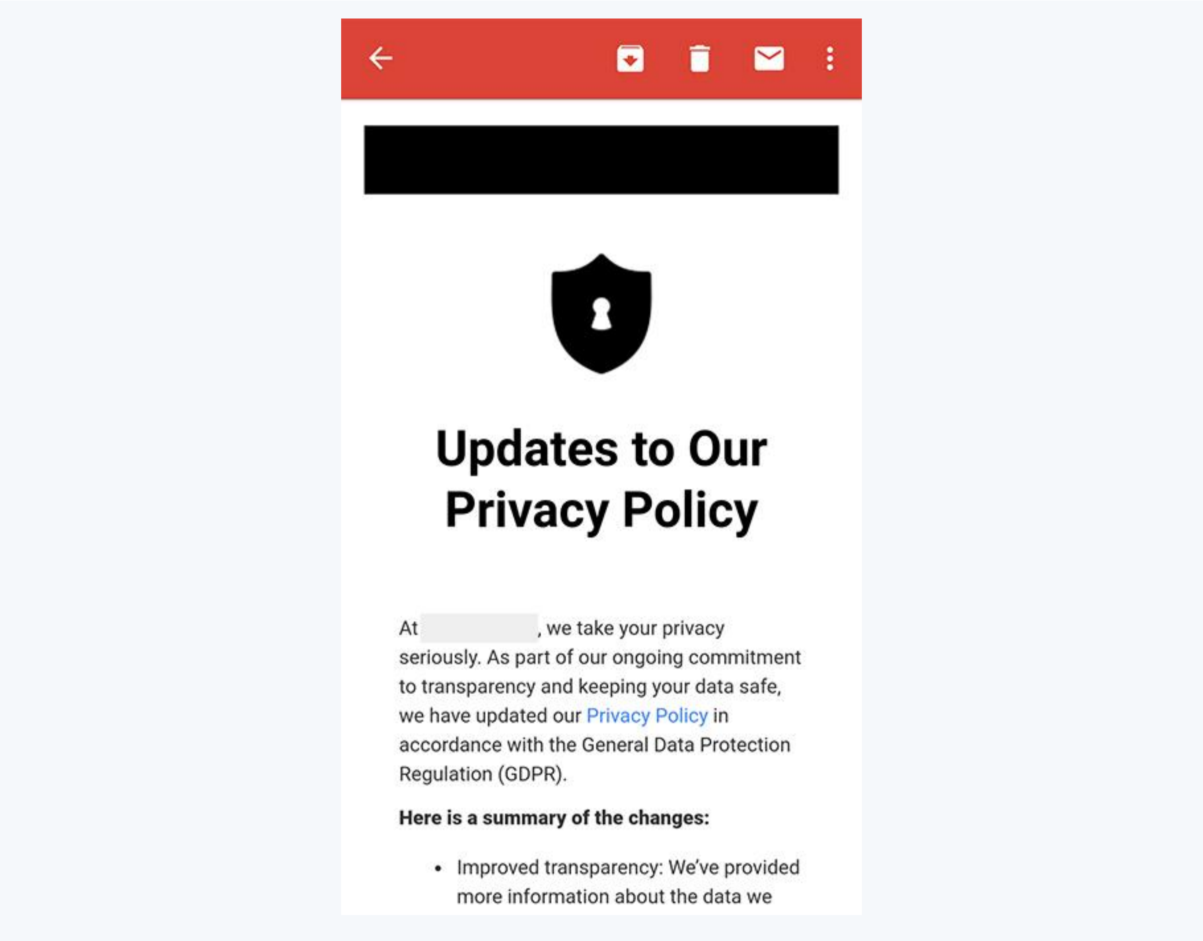
NewsBash must create a Privacy Policy, and it must facilitate data subject rights requests. It must also determine whether it has a **legal basis** for processing

NewsBash has been asking its users to consent to receive marketing communications, and has collected several thousand email addresses in a mailing list. NewsBash decides to outsource its marketing to an **email marketing company**.

Before sharing any personal data with this marketing company, NewsBash and the company must have a **Data Processing Agreement** in place.

NewsBash should consider whether the consent it has obtained from its users will allow it to share its personal data with this third party. If not, it may have to ask its users to consent to this **separately**.

In any case, NewsBash will need to **update its Privacy Policy** to reflect the new arrangement, and it must **make its users aware** that it has done this.



[redacted]

Updates to Our Privacy Policy

At , we take your privacy seriously. As part of our ongoing commitment to transparency and keeping your data safe, we have updated our Privacy Policy in accordance with the General Data Protection Regulation (GDPR).

Here is a summary of the changes:

- Improved transparency: We've provided more information about the data we

Image: Generic mobile email Updates to our Privacy Policy in accordance with GDPR

Responsibilities of GDPR Data Processors

Data processors do **not** generally have a **direct relationship** with data subjects, and they do not have a **direct interest** in the end result of the data processing.

A developer may **create an application or website** that collects personal data. They generally will be the data processor if this app or website is designed to be used by **other companies**, so long as these companies are deciding ***why*** personal data should be collected.

There are some responsibilities which are unique to a data processor:

- Processing personal data under the **strict instructions** of a data controller
- Appointing **sub processors** to do additional processing where required, but only with the **written agreement** of the data controller

- Helping the data controller with **data subject rights requests** if required
- **Assisting** the data controller with **Data Protection Impact Assessments** where required
- Notifying the **data controller** if a **data breach** has occurred

Developer Case Study

Here's an example of where a developer can act as a data processor.

VayCay is developing an app which allows employers to track their employees' vacation days. An employer can enter the names of their employees and make use of a calendar facility. The employer can allow employees to create their own accounts on VayCay's app, and book time off through a central system.

In this scenario, VayCay is a **data processor** and its users (the employers) are **data controllers**. The employer's employees are **data subjects**. VayCay and each of its users must have a **Data Processing Agreement** in place.

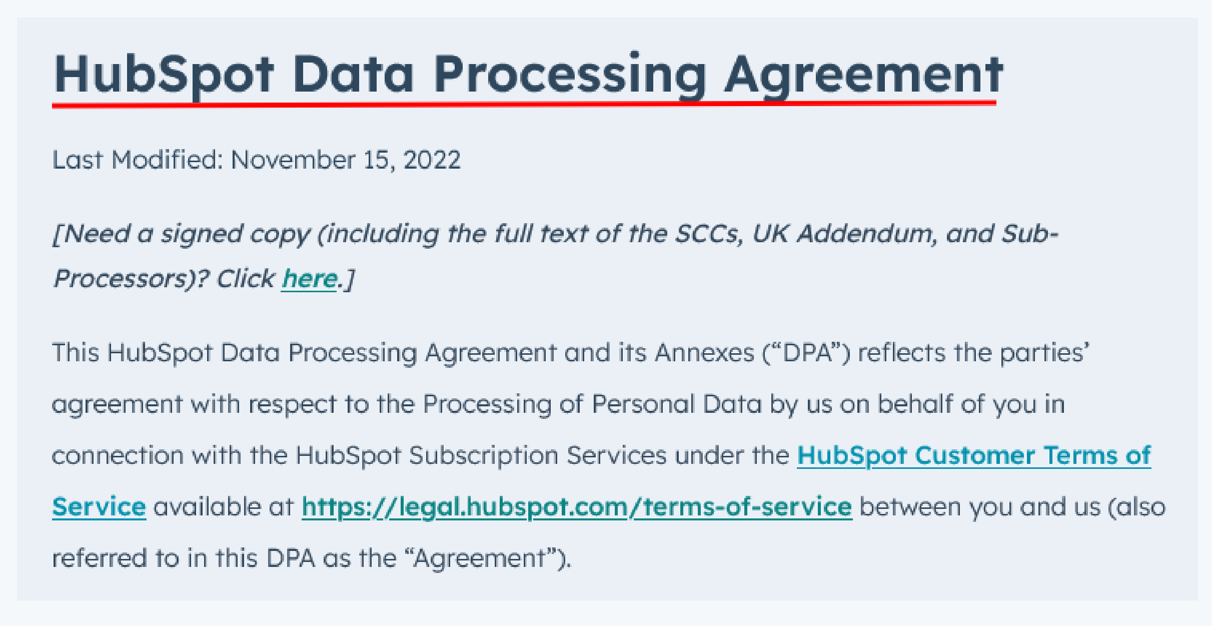
Even though VayCay's users are transferring personal data to it, *they* have **determined the purposes and means** of the processing. The users are responsible for creating a **Privacy Policy** for their employees (the data subjects).

The data controlled by VayCay's users is stored on VayCay's servers. Sometimes when an employee leaves a user's company, the employee submits a data subject rights request directly to VayCay, asking that their personal data is **erased**.

In this event, VayCay must **contact** the relevant user (employer) to let them know that there has been a request from a data subject. As the **data controller**, VayCay's users are responsible for deleting the data.

Because VayCay is receiving a large number of **requests** from data subjects, it decides to work with a **customer service company**. The company will receive requests from data subjects and communicate them to VayCay's users.

The customer service company is a **subprocessor**. Before VayCay shares any personal data with this subprocessor, it must obtain **written permission** from the relevant user (data controller). VayCay must have a written contract in place with its subprocessor, such as the one here from HubSpot:



HubSpot Data Processing Agreement

Last Modified: November 15, 2022

[Need a signed copy (including the full text of the SCCs, UK Addendum, and Sub-Processors)? Click here.]

This HubSpot Data Processing Agreement and its Annexes ("DPA") reflects the parties' agreement with respect to the Processing of Personal Data by us on behalf of you in connection with the HubSpot Subscription Services under the **HubSpot Customer Terms of Service** available at **https://legal.hubspot.com/terms-of-service** between you and us (also referred to in this DPA as the "Agreement").

Image: HubSpot Data Processing Agreement intro

Key Takeaways from This Chapter

The GDPR's model seems complicated at first, but in most situations, it should be obvious where you fit.

- Data controllers **decide why** and **how** personal data is processed
- Data processors process personal data **on behalf** of a data **controller**
- Data controllers have the most **direct responsibilities** over **data subjects**
- Data processors must help data controllers **meet these responsibilities**
- Data controllers and data processors must **only** work together under a **Data Processing Agreement**

Chapter 4:

GDPR Data Protection Officer and GDPR EU Representative

The GDPR is enforced at several different levels:

- At the top, we have the **Data Protection Authorities**, who enforce the law at the national level in each EU Member State.
- At the base level, individual **data subjects** can enforce protection of their own personal data, by exercising their data subject rights and bringing claims against data controllers and data processors.

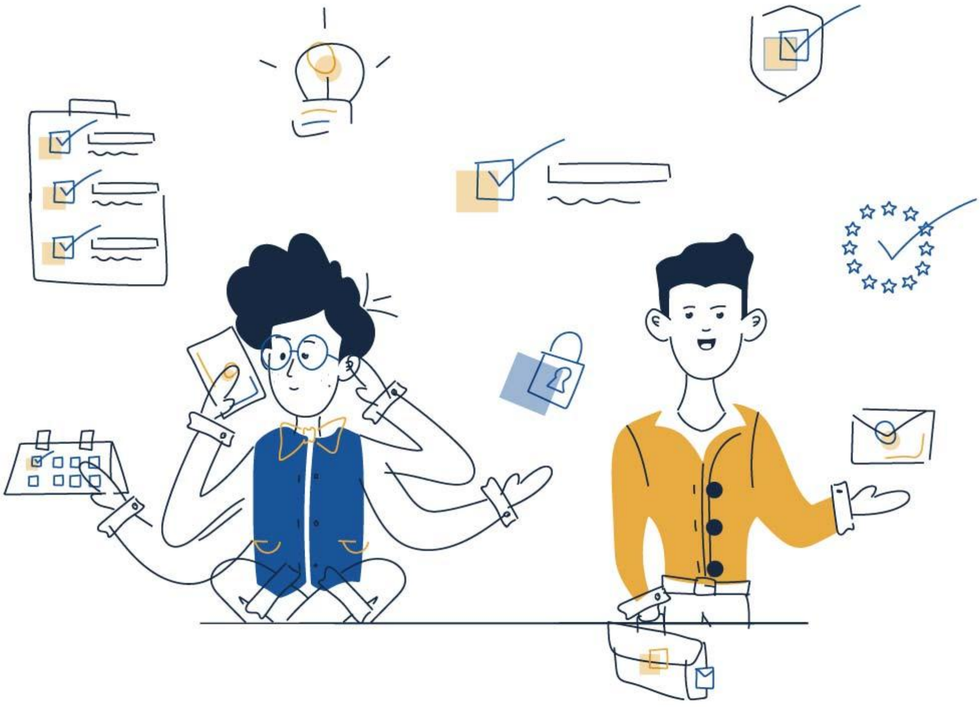


Illustration: GDPR Data Protection Officer and GDPR EU Representative

In this chapter, we'll be introducing two roles that are also important in the context of enforcing the GDPR.

- The **Data Protection Officer** (DPO) - DPOs are appointed by certain organizations to ensure compliance with the GDPR within the organization itself.
- The **EU Representative** - EU Representatives are appointed by organizations based outside of the EU. They can be held accountable by a Data Protection Authority if a non-EU organization fails to comply with the GDPR.

We're going to look at whether you need to appoint someone to either of these roles within your company; and, if so, how you can go about doing this.

GDPR Data Protection Officer

The GDPR sets out the **role** and **status** of the DPO at Articles 37-39, and provides some further information at Recital 97.

What Does a Data Protection Officer Do?

The DPO has certain **tasks** under the GDPR, including:

- **Advising staff** within an organization on matters of data protection, and how they can comply with the GDPR
- **Monitoring compliance** with the GDPR within the organization, and monitoring compliance with that organization's own data protection policies
- **Assigning responsibilities** for particular data processing activities to staff within the organization
- **Providing training** and raising awareness about how to comply with the GDPR
- Conducting or co-ordinating **data protection audits**
- Helping with and monitoring the carrying out of **Data Protection Impact Assessments**
- Cooperating and liaising with the **Data Protection Authority**

You can think of the DPO as the **go-to person** for data protection matters within an organization. If you have any questions about how to comply with the GDPR, or how to carry out a particular act of data processing, the DPO would be your first port of call.

Can Anyone Be a Data Protection Officer?

A DPO isn't required to have any specific qualification or level of experience in the field of data protection. However, the GDPR does have certain requirements regarding who can take up this role.

A DPO may work within your company (an existing employee can take up this role), or **they may be an external contractor**. They must:

- Be chosen on the basis of their "**professional qualities**"
- Have an "**expert knowledge**" of data protection law and practice
- Be **capable** of carrying out the tasks listed in the section above

Note that it may be possible to train someone within your company so that they meet these specifications.

What is the Status of a Data Protection Officer Within a Company?

Given the importance of the tasks that the DPO is required to carry out, they hold a particularly **important place** within a company.

Here's what the GDPR has to say about a DPO's status.

The DPO might be someone who already has a full-time job within your company. However, the GDPR states that a DPO must:

- **Be completely independent** when carrying out their tasks
- **Not be dismissed** or otherwise **disciplined** for an action taken in the course of their duties as DPO
- **Report to** the very **highest level of management** within the company
- **Not** be asked to carry out any other tasks within the company that might bring present them with a **conflict of interest** (e.g. the Head of Human Resources might not be an appropriate person to fulfill the role of DPO as their job requires a lot of data processing)
- Be **consulted** as soon as possible in all matters relating to data protection
- Be given sufficient **time** to carry out their duties effectively
- Receive a **budget** that is sufficient to allow them to carry out their tasks

Does Your Company Need to Appoint a Data Protection Officer?

Not all companies are required to appoint a DPO. Certain criteria are laid out in the GDPR.

Appointing a DPO is **mandatory** if your company:

1. Is a **public authority** or body. There is no guidance in the GDPR as to what constitutes a public authority or body. The Article 29 Working Party suggests that this might include utilities companies, transport services, and public broadcasters.
2. Processes special category data or criminal conviction data on a **large scale** as part of its **core activities**.
3. Engages in regular and **systematic monitoring** of individuals on a **large scale** as part of its **core activities**

This last point is likely to be the most relevant to developers or web and software development companies.

Let's break this specification down.

Monitoring

"**Monitoring**" is defined at Recital 24 of the GDPR. It can include where an individual is "***tracked on the internet***," and where any personal data collected via this tracking is used in order to make decisions about them or predict their **personal preferences**.

This includes **behavioral advertising**, such as personalized ads, retargeting and remarketing campaigns.

Regular and Systematic

According to the Article 29 Working Party, "**regular and systematic**" could mean:

- Ongoing at **regular intervals** over a fixed period
- Constant
- Organized and methodical
- Part of a general **plan** or **strategy** to collect personal data

Large Scale

To determine whether your monitoring is "**large scale**," consider:

- The number of individuals whose personal data is processed

- How much personal data you're processing
- How far-reaching the processing is

It is possible for a very small team of people to process a very large amount of personal data.

Core Activities

"**Core activities**" is not defined in the GDPR. But the Article 29 Working Party is on hand again to interpret this for us.

Here are some examples of activities that would probably ***not*** form part of your core activities:

- Paying your staff
- Monitoring staff sickness
- Keeping a newsletter mailing list

Although these tasks involve processing personal data, sometimes even sensitive data, they are **ancillary** activities that merely support your main business operations. Core activities are those that are **essential** for you to carry out in pursuit of your company's **main goals**. They are the important, **primary activities** of your company.

Examples

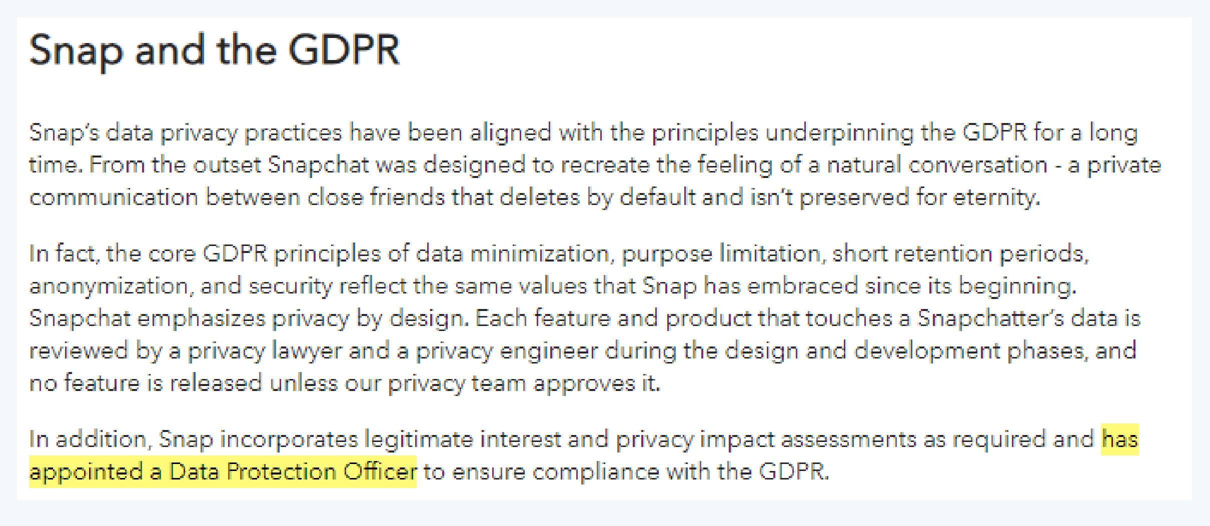
You will have to decide whether to appoint a DPO based on the unique circumstances of your company. But remember that it's better to **have** a DPO and **not need** one than to **need** a DPO and **not have** one. The latter case would be an infringement of the GDPR. Some companies do appoint a DPO voluntarily.

The GDPR is characteristically light on examples of when a DPO might be necessary. But based on the analysis above, let's consider some instances of the sorts of development projects for which it would be appropriate to nominate a DPO.

Your company may need to appoint a DPO if it's involved in developing an **instant messaging** or **social networking** app.

People might use an instant messaging or social networking app to transmit highly sensitive personal data of a **revealing**, **private** or **intimate** nature. People might send each other bank details, love letters, information about their health status - you really can't be too careful if you're controlling or developing this sort of app.

For example, Snap, owner of Snapchat, has a DPO:



Snap and the GDPR

Snap's data privacy practices have been aligned with the principles underpinning the GDPR for a long time. From the outset Snapchat was designed to recreate the feeling of a natural conversation - a private communication between close friends that deletes by default and isn't preserved for eternity.

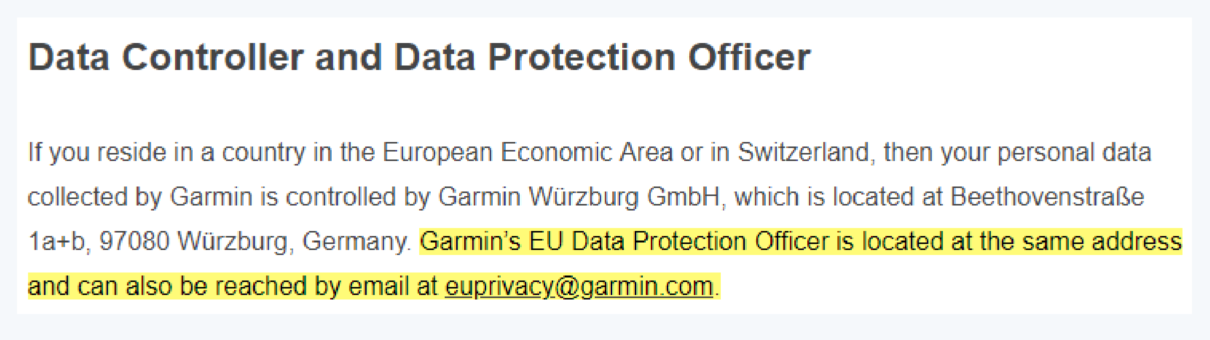
In fact, the core GDPR principles of data minimization, purpose limitation, short retention periods, anonymization, and security reflect the same values that Snap has embraced since its beginning. Snapchat emphasizes privacy by design. Each feature and product that touches a Snapchatter's data is reviewed by a privacy lawyer and a privacy engineer during the design and development phases, and no feature is released unless our privacy team approves it.

In addition, Snap incorporates legitimate interest and privacy impact assessments as required and has appointed a Data Protection Officer to ensure compliance with the GDPR.

Image: Snap and the GDPR: Intro section

You should also consider appointing a DPO if your company develops apps or devices that reveal **precise** (or "fine") **location data**. Processing "coarse" location data is less sensitive and would not in itself require the appointment of a DPO.

For example, Garmin, which makes **GPS receivers** and processes large amounts of location data, has a DPO:



Data Controller and Data Protection Officer

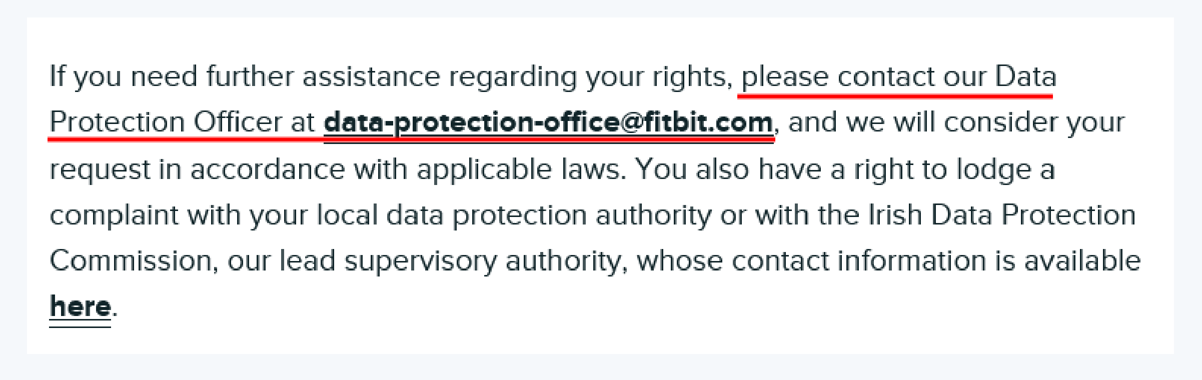
If you reside in a country in the European Economic Area or in Switzerland, then your personal data collected by Garmin is controlled by Garmin Würzburg GmbH, which is located at Beethovenstraße 1a+b, 97080 Würzburg, Germany. Garmin's EU Data Protection Officer is located at the same address and can also be reached by email at euprivacy@garmin.com.

Image: Garmin Connect Privacy Policy: Data Controller and Data Protection Officer clause excerpt

You may need to appoint a DPO if involved in the development of apps or hardware for **wearable devices** that process **health**, **fitness** or **wellbeing data**.

Whilst the law makes a distinction between "health data" (which is "special category" data) and "fitness data" (such as step counts, heart rate, workout information), you must treat both types of personal data carefully.

For example, Fitbit, which tracks health and activity-related data, has a DPO:

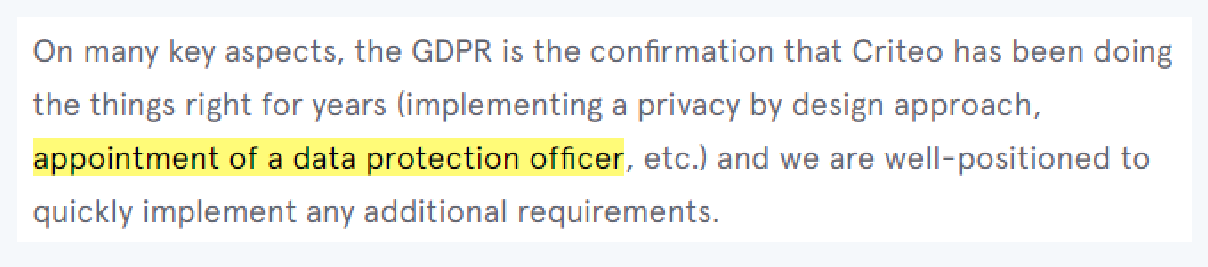


If you need further assistance regarding your rights, please contact our Data Protection Officer at **data-protection-office@fitbit.com**, and we will consider your request in accordance with applicable laws. You also have a right to lodge a complaint with your local data protection authority or with the Irish Data Protection Commission, our lead supervisory authority, whose contact information is available **here**.

Image: Fitbit Privacy Policy: Contact clause with DPO information highlighted

You might require a DPO if conducting large-scale **email remarketing** and other **behavioral advertising** campaigns.

For example, retargeting provider Criteo has a DPO:



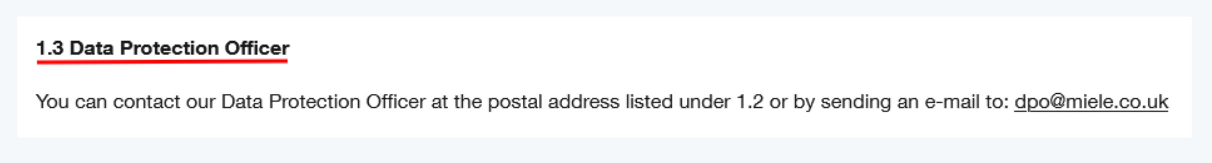
On many key aspects, the GDPR is the confirmation that Criteo has been doing the things right for years (implementing a privacy by design approach, appointment of a data protection officer, etc.) and we are well-positioned to quickly implement any additional requirements.

Image: Criteo: What You Need to Know About the GDPR - Data protection officer section highlighted

This is particularly important where there is some sensitivity to the type of product on offer (e.g. where it is related to health conditions, political views, sex life, etc.), and where these form part of a company's "core activities."

Companies involved in developing apps, software or hardware for **smart home devices** may need to consider appointing a DPO.

Miele manufactures domestic appliances, some of which are connected to the Internet of things. Miele has a DPO:



1.3 Data Protection Officer

You can contact our Data Protection Officer at the postal address listed under 1.2 or by sending an e-mail to: dpo@miele.co.uk

Image: Miele Privacy Notice: Data Protection Officer

National Law

It's important to note that some EU countries, for example, Germany, impose a stricter requirement for appointing a DPO than is contained in the GDPR. You must **check the local**

and national laws of the countries in which your company operates before making a decision about whether to appoint a DPO.

Appointment of a Data Protection Officer Letter

If your company needs to appoint a DPO, you should do so in writing. This requires an appointment letter.

Your appointment letter must include details of:

- The name of your company and your DPO
- The date and term of the appointment (if applicable)
- The DPO's tasks
- The DPO's status within your company

GDPR EU Representative

We've spoken a lot about how even **non-EU companies** are required to comply with the GDPR. This section will be important for you if your company is based **outside of the EU** and meets the criteria for GDPR compliance discussed in previous chapters.

The GDPR can be straightforwardly enforced on non-EU companies if the company has some offices or bases in the EU. For example, Google has an EU headquarters in Ireland.

But it's less straightforward to enforce the GDPR on companies who have **no presence** in the EU whatsoever.

This is where an **EU Representative** comes in.

What Does a GDPR EU Representative Do?

The appointment of an EU Representative is one of the ways that such companies can be held responsible for complying with the GDPR. An EU Representative is based in an **EU country** and can, therefore, be brought before an **EU court**.

An EU Representative has fewer active duties than a DPO. They are responsible for:

- Acting as the **main point of contact** for individuals and Data Protection Authorities in the EU

- **Keeping records** of certain data processing activities in the EU, if the company is required to do so under Article 30 (we looked at this obligation in the previous chapter)
- **Cooperating** with Data Protection Authorities in the event of a **data breach** or an allegation of **infringement** of the GDPR

Can Anyone Be an EU Representative?

An EU Representative must have have the following attributes:

- They must be **established** with some **legal presence** in one of the EU countries
- They must be able to **speak the language** of the country in which they are established, or at least speak one of the official EU languages
- They cannot act as **DPO** and **EU Representative** for the same company

Other than this, you're basically free to choose whoever you wish to represent you in the EU. It might be an individual or a corporation.

What is the Status of an EU Representative Within a Company?

Like a DPO, an EU Representative can either work **directly** for your company, or they can be an **external contractor**.

An EU Representative can represent **multiple companies** at once. There are some agencies which provide EU Representatives.

The EU Representative isn't afforded the same **independence** and **authority** as a DPO. They must, however, be granted **sufficient resources** and have **sufficient availability** to carry out their duties.

Does Your Company Need to Appoint an EU Representative?

If your company is not established in the EU, the threshold for appointing an EU Representative is **much lower** than the threshold for appointing a DPO.

It is mandatory to appoint an EU Representative ***unless*****:**

1. Your company is a **public body**

2. Your company only processes personal data in a way that is **occasional**, is **unlikely** to result in a “**risk to rights and freedoms**,” and
3. Does not involve a large amount of **special category** or **criminal conviction** data

“Non-occasional” processing is a much lower threshold than the “regular and systematic” monitoring on a “large scale” that is a prerequisite of appointing a DPO.

It’s also worth noting that any company carrying out processing which is **high-risk** or involves **special category data** or **criminal conviction** data would **still** need to appoint an EU Representative, even if processing *is* “occasional.”

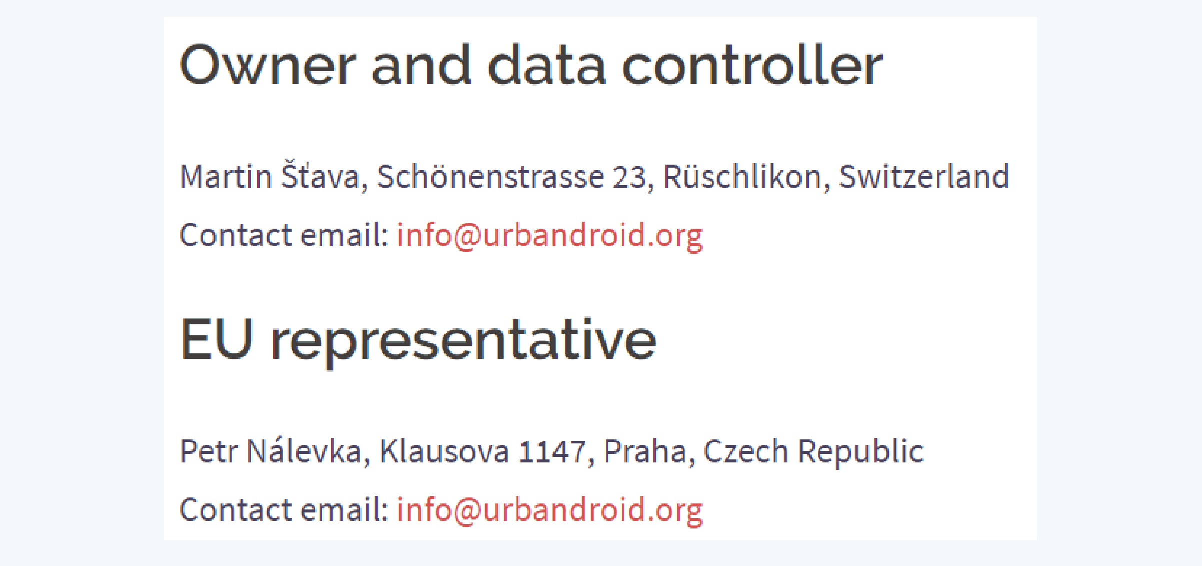
This will cover a lot of companies. The reality is that if you’re likely to receive inquiries from your EU-based data subjects, it’s appropriate to field these inquiries through an EU Representative.

Examples

No examples of the sorts of companies that might need to appoint an EU Representative are provided by the GDPR.

The requirement is so broad that it’s not really to consider what ***types*** of companies would need to appoint an EU Representative. Instead, let’s take a look at some examples of real companies who have made this appointment. All of these examples are of companies whose main product or service involves some web or software **development**.

Urbandroid is an **app developer** based in Switzerland (a non-EU country). Urbandroid’s portfolio of apps includes sleep tracking, translation and alarm apps. Urbandroid has appointed an EU Representative:



Owner and data controller

Martin Šťava, Schönenstrasse 23, Rüschlikon, Switzerland

Contact email: info@urbandroid.org

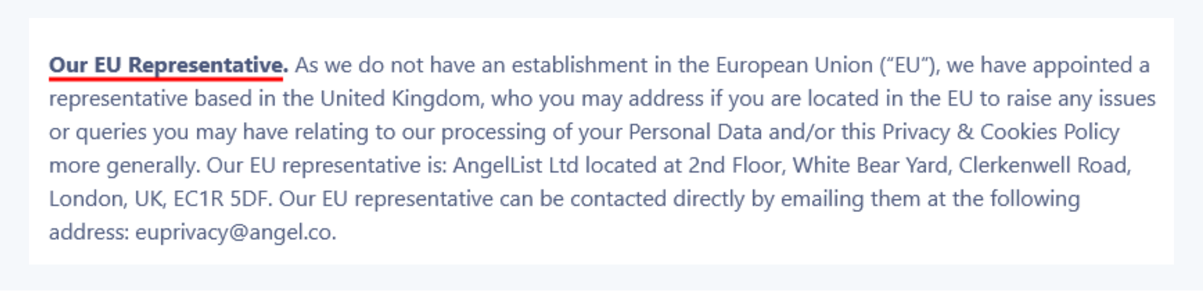
EU representative

Petr Nálevka, Klausova 1147, Praha, Czech Republic

Contact email: info@urbandroid.org

Image: Urbandroid Privacy Policy: Owner and data controller and EU representative clauses

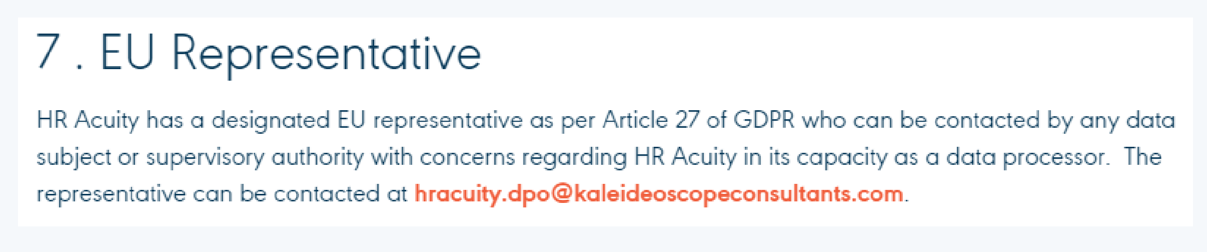
Product Hunt is a **website** for tech enthusiasts to share information about new product releases. Product Hunt has appointed an EU Representative:



Our EU Representative. As we do not have an establishment in the European Union ("EU"), we have appointed a representative based in the United Kingdom, who you may address if you are located in the EU to raise any issues or queries you may have relating to our processing of your Personal Data and/or this Privacy & Cookies Policy more generally. Our EU representative is: AngelList Ltd located at 2nd Floor, White Bear Yard, Clerkenwell Road, London, UK, EC1R 5DF. Our EU representative can be contacted directly by emailing them at the following address: euprivacy@angel.co.

Image: Product Hunt Privacy Policy: EU Representative clause

HR Acuity provides a web-based **SaaS** Human Resources product. HR Acuity has appointed an EU Representative:

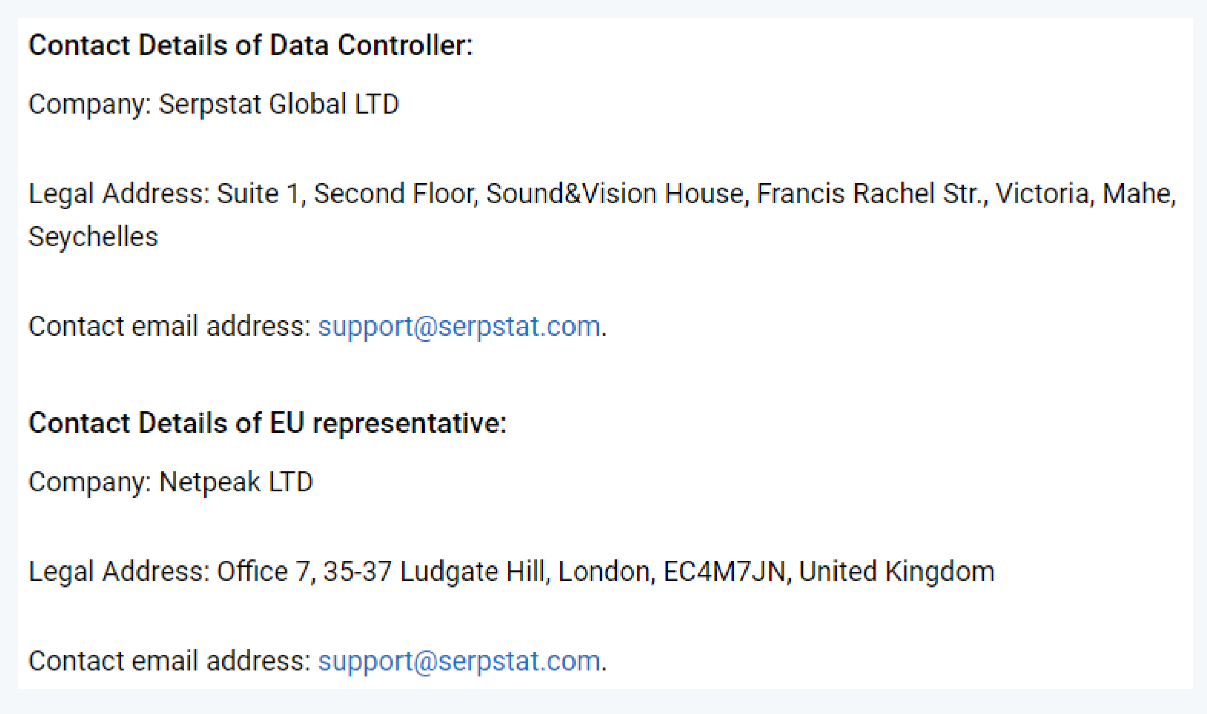


7 . EU Representative

HR Acuity has a designated EU representative as per Article 27 of GDPR who can be contacted by any data subject or supervisory authority with concerns regarding HR Acuity in its capacity as a data processor. The representative can be contacted at **hracuity.dpo@kaleideoscopeconsultants.com**.

Image: HR Acuity Privacy Policy: EU Representative clause

Serpstat is an **SEO platform** established in Seychelles. Serpstat has appointed an EU Representative:



Contact Details of Data Controller:

Company: Serpstat Global LTD

Legal Address: Suite 1, Second Floor, Sound&Vision House, Francis Rachel Str., Victoria, Mahe, Seychelles

Contact email address: support@serpstat.com.

Contact Details of EU representative:

Company: Netpeak LTD

Legal Address: Office 7, 35-37 Ludgate Hill, London, EC4M7JN, United Kingdom

Contact email address: support@serpstat.com.

Image: Serpstat Privacy Policy: COntact Details of Data Controller and EU Representative clause

Appointment of an EU Representative Letter

The GDPR requires that you appoint your EU Representative via a "**written mandate**." This can be a letter which sets out the **terms of the appointment** and makes everything official.

Your appointment letter should include:

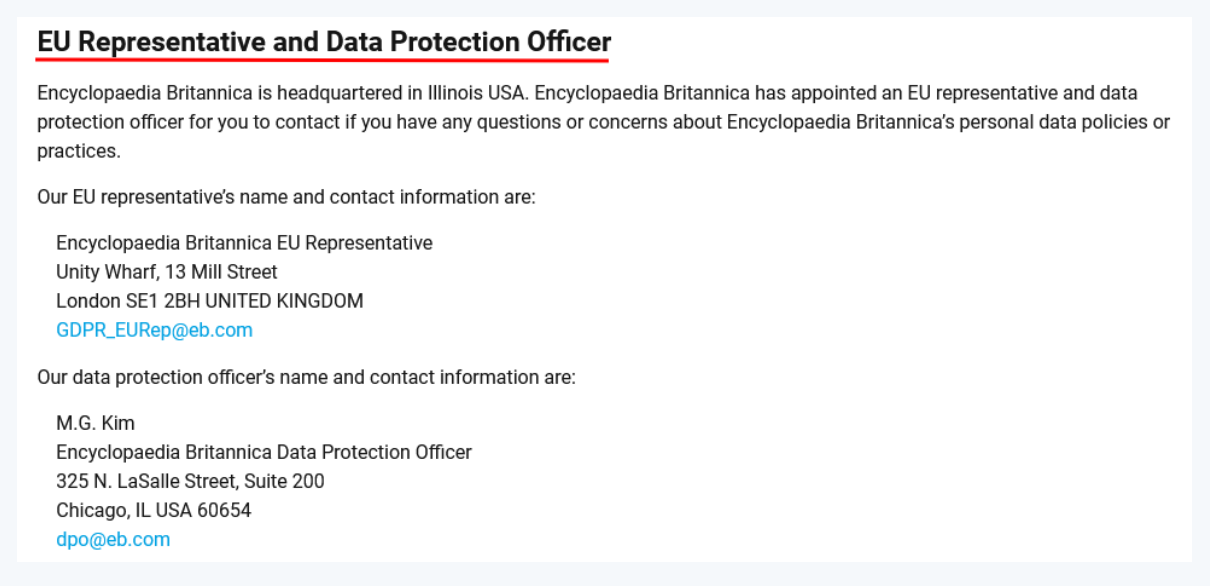
- The **effective date** of the appointment
- The **name and contact details** of your company and your EU Representative
- The **tasks** of the EU Representative as listed above

When considering the country in which your EU Representative should be based, try to choose the country where the **majority of your EU users** reside. If your website is written in English, this is likely to be the UK or Ireland. If you only export to Germany, then your EU Representative should be established there.

Updating Your Privacy Policy

If you're required to appoint either a DPO or an EU Representative, you must make sure people know how to contact them. This includes updating your company's Privacy Policy to include their name and contact details.

Here's how Encyclopaedia Britannica has listed both its DPO and the EU Representative in its Privacy Policy:



EU Representative and Data Protection Officer

Encyclopaedia Britannica is headquartered in Illinois USA. Encyclopaedia Britannica has appointed an EU representative and data protection officer for you to contact if you have any questions or concerns about Encyclopaedia Britannica's personal data policies or practices.

Our EU representative's name and contact information are:

Encyclopaedia Britannica EU Representative
Unity Wharf, 13 Mill Street
London SE1 2BH UNITED KINGDOM
GDPR_EURep@eb.com

Our data protection officer's name and contact information are:

M.G. Kim
Encyclopaedia Britannica Data Protection Officer
325 N. LaSalle Street, Suite 200
Chicago, IL USA 60654
dpo@eb.com

Image: Encyclopaedia Britannica Privacy Policy: EU Representative and Data Protection Officer clause

Key Takeaways from This Chapter

In this chapter we've looked at another two important characters in the GDPR: the **Data Protection Officer** (DPO) and the **EU Representative**.

You should appoint a **DPO** if your company:

- Is a public body
- Processes large amounts of sensitive personal data as part of its core activities
- Regularly and systematically monitors people's behavior on a large scale as part of its core activities

You should appoint an **EU Representative** if your company:

- Is not established in the EU
- Is not a public body
- Processes personal data on a non-occasional basis
- Processes personal data even on an occasional basis, if that processing involves sensitive personal data and could present a risk to individuals

Chapter 5:

Legal Basis: Legitimate Interests vs Consent

In an earlier section of the book, we discussed how important it is for processing of personal data to take place on an appropriate legal basis. We looked briefly at the legal bases provided by the GDPR.

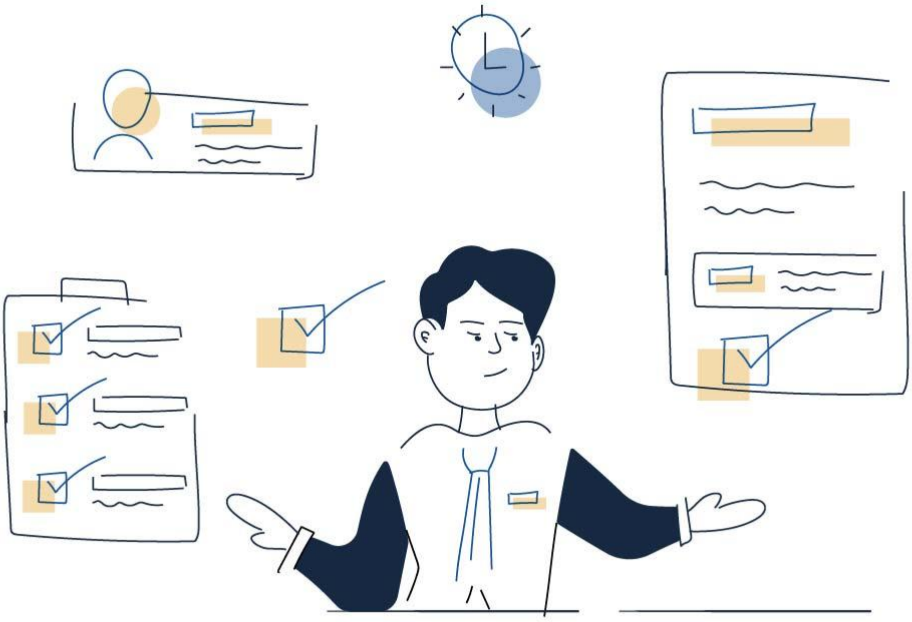


Illustration: Legal Basis - Legitimate Interests vs Consent

In this section, we'll be looking in detail at two legal bases that you need to know about as a developer: **consent** and **legitimate interests**.

Legal Bases

Personal data is sacred under the GDPR. A person's personal data can, to some extent, be thought of as their property. They should be able to maintain a large amount of control over what happens to it.

But whilst personal data is an important resource, it isn't like physical property. Society is arranged in such a way that much of a person's identity and information are out in the open. Sometimes personal data needs to be shared or stored, and it isn't always appropriate or possible for a person to be **asked permission** for this.

For example:

- In any democratic society with an open justice system, people's names and private information will appear in **court records**.
- The press has a right to report people's private affairs when it's in the **public interest** for them to do so.
- Banks and credit institutions need to maintain records of people's **finances**.

The organizations listed above **don't require consent** in these contexts, even though they are processing highly sensitive personal data in sometimes very intrusive ways. These activities would take place under other legal bases, such as legal obligation or public task, or under an exemption.

It's important to understand that the **GDPR does not impose consent as a precondition for all processing of personal data.** But generally speaking, processing of personal data must take place under one of the six legal bases.

Legitimate Interests

The legal basis of legitimate interests is described by the ICO as "*the most flexible of the six legal bases*." This means that it is applicable in the broadest range of situations.

If you're finding that you can't really run your business, or provide your services without processing personal data in a particular way, **legitimate interests may be the answer**.

You often can't ask consent from your data subjects for these sorts of activities, because it might be a fundamental problem for you if they say "no."

Legitimate interests can be particularly relevant when you are **not** processing personal data under a **contract**.

However, you shouldn't think of legitimate interests as the "easy option." There's still some work to be done in determining that relying on legitimate interests is appropriate.

Legitimate Interests Assessment

When considering whether you have a legitimate interest in processing personal data in a particular way, you must conduct a Legitimate Interests Assessment.

If the data processing you want to carry out passes this assessment, you won't need to (and you most likely *shouldn't*) ask for your users' consent.

The ICO suggests a format for your Legitimate Interests Assessment, known as the "three-part test." You can use this test to establish whether you have a legitimate interest. This test is derived from the definition of "legitimate interests" given at Article 6 of the GDPR:

> "*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.*"

The three corresponding parts of your Legitimate Interests Assessment should therefore consider:

1. The **Purpose** you're pursuing
2. The **Necessity** of pursuing that purpose in this particular way
3. The **Balance** of your interests against the privacy of your data subjects

The Purpose Test

If you think you might be able to rely on legitimate interests, here are some questions you should ask yourself about the **purpose** of the processing you want to carry out:

- How does the processing **benefit** your company or a third party?
- Do you have a clear, beneficial **outcome** in mind?
- Is the processing **ethical** and **lawful**?
- What would happen if you were **unable** to process personal data in this way?
- Are you considering any **codes of conduct** in your industry?

For example, under certain circumstances, engaging in direct **marketing** can satisfy this test. But not, for example, if you're flooding people's inboxes with spam. This would probably not be **lawful**, and would certainly not be **ethical**.

The Necessity Test

If your data processing project passes the purpose test, consider these questions about whether your processing is **necessary**:

- Is this processing the **only viable way** to achieve your purpose?
- Do you have to **process personal data** at all?
- Are there other ways to achieve your purposes with a much **smaller** data set, or a **less sensitive** set of personal data?

For example, let's say you want to ensure that your social networking app is not subject to abuse. This is a legitimate purpose. But asking your users to upload a scan of their passport is probably not a **necessary** means by which to achieve that purpose. You might not actually need to process personal data at all in order to achieve this purpose.

The Balance Test

If you believe that your data processing project passes the purpose and necessity test, you must now consider whether it strikes the right **balance** between your interests and those of the people whose data you're processing.

Consider the following questions:

- What is the **nature** of your personal data?
  - Is it "special category" data?
  - Would people consider the personal data private?
  - Are your data subjects children?
- Would the processing be within your data subjects' **reasonable expectations**?
  - Do you have an existing business relationship?
  - How familiar are the data subjects with your company?
  - Are you processing personal data in a risky or new way?
- What might the **impact** of this processing be?
  - Will your data subjects still be able to exercise their rights over their data?
  - Do you think people would be likely to object to the process if allowed?
  - What safeguards have you taken to mitigate the risks or impact?

The balancing test is all about **context**. While you might be able to rely on legitimate interests for processing IP addresses, the same act of processing might fail if it involved payment card data.

Examples

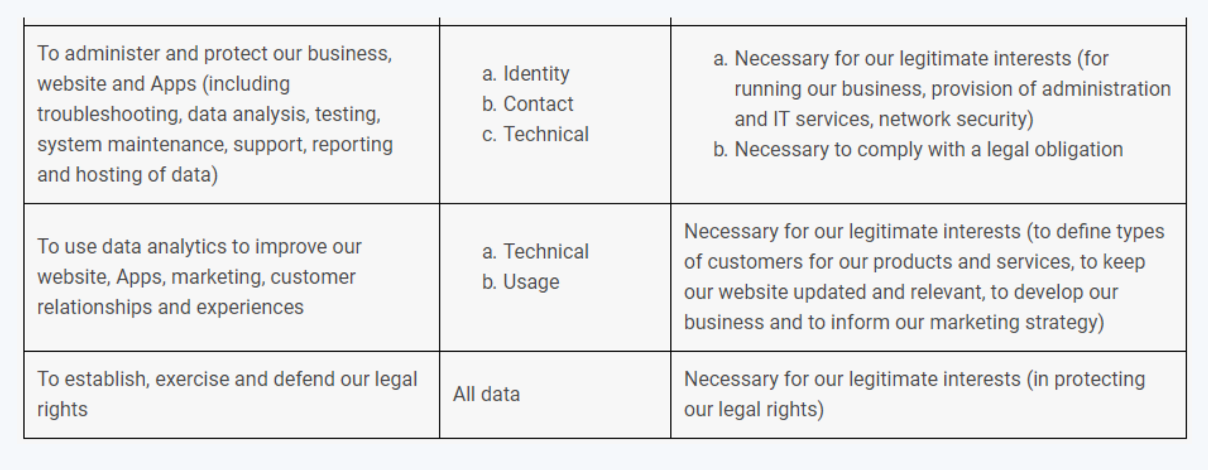
Although the Legitimate Interests Assessment seems arduous, it is an **essential part** of making sure you're processing personal data in a lawful way. The chances are that you'll need to rely on legitimate interests for some element of your data processing, and you should be prepared to demonstrate that you've carried out the assessment.

We're now going to look at some examples of where web or software **development** companies have used legitimate interests for processing personal data.

This is a complicated area. Don't assume that these examples of legitimate interests are necessarily perfect. But none of them represent an egregious violation of the rules on legitimate interests - although it's easy to find many such examples.

We'll be considering whether legitimate interests are appropriate for these sorts of activities in the table at the end of this section.

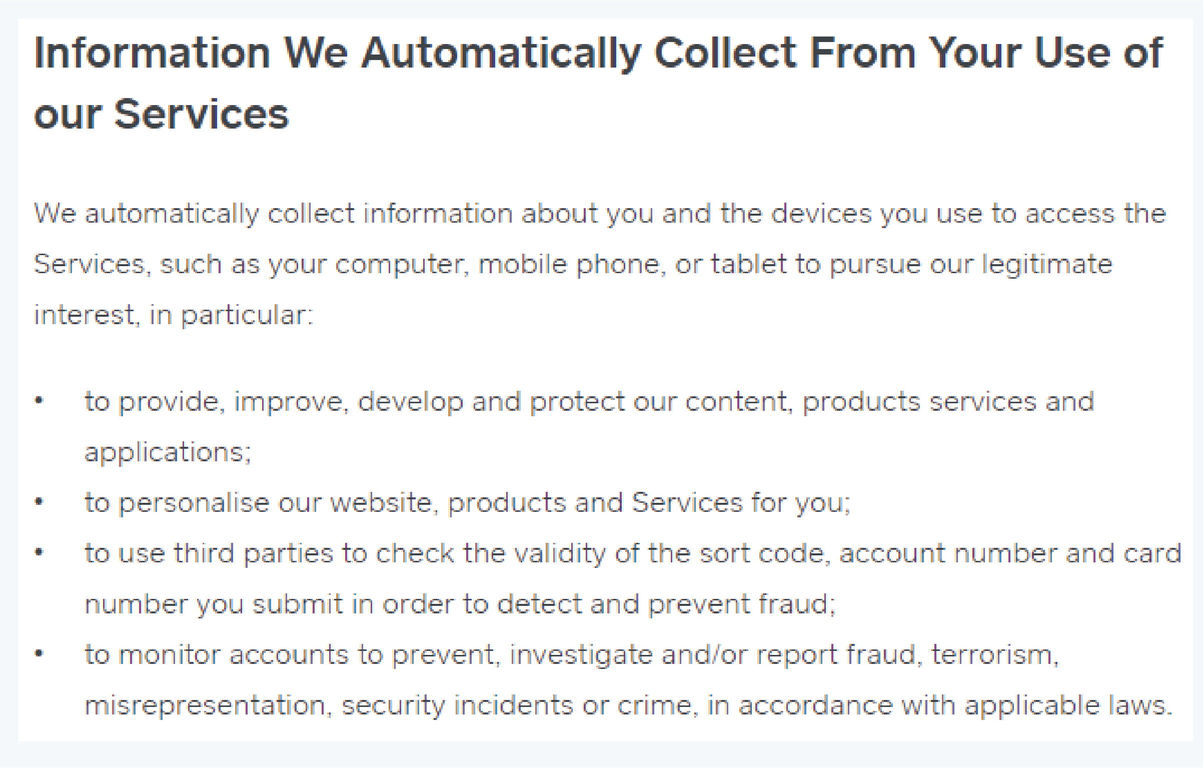
First up, here's an excerpt of a Privacy Policy that addresses the reasons why data is collected and why it's for a legitimate interest:



To administer and protect our business, website and Apps (including troubleshooting, data analysis, testing, system maintenance, support, reporting and hosting of data)	a. Identity b. Contact c. Technical	a. Necessary for our legitimate interests (for running our business, provision of administration and IT services, network security) b. Necessary to comply with a legal obligation
To use data analytics to improve our website, Apps, marketing, customer relationships and experiences	a. Technical b. Usage	Necessary for our legitimate interests (to define types of customers for our products and services, to keep our website updated and relevant, to develop our business and to inform our marketing strategy)
To establish, exercise and defend our legal rights	All data	Necessary for our legitimate interests (in protecting our legal rights)

Image: Generic Privacy Policy: Legitimate interests clause

A financial SaaS company provides two Privacy Policies. One is specifically for data subjects who do not have an account. This policy lists the following activities among those for which the company relies on legitimate interests:



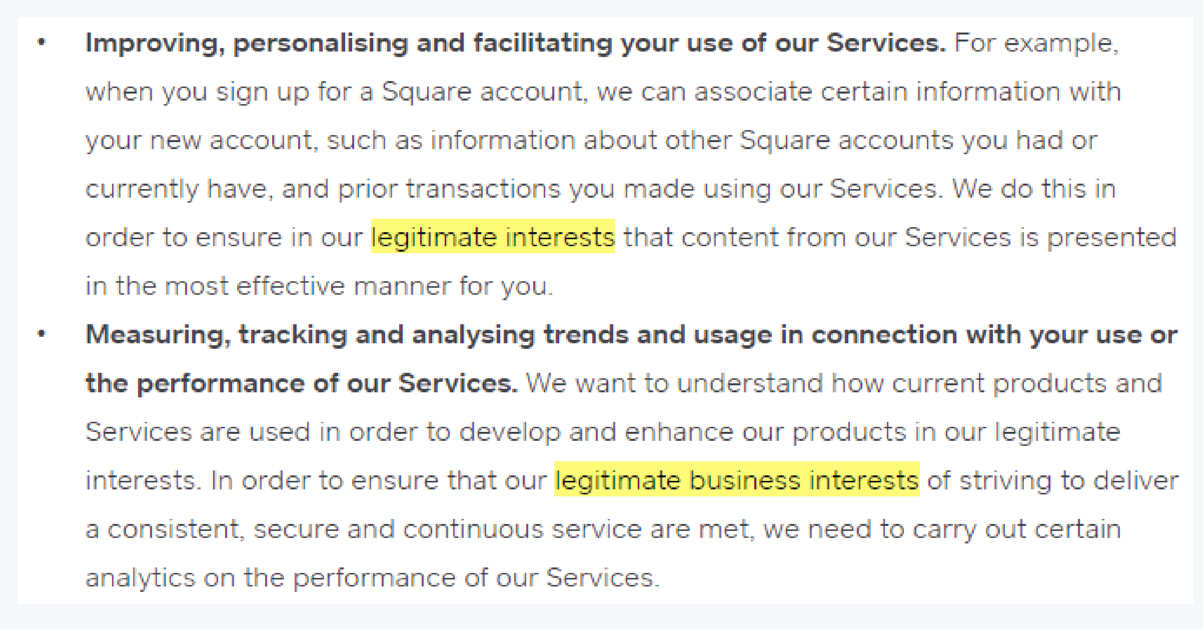
Information We Automatically Collect From Your Use of our Services

We automatically collect information about you and the devices you use to access the Services, such as your computer, mobile phone, or tablet to pursue our legitimate interest, in particular:

- to provide, improve, develop and protect our content, products services and applications;
- to personalise our website, products and Services for you;
- to use third parties to check the validity of the sort code, account number and card number you submit in order to detect and prevent fraud;
- to monitor accounts to prevent, investigate and/or report fraud, terrorism, misrepresentation, security incidents or crime, in accordance with applicable laws.

Image: Generic Privacy Policy: Information We Automatically Collect From Your Use of our Services clause

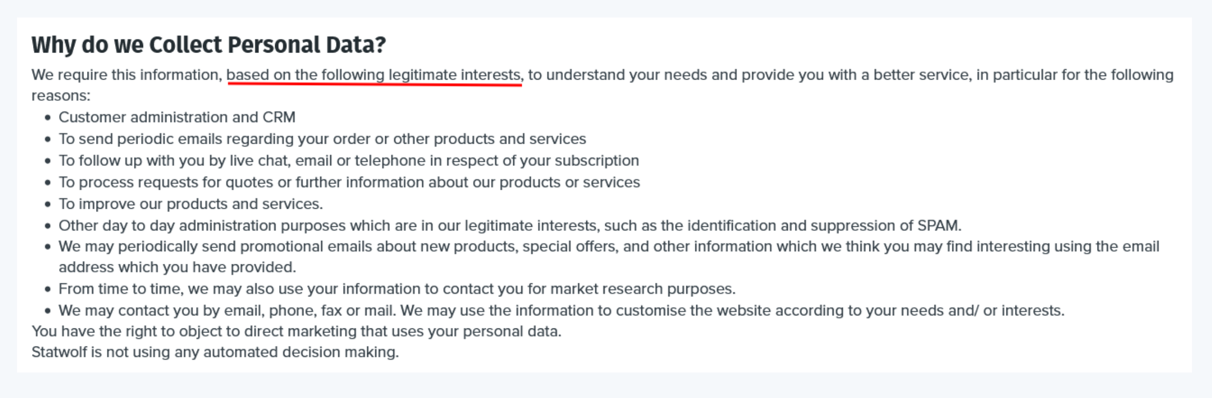
In its Privacy Policy for users who *have* an account, the company relies on legitimate interests for the following activities (amongst others):



- **Improving, personalising and facilitating your use of our Services.** For example, when you sign up for a Square account, we can associate certain information with your new account, such as information about other Square accounts you had or currently have, and prior transactions you made using our Services. We do this in order to ensure in our legitimate interests that content from our Services is presented in the most effective manner for you.
- **Measuring, tracking and analysing trends and usage in connection with your use or the performance of our Services.** We want to understand how current products and Services are used in order to develop and enhance our products in our legitimate interests. In order to ensure that our legitimate business interests of striving to deliver a consistent, secure and continuous service are met, we need to carry out certain analytics on the performance of our Services.

Image: Generic Privacy Policy: Information We Automatically Collect From Your Use of our Services clause

Machine learning software company Statwolf claims a legitimate interest in the following activities:



Why do we Collect Personal Data?

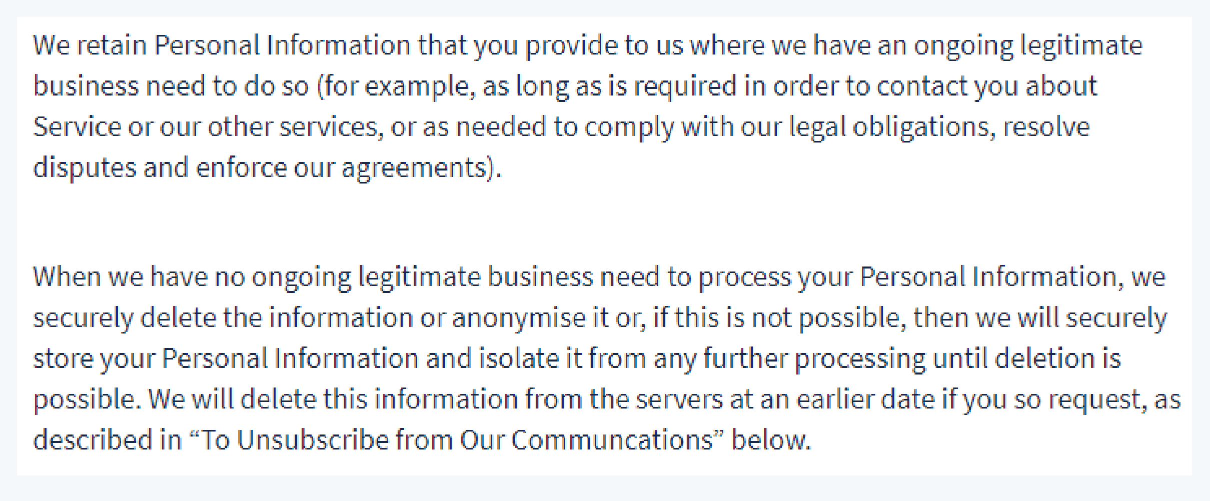
We require this information, based on the following legitimate interests, to understand your needs and provide you with a better service, in particular for the following reasons:

- Customer administration and CRM
- To send periodic emails regarding your order or other products and services
- To follow up with you by live chat, email or telephone in respect of your subscription
- To process requests for quotes or further information about our products or services
- To improve our products and services.
- Other day to day administration purposes which are in our legitimate interests, such as the identification and suppression of SPAM.
- We may periodically send promotional emails about new products, special offers, and other information which we think you may find interesting using the email address which you have provided.
- From time to time, we may also use your information to contact you for market research purposes.
- We may contact you by email, phone, fax or mail. We may use the information to customise the website according to your needs and/ or interests.

You have the right to object to direct marketing that uses your personal data.
Statwolf is not using any automated decision making.

Image: Statwolf Privacy Policy: Why do we Collect Personal Data clause

Here's an example of an additional clause that discloses how a business relies on legitimate interests in respect of the following activities:



We retain Personal Information that you provide to us where we have an ongoing legitimate business need to do so (for example, as long as is required in order to contact you about Service or our other services, or as needed to comply with our legal obligations, resolve disputes and enforce our agreements).

When we have no ongoing legitimate business need to process your Personal Information, we securely delete the information or anonymise it or, if this is not possible, then we will securely store your Personal Information and isolate it from any further processing until deletion is possible. We will delete this information from the servers at an earlier date if you so request, as described in "To Unsubscribe from Our Communcations" below.

Image: Generic Privacy Policy: Retain personal information for a legitimate interest clause

Consent

Consent is an **extremely important** concept in the GDPR. It will probably be the legal basis of choice for a lot of your data processing activity. However, many companies struggle (or neglect) to get consent in a **legally valid way**.

Personal data is sacred under the GDPR. As such, if you're going to request someone's permission to process their personal data, this request has to be valid and **meaningful**. The person must be able to say "no."

Accordingly, there's no point asking for someone's permission if they can't **meaningfully refuse** your request. If you have a legitimate interest in processing someone's personal data in a non-risky or intrusive way, you don't need to ask for their consent.

Equally, for processing that *isn't* necessary, and where you *can* give someone a genuine choice over how you use their personal data, you ***should*** **ask for consent**. But you must do so in a GDPR-compliant way.

The GDPR's high threshold of consent means that many companies fall foul of its requirements. This was evident in January 2019, when Google was fined €50 million by the French Data Protection Authority, CNIL, for violating the GDPR's conditions around consent.

We're going to look at this case, and some others, in detail in a later chapter, to help you understand how you can avoid making these mistakes with your consent request mechanisms.

For now, we won't focus on ***how*** to get consent, but ***when*** to get it. Let's consider some of the situations in which asking for consent might be necessary or appropriate.

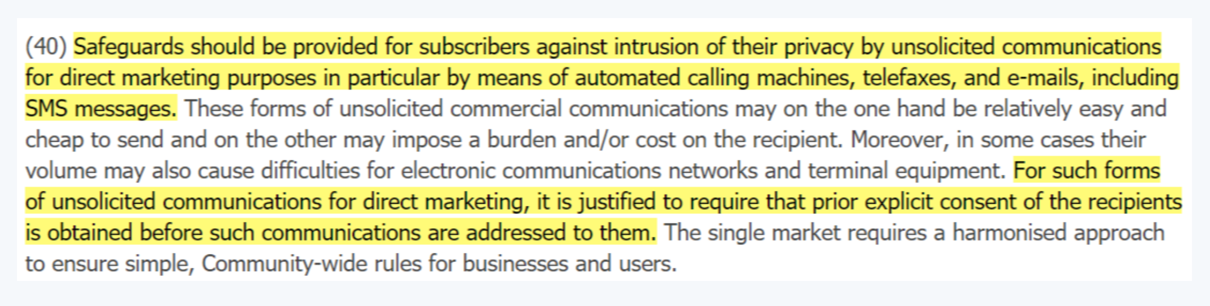
When to Seek Consent

It's important to note that the GDPR isn't the only EU law that requires consent for processing personal data under certain circumstances. Another EU law known as the ePrivacy Directive (sometimes also known as the "Cookies Directive") is very important in this context.

A helpful way to think about the interaction between these two laws is:

- The ePrivacy Directive tells you *what* you need to get consent for
- The GDPR tells you *how* to get consent

Here's an excerpt from the ePrivacy Directive:



(40) Safeguards should be provided for subscribers against intrusion of their privacy by unsolicited communications for direct marketing purposes in particular by means of automated calling machines, telefaxes, and e-mails, including SMS messages. These forms of unsolicited commercial communications may on the one hand be relatively easy and cheap to send and on the other may impose a burden and/or cost on the recipient. Moreover, in some cases their volume may also cause difficulties for electronic communications networks and terminal equipment. For such forms of unsolicited communications for direct marketing, it is justified to require that prior explicit consent of the recipients is obtained before such communications are addressed to them. The single market requires a harmonised approach to ensure simple, Community-wide rules for businesses and users.

Image: ePrivacy Directive Section 40: Safeguards for subscribers against intrusion of privacy by unsolicited communications

This means that you must request consent for sending **unsolicited** marketing communication via email, SMS, automated phone calls, and fax.

The ePrivacy Directive requires that you request consent for using certain **cookies**.

Let’s consider these two requirements in detail.

Consent for Direct Marketing

Your default way of thinking about direct marketing (i.e. marketing to a specific person, rather than the general public) should be that **it requires consent**.

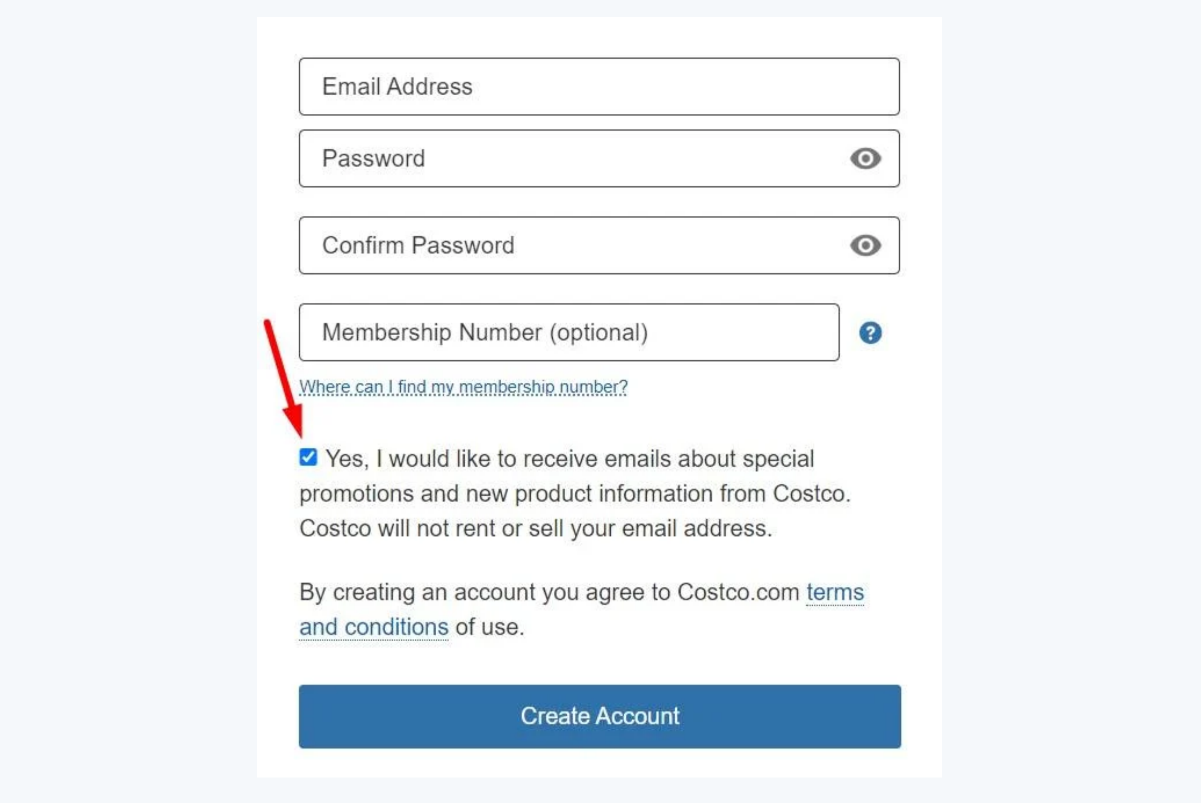
There are certain situations where you *might* be able to rely on legitimate interests, even for electronic marketing, if you have a pre-existing business relationship with a customer. The ICO suggests that this might apply if:

- They have **recently bought something** from you,
- They **provided their contact details**, and
- They didn’t **opt out** despite being given the opportunity

This is sometimes known as the “soft opt-in.”

However, remember that people are quick to complain about what they perceive as **spam**. You must be able to **justify** sending every piece of direct marketing you send. The easiest way you can do this is if you have a record of the recipient having given **GDPR-compliant consent**.

Here’s an example from Costco:



Email Address
Password
Confirm Password
Membership Number (optional)
Where can I find my membership number?

☑ Yes, I would like to receive emails about special promotions and new product information from Costco. Costco will not rent or sell your email address.

By creating an account you agree to Costco.com terms and conditions of use.

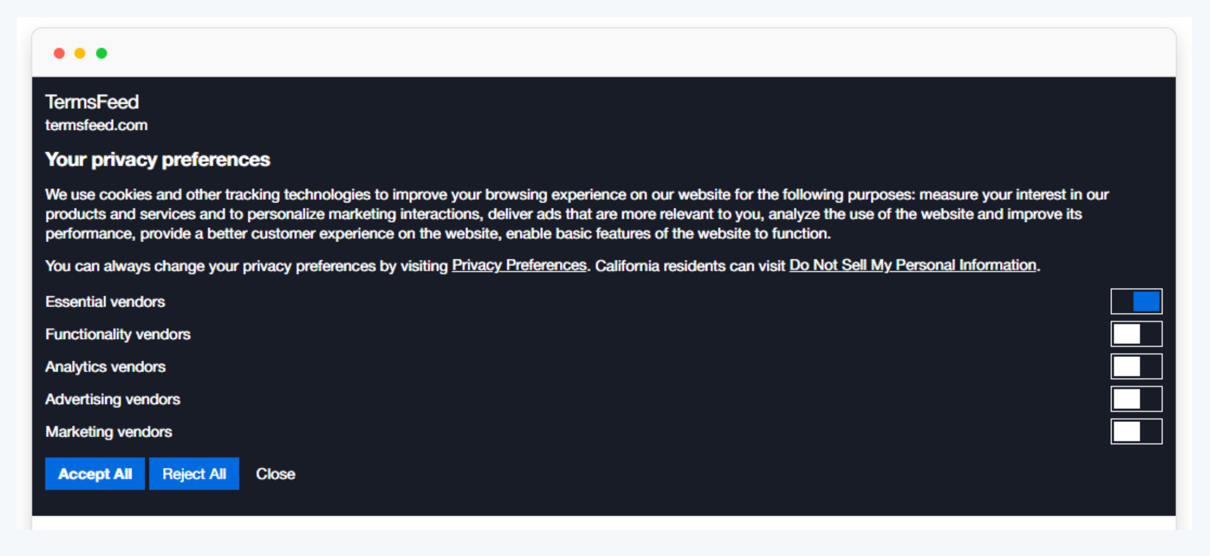
Image: Costco sign-up form with checkbox to receive marketing emails highlighted

Consent for Cookies and Analytics

The ePrivacy Directive's requirements mean that you **must seek consent** for any cookie that is *not* either:

a) used "*for the sole purpose of carrying out the **transmission of a communication** over an electronic communications network*"; or,
b) "***strictly necessary** in order for the provider of an information society service explicitly requested by the subscriber or user to provide the service*"

This means that you must request consent for any cookies involved in **advertising** - personalization, tracking, retargeting and campaign measurement.



TermsFeed
termsfeed.com

Your privacy preferences

We use cookies and other tracking technologies to improve your browsing experience on our website for the following purposes: measure your interest in our products and services and to personalize marketing interactions, deliver ads that are more relevant to you, analyze the use of the website and improve its performance, provide a better customer experience on the website, enable basic features of the website to function.

You can always change your privacy preferences by visiting Privacy Preferences. California residents can visit Do Not Sell My Personal Information.

Essential vendors ☑
Functionality vendors ☐
Analytics vendors ☐
Advertising vendors ☐
Marketing vendors ☐

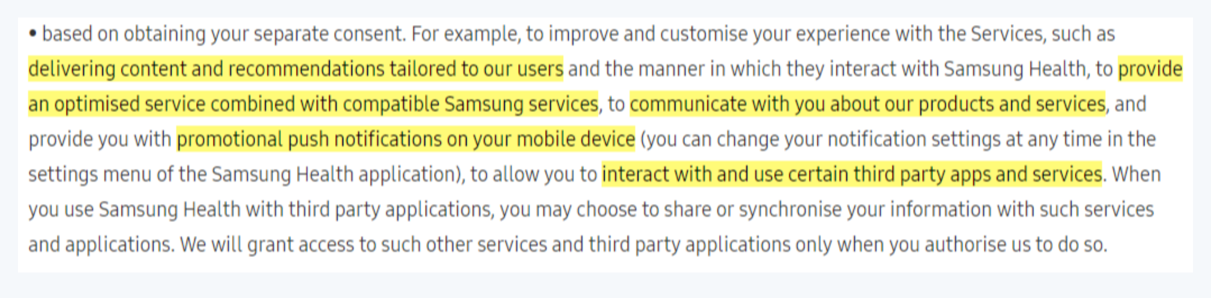
Image: Example of the Privacy Consent Banner from TermsFeed Generator

This also has implications for analytics. The Article 29 Working Party notes that, as the law stands, **even first-party analytics** are *not* exempt from the requirement for consent under the ePrivacy Directive, despite their very low privacy risk. This is because their function is not limited to merely transmitting information, and nor is it "strictly necessary" to allow for the use of a site.

Examples of Consent for Other Activities

There's a potentially **unlimited** number of activities for which you might ask for consent. If you don't actually need to process personal data in a particular way, then consent might be the right legal basis for this activity.

For example, here are some of the purposes for which a health app could rely on consent:



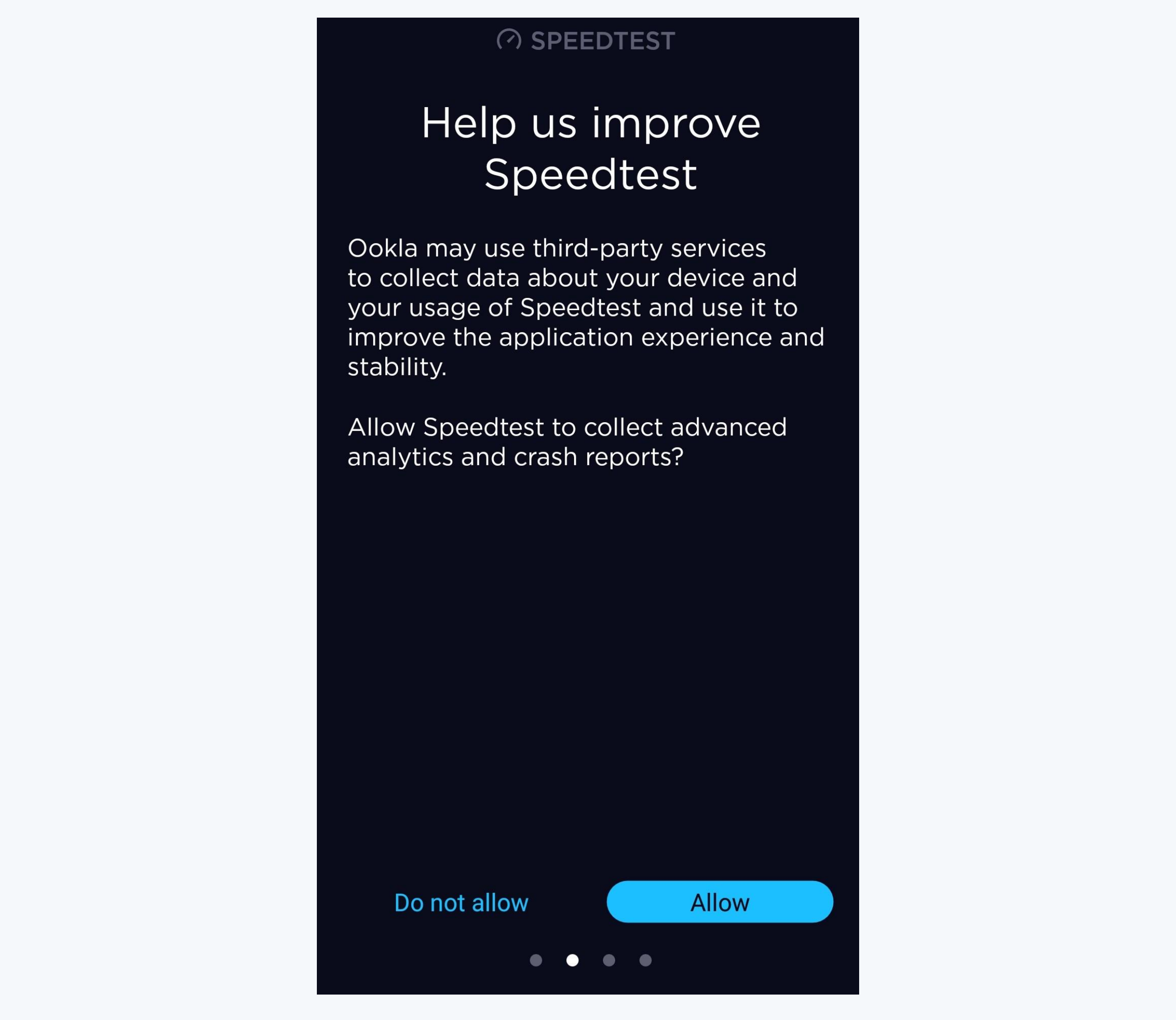
• based on obtaining your separate consent. For example, to improve and customise your experience with the Services, such as delivering content and recommendations tailored to our users and the manner in which they interact with Samsung Health, to provide an optimised service combined with compatible Samsung services, to communicate with you about our products and services, and provide you with promotional push notifications on your mobile device (you can change your notification settings at any time in the settings menu of the Samsung Health application), to allow you to interact with and use certain third party apps and services. When you use Samsung Health with third party applications, you may choose to share or synchronise your information with such services and applications. We will grant access to such other services and third party applications only when you authorise us to do so.

Image: Generic Privacy Policy: Obtaining consent clause

The health app notes that it seeks consent for:

- Tailoring content based on tracking user activity
- Using data to contribute to the optimization of **other** Samsung services
- Direct marketing
- Push notifications
- Third party app integration

Mobile app Speedtest requests consent to send **crash reports**:



Help us improve Speedtest

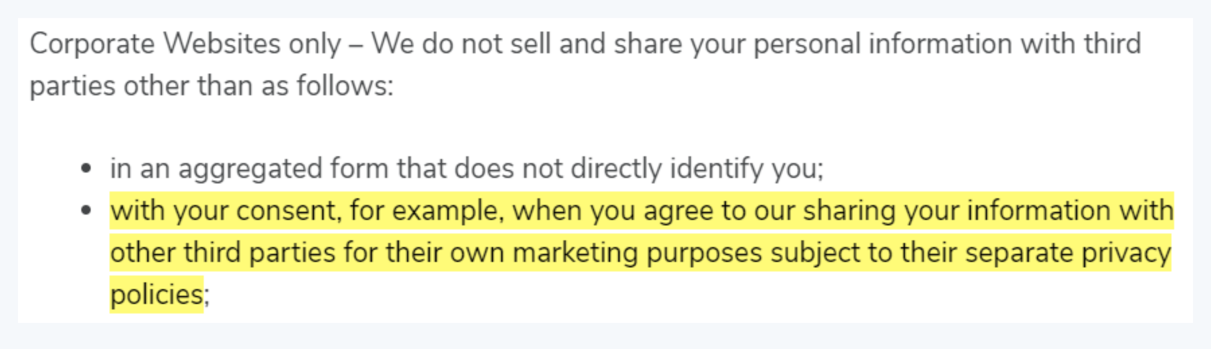
Ookla may use third-party services to collect data about your device and your usage of Speedtest and use it to improve the application experience and stability.

Allow Speedtest to collect advanced analytics and crash reports?

Image: Speedtest app Request consent to collect advanced analytics crash reports screen

Consent can be requested for **sharing personal data** with third parties.

Here's how this can be explained in a Privacy Policy:

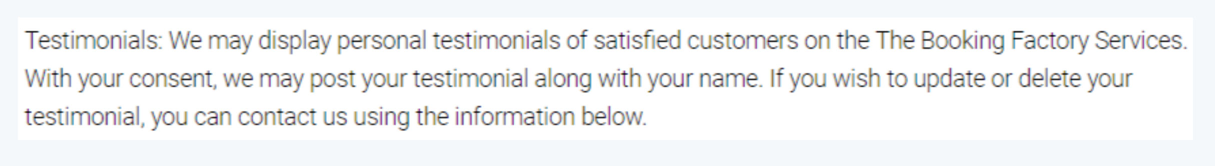


Corporate Websites only – We do not sell and share your personal information with third parties other than as follows:

- in an aggregated form that does not directly identify you;
- with your consent, for example, when you agree to our sharing your information with other third parties for their own marketing purposes subject to their separate privacy policies;

Image: Generic Privacy Policy: Do not sell or share personal information with third parties clause

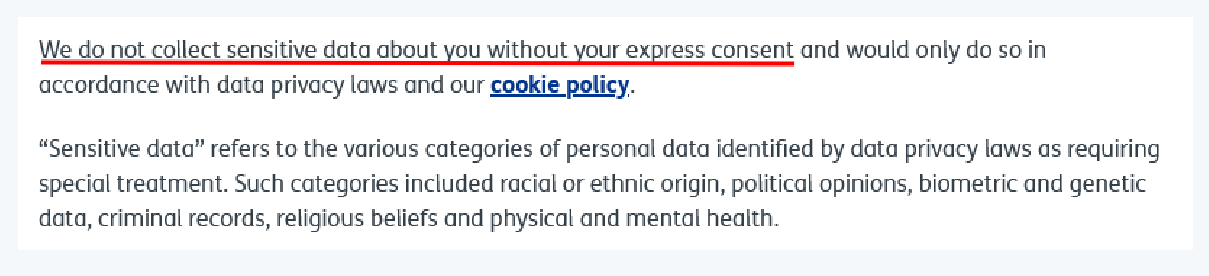
The Booking Factory seeks consent for **displaying customer testimonials** on its website:



Testimonials: We may display personal testimonials of satisfied customers on the The Booking Factory Services. With your consent, we may post your testimonial along with your name. If you wish to update or delete your testimonial, you can contact us using the information below.

Image: The Booking Factory Privacy Policy: Testimonials clause

Baringa seeks consent for **collecting special category data**:



We do not collect sensitive data about you without your express consent and would only do so in accordance with data privacy laws and our **cookie policy**.

"Sensitive data" refers to the various categories of personal data identified by data privacy laws as requiring special treatment. Such categories included racial or ethnic origin, political opinions, biometric and genetic data, criminal records, religious beliefs and physical and mental health.

Image: Baringa Privacy Policy: We do not collect sensitive data without express consent clause

Consent vs Legitimate Interests

Whenever your website, software or app processes personal data, you should consider whether this is **necessary**. If you believe it *is* necessary, conduct a **Legitimate Interests Assessment**. And try to think about this *from your users' perspective.* What's necessary for **you** to improve your business might not be necessary for **your users** when they use your services.

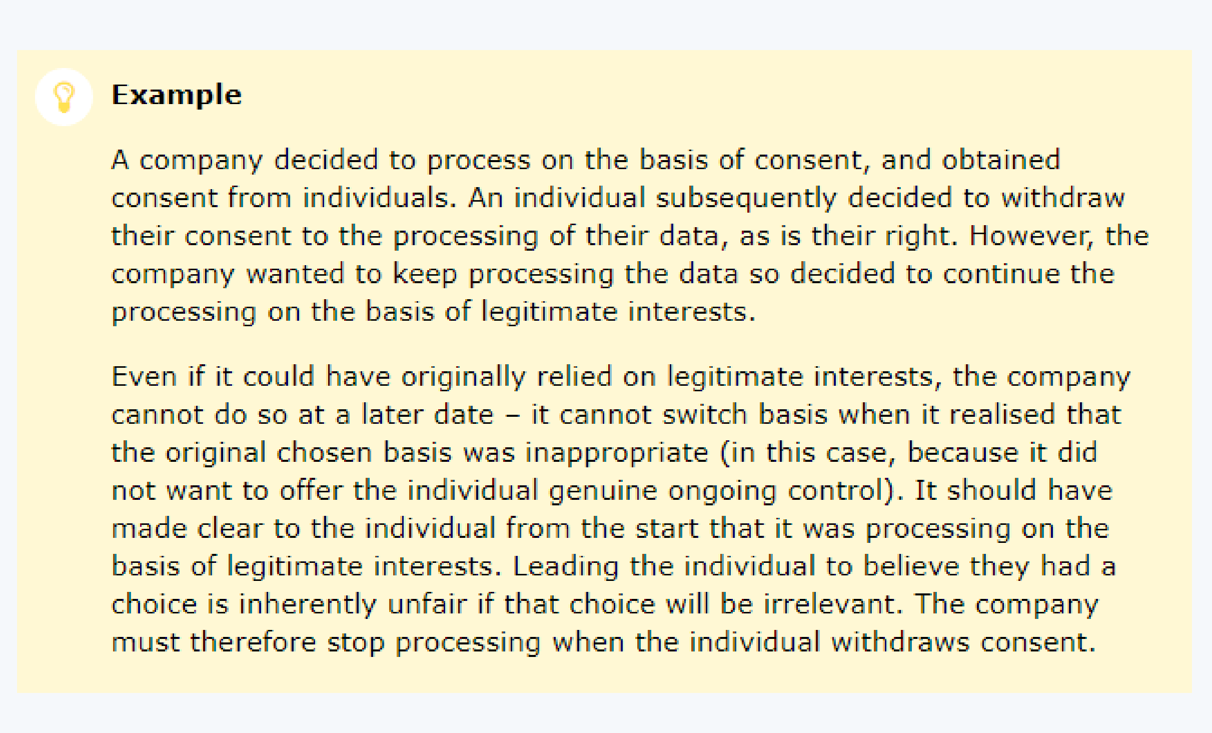
If the activity you have in mind is **not** necessary, or if it fails a Legitimate Interests Assessment, this **doesn't** mean you have to give up on the idea. You should consider whether you can seek **consent** instead.

Switching Legal Bases

It's important to note that if you decide to rely on consent for a particular purpose, you can't simply argue that you have a legitimate interest for that purpose if your data subject **refuses consent**.

So for example, if you ask for consent for cookies, you'll have to **wait** until you get that consent **before** you set cookies on a user's device. You can't set cookies first, *then* ask for permission, then say it was in your legitimate interests all along if your user doesn't consent.

Here's some more information from the ICO:



Example

A company decided to process on the basis of consent, and obtained consent from individuals. An individual subsequently decided to withdraw their consent to the processing of their data, as is their right. However, the company wanted to keep processing the data so decided to continue the processing on the basis of legitimate interests.

Even if it could have originally relied on legitimate interests, the company cannot do so at a later date – it cannot switch basis when it realised that the original chosen basis was inappropriate (in this case, because it did not want to offer the individual genuine ongoing control). It should have made clear to the individual from the start that it was processing on the basis of legitimate interests. Leading the individual to believe they had a choice is inherently unfair if that choice will be irrelevant. The company must therefore stop processing when the individual withdraws consent.

Image: ICO Lawful Basis for Processing Guide: Example box

Choosing Between Consent and Legitimate Interests

Here is a breakdown of the activities for which you might consider relying on consent or legitimate interest. Approach this area with caution, and remember that you can ultimately only figure this stuff out in the **context** of your **own business**.

Activity	Legitimate Interests?	Consent?	Source
Maintaining network security	Maintaining network security **can be a legitimate interest**. This might involve logging IP addresses to detect Distributed Denial of Service (DDoS) attacks.	Consent is **unlikely to be appropriate** for this purpose.	Recital 47 of the GDPR. Article 29 Working Party Opinion 06/2014. ICO's guidance on legitimate interests
Preventing fraud or abuse	Preventing fraud and misuse of services **can be a legitimate interest**. This might include maintaining "ban lists."	Consent is **unlikely to be appropriate** for this purpose.	Recital 47 of the GDPR. Article 29 Working Party Opinion 06/2014. ICO's guidance on legitimate interests
Maintaining website or app functionality.	If relying on legitimate to process personal data for the maintenance of your website, this must be "**necessary**" (from the user's perspective) for the website's functioning. You **may** be able to rely on legitimate interests if you **anonymize** certain personal data.	It's **best to rely on consent** for non-essential website maintenance. For example, many websites and apps request consent for sending crash reports.	ePrivacy Directive Article 5 (3) Article 29 Working Party Opinion 04/2012 on cookie consent
Using analytics	The ICO suggests that running data analytics to maintain or improve service functionality ***may*** constitute a legitimate interest, if personal data is **fully anonymized** beforehand.	The Article 29 Working Party notes that both **first and third-party analytics require consent**. Certain **providers of analytics services** also require customers to earn consent from data subjects as part of the Terms of Service.	ePrivacy Directive Article 5 (3) ICO's guidance on legitimate interests Article 29 Working Party Opinion 04/2012 on cookie consent Google Analytics Terms of Service
Using cookies	You might be able to rely on **legitimate interests** when using certain cookies, including: ● Session ID cookies that	Third-party cookies will generally **require consent**. This is particularly important for **behavioral advertising** ("personalized" or "interest-based" advertising) cookies.	European Commission's guidance on cookies Article 29 Working Party Opinion 04/2012 on cookie consent ICO's guidance on cookies

	keep track of form inputs ● Authentication cookies ● Certain limited-duration security cookies ● Multimedia player session cookies ● Load-balancing session cookies ● UI customization cookies ● Social media plug-in cookies for sharing content where a user is logged in (**not** for other purposes such as tracking).	It is essential to earn consent for **retargeting cookies**. Most retargeting providers (for example Google) require this as in the Terms of Service. Due to the ePrivacy Directive, consent is necessary even for **frequency-capping** and **ad campaign measurement** cookies.	
Direct marketing	For email or SMS, certain direct marketing **might be possible under legitimate interests** where there is a pre-existing business relationship with the customer; you've identified a clear benefit that cannot be achieved in other ways (e.g. indirect marketing); you're sending unintrusive and infrequent direct marketing communications. For non-automated phone calls and postal direct marketing, the rules are less strict thanks to the exemption in the ePrivacy Directive. Individuals have an **absolute right to object** to direct marketing.	Any electronic direct marketing for customers with whom you do not have an existing business relationship will **normally require consent**.	ePrivacy Directive Article 13 ICO's guidance on email marketing Article 29 Working Party Opinion 03/2003 on direct marketing

Sending administrative or transactional emails	This is likely to be **justifiable under legitimate interests** if it contributes to the smooth running of your services and benefits your customer and it's not too intrusive. There should be an opt-out for non-essential transactional emails. It's also possible **that a contract** is an appropriate legal basis for this activity if the emails are necessary for providing your service.	**Consent would only be appropriate** if these were direct marketing emails disguised as transactional emails. UK supermarket Morrison's was fined by the ICO for sending an email like this to customers who had opted out. Don't do it!	Article 6 of the GDPR ICO's action against Morrison Supermarkets
Processing special category data	This is only possible under legitimate interests for certain **non-profits and membership organizations**.	**Consent can be an appropriate solution** if you need to process special category data. You must be completely transparent when seeking consent for this.	Article 9 of the GDPR Recital 51 and 52 of the GDPR
Pursuing and defending legal claims	While many companies list this as a legitimate interest, it is actually more likely to be covered by an **exemption**. This is a technical point, and, in reality, you're likely to be able to justify processing personal data where it's **necessary** to do so in the establishing, exercising or defending of legal rights.	Consent is **unlikely to be appropriate** for this purpose.	ICO's guidance on exemptions

Table 3: Activities to consider when use Consent and Legitimate Interests

This might sound like a frustratingly **strict** approach - but EU privacy law *is* strict. Helping you comply with this law is the purpose of this book.

Chapter 6:

Working with Third Parties

No developer is an island. Even if you're working on a solo project, the chances are that you won't be building absolutely everything from the ground up yourself.

You might need to use a **development platform** to help you create a piece of software. You might want to generate revenue by **displaying ads** on your mobile app. Or you might want to gain insights into your users' activity by running **third-party analytics** on a website.

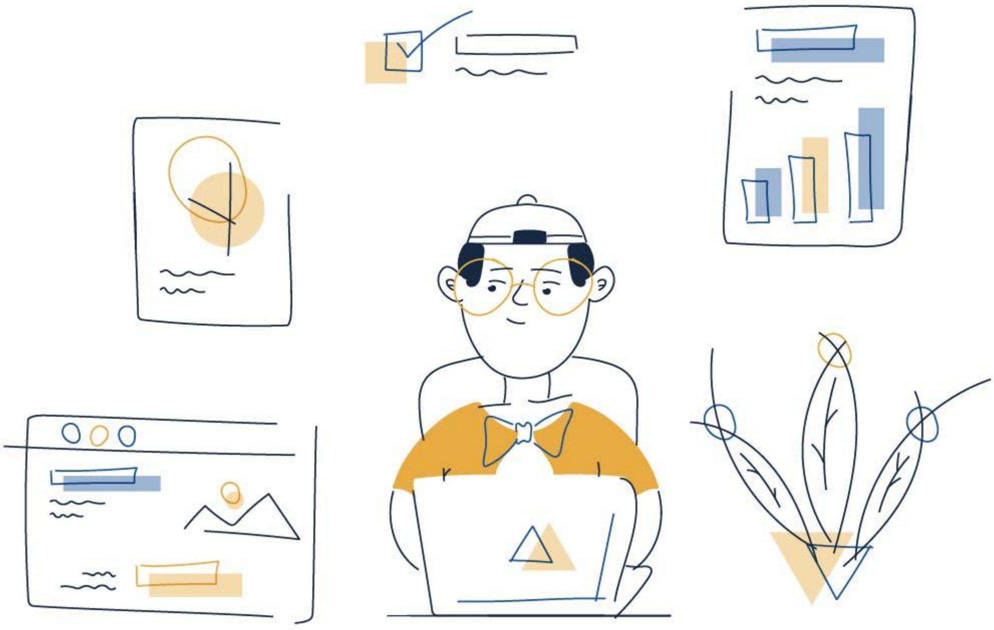


Illustration: Developer Working with Third Parties and the GDPR

For obvious reasons, it's crucial that you obey the law when undertaking these endeavors. But the "law of the land" isn't the only thing you have to consider.

Whenever you sign up to use another company's software or receive a third-party service, **you agree to certain Terms and Conditions and License Agreements (EULA) to which you are legally bound**.

In this chapter, we're going to look at some of the more common terms you're likely to agree to as a developer, and what you'll need to do to adhere to these.

In 2014, data security firm F-Secure set up a free WiFi hotspot in central London. By simply agreeing to F-Secure's Terms and Conditions, anyone could use it. The catch? Buried in the F-Secure's terms was a so-called "Herod clause," which required users to transfer ownership of their first-born child in exchange for logging on. Six people agreed to this. Unsurprisingly, F-Secure never tried to enforce the agreement.

You've probably entered into hundreds of Terms and Conditions agreements in your life. This is the text that you hurriedly scroll through when signing up to a service, or impatiently swipe past when installing an app on your phone.

These are **contracts**, and you're **legally bound** by all of them. As a consumer, it rarely matters all that much. But as a **business**, you need to be very careful.

Working with Other Companies Under the GDPR

The GDPR doesn't exist to **stifle business activity** (although you'd be forgiven for sometimes feeling that it does). You're allowed to work with other companies to process personal data. Under certain conditions, you don't even need your users' **consent** to do this.

But you do need to be absolutely **transparent** about it, and you are **accountable** for selecting legally-compliant third parties to work with. Transparency and accountability, as we know, are two very important principles under the GDPR.

The law provides a base level of protection for individuals, and you mustn't ever fall below this. But other companies might also have other expectations that their partner businesses must fulfill.

Standards imposed on your company by third parties cannot fall below the **minimum level of protection** provided by law. But they may **well rise** above it. And it may also be the case that *their* standards fall below *your* expectations, or mean that you cannot keep your promises to your customers about how you'll protect their personal data.

This is why it’s **crucial** that you **know** what you’re signing up to when you work with a third party.

Advertisers

The global market for digital marketing is reportedly worth $307 billion. The real value in this market, and the advantage that the format holds over traditional advertising, is in the **targeting** and **personalization** that can be achieved by **processing personal data**.

Google

With its high market share of the search engine industry, online advertising market, and sale of smartphones running Google’s Android OS, it’s likely that your company will be doing business with Google in some capacity.

Google has a bewildering number of **terms**, **policies**, and **guidelines** - not to mention products - that all overlap and intermingle. We’re going to sort through some of these documents to help you understand the implications of using certain Google services.

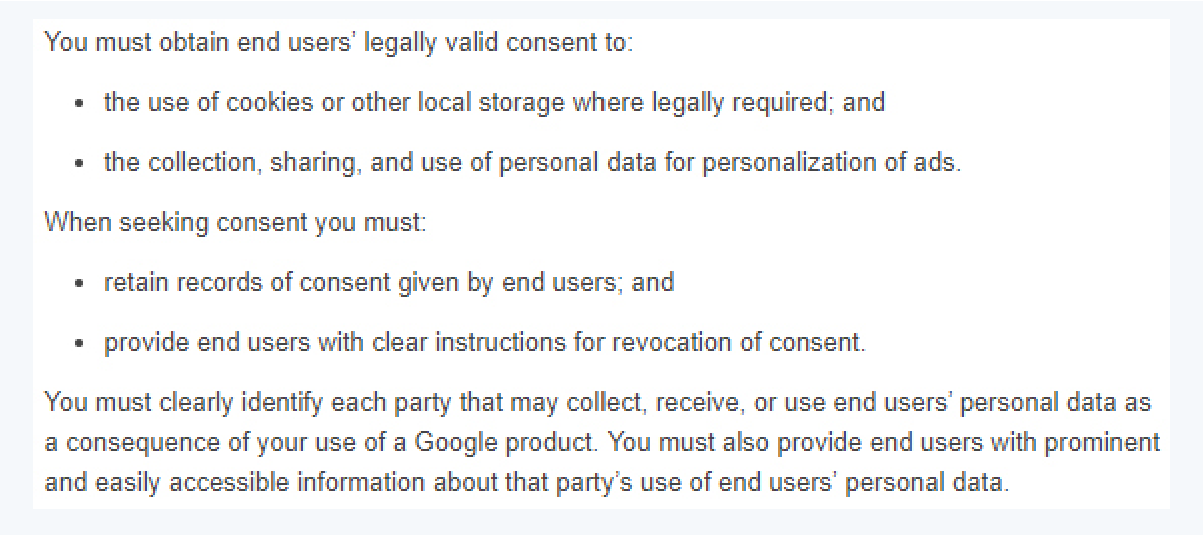
Google EU User Consent Policy

If you’re using one of Google’s products or services to process the personal data of EU citizens, you must agree with Google’s EU User Consent Policy. It applies to Google products such as the following:

- All Google Ads products (e.g. AdSense, AdMob, AdWords) and ad campaign measurement products
- Google Maps APIs
- YouTube API Services
- G+ Buttons
- reCAPTCHA
- Blogger

The EU User Consent Policy requires that you provide clear information to, and earn consent from, your users in the **European Economic Area** (EEA).

Here’s an excerpt from the policy:



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:

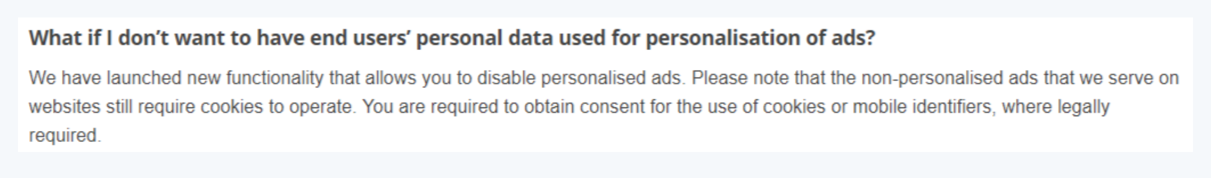
- retain records of consent given by end users; and
- provide end users with clear instructions for revocation of consent.

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

Previously we discussed how important it is to earn **consent** for cookies. Cookies are what enable Google to **personalize** and **measure** your ads.

The policy ostensibly only requires that you earn consent for **personalized ads**. However, note this section from a Google help document about the EU User Consent Policy:



What if I don't want to have end users' personal data used for personalisation of ads?

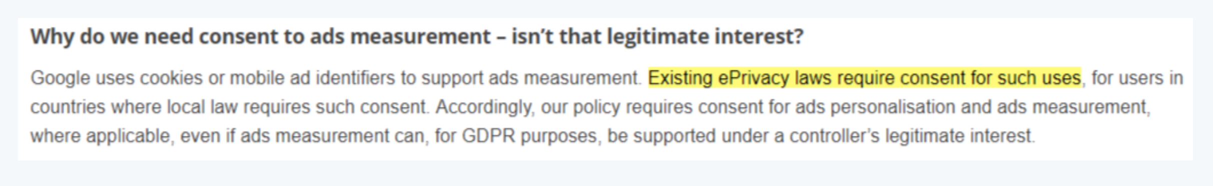
We have launched new functionality that allows you to disable personalised ads. Please note that the non-personalised ads that we serve on websites still require cookies to operate. You are required to obtain consent for the use of cookies or mobile identifiers, where legally required.

Image: Google Help with User Consent Policy: What if I don't want end users personal data for personalisation of ads section

It's possible to turn off ad personalization, but you're **still** required to earn user consent for **non-personalized** ads.

Why? Well, even Google's *non*-personalized ads use **frequency-capping** and **campaign measurement cookies**; and as we know, these require consent under the ePrivacy Act.

Google acknowledges this:



Why do we need consent to ads measurement – isn't that legitimate interest?

Google uses cookies or mobile ad identifiers to support ads measurement. Existing ePrivacy laws require consent for such uses, for users in countries where local law requires such consent. Accordingly, our policy requires consent for ads personalisation and ads measurement, where applicable, even if ads measurement can, for GDPR purposes, be supported under a controller's legitimate interest.

Image: Google Help with User Consent Policy: Why do we need consent to ads measurement section

The implications of this policy are clear. If you use a Google product to process the personal data of people in the EEA, you'll need to:

- **Fully disclose** your practices via a Privacy Policy

- **Seek consent** for both personalized and/or non-personalized ads

We look in detail at how you can implement Google's consent requirements in Chapter 6.

Google Ads

It's worth noting that "Google Ads" refers to a number of different Google products, and that there are different terms and policies applicable depending on which country you're operating from.

Don't forget, though - no matter where you're based, **Google's policies will require you to treat your processing of EU users' personal data according to EU law.**

As we've mentioned, Google Ads customers who run ads in the EU are bound by the EU User Consent Policy. This is applicable to developers **all over the world**.

Because of the nature of the data transfers that take place between you and Google when using Google Ads, you're also bound by the Google Ads Controller-Controller Data Protection Terms.

By signing up to these terms, you're agreeing to only transfer your users' personal data to Google **once you've earned your users' consent**.

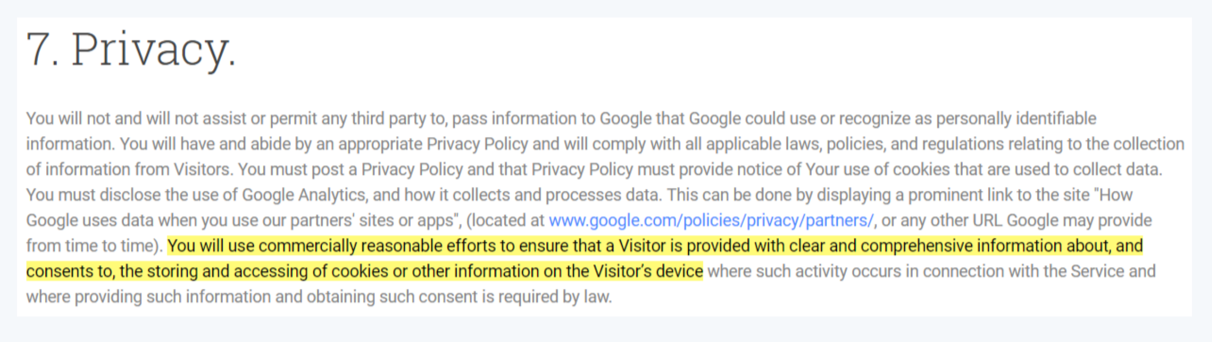
Web Analytics

As we've seen, using analytics requires **full disclosure** and the earning of user **consent** under the ePrivacy Directive.

This is because although the use of analytics software is relatively **low-risk**, particularly in the case of first-party analytics, it is not "**strictly necessary**" for providing a service, nor does it merely **facilitate communication** over a network.

Google Analytics

Google Analytics requires full compliance with EU law, as is clear from the Google Analytics Terms of Service:



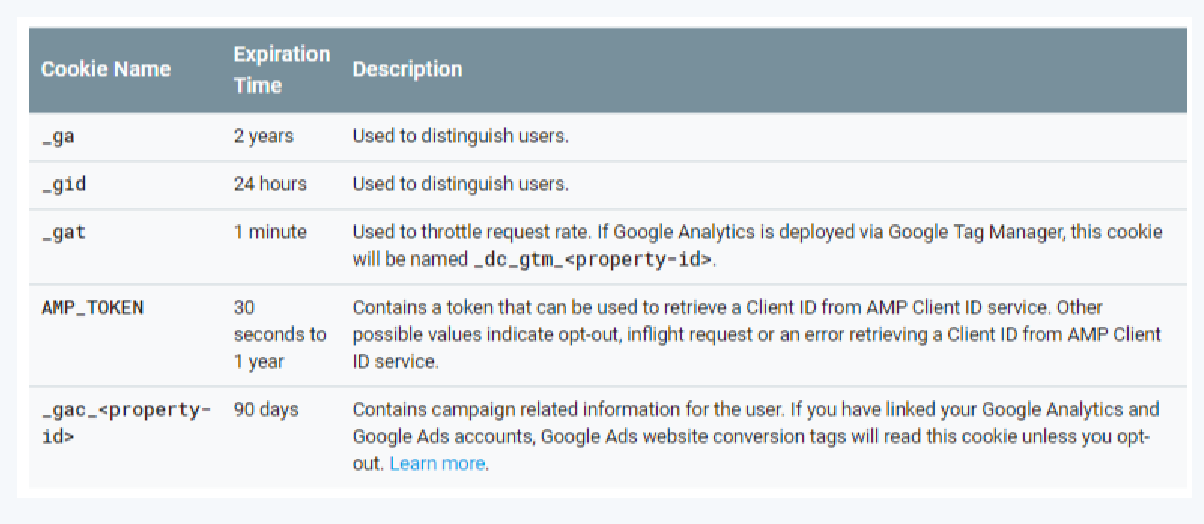
7. Privacy.

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 Visitors. You must post a Privacy Policy and that Privacy Policy must provide notice of Your use of cookies that are 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 Visitor is provided with clear and comprehensive information about, and consents to, the storing and accessing of cookies or other information on the Visitor'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 - Efforts to provide information and obtain consent section highlighted

Providing your users with "clear and comprehensive information" means producing a legally-compliant **Privacy Policy**. This policy must include, among other things, **how long** the cookies involved in Google Analytics are set for.

Here's some information from Google about the retention periods associated with each analytics cookie:



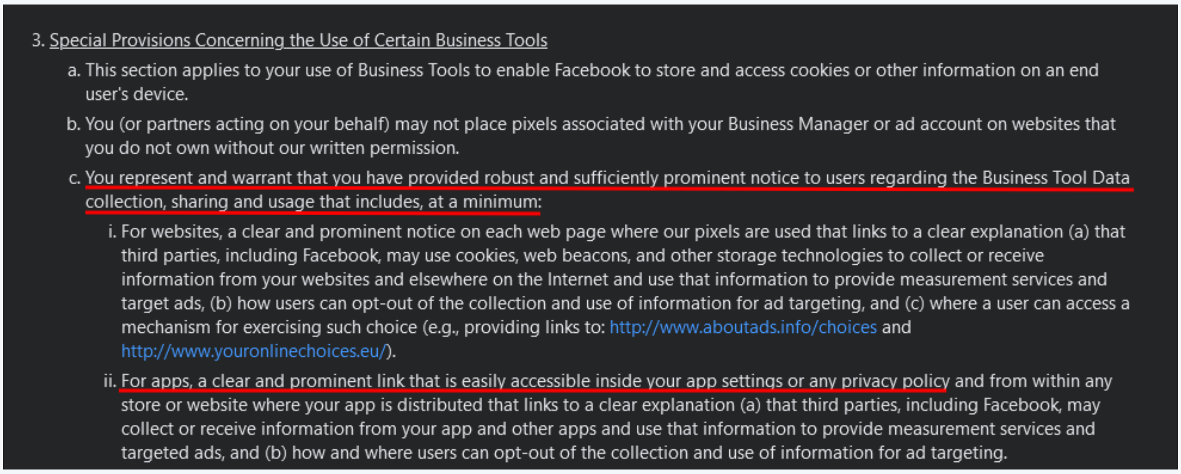
Cookie Name	Expiration Time	Description
_ga	2 years	Used to distinguish users.
_gid	24 hours	Used to distinguish users.
_gat	1 minute	Used to throttle request rate. If Google Analytics is deployed via Google Tag Manager, this cookie will be named _dc_gtm_<property-id>.
AMP_TOKEN	30 seconds to 1 year	Contains a token that can be used to retrieve a Client ID from AMP Client ID service. Other possible values indicate opt-out, inflight request or an error retrieving a Client ID from AMP Client ID service.
gac<property-id>	90 days	Contains campaign related information for the user. If you have linked your Google Analytics and Google Ads accounts, Google Ads website conversion tags will read this cookie unless you opt-out. Learn more.

Image: Google Analytics Cookie Usage on Websites chart

Facebook Analytics

Facebook offers analytics insights and conversion tracking via the **Facebook Pixel**. This is a **web beacon**. Web beacons are considered to be **online identifiers** under EU law, and so must be treated in the same way as tracking cookies.

The Facebook Business Tools Terms requires the following from users of its pixel:



3. Special Provisions Concerning the Use of Certain Business Tools
    a. This section applies to your use of Business Tools to enable Facebook to store and access cookies or other information on an end user's device.
    b. You (or partners acting on your behalf) may not place pixels associated with your Business Manager or ad account on websites that you do not own without our written permission.
    c. You represent and warrant that you have provided robust and sufficiently prominent notice to users regarding the Business Tool Data collection, sharing and usage that includes, at a minimum:
        i. For websites, a clear and prominent notice on each web page where our pixels are used that links to a clear explanation (a) that third parties, including Facebook, may use cookies, web beacons, and other storage technologies to collect or receive information from your websites and elsewhere on the Internet and use that information to provide measurement services and target ads, (b) how users can opt-out of the collection and use of information for ad targeting, and (c) where a user can access a mechanism for exercising such choice (e.g., providing links to: http://www.aboutads.info/choices and http://www.youronlinechoices.eu/).
        ii. For apps, a clear and prominent link that is easily accessible inside your app settings or any privacy policy and from within any store or website where your app is distributed that links to a clear explanation (a) that third parties, including Facebook, may collect or receive information from your app and other apps and use that information to provide measurement services and targeted ads, and (b) how and where users can opt-out of the collection and use of information for ad targeting.

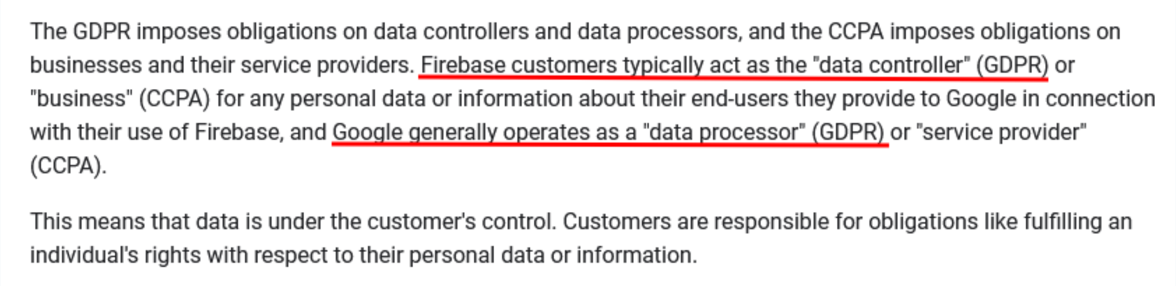
Image: Facebook Business Tools Terms: Special Provisions Concerning the Use of Certain Business Tools

Development Tools

Front-end and back-end development tools are crucial for software and app developers. But no provider of such services will want them to be used for **illegal** or **unlawful** purposes. Therefore, you must agree to strict terms when choosing to use such tools.

Google Firebase

The Firebase platform comprises various products, governed by a number of different agreements and policies. Google's guidance on Privacy and Security in Firebase explains that Google is the data processor in respect of most data processing activities in Firebase:

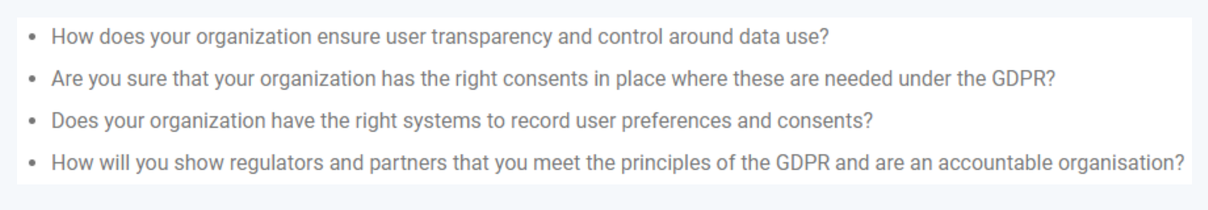


The GDPR imposes obligations on data controllers and data processors, and the CCPA imposes obligations on businesses and their service providers. Firebase customers typically act as the "data controller" (GDPR) or "business" (CCPA) for any personal data or information about their end-users they provide to Google in connection with their use of Firebase, and Google generally operates as a "data processor" (GDPR) or "service provider" (CCPA).

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

Image: Google Firebase Privacy and Security: Data protection clause excerpt

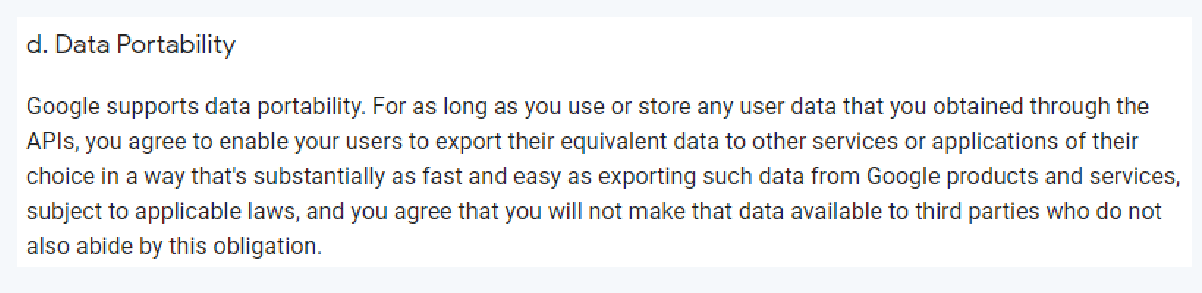
Google asks developers using the platform to consider the **following questions** in the context of the GDPR:



- 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 will you show regulators and partners that you meet the principles of the GDPR and are an accountable organisation?

Image: Google developer questions about the GDPR

Use of many Firebase tools (e.g. Firebase Crash Reporting. Performance Monitoring and In-App Messaging) is governed by the Google APIs Terms of Service. This agreement includes the requirement that you make your users' personal data **accessible** to them, so that they may exercise their right to **data portability**:



d. Data Portability

Google supports data portability. For as long as you use or store any user data that you obtained through the APIs, you agree to enable your users to export their equivalent data to other services or applications of their choice in a way that's substantially as fast and easy as exporting such data from Google products and services, subject to applicable laws, and you agree that you will not make that data available to third parties who do not also abide by this obligation.

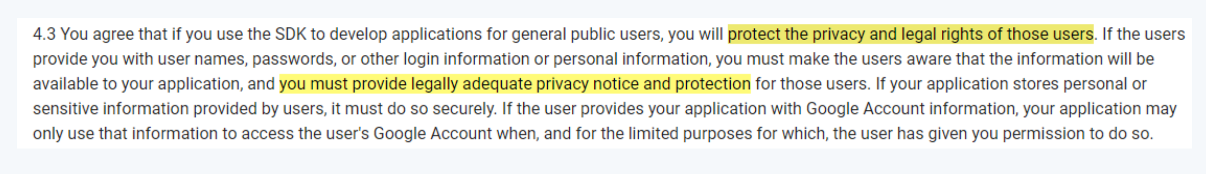
Image: Google APIs Terms of Service: Data Portability clause

We look in detail at how you can meet your obligations to facilitate your users' data subject rights in the next chapter.

Android SDK

If you're developing a mobile app using the **Android Software Development Kit** (SDK), there are a lot of terms and policies you'll need to comply with.

The Android Software Development Kit License Agreement contains the following clause:

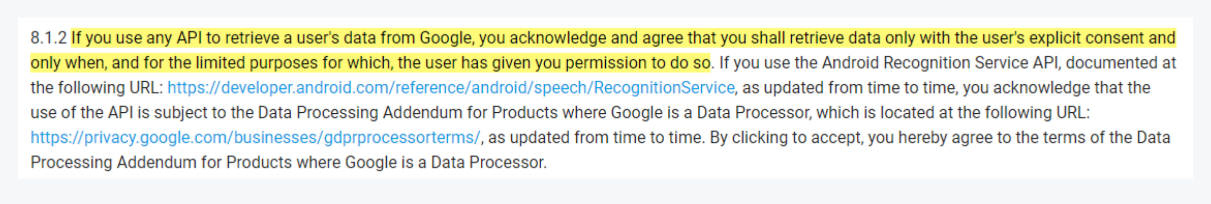


4.3 You agree that if you use the SDK to develop applications for general public users, you will protect the privacy and legal rights of those users. If the users provide you with user names, passwords, or other login information or personal information, you must make the users aware that the information will be available to your application, and you must provide legally adequate privacy notice and protection for those users. If your application stores personal or sensitive information provided by users, it must do so securely. If the user provides your application with Google Account information, your application 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: Android Software Development Kit License Agreement: Use of the SDK clause - Protect privacy section

This requires the app developer to provide legally valid **privacy protection** and **transparent information** to its users.

If your app uses **Android APIs** such as the **Play In-app Billing Library** or **Android Support Library**, you're also bound by the following clause:



8.1.2 If you use any API to retrieve a user's data from Google, you acknowledge and agree that you shall retrieve data only with the user's explicit consent and only when, and for the limited purposes for which, the user has given you permission to do so. If you use the Android Recognition Service API, documented at the following URL: https://developer.android.com/reference/android/speech/RecognitionService, as updated from time to time, you acknowledge that the use of the API is subject to the Data Processing Addendum for Products where Google is a Data Processor, which is located at the following URL: https://privacy.google.com/businesses/gdprprocessorterms/, as updated from time to time. By clicking to accept, you hereby agree to the terms of the Data Processing Addendum for Products where Google is a Data Processor.

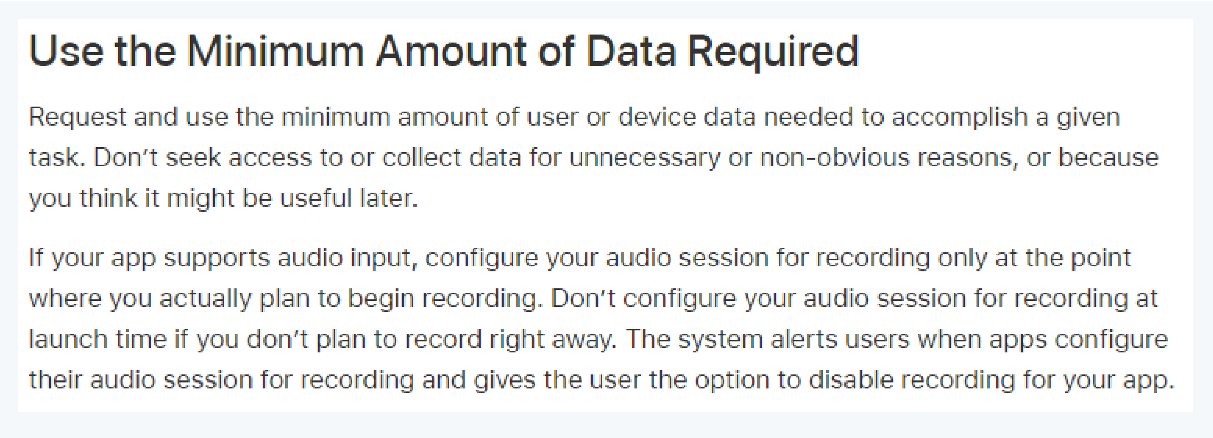
Image: Android Software Development Kit License Agreement: Use of the SDK clause - Consent section

This requires the app developer to **integrate** the appropriate **consent** and **permission request functions** when developing their app. Android provides the Consent SDK, an open source library of utility functions that can be helpful in requesting consent for ads.

iOS

Whereas the monetization of personal data is an integral part of Google's business model, Apple has built a reputation for **respecting** its users' **privacy**. Apple developers are provided with extensive guidance on how to **minimize** and **secure** the personal data collected by their apps.

For example, the documentation provided by Apple for users of its front-end development framework UIKit makes the following recommendation:



Use the Minimum Amount of Data Required

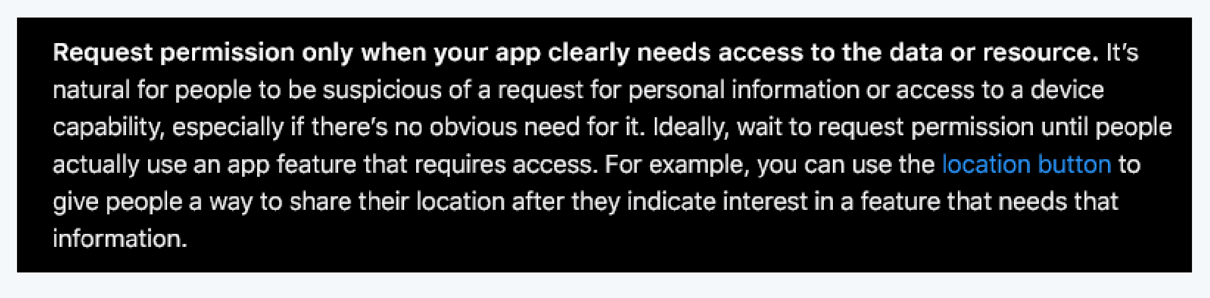
Request and use the minimum amount of user or device data needed to accomplish a given task. Don't seek access to or collect data for unnecessary or non-obvious reasons, or because you think it might be useful later.

If your app supports audio input, configure your audio session for recording only at the point where you actually plan to begin recording. Don't configure your audio session for recording at launch time if you don't plan to record right away. The system alerts users when apps configure their audio session for recording and gives the user the option to disable recording for your app.

Image: Apple Developer UIKit: Protecting Users Privacy - Use the Minimum Amount of Data Required section

This should remind you of the GDPR's principle of **data minimization**.

And here's how Apple's Human Interface Guidelines explain the principle of **purpose limitation**:

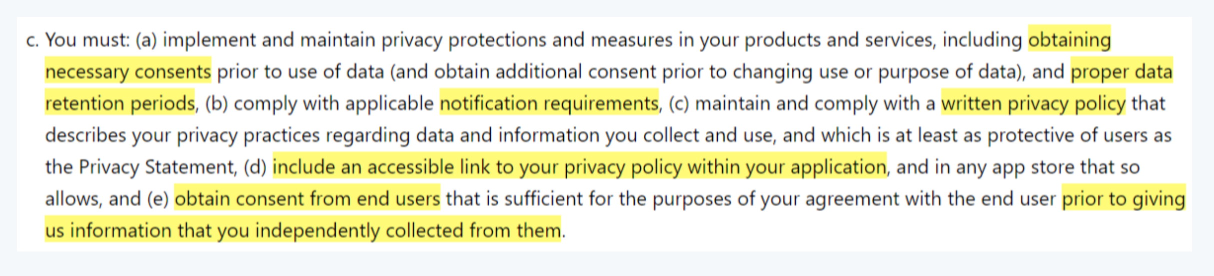


Request permission only when your app clearly needs access to the data or resource. It's natural for people to be suspicious of a request for personal information or access to a device capability, especially if there's no obvious need for it. Ideally, wait to request permission until people actually use an app feature that requires access. For example, you can use the location button to give people a way to share their location after they indicate interest in a feature that needs that information.

Image: Apple Human Interface Guideline: Accessing Private Data - Request permission only when your app clearly needs access to the data or resource section

Microsoft

Use of platforms such as **Microsoft Azure** and **Microsoft Visual Studio** is governed by the Microsoft Developer Agreement, which requires strict adherence to privacy law. Here's an excerpt from the agreement:



c. You must: (a) implement and maintain privacy protections and measures in your products and services, including obtaining necessary consents prior to use of data (and obtain additional consent prior to changing use or purpose of data), and proper data retention periods, (b) comply with applicable notification requirements, (c) maintain and comply with a written privacy policy that describes your privacy practices regarding data and information you collect and use, and which is at least as protective of users as the Privacy Statement, (d) include an accessible link to your privacy policy within your application, and in any app store that so allows, and (e) obtain consent from end users that is sufficient for the purposes of your agreement with the end user prior to giving us information that you independently collected from them.

Image: Microsoft Developer Agreement: Security and Privacy clause - Consent section

Microsoft requires developers to:

- Obtain all necessary **consents** from their users
- Only transfer personal data to Microsoft **after** having obtained this consent
- Maintain a legally-compliant **Privacy Policy** and make it available from **within** their app
- Comply with the law around **data retention** periods

Distribution Channels

If you want people to actually download or buy your app once you've finished developing it, you'll almost certainly want to get it hosted on one or more of the major **app marketplaces**.

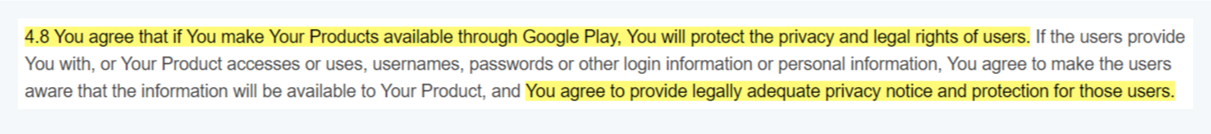
These online stores will only distribute apps that comply with privacy law, as we can see by taking a look at their terms.

Google Play

Image: Google Play logo

If you want to distribute your Android app via Google Play, you'll need to agree to the Google Play Developer Distribution Agreement. This places a considerable number of demands on you as an app developer and/or publisher.

Here's an excerpt from the agreement:

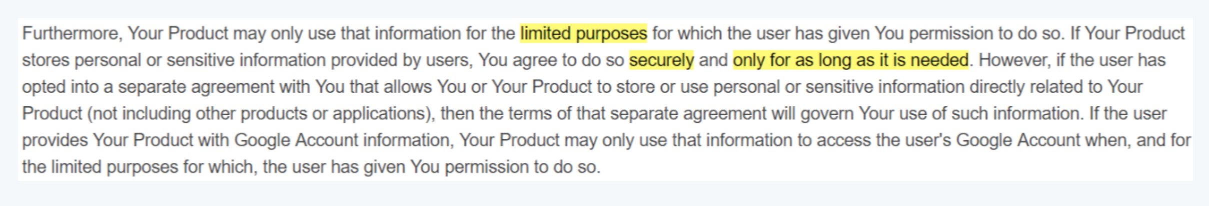


4.8 You agree that if You make Your Products available through Google Play, You will protect the privacy and legal rights of users. If the users provide You with, or Your Product accesses or uses, usernames, passwords or other login information or personal information, You agree to make the users aware that the information will be available to Your Product, and You agree to provide legally adequate privacy notice and protection for those users.

Image: Google Play Developer Distribution Agreement: Agree to protect privacy and legal rights clause intro

This is a requirement for **general** legal compliance, plus a **specific** demand that you produce a Privacy Policy.

Here's the next part of this section:

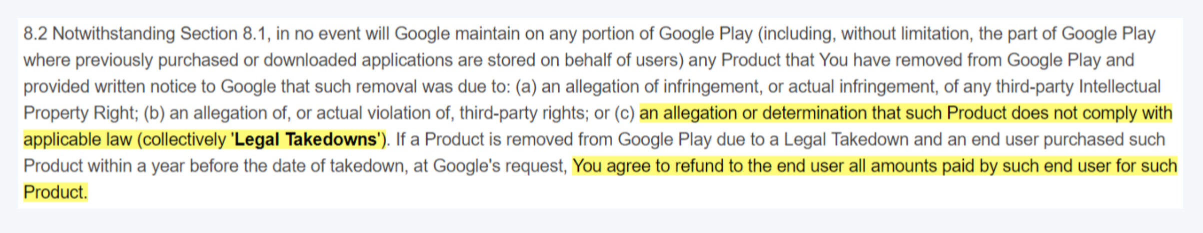


Furthermore, Your Product may only use that information for the limited purposes for which the user has given You permission to do so. If Your Product stores personal or sensitive information provided by users, You agree to do so securely and only for as long as it is needed. However, if the user has 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: Agree to protect privacy and legal rights clause intro - Limited use and purposes section

You're required to only process personal data in connection with a **specified purpose**, and only to **store** personal data for as long as **necessary**. The GDPR makes these same demands at Article 5, by imposing the principles of purpose limitation and storage limitation.

Any suggestion that your app does not comply with the law can lead to a "**Legal Takedown**," as explained in Section 8.2 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 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: Legal takedowns clause

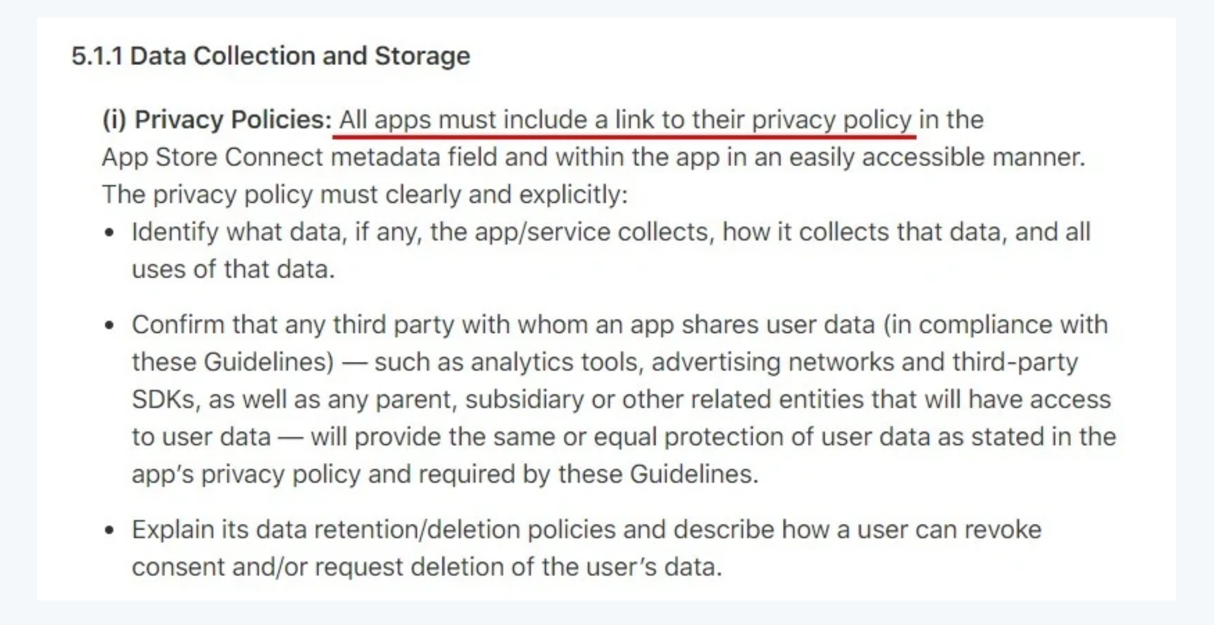
Even an ***allegation*** of unlawful data processing can lead to you losing your spot in Google Play and being required to refund everyone who has purchased your app in the last year.

This might sound unfair, but remember that **this is what you're agreeing to** when you sign up to distribute your app via Google Play.

Apple App Store

Image: Apple App Store logo

Apple makes some very specific demands about the apps it distributes through its platform. For example, here are the **minimum requirements** from the App Store Review Guidelines regarding each app's Privacy Policy:



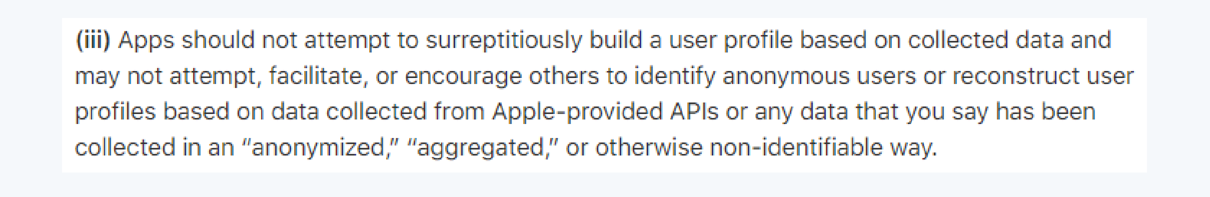
5.1.1 Data Collection and Storage

(i) Privacy Policies: All apps must include a link to their privacy policy in the App Store Connect metadata field and within the app in an easily accessible manner. The privacy policy must clearly and explicitly:

- Identify what data, if any, the app/service collects, how it collects that data, and all uses of that data.
- Confirm that any third party with whom an app shares user data (in compliance with these Guidelines) — such as analytics tools, advertising networks and third-party SDKs, as well as any parent, subsidiary or other related entities that will have access to user data — will provide the same or equal protection of user data as stated in the app's privacy policy and required by these Guidelines.
- Explain its data retention/deletion policies and describe how a user can revoke consent and/or request deletion of the user's data.

Image: Apple App Store Review Guidelines: Data Collection and Storage section - Privacy Policy Link required section highlighted

And the following section effectively prohibits the practice of "**profiling**," even where data is supposedly anonymized or used in aggregate:



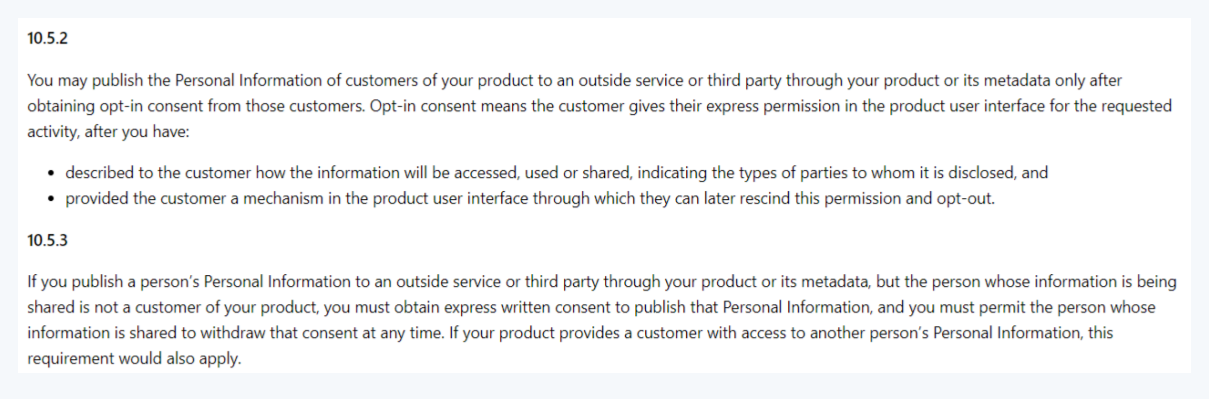
(iii) Apps should not attempt to surreptitiously build a user profile based on collected data and may not attempt, facilitate, or encourage others to identify anonymous users or reconstruct user profiles based on data collected from Apple-provided APIs or any data that you say has been collected in an "anonymized," "aggregated," or otherwise non-identifiable way.

Image: Apple App Store Review Guidelines: Data Use and Sharing section - User profile section

Windows Store

Image: Microsoft Windows Store logo

In addition to the usual requirements for maintaining a Privacy Policy, the Microsoft Store Policies has specific rules about the **sharing** of your users' personal data:



10.5.2

You may publish the Personal Information of customers of your product to an outside service or third party through your product or its metadata only after obtaining opt-in consent from those customers. Opt-in consent means the customer gives their express permission in the product user interface for the requested activity, after you have:

- described to the customer how the information will be accessed, used or shared, indicating the types of parties to whom it is disclosed, and
- provided the customer a mechanism in the product user interface through which they can later rescind this permission and opt-out.

10.5.3

If you publish a person's Personal Information to an outside service or third party through your product or its metadata, but the person whose information is being shared is not a customer of your product, you must obtain express written consent to publish that Personal Information, and you must permit the person whose information is shared to withdraw that consent at any time. If your product provides a customer with access to another person's Personal Information, this requirement would also apply.

Image: Microsoft Store Policies sections 10 5 2 and 10 5 3

You may only share data with third parties with your users' consent. This is a **higher standard** of privacy than that mandated by the GDPR, under which personal data may be sometimes shared with third parties on legal bases **other** than consent.

Cloud Services

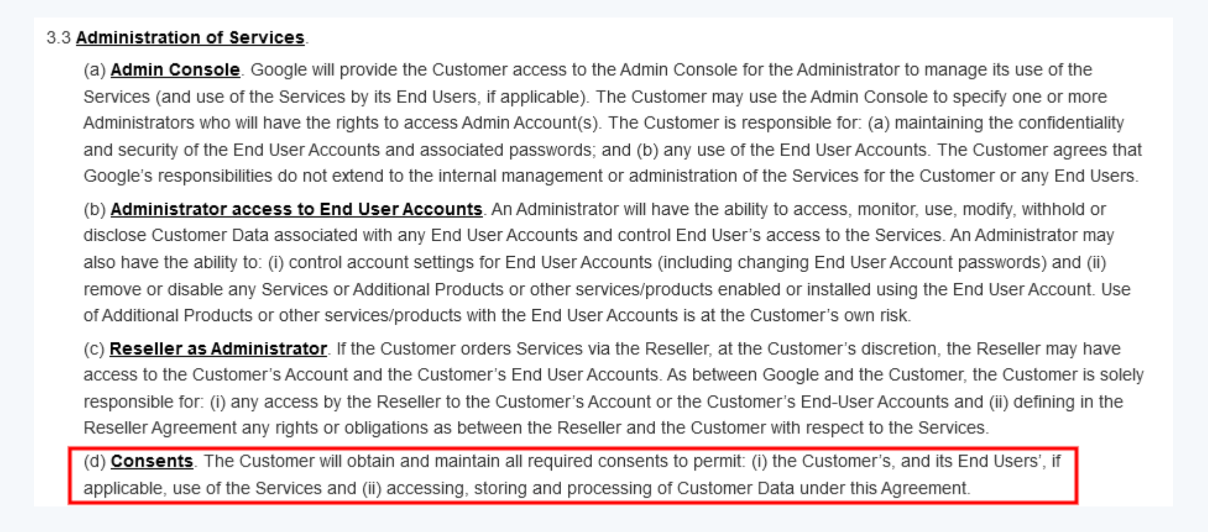
If using **cloud services** to store or otherwise process your users' personal data, you must, of course, be completely **transparent** about this. And you must also take care to choose a cloud services provider that can guarantee compliance with the GDPR.

Google Workspace

Image: Google Workspace logo

Google's Workspace range of cloud-based tools allows customers to delegate **admin access** to one or more people within their company. Administrators have a large degree of access and control over user personal data.

This is set out in this section of the Google Workspace Terms of Service, which requires you to earn your users' **consent** for this:



3.3 **Administration of Services**.

(a) **Admin Console**. Google will provide the Customer access to the Admin Console for the Administrator to manage its use of the Services (and use of the Services by its End Users, if applicable). The Customer may use the Admin Console to specify one or more Administrators who will have the rights to access Admin Account(s). The Customer is responsible for: (a) maintaining the confidentiality and security of the End User Accounts and associated passwords; and (b) any use of the End User Accounts. The Customer agrees that Google's responsibilities do not extend to the internal management or administration of the Services for the Customer or any End Users.

(b) **Administrator access to End User Accounts**. An Administrator will have the ability to access, monitor, use, modify, withhold or disclose Customer Data associated with any End User Accounts and control End User's access to the Services. An Administrator may also have the ability to: (i) control account settings for End User Accounts (including changing End User Account passwords) and (ii) remove or disable any Services or Additional Products or other services/products enabled or installed using the End User Account. Use of Additional Products or other services/products with the End User Accounts is at the Customer's own risk.

(c) **Reseller as Administrator**. If the Customer orders Services via the Reseller, at the Customer's discretion, the Reseller may have access to the Customer's Account and the Customer's End User Accounts. As between Google and the Customer, the Customer is solely responsible for: (i) any access by the Reseller to the Customer's Account or the Customer's End-User Accounts and (ii) defining in the Reseller Agreement any rights or obligations as between the Reseller and the Customer with respect to the Services.

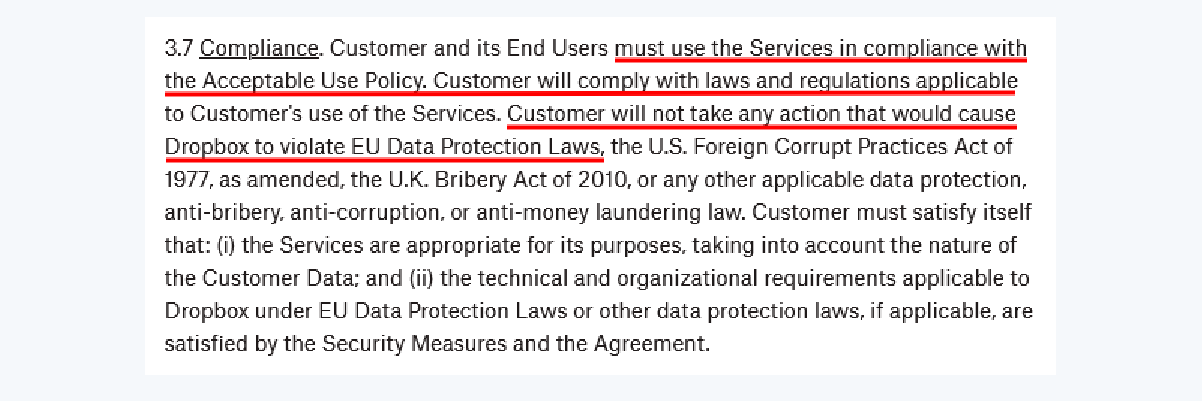
(d) **Consents**. The Customer will obtain and maintain all required consents to permit: (i) the Customer's, and its End Users', if applicable, use of the Services and (ii) accessing, storing and processing of Customer Data under this Agreement.

Image: Google Workspace Terms of Service: Administration of Services - Consents section

Dropbox

Image: Dropbox logo

Use of Dropbox as a business customer is governed by the [Dropbox]() Services Agreement. Dropbox requires customers and users to **comply** with various **privacy laws**. Here's the relevant section of the agreement:



3.7 Compliance. Customer and its End Users must use the Services in compliance with the Acceptable Use Policy. Customer will comply with laws and regulations applicable to Customer's use of the Services. Customer will not take any action that would cause Dropbox to violate EU Data Protection Laws, the U.S. Foreign Corrupt Practices Act of 1977, as amended, the U.K. Bribery Act of 2010, or any other applicable data protection, anti-bribery, anti-corruption, or anti-money laundering law. Customer must satisfy itself that: (i) the Services are appropriate for its purposes, taking into account the nature of the Customer Data; and (ii) the technical and organizational requirements applicable to Dropbox under EU Data Protection Laws or other data protection laws, if applicable, are satisfied by the Security Measures and the Agreement.

Image: Dropbox Services Agreement: Compliance clause

Key Takeaways from this Chapter

If you learn one thing from this chapter, let it be this - **Make sure you read the Terms and Conditions when you enter into any arrangement with a third party**.

This is important for two main reasons:

- **They** will expect **you** to adhere to the law, and may have specific additional requirements.
- **You** must also ensure that **they** are legally-compliant, in-line with the GDPR's principle of accountability.

Chapter 7:

User Rights Developers Need To Know

The data subject rights are a way for individuals to maintain maximum control over their personal data. They are a cornerstone of the GDPR and deeply empowering for individuals in the EU.

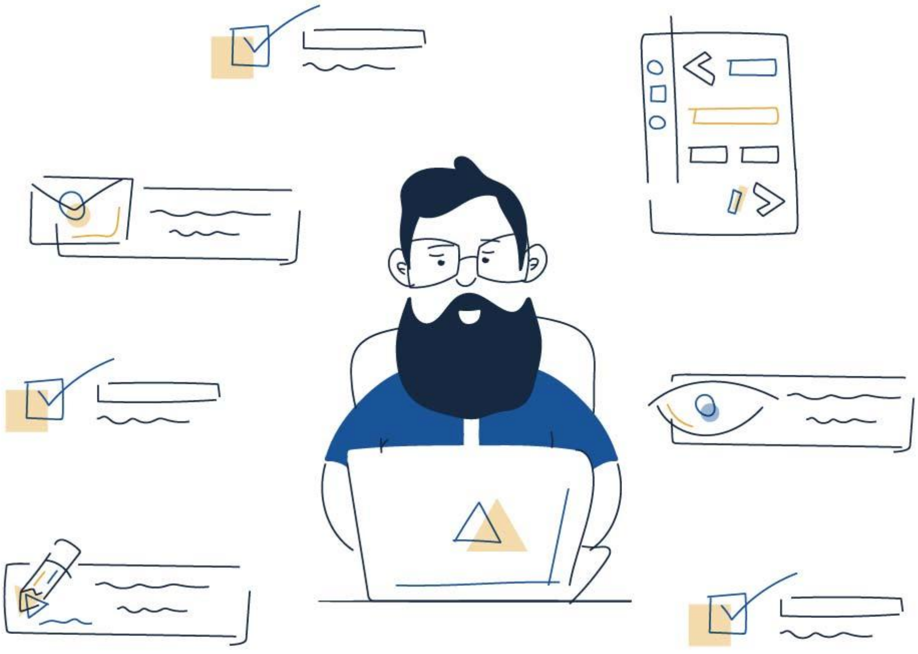


Illustration: User Rights Developers Need To Know

However, facilitating data subject rights requests can represent something of a burden for a business. In this chapter, you'll be learning how to reduce this burden by **being prepared** and having the **right systems** in place.

Data Subject Rights

These are the eight data subject rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Right related to automated decision-making

Individuals can access their data subject rights simply by **contacting you** and making a coherent request.

Each of the data subjects right has **different rules** associated with it. However, there are certain conditions that are common to most of the rights:

- You must normally **comply** with any request
- You may **not** normally **charge** data subjects for exercising their rights
- You may ask for **ID**
- You must respond “**without undue delay**.” Normally, you have a maximum of **one calendar month** to respond. A further two-month extension can apply in complex cases

You’ll notice there is a “**normally**” in some of the points above. Like with practically everything in the GDPR, there are exceptions. We’ll look at these towards the end of this chapter.

The Role of Data Processors

Data subject rights are largely a **data controller’s** responsibility. A **data processor** must not respond directly to data subjects who have made a request. The sections of the GDPR are addressed to data controllers.

However, data processors still play an **important role** when it comes to data subject rights. For instance, they are required to:

- **Inform** data controllers if they have received a request (allowing the controller to respond)
- **Assist** the data controller in retrieving, modifying or erasing the relevant personal data

Data processors should also:

- Develop data processing systems in such a way that data subjects and/or data controllers can control personal data (**front end**)
- Ensure that their databases and systems maintain personal data in such a way that it can be easily accessed or modified when required (**back end**)

Dealing with Data Subject Rights

Your users could be in contact at any moment to **request copies** of, **delete**, or **make amendments** to, their personal data. This should keep your data processing practices in check.

There are two ways to significantly reduce the amount of work you'll have to in relation to data subjects rights requests:

1. Collect and store as little personal data as possible
2. Have your users do the work themselves.

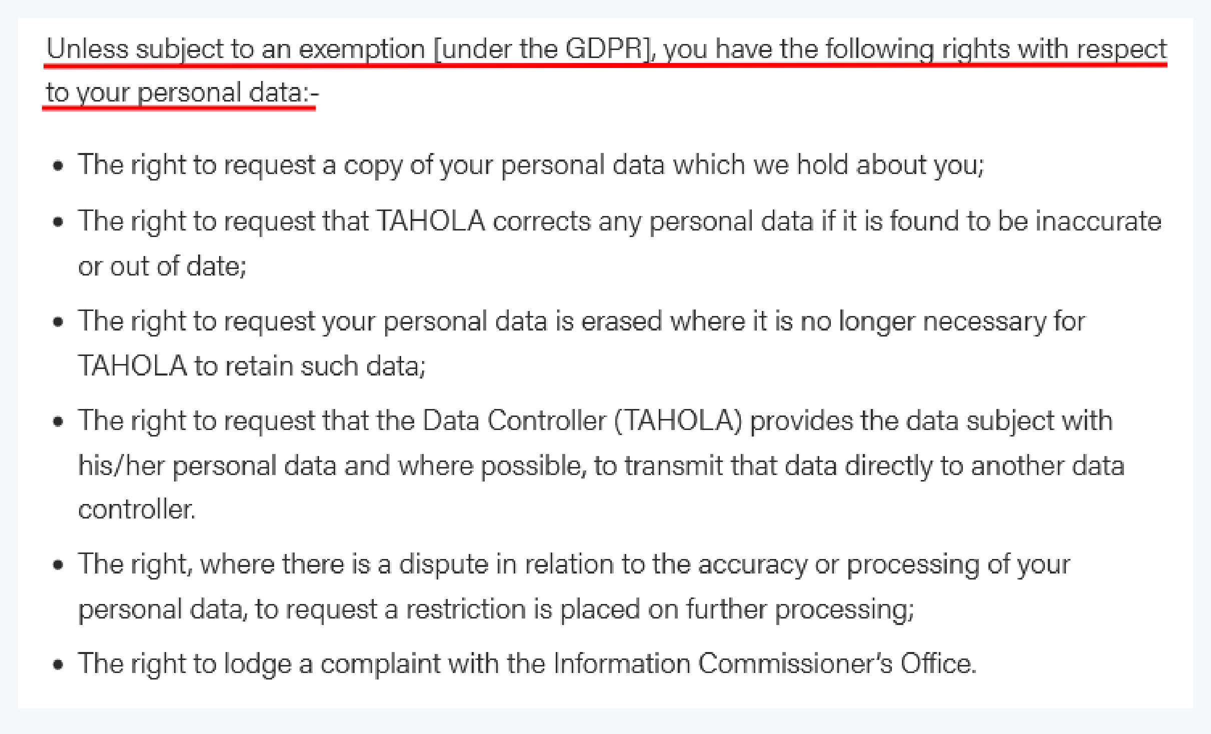
"Catch All" Approaches

We're going to look at some specific solutions and considerations in relation to each data subject right. But first, it's worth noting that many companies provide a "**catch all**" method that allows data subjects to access most or all of their rights in one place.

Bare Minimum

The **bare minimum** you can do to allow individuals the opportunity to exercise their data subject rights is to **provide an email address** via which they can make requests. You must disclose this, along with details of the data subject rights, in your Privacy Policy.

Here's an example of this "bare minimum" approach from Tahola. First Tahola lists the data subject rights:

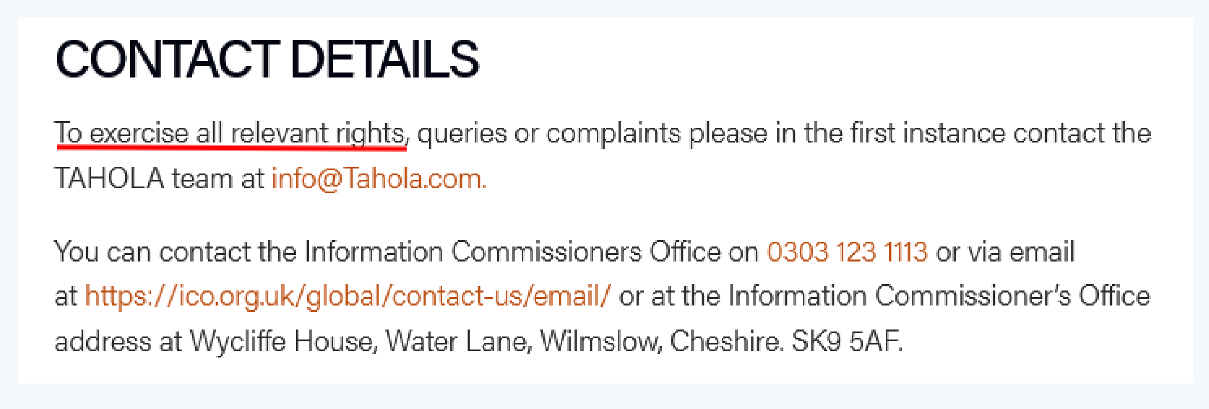


Unless subject to an exemption [under the GDPR], you have the following rights with respect to your personal data:-

- The right to request a copy of your personal data which we hold about you;
- The right to request that TAHOLA corrects any personal data if it is found to be inaccurate or out of date;
- The right to request your personal data is erased where it is no longer necessary for TAHOLA to retain such data;
- The right to request that the Data Controller (TAHOLA) provides the data subject with his/her personal data and where possible, to transmit that data directly to another data controller.
- The right, where there is a dispute in relation to the accuracy or processing of your personal data, to request a restriction is placed on further processing;
- The right to lodge a complaint with the Information Commissioner's Office.

Image: Tahola Privacy Policy: GDPR Rights clause

Then a contact email address is provided for those who wish to exercise their rights:



CONTACT DETAILS

To exercise all relevant rights, queries or complaints please in the first instance contact the TAHOLA team at info@Tahola.com.

You can contact the Information Commissioners Office on 0303 123 1113 or via email at https://ico.org.uk/global/contact-us/email/ or at the Information Commissioner's Office address at Wycliffe House, Water Lane, Wilmslow, Cheshire. SK9 5AF.

Image: Tahola Privacy Policy: Contact Details clause

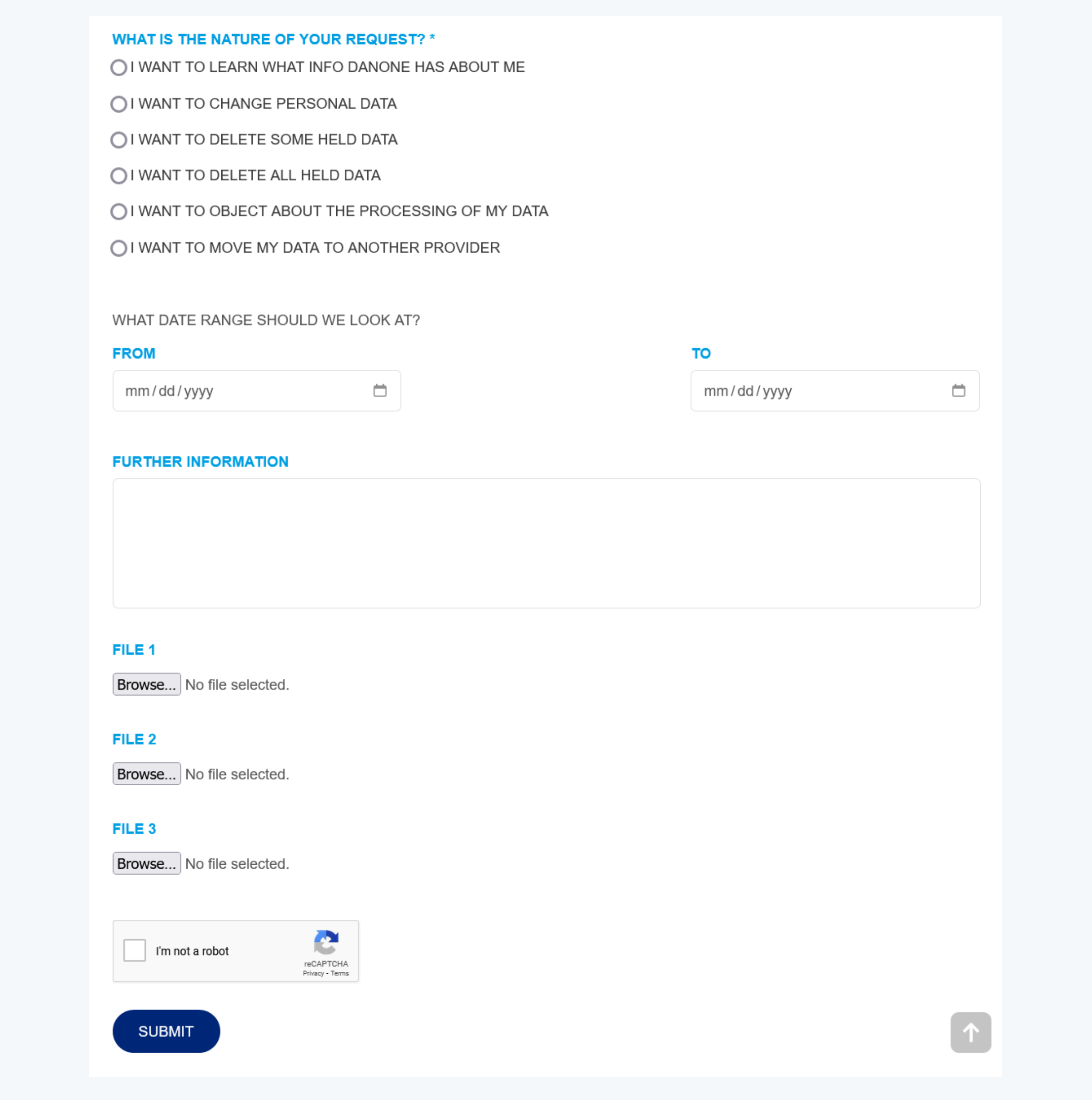
This is not an ideal solution from your users' perspective, and it's actually probably not going to be the most efficient method from your perspective, either.

Even if you're looking at other solutions, you should still let people know that they can email you if they want to make a data subject rights request. This ensures you're **covering all bases**.

Multi-purpose Form

You may sometimes receive illegible, confusing or invalid requests. You can reduce the possibility of this by asking people to make their requests in a **specific format**. This could save you a lot of back-and-forth with your users, and it also makes things easier from their perspective.

Here's Danone's "catch-all" solution. After an individual fills in their identity and contact details, they are presented with this **web form**:



WHAT IS THE NATURE OF YOUR REQUEST? *

○ I WANT TO LEARN WHAT INFO DANONE HAS ABOUT ME

○ I WANT TO CHANGE PERSONAL DATA

○ I WANT TO DELETE SOME HELD DATA

○ I WANT TO DELETE ALL HELD DATA

○ I WANT TO OBJECT ABOUT THE PROCESSING OF MY DATA

○ I WANT TO MOVE MY DATA TO ANOTHER PROVIDER

WHAT DATE RANGE SHOULD WE LOOK AT?

FROM

mm / dd / yyyy

TO

mm / dd / yyyy

FURTHER INFORMATION

FILE 1

Browse... No file selected.

FILE 2

Browse... No file selected.

FILE 3

Browse... No file selected.

□ I'm not a robot

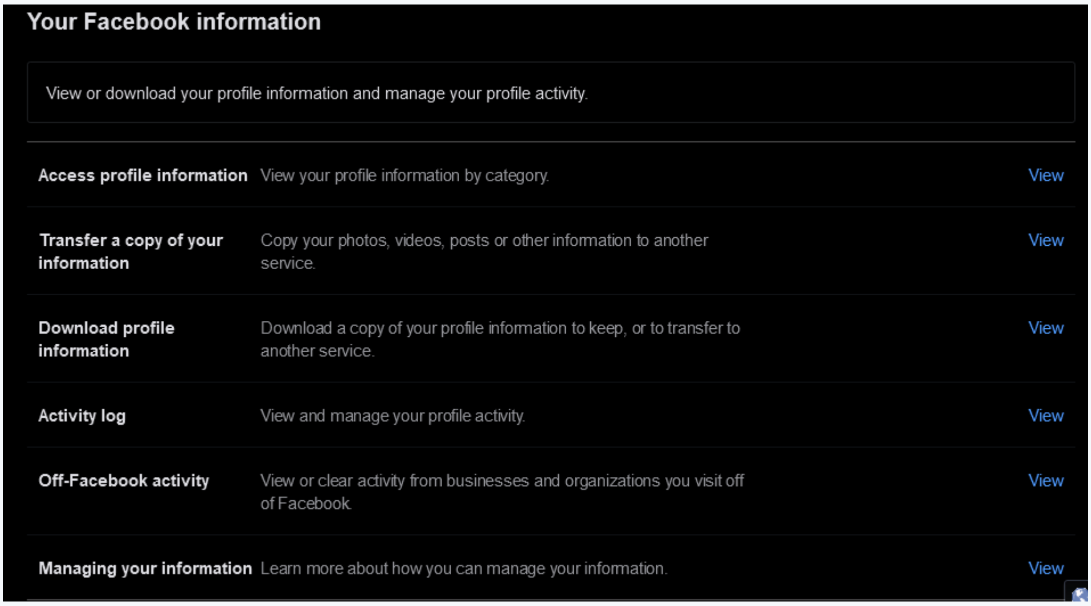
Image: Excerpt of Danone Data Subject Rights Request form

A form like this should help make sure you receive coherent, actionable data subject rights requests.

Privacy Dashboard

The ideal solution is to provide your users with **account controls** or a "privacy dashboard" that will allow them to access and modify personal data directly.

Facebook offers its use a range of account controls. Many of these correlate with the GDPR's data subject rights. Here's the "Your Facebook Information" screen in Facebook's settings:



Your Facebook information

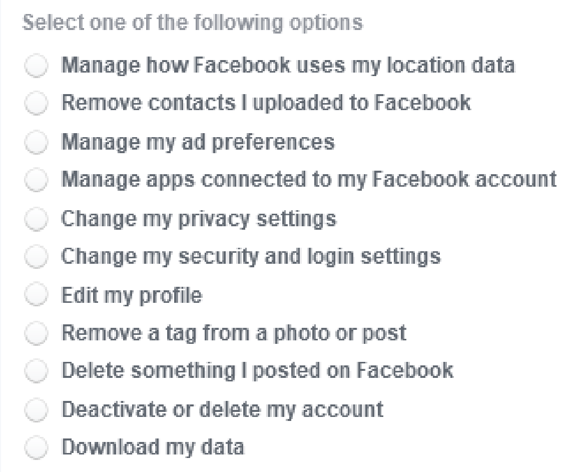
View or download your profile information and manage your profile activity.

Access profile information	View your profile information by category.	View
Transfer a copy of your information	Copy your photos, videos, posts or other information to another service.	View
Download profile information	Download a copy of your profile information to keep, or to transfer to another service.	View
Activity log	View and manage your profile activity.	View
Off-Facebook activity	View or clear activity from businesses and organizations you visit off of Facebook.	View
Managing your information	Learn more about how you can manage your information.	View

Image: Facebook: Your Facebook Information screen

These options allow users to directly exercise a number of their rights.

Choosing "Managing your information" leads to a series of other options, which satisfy other data subject rights:



Select one of the following options

○ Manage how Facebook uses my location data
○ Remove contacts I uploaded to Facebook
○ Manage my ad preferences
○ Manage apps connected to my Facebook account
○ Change my privacy settings
○ Change my security and login settings
○ Edit my profile
○ Remove a tag from a photo or post
○ Delete something I posted on Facebook
○ Deactivate or delete my account
○ Download my data

Image: Facebook Manage Data page: Options menu

For all of Facebook's controversies around privacy, this is a great example of how to hand personal data control to your users.

Bear in mind, however, that if you provide account controls to your users, you must **still respond** to requests from individuals who **do not have an account with your company**.

Let's take a look at some different considerations and approaches in respect of the individual data subject rights.

Right to Be Informed

The **right to be informed** is mostly a "passive" right - users do not have to do anything in order to invoke it. Ideally, everything a customer needs to know will be detailed in your **Privacy Policy**.

However, if anything is missing from your public-facing privacy information, or if users want a **greater level of detail** about how you treat personal data, they can make a request under the right to be informed.

If you're a **data controller**, your obligations under the right to be informed are to:

- Create a "concise, transparent, intelligible and easily accessible" **Privacy Policy** that provides comprehensive information about what personal data you process.
- Make sure this information is **made available** to individuals at key points (e.g. when you collect personal data from them, and when you communicate with them using that personal data).
- If you have obtained personal data from **another source**, provide the data subjects with all relevant information within one month (unless it would involve a disproportionate effort to do so).

Data processors must offer all requisite information to their data controllers, and be rigorous in their record-keeping.

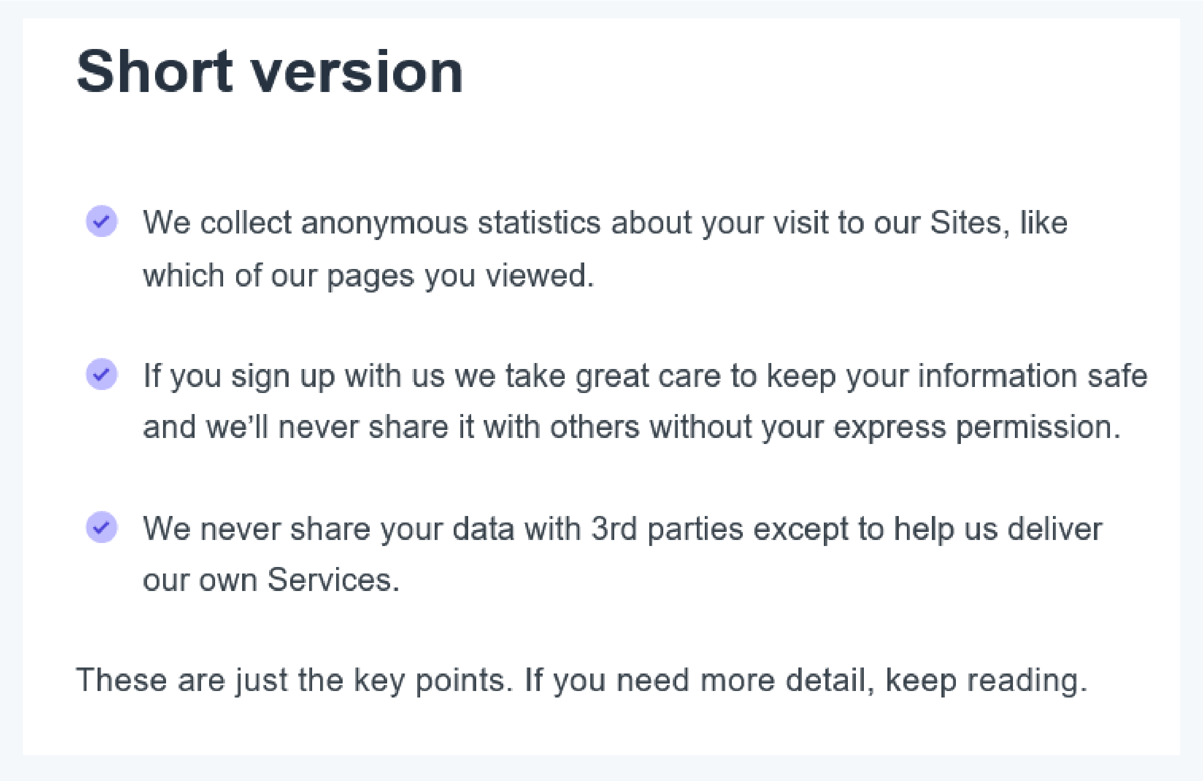
Fulfilling the Right to Be Informed

The Article 29 Working Party suggests taking a "**layered approach**" to providing individuals with privacy information. Consider all the different ways you can **provide** this information and how you can make it easy for individuals to **access** it.

You must ensure your Privacy Policy and all associated information is presented in "**clear and plain language**."

To help you achieve this, you can provide a **short version** of your Privacy Policy alongside the full version.

Here's how Silktide does this:



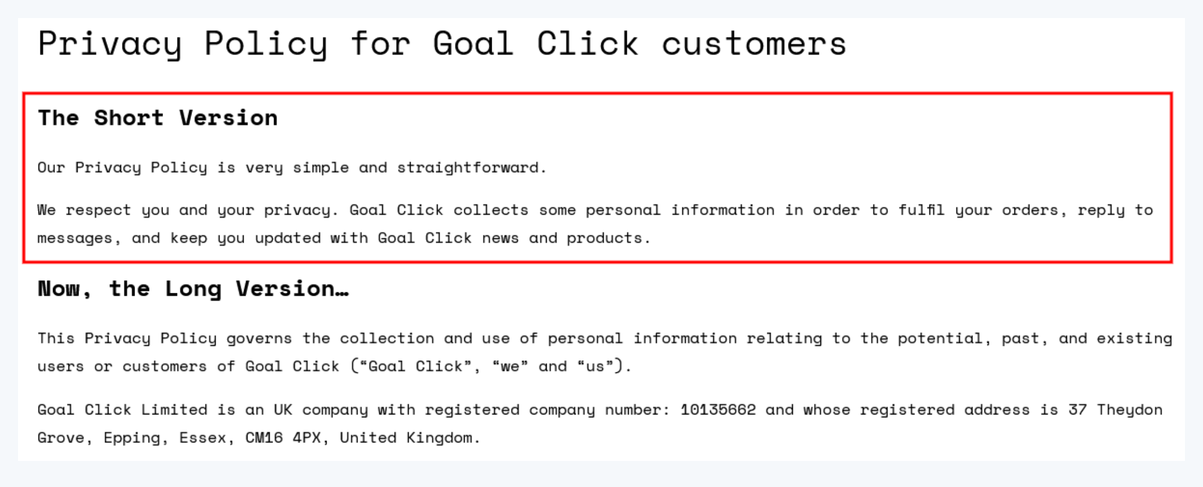
Short version

- ✓ We collect anonymous statistics about your visit to our Sites, like which of our pages you viewed.
- ✓ If you sign up with us we take great care to keep your information safe and we'll never share it with others without your express permission.
- ✓ We never share your data with 3rd parties except to help us deliver our own Services.

These are just the key points. If you need more detail, keep reading.

Image: Silktide Privacy Policy: Short version

And here's an example from Goal Click:



Privacy Policy for Goal Click customers

The Short Version

Our Privacy Policy is very simple and straightforward.

We respect you and your privacy. Goal Click collects some personal information in order to fulfil your orders, reply to messages, and keep you updated with Goal Click news and products.

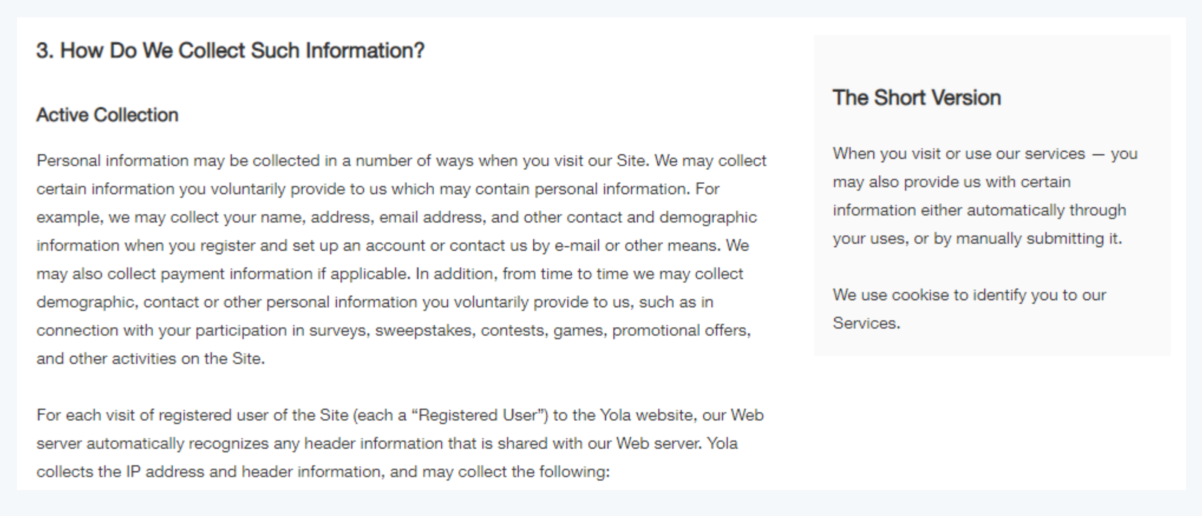
Now, the Long Version…

This Privacy Policy governs the collection and use of personal information relating to the potential, past, and existing users or customers of Goal Click ("Goal Click", "we" and "us").

Goal Click Limited is an UK company with registered company number: 10135662 and whose registered address is 37 Theydon Grove, Epping, Essex, CM16 4PX, United Kingdom.

Image: Goal Click Privacy Policy: Short Version highlighted

Yola provides a short summary of **each section** of its Privacy Policy alongside the full information:



3. How Do We Collect Such Information?

Active Collection

Personal information may be collected in a number of ways when you visit our Site. We may collect certain information you voluntarily provide to us which may contain personal information. For example, we may collect your name, address, email address, and other contact and demographic information when you register and set up an account or contact us by e-mail or other means. We may also collect payment information if applicable. In addition, from time to time we may collect demographic, contact or other personal information you voluntarily provide to us, such as in connection with your participation in surveys, sweepstakes, contests, games, promotional offers, and other activities on the Site.

For each visit of registered user of the Site (each a "Registered User") to the Yola website, our Web server automatically recognizes any header information that is shared with our Web server. Yola collects the IP address and header information, and may collect the following:

The Short Version

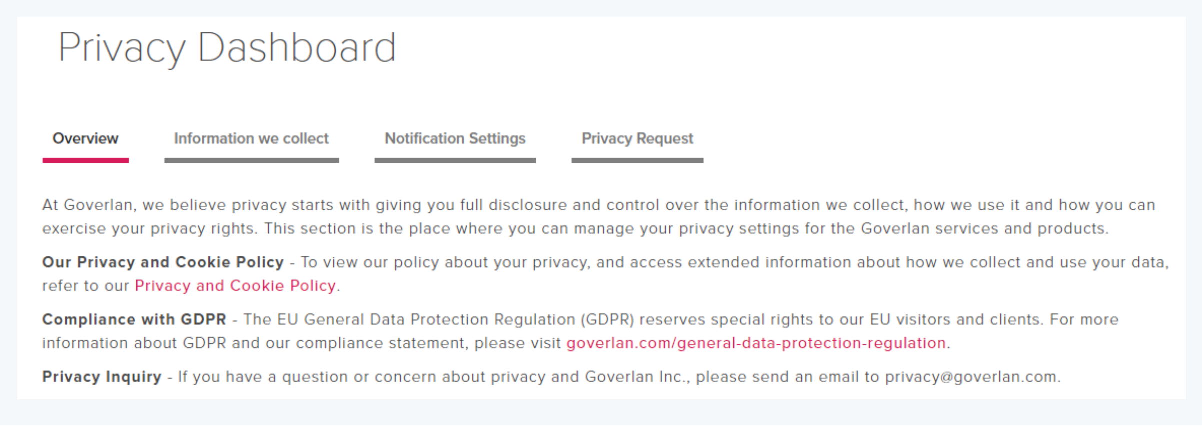
When you visit or use our services — you may also provide us with certain information either automatically through your uses, or by manually submitting it.

We use cookise to identify you to our Services.

Image: Yola Privacy Policy: How Do We Collect Such Information clause - Active Collection section with Short Version

You can make your Privacy Policy available alongside **account controls** and **contact details** in a "privacy dashboard." This is a good way to ensure all relevant information is available in one place.

Here's how Goverlan does this:



Privacy Dashboard

At Goverlan, we believe privacy starts with giving you full disclosure and control over the information we collect, how we use it and how you can exercise your privacy rights. This section is the place where you can manage your privacy settings for the Goverlan services and products.

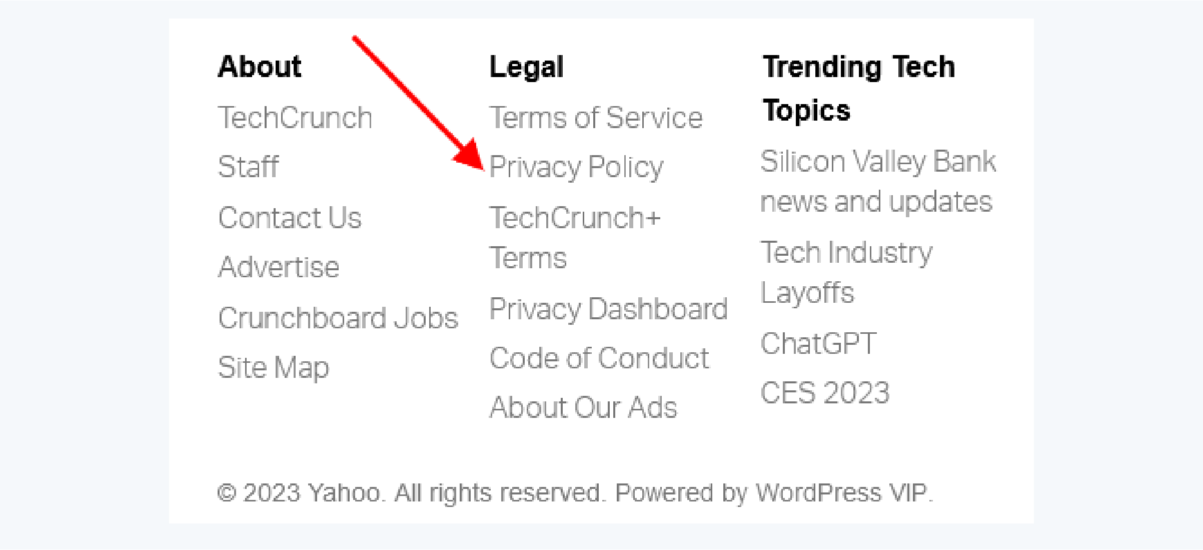
Our Privacy and Cookie Policy - To view our policy about your privacy, and access extended information about how we collect and use your data, refer to our Privacy and Cookie Policy.

Compliance with GDPR - The EU General Data Protection Regulation (GDPR) reserves special rights to our EU visitors and clients. For more information about GDPR and our compliance statement, please visit goverlan.com/general-data-protection-regulation.

Privacy Inquiry - If you have a question or concern about privacy and Goverlan Inc., please send an email to privacy@goverlan.com.

Image: Screenshot of Goverlan Privacy Dashboard

Your Privacy Policy could be present in a **footer** that persists across the pages of your website. Here's an example from TechCrunch:



About

TechCrunch

Staff

Contact Us

Advertise

Crunchboard Jobs

Site Map

Legal

Terms of Service

Privacy Policy

TechCrunch+ Terms

Privacy Dashboard

Code of Conduct

About Our Ads

Trending Tech Topics

Silicon Valley Bank news and updates

Tech Industry Layoffs

ChatGPT

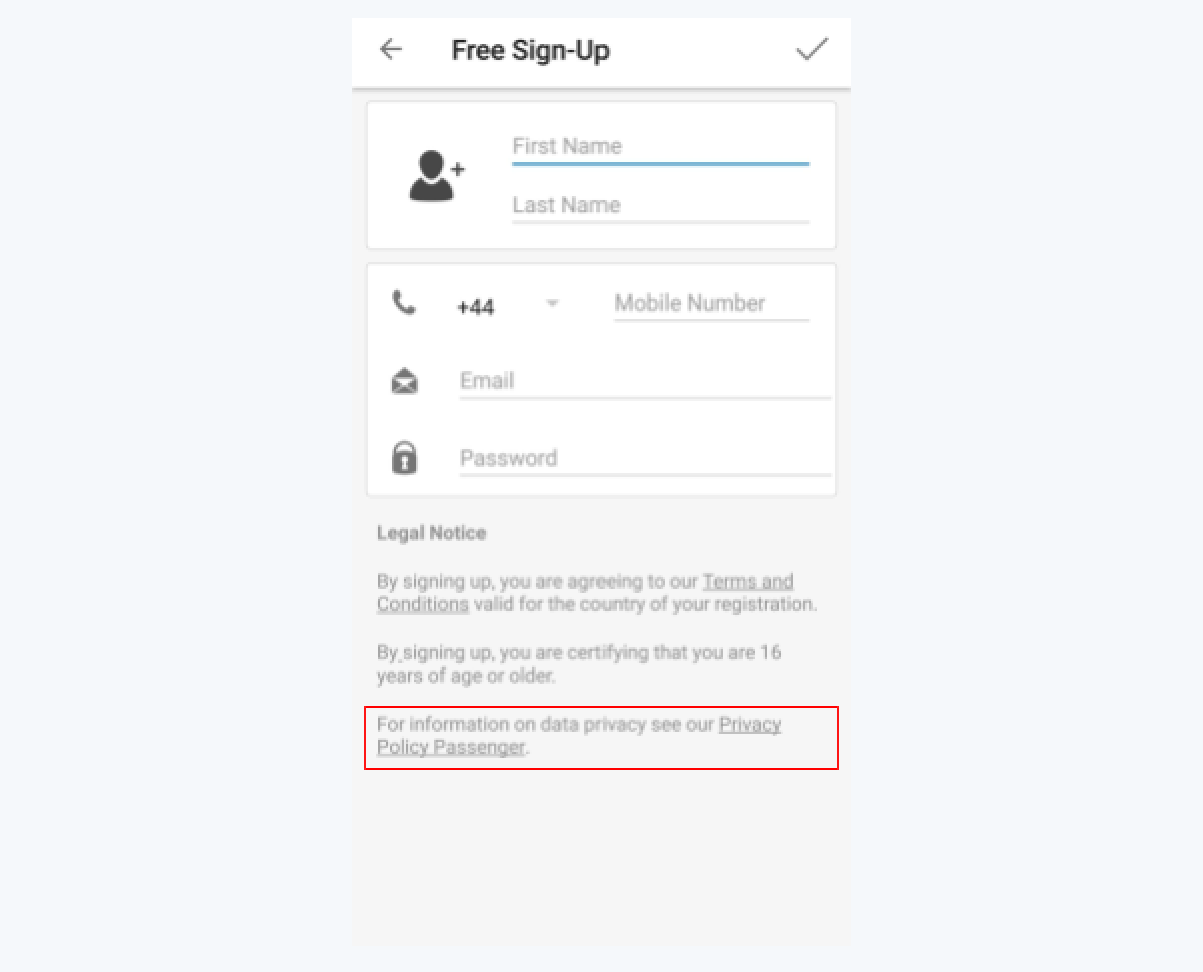
CES 2023

© 2023 Yahoo. All rights reserved. Powered by WordPress VIP.

Image: TechCrunch website footer with Privacy Policy link highlighted

You must also make sure your Privacy Policy is presented at key points when you **collect user data**.

For example, here's how a mobile app can provide a link to its Privacy Policy at **account creation** in its mobile app:



Legal Notice

By signing up, you are agreeing to our Terms and Conditions valid for the country of your registration.

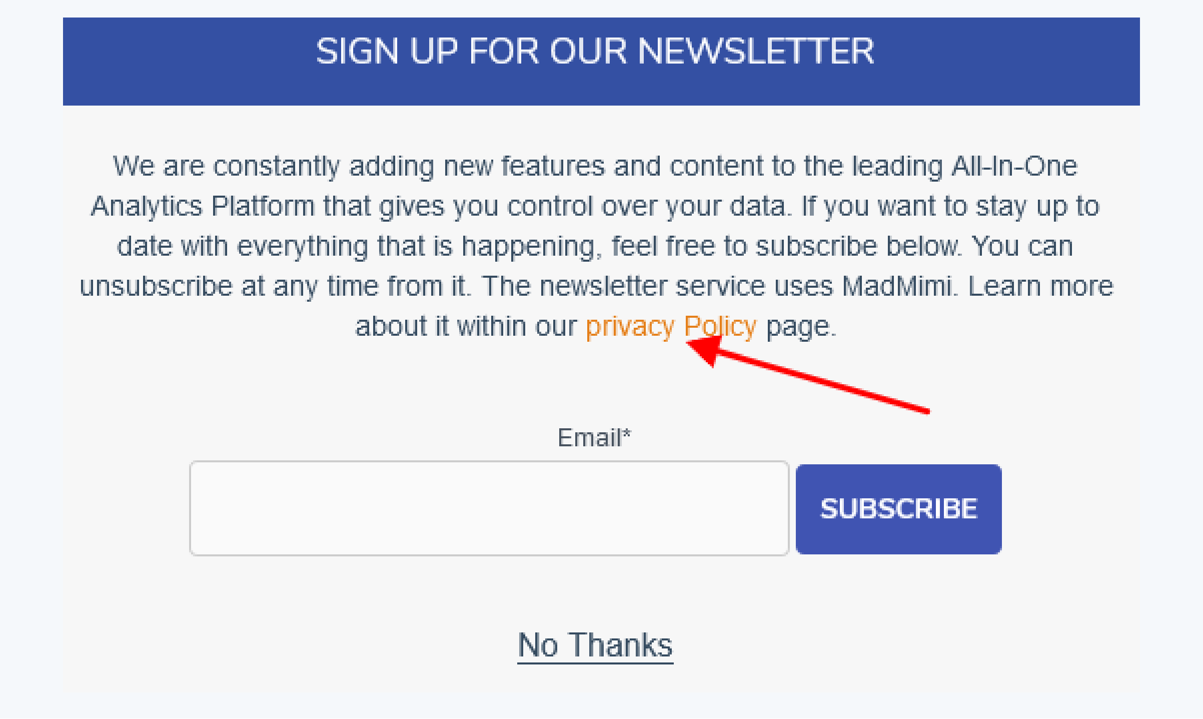
By signing up, you are certifying that you are 16 years of age or older.

For information on data privacy see our Privacy Policy Passenger.

Image: Mobile app sign-up screen with Privacy Policy link highlighted

You should present your Privacy Policy even when you're only asking for a **small amount** of personal data, such as when a user **signs up for your newsletter**.

Here's an example from Matomo:



SIGN UP FOR OUR NEWSLETTER

We are constantly adding new features and content to the leading All-In-One Analytics Platform that gives you control over your data. If you want to stay up to date with everything that is happening, feel free to subscribe below. You can unsubscribe at any time from it. The newsletter service uses MadMimi. Learn more about it within our privacy Policy page.

Image: Matomo sign up for newsletter pop-up with Privacy Policy link highlighted

Right of Access

The right of access requires you to provide users with a **copy** of **any personal data you hold on them**. This is probably the most commonly exercised of the data subject rights, and you should make sure it's a simple process for you and your users.

Failing to comply with a "subject access request" can lead to **big problems** for your company.

It's important to remember that the personal data amenable to subject access requests might not reside in **neatly arranged databases**.

The types of personal data you need to provide could include:

- Emails (including internal emails) that mention or could identify a person
- Log data
- Chat logs
- Phone records
- Access records (e.g. occasions on which a user logged into their account)

- Information associated with behavioral advertising
- Confirmation of whether or not you're processing a person's personal data

Here are some things to think about in respect of the right of access:

- Make sure you have **data minimization** locked down, so the amount of data you're required to provide users with is kept to a minimum.
- Conduct a **data audit** to ensure you know where customer data is "hiding."
- Consider using a **Content Services Platform** (CSP) if you keep voluminous records for each user. This can help you centralize access to all personal data associated with a given user.
- Ensure that everyone within your company can **recognize a subject access request**, and knows what to do when they receive one.

These considerations apply **equally** to data controllers and data processors.

Although data processors won't be providing personal data to a user directly, they must provide it to the data controller on demand.

Data processors must be aware that the controller has one month maximum to respond to the request, and this **includes** the time they spend communicating with the data processor. Flustering, delaying or providing incomplete records is an easily avoidable way for a data processor to lose clients.

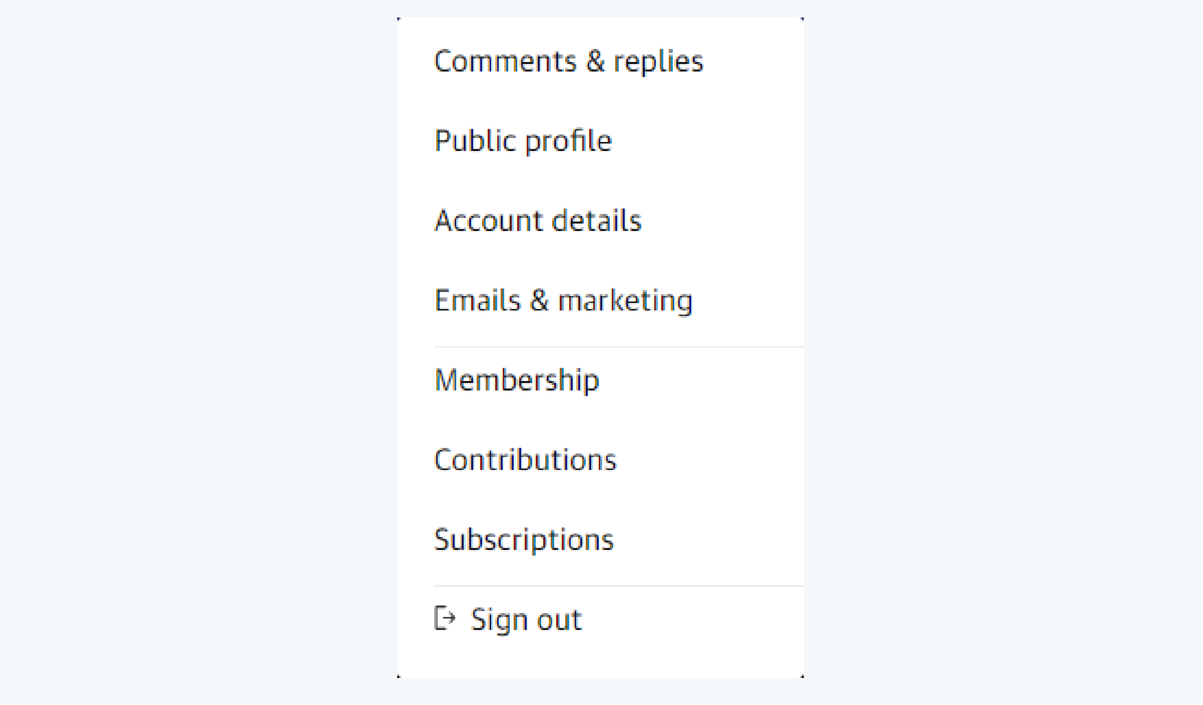
Facilitating Requests for Access

Where you *can* provide personal data to a user up-front, make it easy for them to **access it directly** via account controls. This should reduce the number of actual subject access requests you receive. This is a common feature for websites and apps which allow users to create an account.

Account controls will generally allow access to personal data that the user provided your company in the first place. It might include:

- Account details
- Contact details
- Post or comment history

You could offer a menu of options within an account that offers options, such as the following:



Comments & replies

Public profile

Account details

Emails & marketing

Membership

Contributions

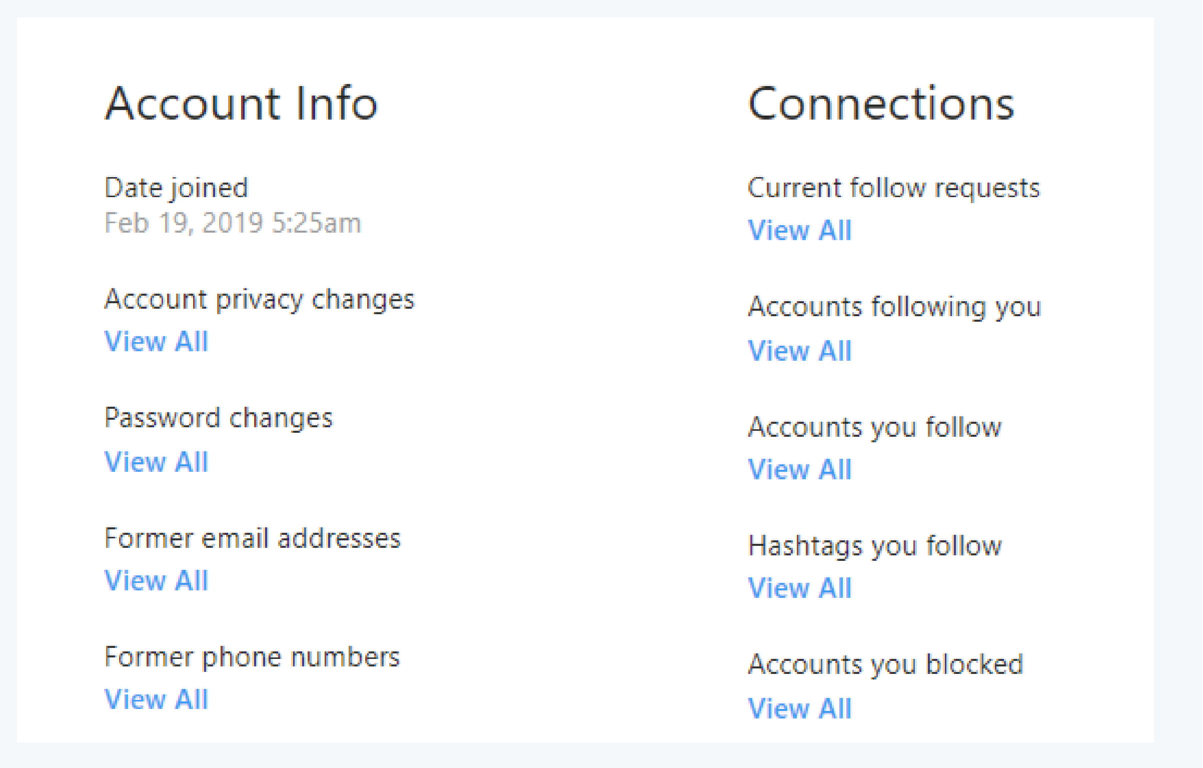
Subscriptions

Sign out

Image: Generic account menu options list

Any of this information could constitute personal data, and there is no reason not to give the user direct access to it.

Providing something like “Access Tool” can help give extensive, instant access to personal data associated with an account. Here’s some of the information a user could access:



Account Info

Date joined
Feb 19, 2019 5:25am

Account privacy changes
View All

Password changes
View All

Former email addresses
View All

Former phone numbers
View All

Connections

Current follow requests
View All

Accounts following you
View All

Accounts you follow
View All

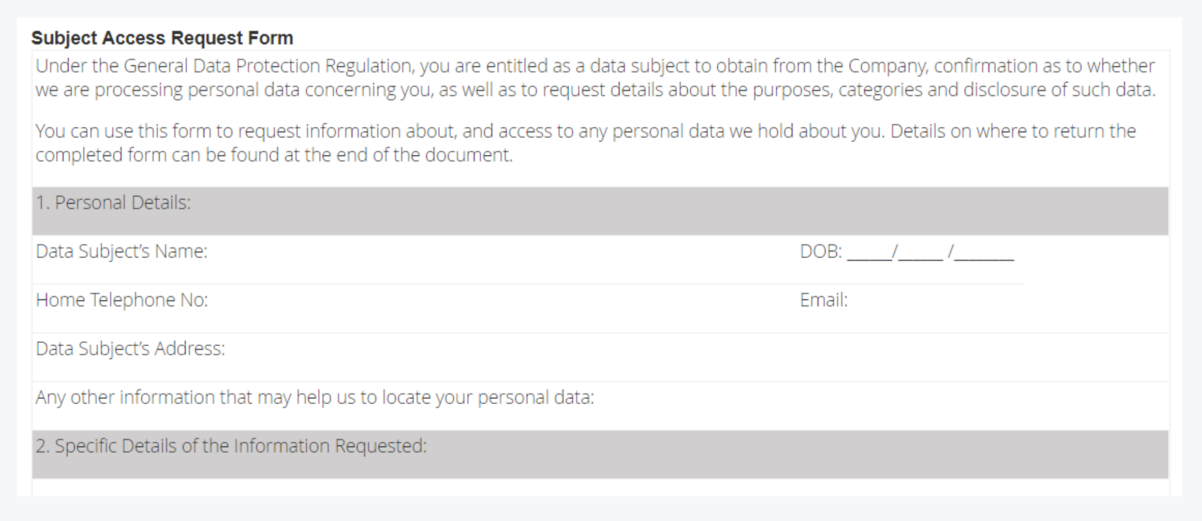
Hashtags you follow
View All

Accounts you blocked
View All

Image: Generic account info and connections options

Remember, though, that you still need a way to respond to subject access requests for **non-account holders**. Many organizations provide a **subject access request form** specifically for facilitating the right of access. This could be a secure web form, or a downloadable document that can be sent to you via email.

Here's an example:



Subject Access Request Form

Under the General Data Protection Regulation, you are entitled as a data subject to obtain from the Company, confirmation as to whether we are processing personal data concerning you, as well as to request details about the purposes, categories and disclosure of such data.

You can use this form to request information about, and access to any personal data we hold about you. Details on where to return the completed form can be found at the end of the document.

1. Personal Details:

Data Subject's Name: DOB: ____/____/_____

Home Telephone No: Email:

Data Subject's Address:

Any other information that may help us to locate your personal data:

2. Specific Details of the Information Requested:

Image: Generic Subject Access Request Form

Right to Rectification

The right to rectification allows individuals to request that any **inaccurate data** held on them is corrected. This is in accordance with the GDPR's principle of accuracy.

Allowing users to keep their personal data accurate and up-to-date works for everyone's benefit. It can even reduce the likelihood of a **data breach** occurring. For example, having **mismatched contact details** on file can cause personal data to be sent to the wrong person.

The right of rectification is important in **ensuring confidentiality** and minimizing **unwanted contact**.

Here are some things to think about in respect of the right to rectification:

- The more personal data you collect, the more likely you are to be storing inaccurate personal data. This is relevant to the principle of **data minimization**.
- The older the data is, the more likely it is to be inaccurate. People move house, get new email addresses, they could change their name, title, or gender identity. This is one of many reasons to ensure you comply with the principle of **storage limitation**.
- Depending on the context of your business, a **Customer Relationship Management** system can be particularly helpful in allowing your users to take ownership over their personal data.

You're responsible for communicating the changes to any **third parties** with whom you have shared the personal data. This is particularly important for data controllers working with data processors, but it could also apply to **data processors** working with **subprocessors**.

You don't **have** to change personal data if you are certain that the personal data is correct. You must justify your decision and let the individual know why you have come to this decision.

Facilitating Requests for Rectification

Again, your obligations under the right to rectification can be partly met by user **account controls**.

Let's look at an example from Pinterest. A simple "edit" icon is included as part of the main profile page:

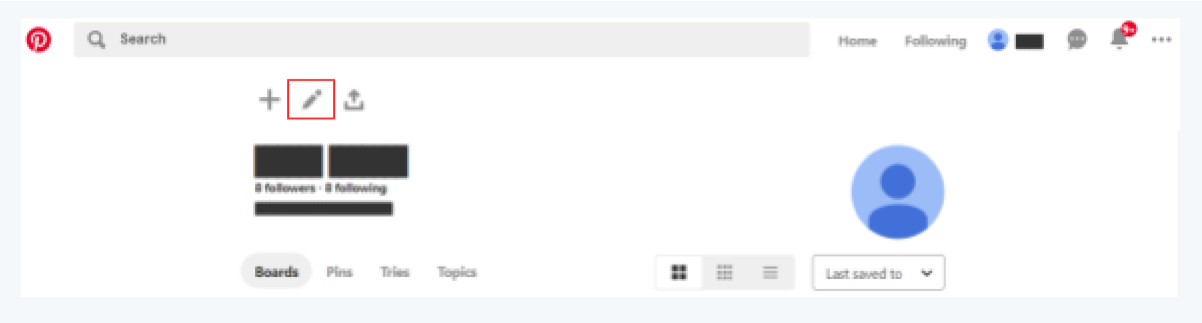
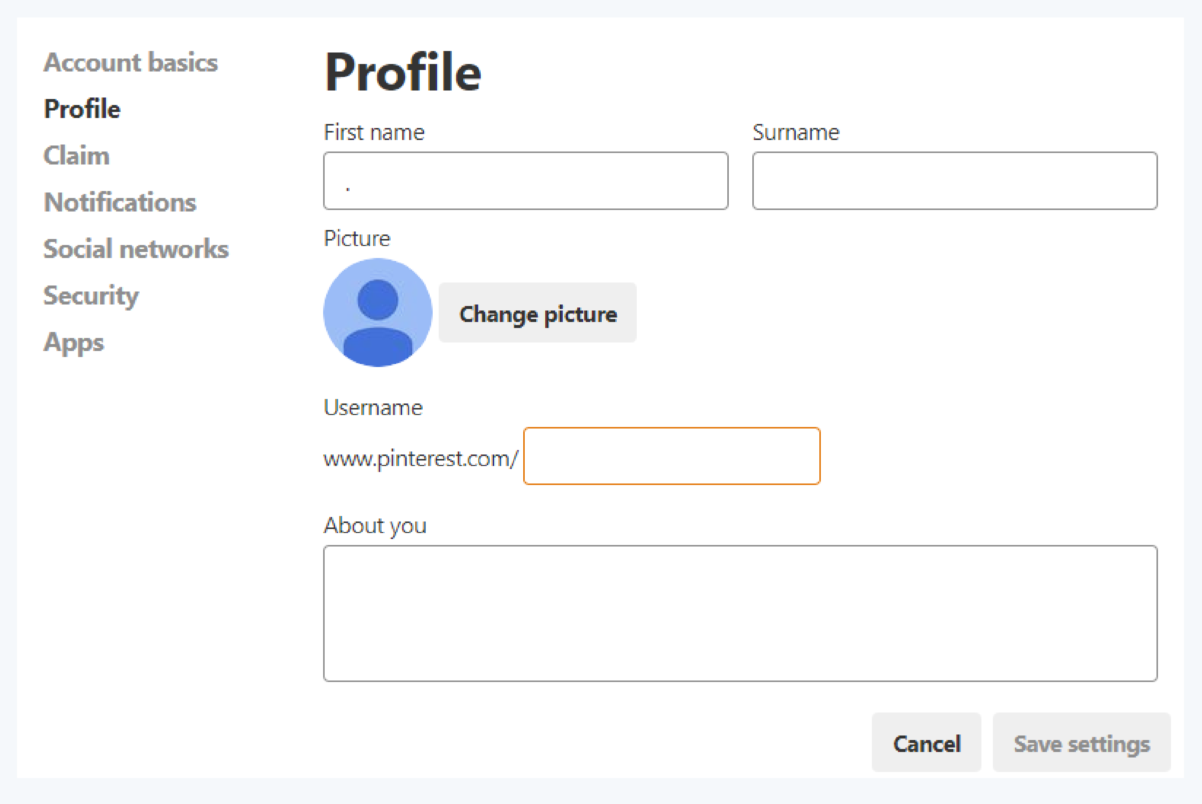


Image: Pinterest Profile page with Edit option highlighted

Clicking on this icon directs users to an **account overview**, where they can change personal details associated with their account:



Account basics
Profile
Claim
Notifications
Social networks
Security
Apps

Profile

First name: .

Surname:

Picture

Change picture

Username

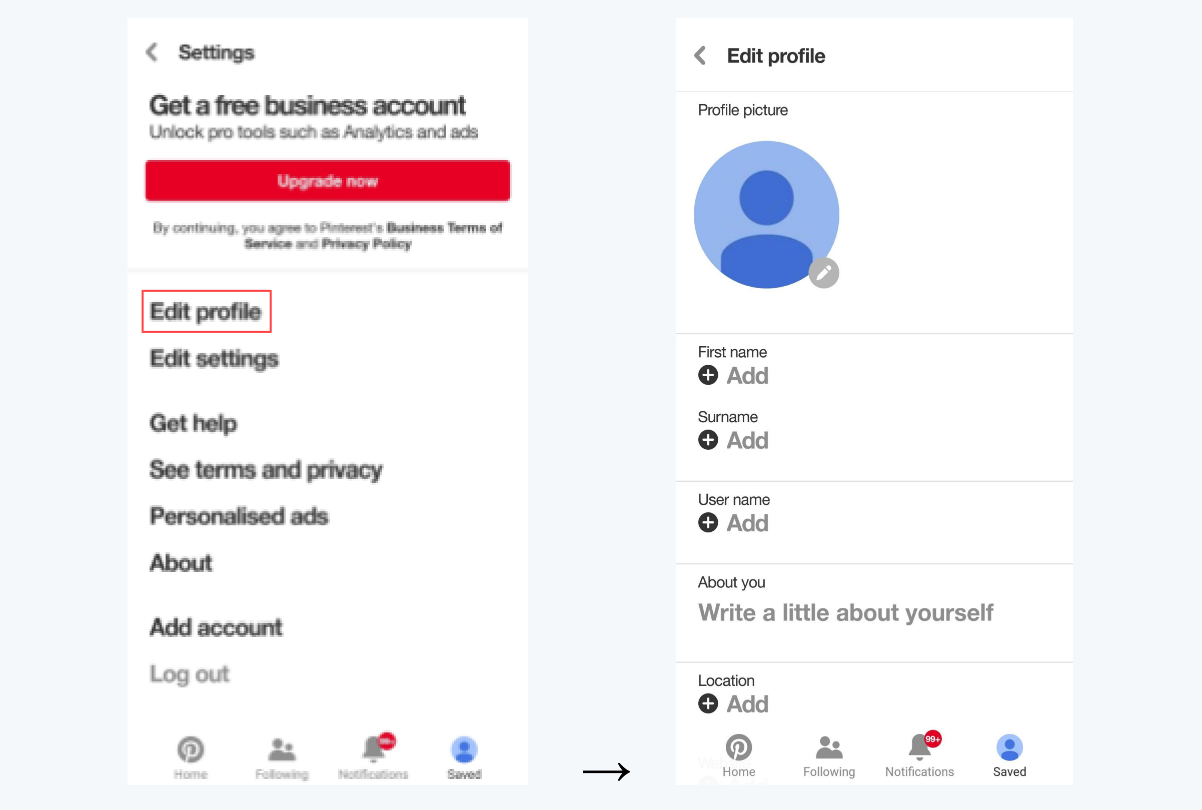
www.pinterest.com/

About you

Cancel
Save settings

Image: Pinterest edit profile page

And here's how this looks in the Pinterest mobile app. First, the settings menu. Then, the "Edit profile" screen itself after clicking:



Settings

Get a free business account
Unlock pro tools such as Analytics and ads

Upgrade now

By continuing, you agree to Pinterest's **Business Terms of Service** and **Privacy Policy**

Edit profile
Edit settings
Get help
See terms and privacy
Personalised ads
About
Add account
Log out

Home Following Notifications Saved

Edit profile

Profile picture

First name: Add

Surname: Add

User name: Add

About you: Write a little about yourself

Location: Add

Home Following Notifications Saved

Image on the left: Pinterest app Settings menu with Edit profile link highlighted
Image on the right: Pinterest Edit profile screen

Pinterest collects only very basic user information, but you can extend this principle as far as is appropriate for your users.

Right to Erasure

The **right to erasure** is also known as the "**right to be forgotten**." It ties in closely with the principle of storage limitation.

People have a right to request that you **delete any personal data** you are holding on them. But this is not an absolute right.

Rather than listing the exceptions to the right to erasure, it's actually easier to list the situations in which you ***will*** need to comply.

You must comply with this request if one of the following applies:

- You're relying on the person's **consent** to store this personal data, and the individual wishes to withdraw their consent.
- You're relying on **legitimate interests** to store this personal data, and the individual's interests in having the data deleted outweigh your interests in storing it.
- You're holding the personal data in connection with relation to direct marketing, and the individual has registered their **objection** to this.
- You collected or are using the personal data in an **unlawful** way.
- You don't **need** the personal data anymore for the purpose for which you collected it.
- The person has a **legal right** to have the personal data erased.

You must be especially willing to comply with requests from **children** (or their guardians), or in relation to personal data that was collected from an individual when they were a child.

The GDPR protects your right to **freedom of speech**. You don't always have to erase personal data in the public domain simply because a person doesn't like what you have written about them.

Here are some things to think about in respect of the right to erasure:

- You should make a habit of deleting data that is no longer necessary. This is relevant to the principle of **storage limitation**.
- If you're asked to erase personal data, you must also erase **backups** of that data.
- In your initial response to the individual, you must ensure that they **understand the implications** of their request (without trying to dissuade them).
- When complying with a request for erasure, it isn't normally enough to simply **archive** the personal data. Identifiers must be **completely overwritten** where possible.

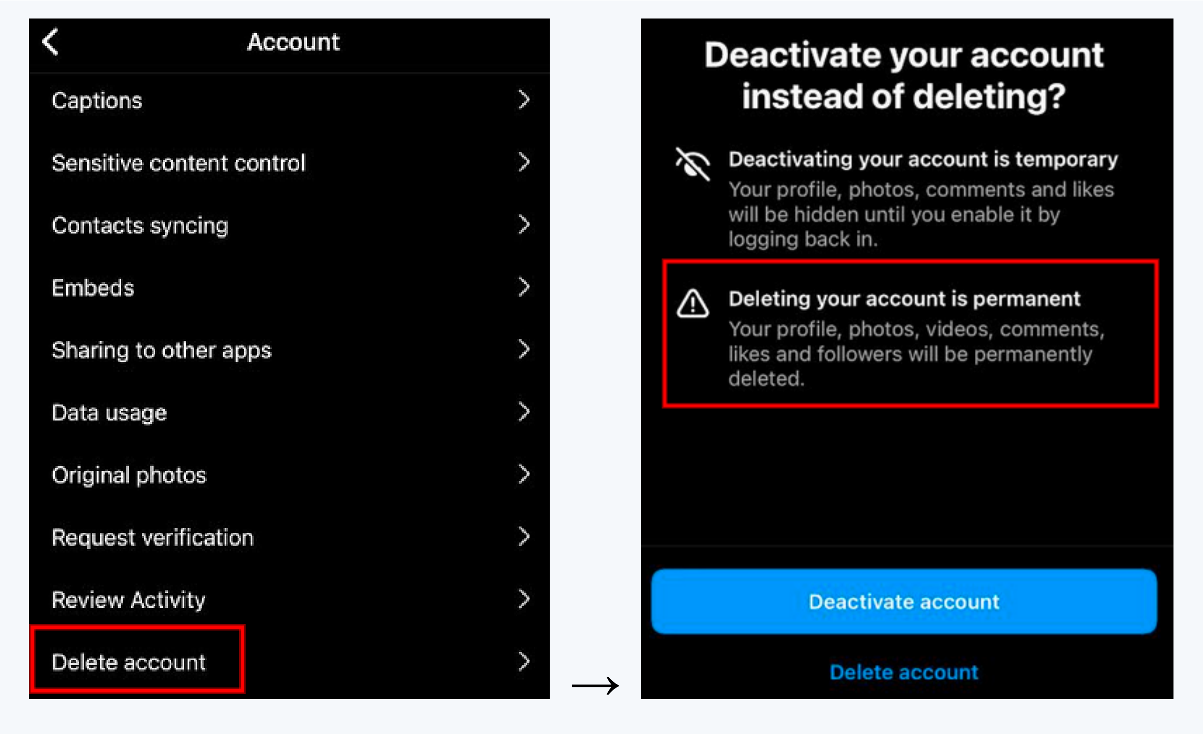
- If you genuinely cannot delete personal data following an erasure request, for example because it would require you to delete an entire batch including other personal data, for you must do your best to put it **beyond use**. This may mean that you have to resort to a form of archiving.

Facilitating Requests for Erasure

If you allow users to create an account, you should make it as **easy as possible** for them to delete it.

It can be painful to lose customers in this way. But if people are not allowed to erase their personal data easily, they may become **frustrated** and **suspicious**.

This can be as simple as offering a link in a menu that lets the user delete the account:



Deactivate your account instead of deleting?

Deactivating your account is temporary
Your profile, photos, comments and likes will be hidden until you enable it by logging back in.

Deleting your account is permanent
Your profile, photos, videos, comments, likes and followers will be permanently deleted.

Image on the left: Instagram Account menu with Delete account highlighted
Image on the right: Instagram Delete or Deactivate account screen

If you're going to ask users to give a **reason** for deleting their account, then you must include an "other" or "rather not say" option. Individuals **do not need to justify** their decision to exercise their data subject rights.

You should explain briefly what will happen when the account is deleted. Adding an option to simply deactivate the account may help with customer retention.

Right to Restrict Processing

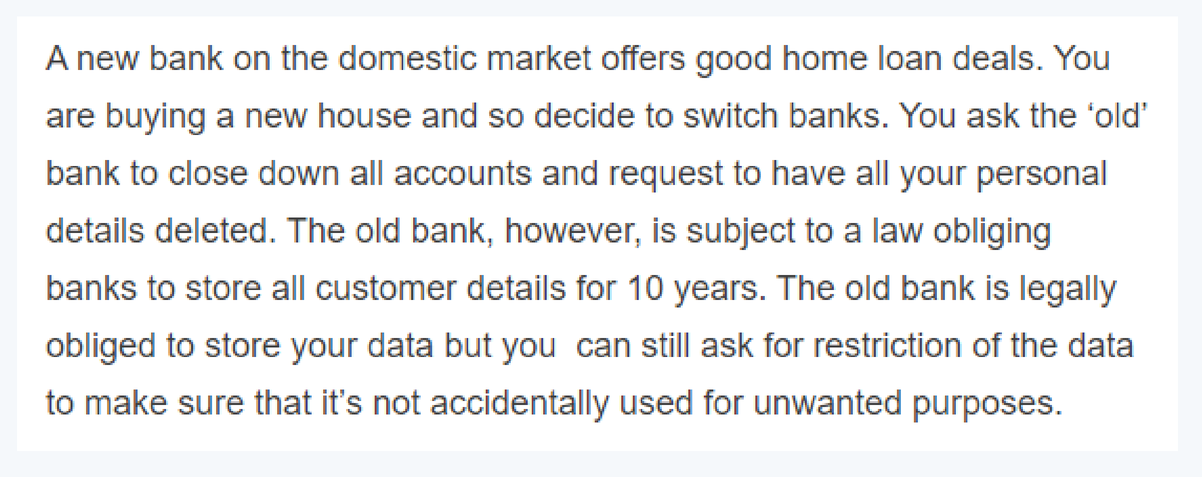
The right to **restrict processing** allows individuals to limit how you process their personal data. Restricted personal data can still be stored, but cannot be processed in any other way.

Personal data might also be “restricted” if a user has asked to exercise their right to erasure or rectification, and you’re waiting for them to provide ID. This puts processing **on pause**.

Here are some things to consider in respect of the right to restrict processing:

- You need to have a way to **distinguish** personal data that has been restricted. You could have a **separate**, **inactive system** for storing restricted personal data.
- Develop a way to render restricted personal data **inaccessible** to users, and only accessible to certain staff in your company.
- You may need to temporarily **take content down** from your website. Consider the measures you can take to secure this data in the meantime.

The European Commission provides the following example of when a restriction of processing would be appropriate:



A new bank on the domestic market offers good home loan deals. You are buying a new house and so decide to switch banks. You ask the ‘old’ bank to close down all accounts and request to have all your personal details deleted. The old bank, however, is subject to a law obliging banks to store all customer details for 10 years. The old bank is legally obliged to store your data but you can still ask for restriction of the data to make sure that it’s not accidentally used for unwanted purposes.

Image: European Commission: When should I exercise my right to restriction of processing of my personal data - Bank example

Facilitating Requests for Restriction of Processing

The right to restrict processing is somewhat obscure for most people’s purposes. If you get requests for restriction of processing, these are likely to be part of a **wider request** involving other rights.

However, there are contexts in which you will want to provide an **easy way** for your users to exercise this right. It is possible to build this functionality into the front end of a website or app.

Right to Data Portability

The right to **data portability** allows individuals to take true ownership of their personal data. To comply with a request for data portability, you must offer the users a copy of their personal data in a **well-organized, commonly used format**, so they can transfer it to another data controller if they choose to do so. You should even try to **carry out this transfer** yourself if they ask you to.

The right to data portability is closely linked to the right of access, but there are key differences:

	Right of access	**Right to data portability**
Source of personal data	Can apply to personal data received from any source.	Only applies to personal data received directly from the user.
Type of personal data	All personal data.	Excludes paper files.
Format of personal data	No restrictions, except that the personal data must be provided in a "commonly used electronic form" when the request has been made by "electronic means" (e.g. via email or a web form).	Must be a "structured, commonly used and machine-readable format."
Legal bases	Applies by default under all legal bases.	Only applies where the personal data is being processed under consent or contract.

Table 4: Differences between the right to access and right to data portability

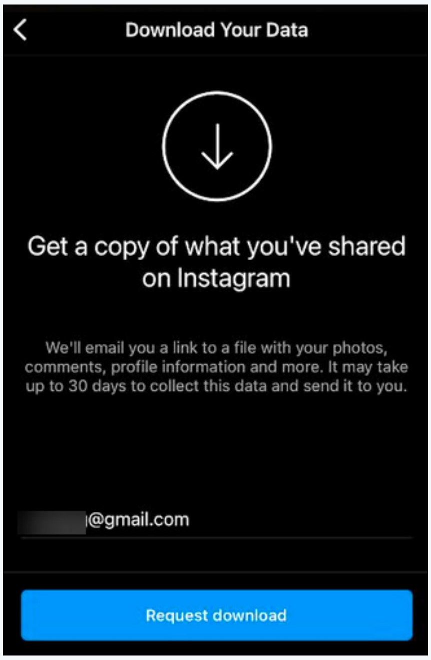
Here are some things to consider in respect of the right to data portability:

- You need to include **all personal data** in your possession that you've **collected directly** from the individual in question. This might include their:
    - Contact details
    - Account search history
    - Location data
    - Previous contact details
- You should supply this personal data in an **open file format** such as CSV, XML, or JSON.
- If a user requests that you **transfer** their personal data to **another data controller**, you should try to find a way of doing this. However, if it's not possible, you can **decline** this part of their request.

Facilitating Requests for Data Portability

Some social networks have set up **automated systems** that make it easy for them to fulfill a request for data portability.

Let's take a look at Instagram's method. Users can navigate to a "Your activity" menu with an option to "Download your information:"



Get a copy of what you've shared on Instagram

We'll email you a link to a file with your photos, comments, profile information and more. It may take up to 30 days to collect this data and send it to you.

[redacted]@gmail.com

Image: Instagram Download Your Data screen

After a short delay while the file is prepared, Instagram emails the user with the relevant information.

Right to Object

The **right to object** gives individuals a high degree of control over the ways in which their personal data is processed. Individuals can request you to **stop** processing their personal data in a particular way.

Technically speaking, the right to object is used to object to processing carried out on the grounds of **legitimate interests** and **public tasks**. However, **practically** speaking, it's also helpful to consider the **withdrawal of consent as** an objection to processing.

If an individual originally consented for you to process their personal data in a particular way, they may also **withdraw their consent** at any time. The "right to **withdraw consent**" is, in this context, analogous to the "right to **object**."

The right to object is mostly about **direct marketing**. There are other contexts in which the right to object can be invoked, and it can be helpful to think about the right to object in any areas where you're relying on consent.

The right to object to receiving direct marketing is **absolute**. If you're directly marketing to an individual, **regardless of your legal basis** for doing so, you must stop if requested.

Here are things to consider in respect of the right to object:

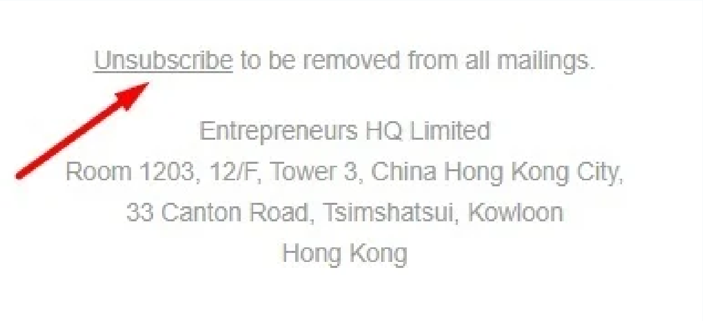
- At the point that you collect a user's personal data, you must **inform** them about any rights to object or withdraw consent.
- It's very important to refer to the rights to object or withdraw consent in your **Privacy Policy**.
- You should make **absolutely sure** you do **not** send marketing material, in any format, to anyone who has withdrawn consent or, if you're relying on legitimate interests, opted out.
- The right to object applies to all **non-essential cookies**, even where they aren't being used for ads. If you're going to refuse an objection, and persist in placing cookies on a user's device, then you must be able to demonstrate an **overriding legitimate interest**

Data processors, such as email marketing companies, play an important role here. They must provide their data controllers with an efficient way to alert them about any users who have objected to receiving marketing.

Facilitating Requests Under the Right to Object

Where you're relying on **legitimate interests**, it can sometimes be tricky to offer users an up-front way to exercise their right to object. But there is one context in which this is very simple, and absolutely crucial. You **must** include an **unsubscribe** link in all marketing emails.

Here's an unsubscribe link in an email from Entrepreneurs HQ:



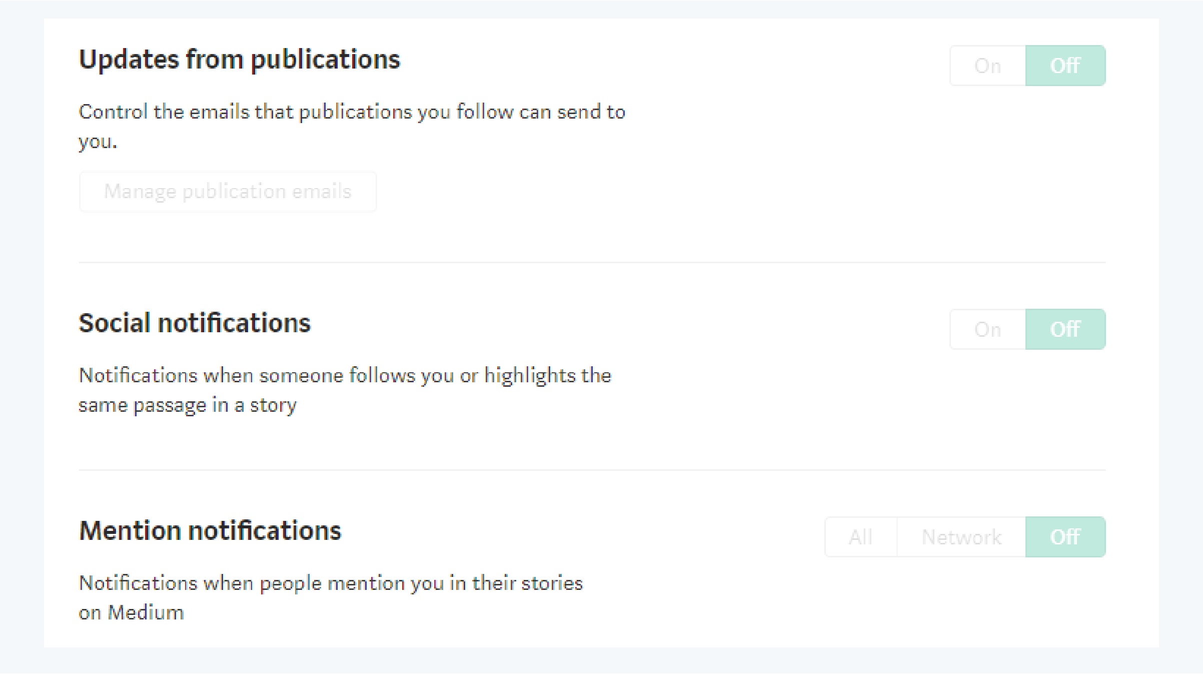
Unsubscribe to be removed from all mailings.

Entrepreneurs HQ Limited
Room 1203, 12/F, Tower 3, China Hong Kong City,
33 Canton Road, Tsimshatsui, Kowloon
Hong Kong

Image: Entrepreneurs HQ email footer with Unsubscribe link highlighted

You could also provide unsubscribe options for non-essential “**service**” or “**transactional**” emails.

For example, you can offer different email **notification** options like so:



Updates from publications

On [✓ Off]

Control the emails that publications you follow can send to you.

Social notifications

On [✓ Off]

Notifications when someone follows you or highlights the same passage in a story

Mention notifications

All Network [✓ Off]

Notifications when people mention you in their stories on Medium

Image: Medium notifications settings screen

This isn’t direct marketing, but it does involve the **processing** of **personal data**, and therefore might still be subject to a request under the right to **object**.

Rights Related to Automated Decision-Making and Profiling

The rights related to **automated decision-making and profiling** only apply in very particular circumstances. This is not within the scope of this book.

Individuals have a right not to be subject to purely automated decision-making in certain circumstances. You should check Article 22 of the GDPR and guidance from the ICO to see if this applies to your company.

Exceptions to the Rights

We’ve looked at how you can serve the needs of your users in relation to their data rights.

As a data controller, the default position should be that you **will** be required to facilitate data subject rights requests. But there are many reasons why you might **not** have to comply with a data subject rights request.

Whenever you refuse to comply with a request, you must **keep a record** of your decision. You must also inform the individual **in writing** of the reasons for your decision, and let them know that they have the right to make a complaint with a Data Protection Authority, or go to court.

Manifestly Unfounded or Excessive Requests

The GDPR recognizes that some data subject rights requests might be unreasonable, or "**manifestly unfounded or excessive**."

This exception can apply in respect of the rights of access, erasure, rectification, restriction of processing, data portability, and, **except** in the context of direct marketing, the right to object.

The UK Bar Council (an organization that regulates UK lawyers) suggests that you might consider the following factors when deciding whether a request is "manifestly unfounded or excessive":

- The **number** of repeat requests that have been made
- The **nature** of the personal data requested
- The **purpose** for which you're processing the personal data
- The **frequency** with which the personal data **changes** (for example, if the data has not changed between repeated access requests, you may be justified in not providing a copy of the same personal data several times)

If you decide that a request is unreasonable, you can:

- Charge a reasonable fee
- Refuse to carry out the request

You might also be justified in **exceeding the one-month deadline**, if trying to comply with such a request.

You must be able to **justify your decision** to refuse or charge for a request.

Legal Basis

If you're processing personal data on certain **lawful bases**, you may not be required to comply with certain data subject rights requests.

None of the rights are absolute on any legal basis, but here are some of the more straightforward exceptions, based on guidance from the ICO.

A tick indicates that you normally **will** need to comply, a cross indicates that you normally will **not** need to.

	Right to erasure	Right to data portability	Right to object
Consent	✓	✓	The data subject may withdraw their consent
Contract	✓	✓	Only applies in the context of direct marketing
Legal obligation	×	×	×
Vital interests	✓	×	×
Public task	×	×	✓
Legitimate interests	✓	×	Unless there remains an overriding legitimate interest for the processing

Table 5: Legal bases comparison with user rights

These exceptions make sense in context. For example:

- If you're required to share someone's personal data with the police, the individual cannot stop you from doing this (**legal obligation/right to object**)
- If a tax authority holds a person's name and address, they can't be asked to delete them (**public interest/right to erasure**)
- If a company has logged someone's contact details and correspondence in connection with the prevention of fraud, it wouldn't be appropriate to provide the person with a copy of this data in a portable format so that it can be transferred to another data controller (**legitimate interests/data portability**)

Exemptions

There are **certain situations** where one or more of the data subject rights will simply **not apply**. For example, a suspected criminal under the investigation of the police cannot be granted access to their file.

EU countries have all implemented their own **national data protection law**, based on the GDPR. Each has slightly different exemptions. For example, the UK's Data Protection Act 2018 restricts the data subject rights in certain contexts related to immigration control.

The exemptions are unlikely to be relevant for your purposes as a developer, but you should get to know the relevant national laws just in case.

Requesting ID

It’s fine to request that a person provides you with some form of ID before you carry out their request. If they don’t provide it, you might be justified in refusing the request.

You must be **reasonable in** your request for ID. Don’t be obstructive**.**

If you have asked a person for ID, the one month deadline period begins once you’ve received it.

Key Takeaways from This Chapter

The data subject rights are one of the most important aspects of the GDPR. It’s down to you to either **facilitate** (in the case of a data **controller**) or **help facilitate** (in the case of a data **processor**) these rights. There are serious consequences for companies who fail to do this.

- Be **transparent** about the data subject rights. Make people aware of their rights in your **Privacy Policy** and at **key points** when you collect their personal data.
- Be **ready** to comply. Make sure people in your company know what a data subject right request looks like.
- Make **sure** you are actually **required** to carry out a request before you do so.
- Provide **functions** within your website or app that allow a user (or data controller) to access their rights **directly**, so that they don’t need to contact you with this request.
- Remember that you may have to facilitate rights for **non-users**, too.

Chapter 8:

Principles of the GDPR for Developers

We've mentioned the principles of the GDPR a few times throughout the preceding chapters. It's important to recognize that these principles aren't abstract philosophical notions - they are **directly applicable** to your operations as a developer.

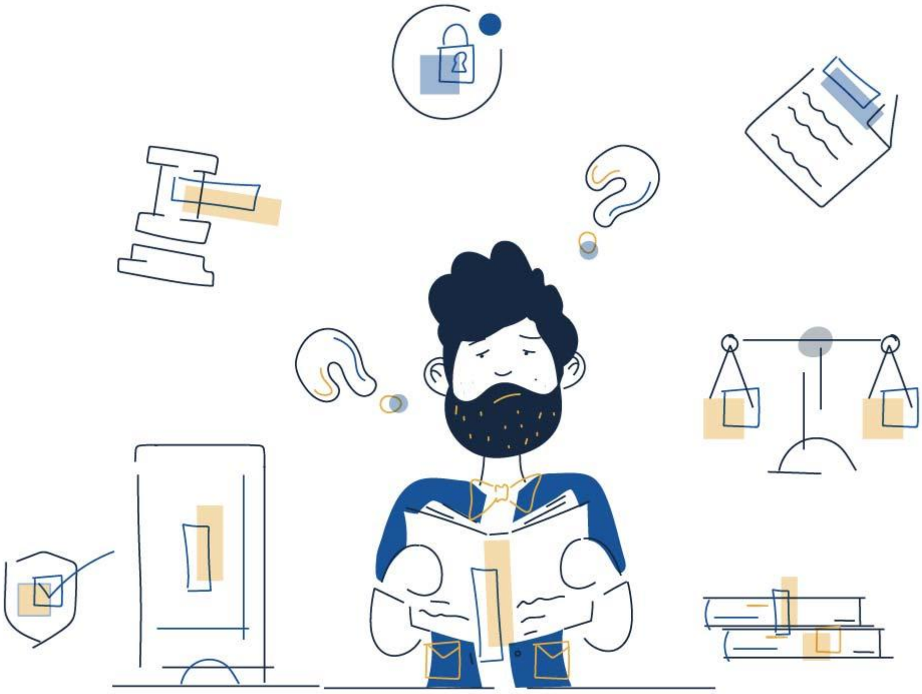


Illustration: Principles of the GDPR for Developers

Lawfulness, Fairness, and Transparency

The principle of “**lawfulness, fairness, and transparency**” requires that you:

- Always comply with the GDPR and any **other applicable laws**
- Process personal data in a way that people would **reasonably expect**
- Always be **honest** about your activities, and provide as much **information** as people need

Some practical steps you can take towards complying with this principle include:

- Creating a **Privacy Policy**
- Identifying and demonstrating your **legal basis** for every act of data processing
- Making sure you’re complying with **specific rules** around particular types of data and activities

Creating a Privacy Policy

Creating a **Privacy Policy** is essential wherever you’re acting as a data controller.

If you’ve developed an app or website, you’re almost certainly going to be acting as a data controller in respect of anyone using that app or website, even if your company’s primary role is as a data processor for other companies.

Your Privacy Policy will be **totally unique** to your circumstances, but there are some **mandatory sections** that every Privacy Policy must cover.

As we work through this chapter, we’ll be seeing how these mandatory Privacy Policy requirements tie in with the principles of the GDPR.

Demonstrating Your Legal Bases

We’ve looked closely at the two **legal bases** that are probably going to be most commonly relied upon for developers: **Consent** and **legitimate interests**.

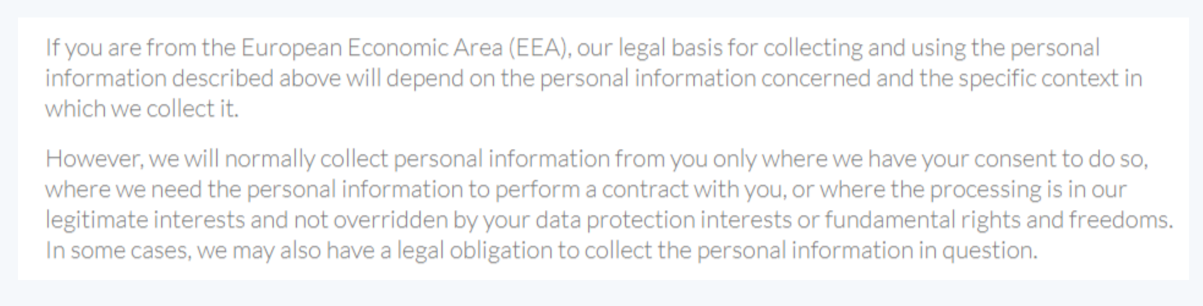
Consent and legitimate interests are the most relevant legal bases for operations that depend on **advertising**. If your app, software or service operates under a “paid” model -

either a one-off payment or a subscription, you may need to rely on the legal basis of "**contract**."
In any case, complying with the principle of fairness, lawfulness and transparency means determining your legal basis for ***every* act of processing** of personal data that you do, and **demonstrating** that you've done this in your Privacy Policy.

There are two approaches to providing this information in your Privacy Policy.

Firstly, there is a broad approach of simply **listing** the various legal bases on which you rely.

Here's an example of an approach you can take:



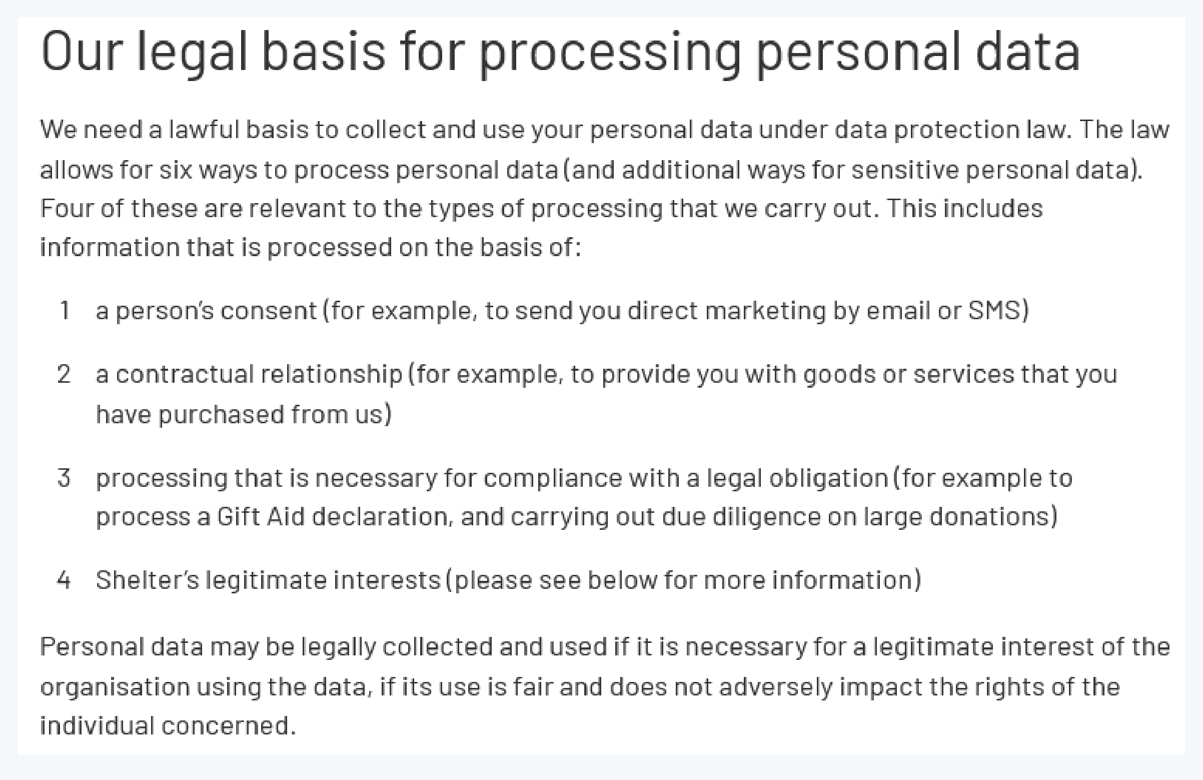
If you are from the European Economic Area (EEA), our legal basis for collecting and using the personal information described above will depend on the personal information concerned and the specific context in which we collect it.

However, we will normally collect personal information from you only where we have your consent to do so, where we need the personal information to perform a contract with you, or where the processing is in our legitimate interests and not overridden by your data protection interests or fundamental rights and freedoms. In some cases, we may also have a legal obligation to collect the personal information in question.

Image: Generic Privacy Policy: Legal basis clause

Secondly, there is a **more detailed** approach, wherein the ways in which you process personal data are listed alongside the legal basis that underpins this.

Here's an example from Shelter:



Our legal basis for processing personal data

We need a lawful basis to collect and use your personal data under data protection law. The law allows for six ways to process personal data (and additional ways for sensitive personal data). Four of these are relevant to the types of processing that we carry out. This includes information that is processed on the basis of:

1 a person's consent (for example, to send you direct marketing by email or SMS)

2 a contractual relationship (for example, to provide you with goods or services that you have purchased from us)

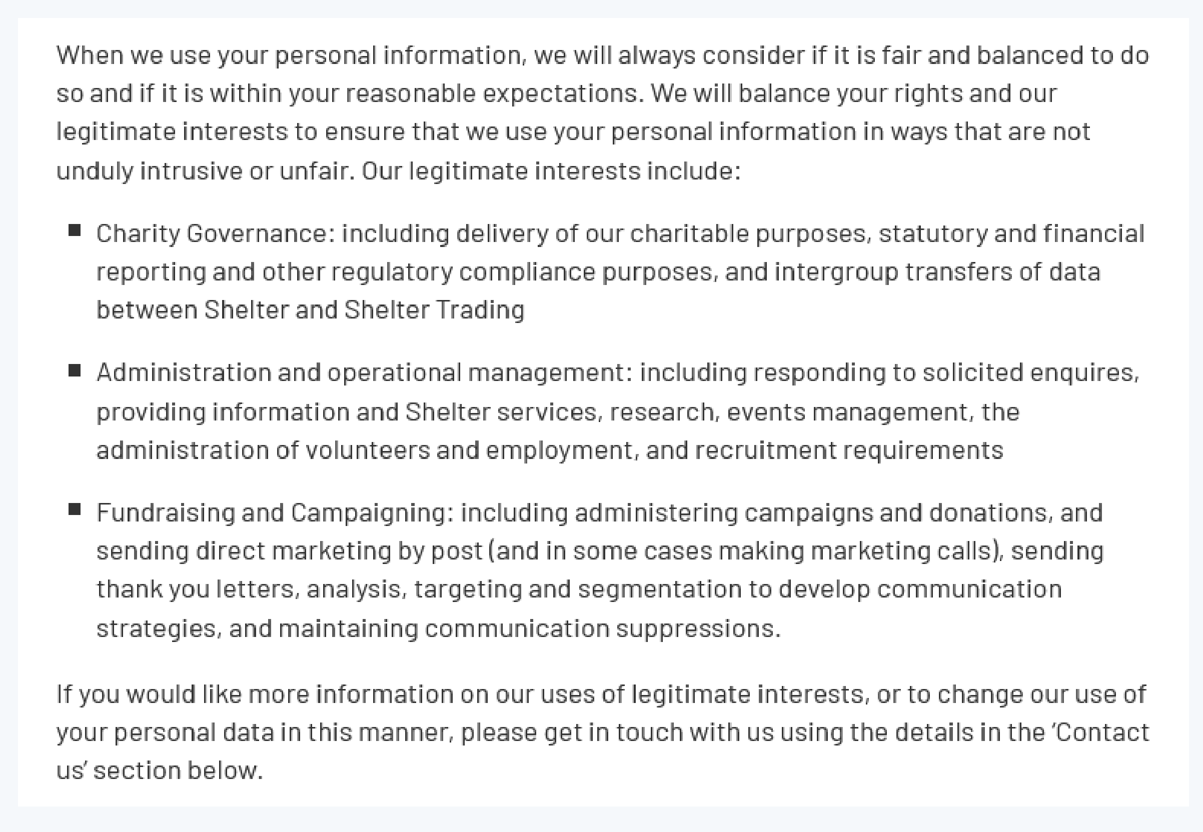
3 processing that is necessary for compliance with a legal obligation (for example to process a Gift Aid declaration, and carrying out due diligence on large donations)

4 Shelter's legitimate interests (please see below for more information)

Personal data may be legally collected and used if it is necessary for a legitimate interest of the organisation using the data, if its use is fair and does not adversely impact the rights of the individual concerned.

Image: Shelter Privacy Policy: Legal basis for processing personal data clause excerpt

Shelter then goes into more specific detail about its **legitimate interests** in processing personal data:



When we use your personal information, we will always consider if it is fair and balanced to do so and if it is within your reasonable expectations. We will balance your rights and our legitimate interests to ensure that we use your personal information in ways that are not unduly intrusive or unfair. Our legitimate interests include:

- Charity Governance: including delivery of our charitable purposes, statutory and financial reporting and other regulatory compliance purposes, and intergroup transfers of data between Shelter and Shelter Trading
- Administration and operational management: including responding to solicited enquires, providing information and Shelter services, research, events management, the administration of volunteers and employment, and recruitment requirements
- Fundraising and Campaigning: including administering campaigns and donations, and sending direct marketing by post (and in some cases making marketing calls), sending thank you letters, analysis, targeting and segmentation to develop communication strategies, and maintaining communication suppressions.

If you would like more information on our uses of legitimate interests, or to change our use of your personal data in this manner, please get in touch with us using the details in the 'Contact us' section below.

Image: Shelter Privacy Policy: Legal basis for processing personal data clause excerpt-2

Obeying Specific Rules and Other Data Protection Laws

The principle of lawfulness, fairness, and transparency requires that you obey **all relevant rules and laws** when processing personal data.

This book is all about **obeying the law**. The provisions of the GDPR are all important, and failing to comply with any one of them could result in serious problems. And you must also be aware of **other relevant laws** that may impose rules **over and above** those set out in the GDPR.

For example, under the GDPR, you may only process **health data** in accordance with special rules set out in Article 9 of the GDPR.

When processing health data, you may also need to obey **other laws**, such as the **Health Insurance Portability and Accountability Act** (HIPAA) in the United States.

And under Article 8 of the GDPR, there are special rules around processing the **personal data of children** in order to offer or provide them with online services. You must get the consent of their **parent or guardian**, and you must also take "**reasonable steps**" to confirm it was their parent or guardian that consented.

And in this context, you may also need to obey **other laws**, such as the ones noted earlier in the book:

- The Colorado Privacy Act (CPA)
- The Virginia Consumer Data Protection Act (VCDPA)
- The California Online Privacy Protection Act (CalOPPA)
- The California Consumer Privacy Act (CCPA) and its amendments known as the California Privacy Rights Act (CPRA).
- Personal Information Protection and Electronic Documents Act (PIPEDA) in Canada
- The Enhancing Privacy Protection Act (Privacy Act) in Australia
- Several Southeast Asian countries
- The Children's Online Privacy Protection Act (COPPA) in the United States

These are just some of the many rules that may or may not apply to your project. Reading this book means that you've made a great start towards legal compliance. But you should also **read the GDPR itself**, and be aware of **other local laws**.

Purpose Limitation

The principle of "**purpose limitation**" means that you only process personal data when you have a **specific purpose** for doing so.

Some practical steps you can take towards complying with this principle include:

- **Reviewing** all your data processing methods and **determining your purpose** for each one
- **Demonstrating** your purposes to your users wherever you **collect** their personal data
- Ensuring that you don't collect personal data for **one purpose** and then use it for incompatible **further purposes**

Reviewing Your Purposes

An essential part of GDPR compliance involves becoming aware of *what* personal data you're processing. But in addition to *what* you're processing, you also need to consider *why* you're processing it.

You can apply the principle of purpose limitation to each method of personal data processing you engage in.

Consider:

- **Why** do you need to process personal data in this way?
- Is this a **good enough** purpose to justify the processing?
- How do your users **know** what your purposes are?

Demonstrating Your Purposes

There are three key ways you can go about demonstrating your purposes to your **users**, and your **Data Protection Authority** (if you ever need to do so).

You should disclose your purposes in:

1. Your **Privacy Policy**
2. **Information** you provide when **collecting** personal data
3. Your **data processing records**

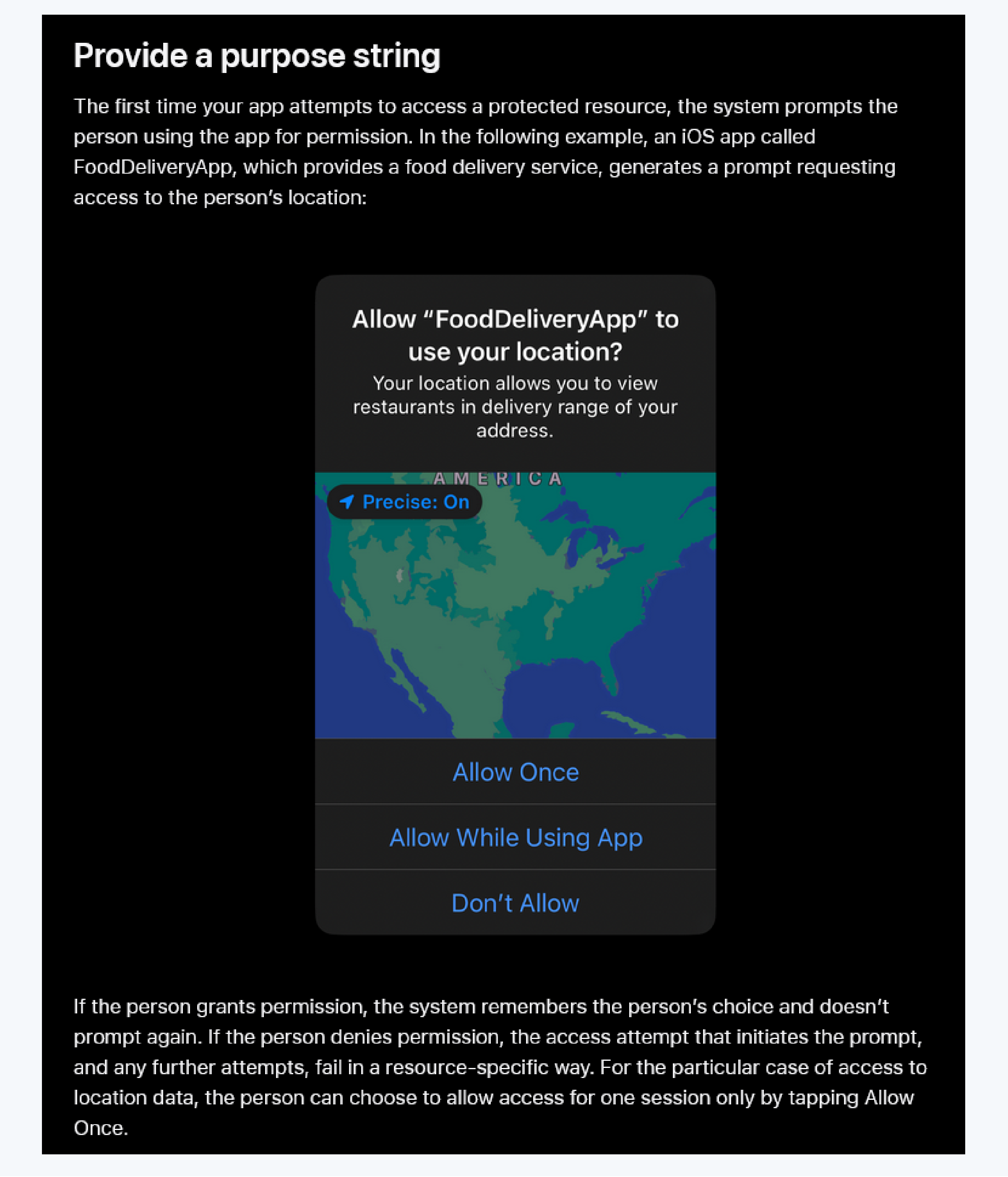
When **collecting personal data**, it's important to tell your users about the purpose for which you require it. If people understand **why** you need to collect their personal data, they'll be **more likely** to provide it.

This is evident in the context of **mobile app development**. Users are more likely to grant permission for an app to access their personal data if they know that the app requires such access for a **good reason**.

This was confirmed in a 2014 study by Lin et al, which revealed that:

> "*a user's willingness to grant a given permission to a given mobile app is strongly influenced by the purpose associated with such a permission.*"

In iOS, developers can add a **purpose string** to accompany their permission requests. This is explained by Apple in its guidance for developers:



Provide a purpose string

The first time your app attempts to access a protected resource, the system prompts the person using the app for permission. In the following example, an iOS app called FoodDeliveryApp, which provides a food delivery service, generates a prompt requesting access to the person's location:

Allow "FoodDeliveryApp" to use your location?

Your location allows you to view restaurants in delivery range of your address.

If the person grants permission, the system remembers the person's choice and doesn't prompt again. If the person denies permission, the access attempt that initiates the prompt, and any further attempts, fail in a resource-specific way. For the particular case of access to location data, the person can choose to allow access for one session only by tapping Allow Once.

Image: Apple Developer Guide: Requesting Access to Protected Resources - Provide a purpose string section

Avoiding "Purpose Creep"

Where personal data is collected for a **specific purpose**, it must not be used for any **further purposes** that are "incompatible" with the purposes for which you collected it.

There are some types of "**further processing**" that will be considered **compatible by default**:

- **Archiving** in the public interest
- Scientific or historical **research**
- Certain **statistical** purposes

Recital 50 of the GDPR suggests that the following factors should be taken into account when assessing whether further processing will be **compatible** with your original purpose:

- The **nature** of the personal data
- The data subject's **reasonable expectations**
- Any **safeguards** you can take to protect privacy

Data Minimization

The principle of "**data minimization"** requires that you **only** collect the personal data that you actually **need** - no more, no less.

Web and software developers are at the forefront of applying this principle. Systems developed to collect and process personal data must have **data minimization** built into their functioning.

Developers who are integrating such systems into their websites and software must ensure that the optional collection of personal data is **"off" by default**.

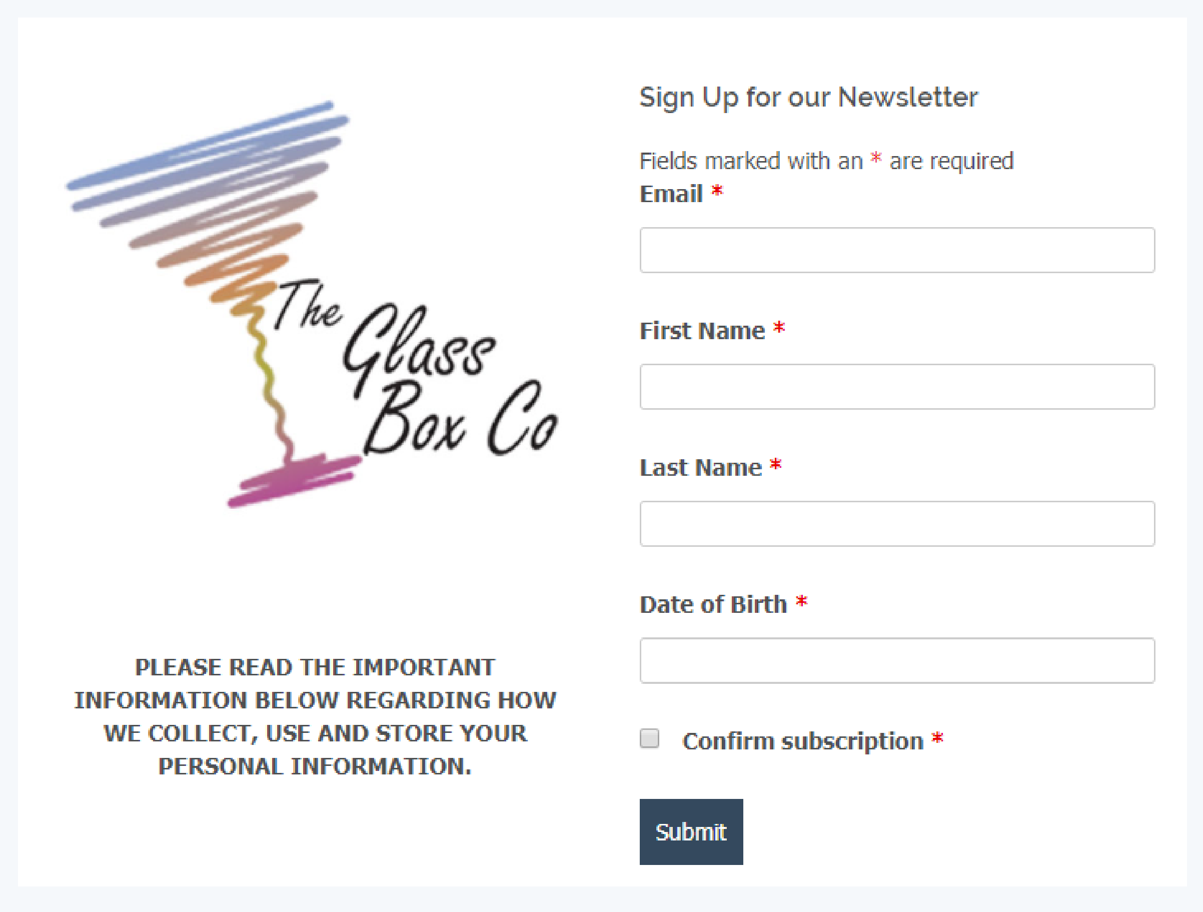
Some practical steps you can take towards complying with this principle include:

- Never asking your users to **provide** personal data unless you **need** it
- Ensuring that you are not collecting personal data in **server logs** (unless you need to)
- Ensuring that you are not unnecessarily harvesting personal data via **web analytics**

Minimizing Data Collection in Web Forms

Most of the personal data you collect is probably going to be **provided directly** by your users. You must only ask for what you need. This ties in closely with the principle of **purpose limitation**. "Necessary" can be interpreted quite broadly, to mean necessary to achieve a specific purpose.

Let's look at an example. Ecommerce company The Glass Box Co provides a **monthly newsletter**. Here's the sign-up form:



Sign Up for our Newsletter

Fields marked with an * are required

Email *

First Name *

Last Name *

Date of Birth *

□ Confirm subscription *

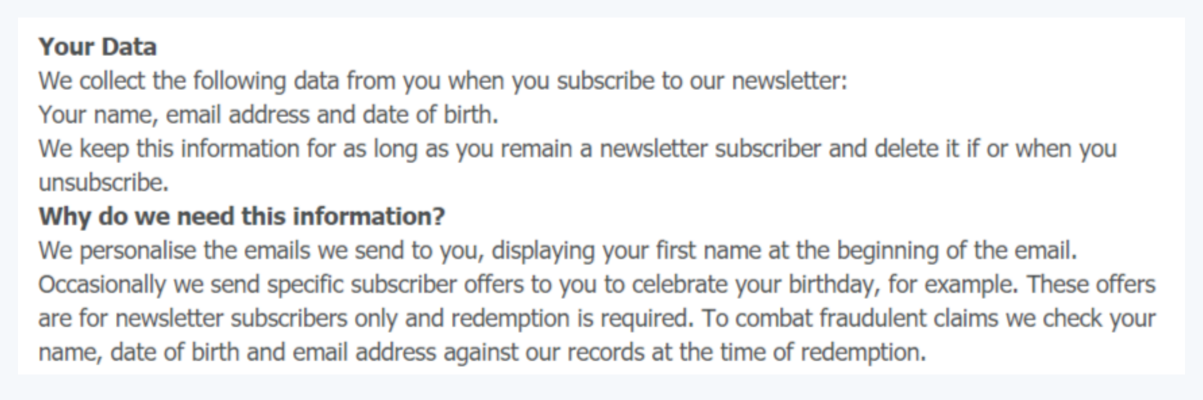
PLEASE READ THE IMPORTANT INFORMATION BELOW REGARDING HOW WE COLLECT, USE AND STORE YOUR PERSONAL INFORMATION.

Image: The Glass Box Co Newsletter sign up form

Users are asked to provide not only their email address, but also their **first and last name**, and **date of birth**.

This seems a little unnecessary at first. Is a date of birth, or even a name, really required to provide someone with a newsletter?

Helpfully, The Glass Box Co does provide accompanying information about why it needs this personal data, directly below where the information is requested:



Your Data

We collect the following data from you when you subscribe to our newsletter:
Your name, email address and date of birth.
We keep this information for as long as you remain a newsletter subscriber and delete it if or when you unsubscribe.

Why do we need this information?

We personalise the emails we send to you, displaying your first name at the beginning of the email. Occasionally we send specific subscriber offers to you to celebrate your birthday, for example. These offers are for newsletter subscribers only and redemption is required. To combat fraudulent claims we check your name, date of birth and email address against our records at the time of redemption.

Image: The Glass Box Co Newsletter sign up form - Your Data section

A date of birth, then, is used to offer newsletter subscribers special deals around their birthday. This could, in theory, represent a compelling reason to request this data, if appropriate safeguards are employed to keep it safe.

Minimizing Data Collection in Server Logs

Your server logs must **not** be a repository for personal data.

In theory, log files can contain just about anything, including personal data. However, any personal data you hold should be **limited**, **well-organized** and **secure**. This means that server logs are **not** a good means of collecting or storing it.

One way to end up with personal data in your logs is by collecting data such as **IP addresses** by default. There is often little need to collect the IP address of everyone who visits your site.

If you ***do*** need to collect your visitors' IP addresses, you probably **don't** need to collect the whole thing.

Writing for the Internet Engineering Task Force, Amelia Andersdotter recommends that providers of Internet-facing servers should:

> "*keep only the first two octets (of an IPv4 address) or the first three octets (of an IPv6 address) with remaining octets set to zero, when logging.*"

This would result in the following:

IPv4 address	**IPv6 address**
69.29.31.236	A624:71D3:2C80:EE02:0029:EC2A:002B:EB73
↓	↓
69.29.00.000	A624:71D3:2C80:0000:0000:0000:0000:0000

Table 6: IP addresses server logs examples of data collection minimization

Andersotter also recommends that you should **not**:

> "*log unnecessary identifiers, such as source port number, time stamps, transport protocol numbers or destination port numbers.*"

All of these types of data could qualify as personal data in certain circumstances. Unless you have a good reason with a suitable legal basis, **do not log them**.

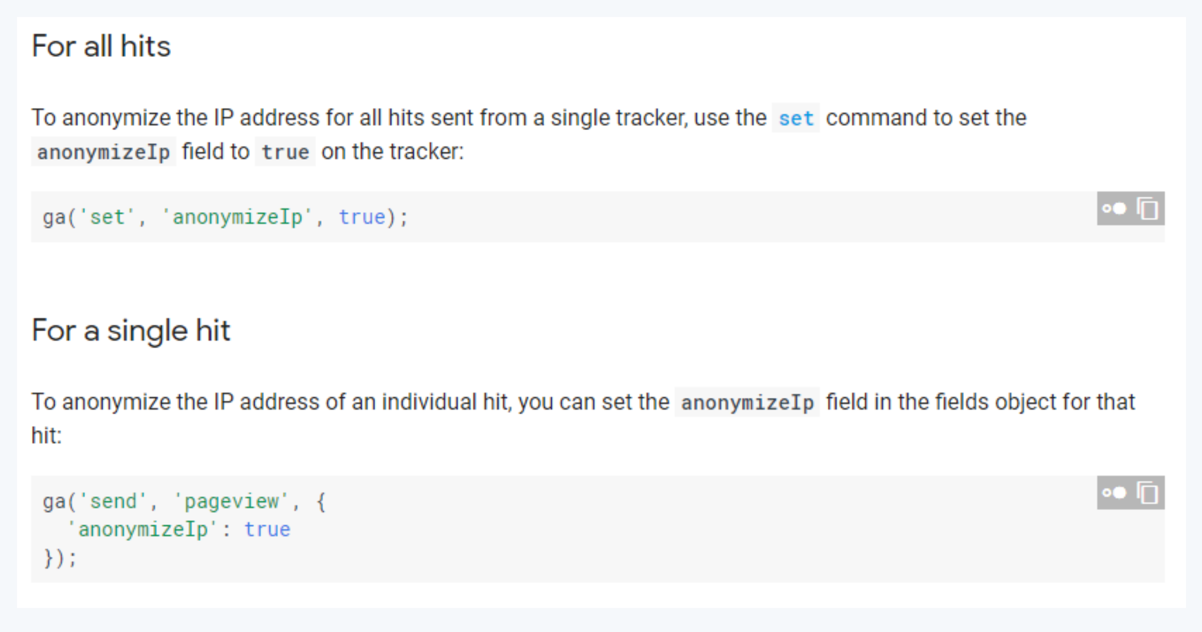
Minimizing Data Collection in Analytics

It's important to understand that personal data is collected by **web analytics**. Any information about a person's activities on a website could constitute personal data if it can theoretically be linked to them.

As with log data, one way to minimize the amount of personal data collected by analytics software is to **anonymize IP addresses**.

IP address anonymization is a feature of many analytics suites. For example, in **Google Analytics**, the last octet of IPv4 addresses and the last 80 bits of IPv6 addresses can be set to "zero."

Here's an extract from Google's guidance on how to anonymize IP addresses in Google Analytics:



For all hits

To anonymize the IP address for all hits sent from a single tracker, use the `set` command to set the `anonymizeIp` field to `true` on the tracker:

```
ga('set', 'anonymizeIp', true);
```

For a single hit

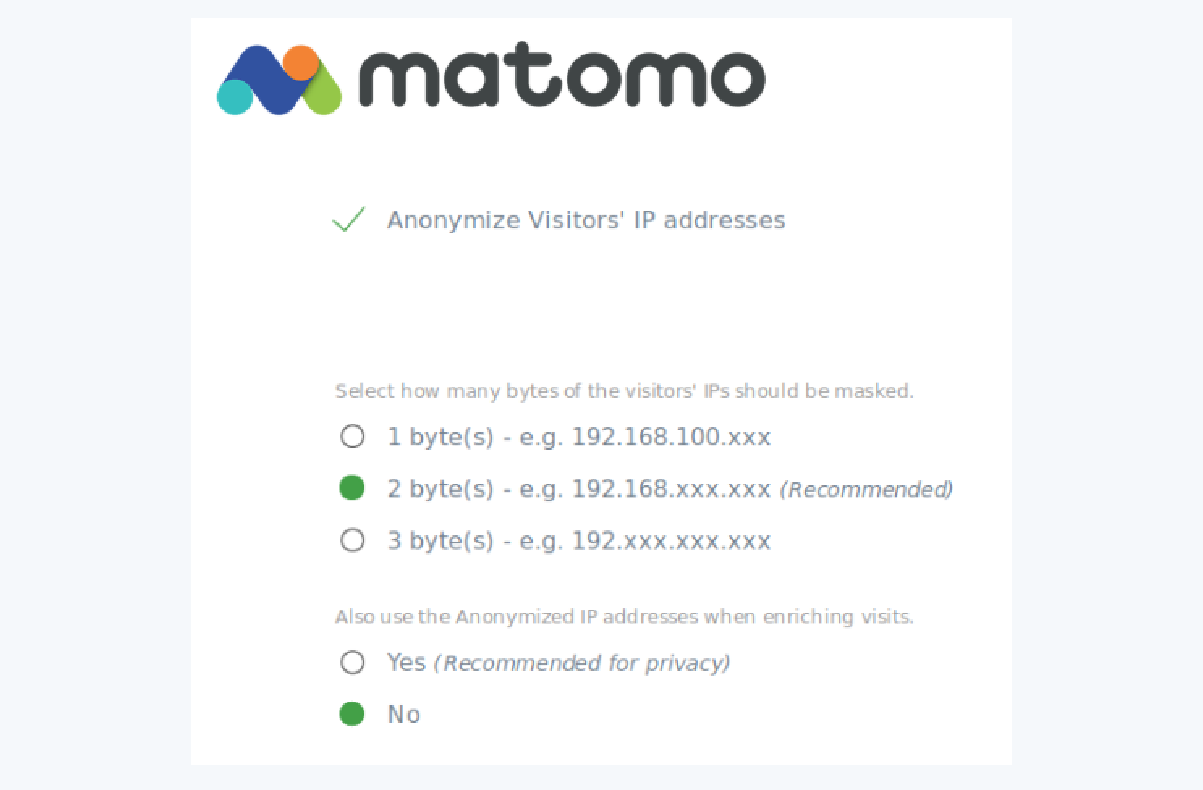
To anonymize the IP address of an individual hit, you can set the `anonymizeIp` field in the fields object for that hit:

```
ga('send', 'pageview', {
  'anonymizeIp': true
});
```

Image: Google Analytics IP Anonymization: For all hits and for single hit sections

Google's method of IP anonymization allows you to still gain **meaningful insights** into the use of your website, but goes **some way** to protecting your users' identities. It is worth noting however, that Google does not remove as much of the IP address as is recommended by Intarea (above).

Matomo Analytics allows you to go further, and mask the last two or even three octets of an IPv4 address:



matomo

✓ Anonymize Visitors' IP addresses

Select how many bytes of the visitors' IPs should be masked.

○ 1 byte(s) - e.g. 192.168.100.xxx

● 2 byte(s) - e.g. 192.168.xxx.xxx *(Recommended)*

○ 3 byte(s) - e.g. 192.xxx.xxx.xxx

Also use the Anonymized IP addresses when enriching visits.

○ Yes *(Recommended for privacy)*

● No

Image: Matomo Anonymize Visitors IP Addresses options screen

Like many aspects of data protection, this is an exercise in balancing your own interests against the risks to your users' privacy.

Accuracy

The principle of "**accuracy**" requires you to keep all the personal data you process accurate and up-to-date.

Some practical steps you can take towards complying with this principle include:

- Keeping any personal data in your possession **up-to-date** where practical
- Complying with requests under the **right to rectification**
- Allowing your users the right to **maintain their own personal data** through account controls

Whilst it is important for all data controllers to ensure the accuracy of their personal data, the extent to which this is relevant will depend on the nature of the product that you're developing.

Inaccurate personal data can cause big problems. **False information** recorded about a person can cause reputational damage. **Inaccurate contact details** can mean that the wrong person is targeted with direct marketing, or sent correspondence containing another individual's personal data.

Storage Limitation

The principle of "**store limitation**" requires that you do not keep personal data for **longer than you need it**.

Some practical steps you can take towards complying with this principle include:

- Automatically scheduling the erasure of personal data in your **server logs**
- Automatically scheduling the erasure of other personal data in collected by **analytics**
- Drawing up a **Retention Schedule** to demonstrate your data storage practices

Scheduling Erasure of Log Data

As we have seen, you must avoid collecting personal data in your **log files** wherever possible. Where it is necessary to collect, for example, IP addresses, you should ensure that it is **automatically erased** at regular intervals.

The Internet Engineering Task Force suggests that IP addresses in server logs, even if they have been subject to anonymization techniques as described above, should not be retained for longer than **three days**.

Your web server provider may provide a function for automating log data deletion. Let's take the example of **Amazon Web Services** (AWS) which offers a centralized logging solution.

Log data is stored as objects in a centralized "bucket." The object lifecycle management allows users to set **automated expiry dates** for particular classes of object (e.g. IP addresses).

A lifecycle rule can be created via the "Management" tab in the AWS console:

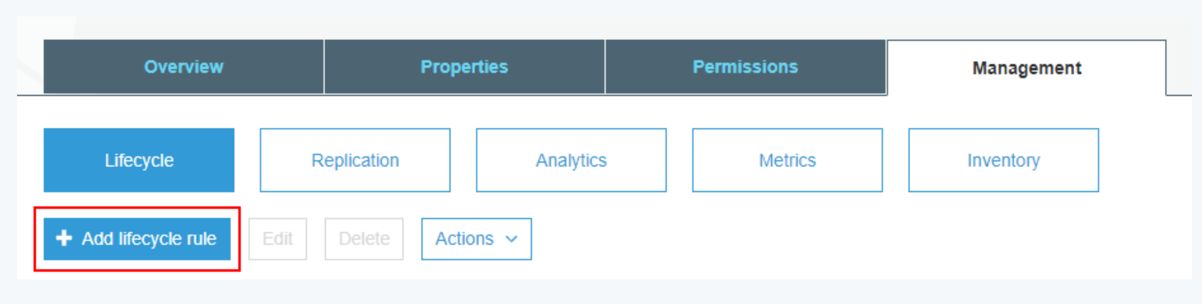
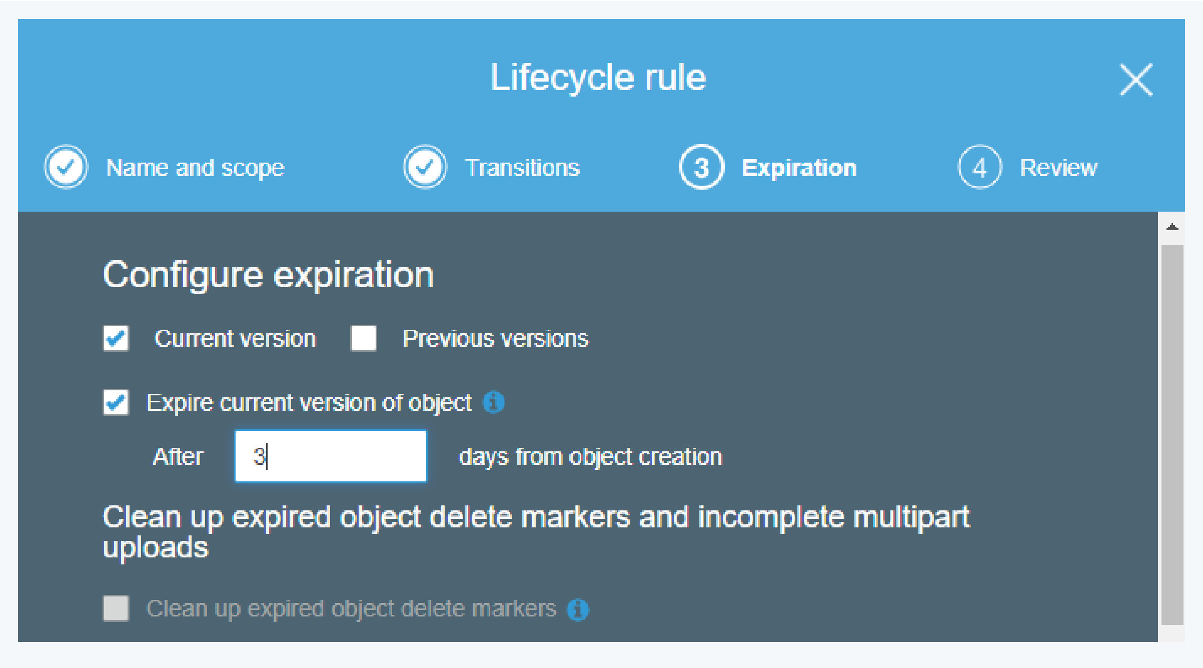


Image: Amazon Web Services Console: Management tab - Add lifecycle rule option highlighted

After defining the name and scope of the object, users can set its expiration period in days:



Configure expiration

☑ Current version □ Previous versions

☑ Expire current version of object

After 3 days from object creation

Clean up expired object delete markers and incomplete multipart uploads

□ Clean up expired object delete markers

Image: Amazon Web Services Console: Lifecycle rule screen

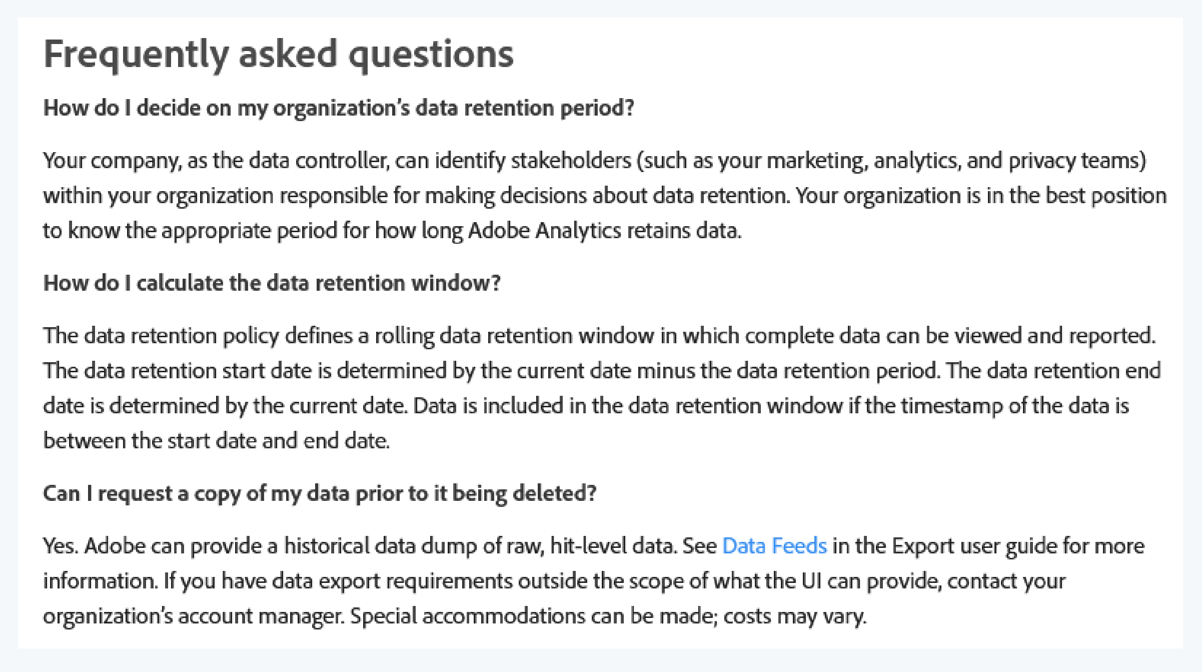
Alternatively, the logrortate utility can be used to automatically delete log files in Linux. You can also use the shred function to ensure that log files are not readable post-deletion.

Scheduling Erasure of Analytics Data

We've looked at how you can minimize the amount of personal data you collect via analytics. Any data you do collect should be kept only as long as you need it.

If you have your users' consent for analytics, and you have explained the implications in your **Privacy Policy**, you might be justified in retaining analytics data for **longer** than you keep log data.

Analytics providers will generally allow their users to set **custom retention periods**. The focus is often ***extending*** retention periods, sometimes for an additional fee. However, good data protection practice would obviously advocate ***reducing*** the retention period. Adobe Analytics provides an FAQ about data retention periods:



Frequently asked questions

How do I decide on my organization's data retention period?

Your company, as the data controller, can identify stakeholders (such as your marketing, analytics, and privacy teams) within your organization responsible for making decisions about data retention. Your organization is in the best position to know the appropriate period for how long Adobe Analytics retains data.

How do I calculate the data retention window?

The data retention policy defines a rolling data retention window in which complete data can be viewed and reported. The data retention start date is determined by the current date minus the data retention period. The data retention end date is determined by the current date. Data is included in the data retention window if the timestamp of the data is between the start date and end date.

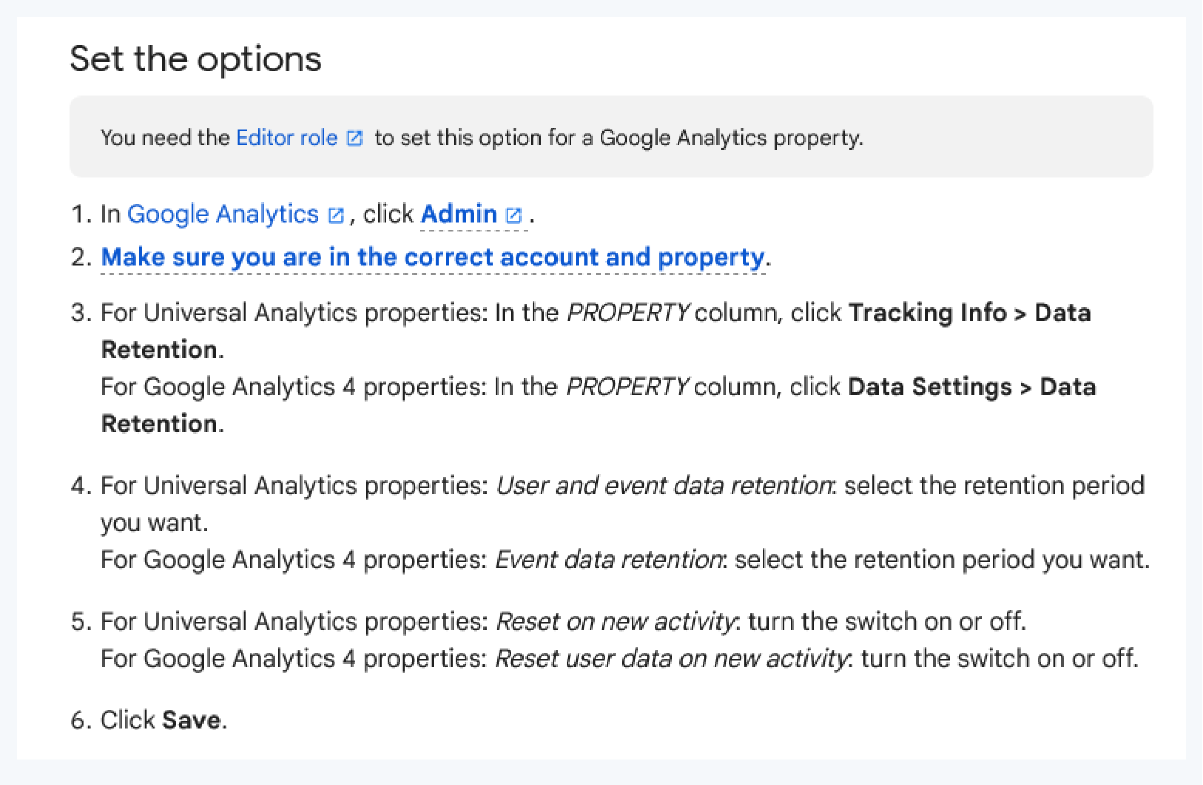
Can I request a copy of my data prior to it being deleted?

Yes. Adobe can provide a historical data dump of raw, hit-level data. See Data Feeds in the Export user guide for more information. If you have data export requirements outside the scope of what the UI can provide, contact your organization's account manager. Special accommodations can be made; costs may vary.

Image: Adobe Analytics Data Retention Policy: FAQ section excerpt

Google Analytics allows you to set your retention period for all identifiers (e.g. user IDs, advertising IDs, DoubleClick cookies) at 14, 26, 38 or 50 months.

Here are some instructions from Google on how to do this:



Set the options

You need the Editor role ⧉ to set this option for a Google Analytics property.

1. In Google Analytics ⧉ , click **Admin** ⧉ .
2. **Make sure you are in the correct account and property**.
3. For Universal Analytics properties: In the *PROPERTY* column, click **Tracking Info > Data Retention**.
   For Google Analytics 4 properties: In the *PROPERTY* column, click **Data Settings > Data Retention**.
4. For Universal Analytics properties: *User and event data retention*: select the retention period you want.
   For Google Analytics 4 properties: *Event data retention*: select the retention period you want.
5. For Universal Analytics properties: *Reset on new activity*: turn the switch on or off.
   For Google Analytics 4 properties: *Reset user data on new activity*: turn the switch on or off.
6. Click **Save**.

Image: Google Analytics Help: Data Retention - Set the options section

Creating a Retention Schedule

The GDPR requires that you provide details on your storage period as part of your Privacy Policy. This will be relevant for any **data controller**. Even where a data processor ultimately carries out the deletion of personal data, the data controller should be establishing the retention period.

Creating a Retention Schedule is a good way to demonstrate that you are taking the necessary steps to comply with the principle of storage limitation. It also serves to ensure that you take a **systematic approach** to managing the personal data stored in your systems.

A Retention Schedule can be set out in a table. It can provide information about:

- The **categories** of personal data you collect
- The retention **period**
- The **purpose** and **rationale** for keeping the data for this period
- The **action taken** at the end of that period (e.g. erasure, anonymization)

You may also need to include the “**trigger**” that starts the clock ticking on a retention period. For example, you may need to retain a user’s account data for a particular period after they have closed their account. In this case, the trigger would be “**account closure**.”

Integrity and Confidentiality (Security)

The principle of “**integrity and confidentiality**” requires that you take technical measures to ensure security and prevent data breaches at every stage of processing personal data.

Some practical steps you can take towards complying with this principle include:

- Creating procedures for **assessing** and **responding to risk**
- **Pseudonymization** of personal data
- **Encryption** of personal data

Assessing and Responding to Risk

In order to determine what would be an appropriate level of security for a given project, it's important to take a **systematic approach** to **assessing risk**.

In some cases, it is legally mandatory to conduct an **in-depth assessment**. This is known as a Data Protection Impact Assessment (DPIA).

A DPIA is a process that:

- **Describes** a data processing project in detail
- Assesses whether the project is **necessary**, and the methods are **proportionate**
- Identifies the associated **risks**
- Considers how to **mitigate** those risks

Under Article 35 of the GDPR, a DPIA is **mandatory** if you're undertaking a project which:

- Uses **new technology** to process personal data, or applies existing technology in a novel way
- Presents a **high risk** to people's right to privacy

When considering the need for a DPIA, you can take into account such factors as:

- The **nature** of the personal data you're processing (for example, **how sensitive** it is)
- The **scope** of the project (for example, **how many** people it will affect)
- The **context** of the project (for example, whether your users would **expect** you to process their personal data in this way)
- The **purpose** of the project (for example, the **benefits** that it might produce)

Bear in mind that even if you're not legally required to conduct a DPIA, it is a good way to protect against data breaches in any particularly complex project involving personal data.

The minimum requirements for what a DPIA is set out at Article 35 (7) of the GDPR and in guidance by the Article 29 Working Party.

A DPIA should document:

- A description of your **project**
- A description of the **reasons why** you need to carry out the processing and why the **methods** you have chosen are appropriate
- An assessment of the **risks**
- Details of the safeguards and other measures you have taken to **mitigate** those risks

You may need to consult with your **Data Protection Authority** if you find that there are risks that you can't adequately address.

Pseudonymization

Pseudonymization is a measure that **replaces identifiers** within a dataset with **non-identifying alternatives**. The remaining non-personal data can remain intelligible.

The pseudonymized data can be **rendered identifiable** again with reference to **additional information**. This means that it can be fairly easy to work with pseudonymized personal data. But equally, certain methods of pseudonymization may not be very secure.

Here's a very basic example of pseudonymization. This is just for context - please do not consider this a secure example.

Below is the original data set, which includes **categories**, **identifiers** and **non-identifiers**.

Name	Username	Mailing Address	Payment Status	Due Date
Thom Yorke	singer198	9 Bends Street	Paid	-
Jonny Greenwood	lead885	5 Pablo Honey	Unpaid	20/11/23
Ed O'Brien	rhythm992	9 Palo Alto	Paid	-
Colin Greenwood	bassist555	29 Rainbow Road	Incomplete	25/03/23
Philip Selway	drummer692	5 King Limb	Unpaid	25/12/23

Table 7: Example of original data set

Here is the same data set after pseudonymization:

Name	Username	Mailing Address	Payment Status	Due Date
}^+_ ;+{(€	[&-%€{@/?	/ "€-$[[]{€€}	Paid	-
*+--; %{€€-:++$	)€!$??<	< =!")+ ^+-€;	Unpaid	20/11/23
€$ +'"{&€-	{^;}^_//'	/ =!)+ !)}+	Paid	-
£+)&- %{€€-:++$	"![[&[}<<<	'/ {!&-"+:[{+!$	Incomplete	25/03/23
=^&)&= [€):!;	${]__€{,/'	< (&-%)&_"	Unpaid	25/12/23

Table 8: Example of the sane data set after pseudonymization

Each letter in the identifying information has been replaced by a **special character**. Unless it was decoded, the data is no longer intelligible without reference to **additional information** (i.e. a reference key). But the non-identifying information data (the categories of data, payment status, and due date) remains intact.

Pseudonymization can result in a data set that is both **secure** and **usable** if the method used is **sophisticated** enough. However, such data should still be treated as personal data. It must be stored **securely**, with **access** limited to those who need it. Any additional information used to interpret the data should be kept **separately** (and securely).

Encryption

Encryption encodes an entire data set. It turns a given set of "**plaintext**" into "**ciphertext**" without discriminating between personal data and non-personal data. A key is required to decode the data.

There are several options for encryption of personal data:

- **Application** level - The encryption is performed on any data controlled by a given application, for example, a database program.
- **Individual file** level - Specific files can be individually encrypted and then stored or transferred.
- **Full disk** - All data on a given disk is encrypted. Operating systems such often offer such functionality, for example, Windows features BitLocker and Mac OS features FileVault.

It is possible that **all three** methods will apply to your operations in different contexts.

For example, individual files can be encrypted before they are **emailed as attachments**. Or encryption of the **email message body** can be achieved by an application running OpenPGP or via Transport Layer Security (TLS/SSL).

Accountability

Alongside the six data processing principles set out above, the GDPR provides a separate, seventh principle of "**accountability**." This requires that you are accountable for your compliance with all of the GDPR's principles and requirements.

Some practical steps you can take towards demonstrating your compliance with the principles of the GDPR include:

- Producing **internal policies** such as a:
    - Data Protection Policy

    - Data Retention Schedule
    - Data Breach Notification Policy
- Maintaining **data processing records**
- Appointing a **Data Protection Officer**
- Ensuring you have **Data Processing Agreements** in place, where required

Key Takeaways From This Chapter

The principles of the GDPR must permeate all aspects of your data processing operations:

- Always process personal data in a **lawful, fair and transparent** way
- Only ever process personal data in connection with a **specified purpose**
- Only **collect** the personal data that you actually **need**
- Ensure you keep personal data **accurate** and up-to-date
- Only **store** personal data for as long as you **need** it
- Ensure that personal data is processed **securely**

Lastly, you need to be **accountable**, and able to **demonstrate your compliance** with these principles.

Chapter 9:

Final Steps to Take for GDPR Compliance

Having read this far, you know a lot about the GDPR. You should understand the law, your obligations under it, and know how to facilitate your users' rights.

Throughout the book, we've been focused on the **practical steps** you can take to implement the law.

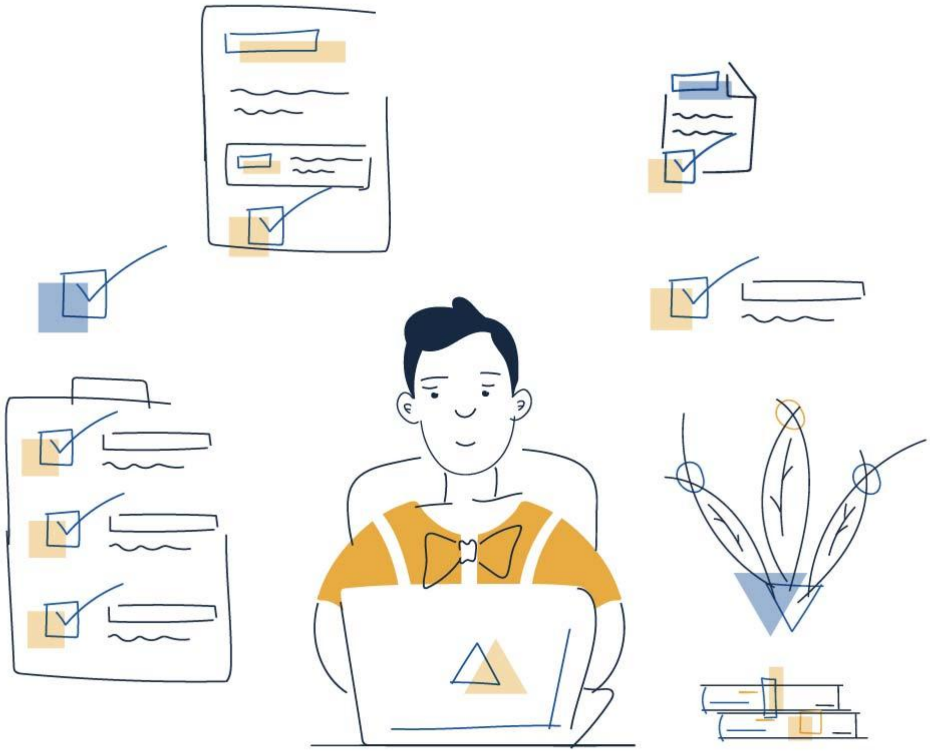


Illustration: Final Steps to Take for GDPR Compliance

Now we're going to take a look at some remaining things you can do to ensure that your project is GDPR-compliant.

Do You Know What Personal Data You Process?

Whether you're planning a **new development project** or trying to bring an **existing project** in-line with the GDPR, one of your first steps towards compliance should be to try to get a full picture of **how** personal data is processed within your company.

Mapping Data In-Flows

It's important to determine how data **enters** your company's systems. Consider the **sources** of personal data in your operation and the **means** by which data flows in.

For example, for **data controllers**:

Data **provided directly** by your users	● Web forms ● Email ● Telephone ● Post
Data collected **automatically**	● IP addresses ● Cookie data ● Analytics data ● Ad IDs
Data provided by **third parties**	● From users about others via email or web forms ● Social media data (e.g. via third-party website integrations) ● Via data processors who collect it on your behalf ● Publicly available sources

Table 9: Entering of data (data flow-in)

For **data processors**, all personal data flowing into your company (except for situations where you are the data controller) will be arriving from **third parties**, unless you are collecting it on a controller's behalf. Consider the different means by which you receive this data - how is it transferred to you?

Once you have identified all your sources of personal data, you can **erase** any:

- Personal data you **don't need**

- **Duplicate** personal data
- Personal data that you don't have a **legal basis** to process

Transferring Personal Data Out of the EU

There are strict conditions that apply to the **transfer** of personal data to **non-EU countries**.

This could apply in the following situations:

- Where personal data is collected by a **non-EU** company from a **person in the EU**. For example, a U.S. company asks a person in the UK to enter personal data in a web form. The data from the web form is to be stored on a server based in the United States.
- Where an **EU company** sends personal data to a **non-EU location**. For example, a UK data controller sends personal data to a data processor based in the United States.

There are a number of **rules** around transferring personal data to third countries, which we'll look at below.

Complying with these rules can take considerable effort. But the rules ***don't*** apply if the recipient of the personal data is based in an "approved" non-EU country which has a current adequacy decision from the European Commission (such companies include Canada, Israel, and New Zealand).

If this doesn't apply, you must have one of the following safeguards in place:

- If the transfer is taking place between two **separate companies**, for example, a data controller and a data processor, a **contract** containing standard data protection clauses can be put in place.
- If the transfer takes place within a **multinational company**, it can implement binding corporate rules.

There are also some exceptions to the rule, such as where the transfer is required to **fulfill a contractual obligation**. And as a "last resort," a person can **consent** to their personal data being transferred to a non-EU country without any of the above safeguards in place.

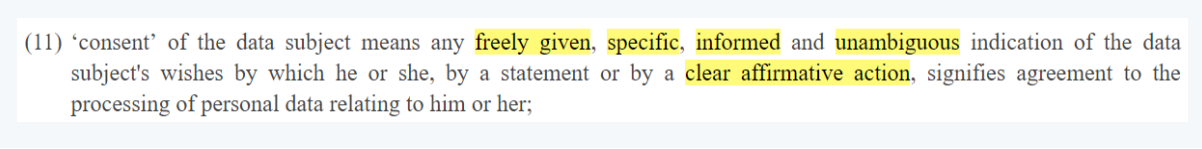
Do You Have a GDPR-Compliant Consent Solution?

We've talked a lot about **consent** throughout this book. You should now know when you need to request consent, and when you can rely on another legal basis such as **legitimate interests**.

It's important to make sure that, where you have identified consent as the appropriate legal basis, you also **ask for consent** in a **GDPR-compliant way**.

The Six Conditions of Consent

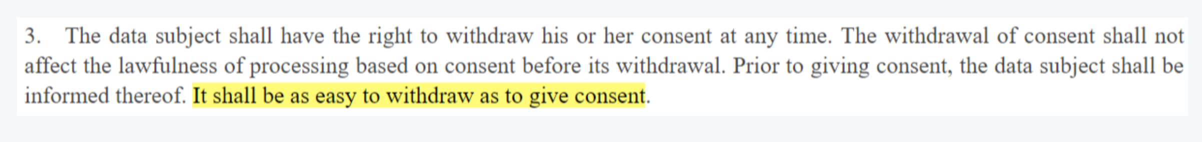
Here's the GDPR's main definition of consent at Article 4:



(11) 'consent' of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her;

Image: GDPR Article 4 definition of consent - for ebook

Here's another important insight from Article 7:



3. The data subject shall have the right to withdraw his or her consent at any time. The withdrawal of consent shall not affect the lawfulness of processing based on consent before its withdrawal. Prior to giving consent, the data subject shall be informed thereof. It shall be as easy to withdraw as to give consent.

Image: GDPR Article 7 Withdraw consent - for ebook

We can distill these requirements down into **six conditions**. Consent must be:

1. Freely given
2. Specific
3. Informed
4. Unambiguous
5. Given via a clear, affirmative action
6. Easy to withdraw

This is a high bar. But remember that it only applies ***if*** you're asking for consent.

Problematic Consent Solutions

There are some common ways of (supposedly) earning consent that are **no longer valid** under the GDPR. Here are some methods of requesting consent that you might be wise to **avoid**, or **remove** from your website, when becoming GDPR-compliant.

Cookie Walls

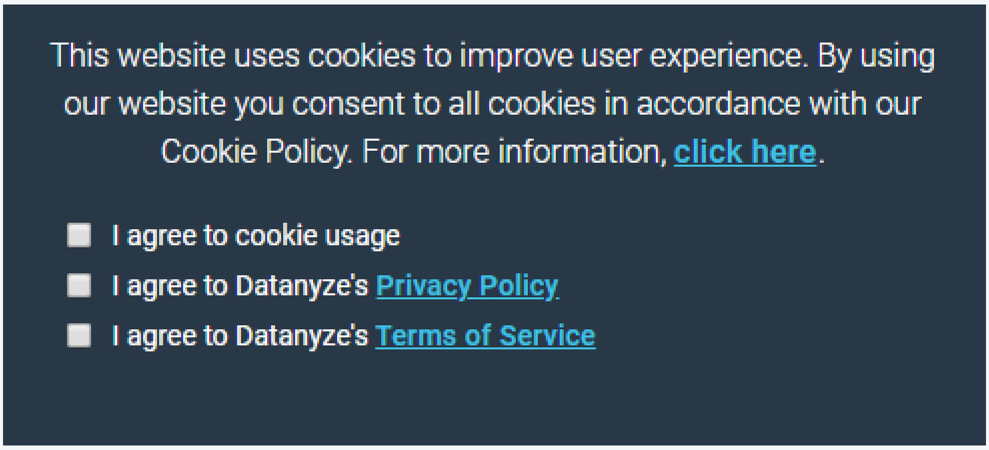
A cookie wall prevents users from accessing a website unless they consent to have cookies placed on their device. This is highly problematic in the light of the GDPR's requirement that consent is "**freely given**."

Here's what the European Data Protection Board recommends regarding cookie walls:

> "*In order for consent to be freely given as required by the GDPR, access to services and functionalities* ***must not be made conditional on the consent of a user*** *to the processing of personal data* [...] *meaning that cookie walls should be explicitly prohibited.*"

Admittedly, this might seem a little draconian. Why shouldn't you be allowed to govern the terms of access to your own website? Well, there's no rule against charging people money for access - the rule simply prohibits the "commodification" of people's personal data. You may consider this unreasonable, but remember that **this is the law** as it stands.

Here's an older example of what appears to be a cookie wall from Datanyze. The dialog box is displayed over Datanyze's website. There is no option to close the dialog or consent:



This website uses cookies to improve user experience. By using our website you consent to all cookies in accordance with our Cookie Policy. For more information, click here.

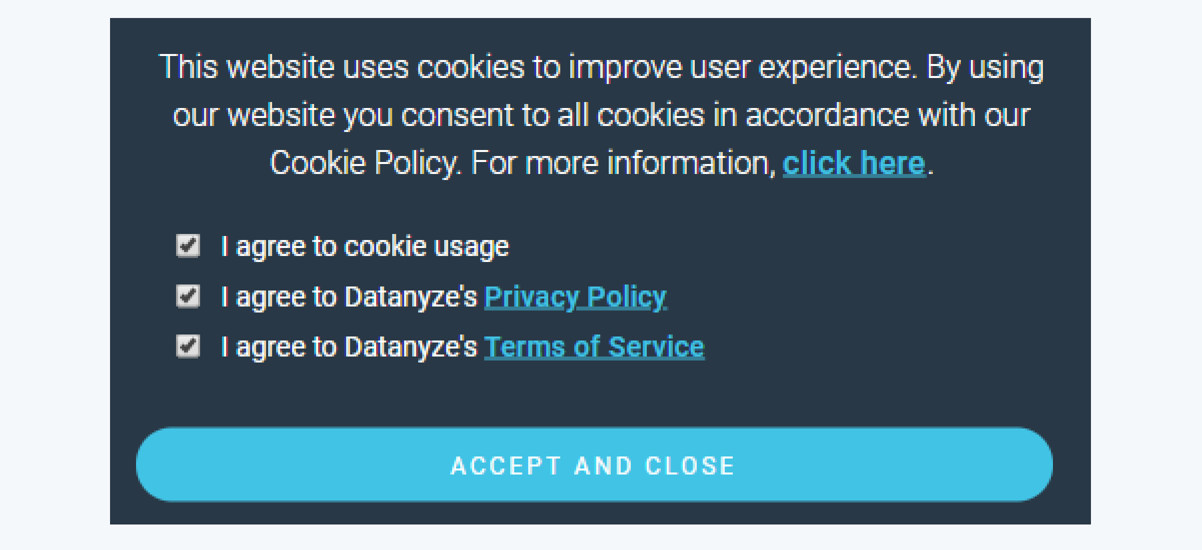
□ I agree to cookie usage

□ I agree to Datanyze's Privacy Policy

□ I agree to Datanyze's Terms of Service

Image: Datanyze cookie wall with boxes unchecked

When you tick all three boxes, you're only then allowed to close the dialog and access the site:



This website uses cookies to improve user experience. By using our website you consent to all cookies in accordance with our Cookie Policy. For more information, click here.

☑ I agree to cookie usage

☑ I agree to Datanyze's Privacy Policy

☑ I agree to Datanyze's Terms of Service

Image: Datanyze cookie wall with boxes checked

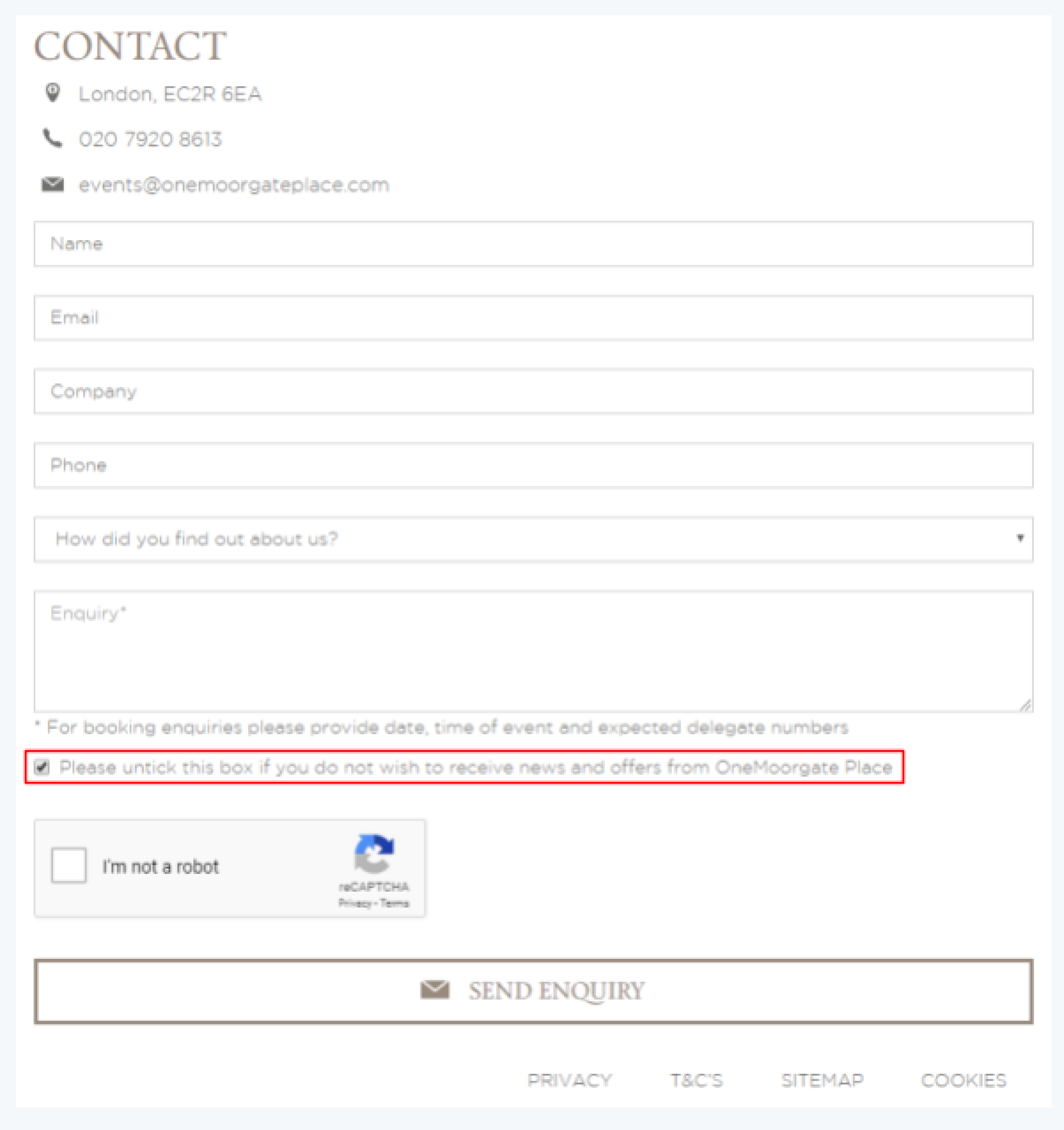
It's only possible to access Datanyze's site if you agree to cookies, and all the information present in its Privacy Policy and Terms. This is not **freely-given consent** as conceived by the GDPR.

Pre-Checked Boxes

Pre-checked boxes are a classic example of how a consent request can fall short of the requirements to be "unambiguous" and "given via a clear, affirmative action." Neglecting to refuse consent ***is not the same thing*** as giving consent.

When developing your front-end consent requesting mechanism, do not include a box that's already been checked. There should be no situation where this is necessary.

Here's an example of a pre-checked box, from an old version of a form from One Moorgate Place (note that the form has since been updated to be compliant):



CONTACT

London, EC2R 6EA

020 7920 8613

events@onemoorgateplace.com

Name

Email

Company

Phone

How did you find out about us? ▾

Enquiry*

* For booking enquiries please provide date, time of event and expected delegate numbers

☑ Please untick this box if you do not wish to receive news and offers from OneMoorgate Place

□ I'm not a robot

SEND ENQUIRY

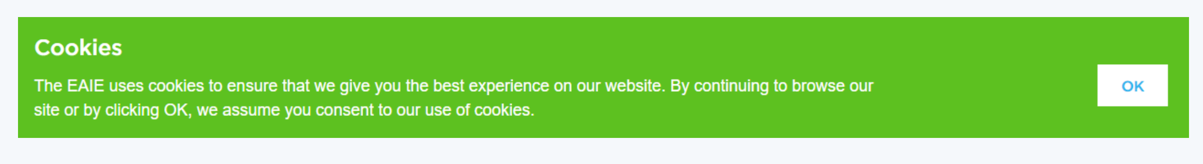
Image: One Moorgate Place contact form with pre-ticked checkbox highlighted

This is an inquiry form. When people make an inquiry via your company's website, it's ok to ask them if they **also consent** to receive marketing communications from you. But this should be a **proactive decision** on their part. There should be no mistaking that they **want** to receive marketing communications.

Presumption of Consent

Because of the strict standards of consent required under the GDPR, you'll want to **remove** (or avoid adding) any wording on your website which implies that you "**assume**" users are giving consent.

This is a very common feature of cookie banners. Here's an example from EAIE:



Cookies

The EAIE uses cookies to ensure that we give you the best experience on our website. By continuing to browse our site or by clicking OK, we assume you consent to our use of cookies.

Image: EAIE cookie consent notice

It may be that these are **essential** cookies that do not require consent. In which case, there should be no implication that consent has been granted.

Or it may be that these are **targeted advertising cookies**. In which case, it cannot be **assumed** that the user has consented merely because they continue to browse your website.

Compliant Consent Solutions

It's not that difficult to implement a GDPR-compliant consent process, both for cookies usage (a cookie consent notice), or for general data processing (such as implementing an "I Agree" checkbox).

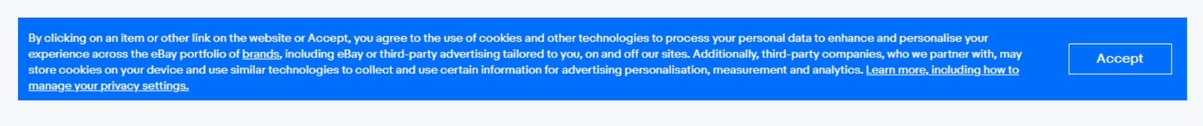
Just keep the **six conditions of consent** in mind, and do not take action until you have received consent.

Clickwrap v Browsewrap

As we've seen, it's not appropriate to **assume** that someone has granted consent to cookies simply because they visit your website. Such an approach is sometimes known as "**browsewrap**."

A more appropriate solution under the GDPR would involve having the user give a "**clear, affirmative action**" to confirm their consent. For example, clicking "I accept" or "OK." This is known as "**clickwrap**."

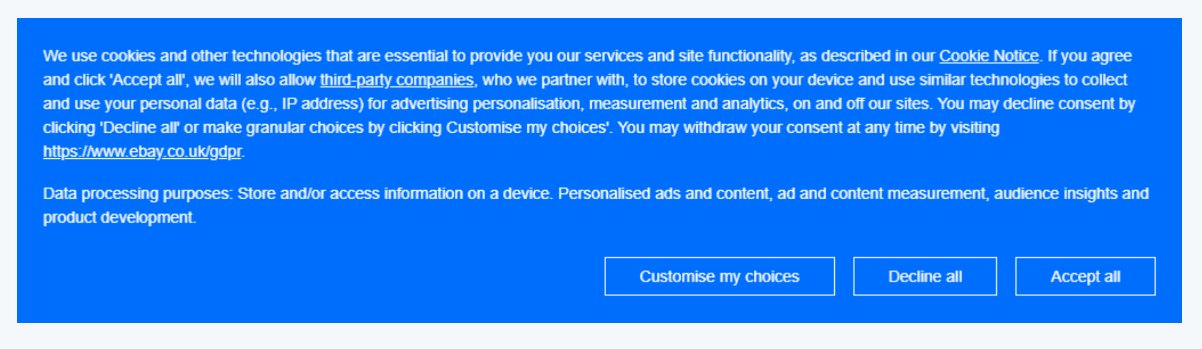
Here's an unclear, not so robust cookie consent banner from eBay (note that it has since been updated):



By clicking on an item or other link on the website or Accept, you agree to the use of cookies and other technologies to process your personal data to enhance and personalise your experience across the eBay portfolio of brands, including eBay or third-party advertising tailored to you, on and off our sites. Additionally, third-party companies, who we partner with, may store cookies on your device and use similar technologies to collect and use certain information for advertising personalisation, measurement and analytics. Learn more, including how to manage your privacy settings.

Image: eBay UK cookie consent notice - Old version

Here’s an updated version with more options for customization and the option to decline all cookies:



We use cookies and other technologies that are essential to provide you our services and site functionality, as described in our Cookie Notice. If you agree and click 'Accept all', we will also allow third-party companies, who we partner with, to store cookies on your device and use similar technologies to collect and use your personal data (e.g., IP address) for advertising personalisation, measurement and analytics, on and off our sites. You may decline consent by clicking 'Decline all' or make granular choices by clicking Customise my choices'. You may withdraw your consent at any time by visiting https://www.ebay.co.uk/gdpr.

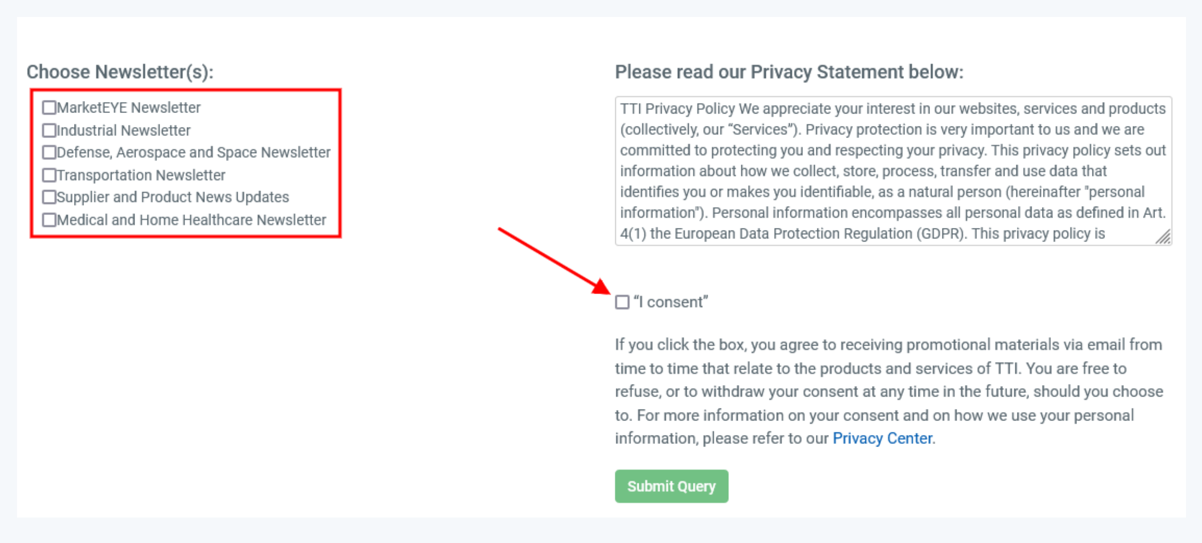
Data processing purposes: Store and/or access information on a device. Personalised ads and content, ad and content measurement, audience insights and product development.

Image: eBay UK cookie consent notice - Updated version

Specific Consent

The requirement that consent is “**specific**” means that you should not “bundle” requests for consent. Consent should be requested for **one specific thing at a time**. This means that where a person consents, for example, to receive your newsletter, they aren’t consenting to also receive special offers or third-party marketing.

Here’s an example of how you can make your consent requests **specific**, from TTI Europe:



Choose Newsletter(s):

□MarketEYE Newsletter
□Industrial Newsletter
□Defense, Aerospace and Space Newsletter
□Transportation Newsletter
□Supplier and Product News Updates
□Medical and Home Healthcare Newsletter

Please read our Privacy Statement below:

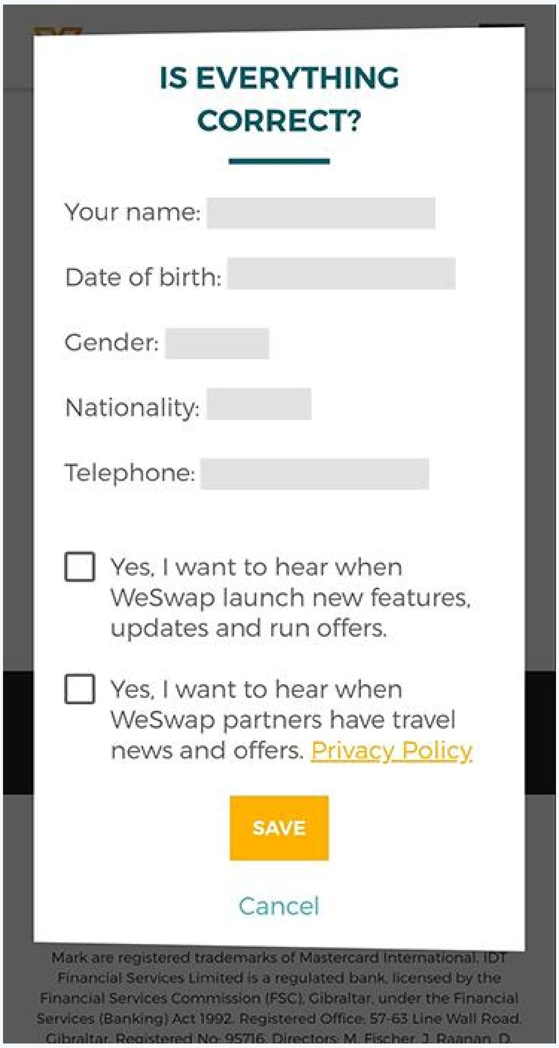
TTI Privacy Policy We appreciate your interest in our websites, services and products (collectively, our “Services”). Privacy protection is very important to us and we are committed to protecting you and respecting your privacy. This privacy policy sets out information about how we collect, store, process, transfer and use data that identifies you or makes you identifiable, as a natural person (hereinafter "personal information"). Personal information encompasses all personal data as defined in Art. 4(1) the European Data Protection Regulation (GDPR). This privacy policy is

□ “I consent”

If you click the box, you agree to receiving promotional materials via email from time to time that relate to the products and services of TTI. You are free to refuse, or to withdraw your consent at any time in the future, should you choose to. For more information on your consent and on how we use your personal information, please refer to our Privacy Center.

Image: TTI Europe subscribe to email newsletter form with consent checkboxes highlighted

Here’s another example of how to request specific consent to both first- and third-party direct marketing, from the WeSwap Android app:



IS EVERYTHING CORRECT?

Your name: [redacted]

Date of birth: [redacted]

Gender: [redacted]

Nationality: [redacted]

Telephone: [redacted]

□ Yes, I want to hear when WeSwap launch new features, updates and run offers.

□ Yes, I want to hear when WeSwap partners have travel news and offers. Privacy Policy

Mark are registered trademarks of Mastercard International. IDT Financial Services Limited is a regulated bank, licensed by the Financial Services Commission (FSC), Gibraltar, under the Financial Services (Banking) Act 1992. Registered Office: 57-63 Line Wall Road, Gibraltar. Registered No: 95716. Directors: M. Fischer, J. Raanan, D.

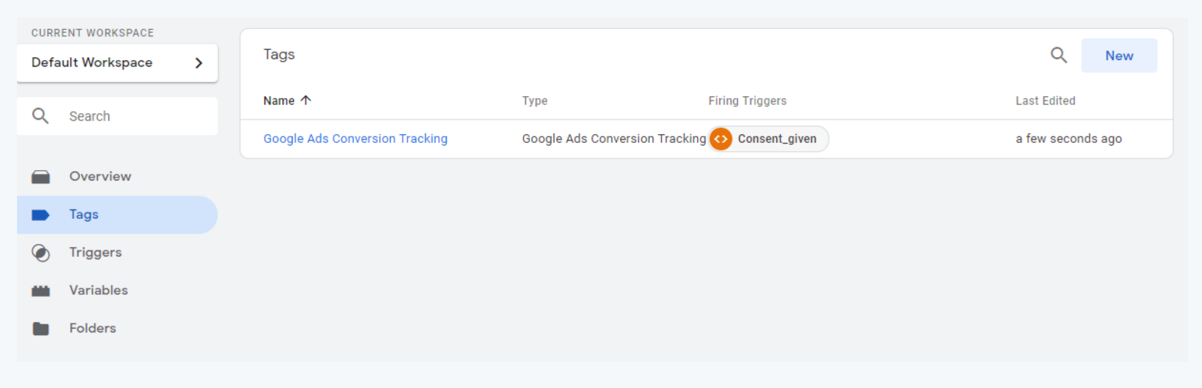
Image: WeSwap app sign-up screen

Setting Cookies After You Have Consent

We've seen that if you have identified a need to request consent, you have to ask for it in the **proper way**. But that's not all - you also have to **properly implement** your **response** to this request.

If you're asking for consent for cookies, the proper thing to do is to **only set cookies after you've received consent**.

This can be achieved in a number of ways. For example, in Google Tag Manager, tags fire by default as a result of a **PageView** event. If you have a tag associated with setting non-essential cookies, you should set up a **custom trigger** which fires only once consent has been granted.



Name ↑	Type	Firing Triggers	Last Edited
Google Ads Conversion Tracking	Google Ads Conversion Tracking	Consent_given	a few seconds ago

Image: Screenshot of Google Tag Manager dashboard

Do You Have the Right Policies in Place?

Having appropriate **policies** in place can improve the efficiency, accountability, and reputation of your company.

There are certain written documents are **mandatory** under certain conditions, for example:

- A Privacy Policy. This is only mandatory for data controllers. But if your company primarily acts as a data processor, you'll still need a Privacy Policy that covers any data processing activities for which you are a data controller (for example, processing the personal data of your own staff and customers).
- **Data processing records**. You may not be required to produce these if you are a small or medium-sized company, and you only process non-sensitive personal data occasionally.
- An EU Representative Appointment Letter. This only applies if your company is not established in the EU.

There are a number of **other policies** that can help contribute toward your compliance with the GDPR. Depending on the context of the project you're developing, you may or may not need to produce all of these policies.

You can consider:

- The **sensitivity** of the personal data you process
- The **amount** of personal data you process
- The extent to which processing personal data is a **core activity** of your company
- The **size** of your company

Data Protection Policy

A Data Protection Policy is an internal document which sets out the **principles**, **standards**, and **practices** of data protection within your organization. Even if your company is very small, it can still be helpful to have this sort of policy in place.

A Data Protection Policy can include information about:

- **Who** is primarily **responsible** for data protection matters in your company
- Your **procedures** for facilitating **data subject rights** requests
- The **safeguards** you have in place for facilitating **international data transfers**
- **Data security** standards and practices
- **Other policies** such as your Data Retention Schedule and Data Breach Policy

Your Data Protection Policy should function as a guide, used by e**veryone in your company**, that **explains what to do** when a data protection issue comes up.

Data Breach Policy

If a serious **data breach** occurs, companies are obliged to report it to their Data Protection Authority **within 72 hours**.

A Data Protection Authority can issue fines and other penalties to a company that is responsible for a data breach. When deciding on what penalties to issue, Recital 148 states that the Data Protection Authority can consider **how the company responded** when the breach occurred.

This is why it's important to have a Data Breach Policy in place that provides information about:

- Who within your company should be **informed** about a data breach
- What should be done to **contain** the breach (e.g. taking systems offline, resetting passwords)
- What **investigation** should occur into the nature of the breach (e.g. who is affected, what data was lost, what caused the breach)
- How to assess whether the breach is **sufficiently serious** to warrant reporting to your Data Protection Authority, and/or the individuals that are affected
- Where to find your company's template Data Breach Notice Letter;
- The post-breach **evaluation** process (i.e. how to avoid a recurrence)

Data processors should also have such a policy in place. However, a data processor is required to inform their **data controller** about a breach, rather than their Data Protection Authority.

GDPR Compliance Statement

A GDPR Compliance Statement is a public-facing document, written in your company's brand voice.

This is your opportunity to **tell the world** about all your efforts to become GDPR-compliant. You can include information about:

- **The GDPR**, why it is important, and why your company is committed to it
- The **safeguards** you have in place around data security, data sharing and international data transfers
- Your **policies** and procedures
- How you'll be facilitating **data subject rights**
- Whether you have appointed a **Data Protection Officer** and/or **EU Representative**

This is reassuring for your customers, whether they are consumers or other businesses.

GDPR Compliance Checklist

Below is a checklist of the things you need to know and to do in an effort to become GDPR-compliant. You'll want to consider **all** of these factors, no matter how big or small your development project is.

The list **isn't exhaustive**, and there may be additional considerations in particular contexts (for example, if you're offering services to children, or processing sensitive data).

Data controllers are required to consider all of these points, but only certain points apply to data processors.

Subject	Questions	Are data processors required to comply?
Personal data	Do you know which **categories** of personal data you process within your company? Some common categories of personal data include: ● Names ● Email addresses ● IP addresses	Yes

	● Usernames ● Advertising IDs ● Mailing addresses ● Cookie data ● Contents of emails, posts or comments	
Data flows	Do you understand how data: ● **Enters** your company? ● Is it processed **within** your company? ● **Exit** your company? Consider who you **receive** personal data from, who you **share** it with, and what **happens** to that data in between.	Yes
Legal bases	Have you determined your **legal basis** for processing? List all the categories of personal data you process and determine whether you can **justify** your processing under a legal basis.	No
Consent	Are you asking for **consent** where appropriate to do so? Are you **requesting** consent in a GDPR-compliant way?	No
Legitimate interests	If you are relying on legitimate interests, have you conducted a **Legitimate Interests Assessment**?	No
Third parties	Can you ensure that you're meeting the **terms** of all the third parties you work with? Have you checked that you have **Data Processing Agreements** in place with any data processors you're using?	Yes. Data processors must ensure they have Data Processing Agreements with all data controllers **and sub processors** they work with.
Data subject rights	Have you set up **systems** to allow you to respond to **data subject rights** requests? You may also consider integrating user account controls into your website or app.	Data processors must ensure they are ready to **assist their data controllers** with such requests (but must not deal directly with the data subject).

Internal policies	If appropriate, have you written any of the following policies: ● Data Protection Policy ● Data Breach Notification Policy ● Data Protection Impact Assessment(s) Depending on the context of your operations, it might not be necessary to create such internal policies.	Yes
External policies	Have you written a **Privacy Policy** and displayed it on your website? Have you considered writing a GDPR Compliance Statement?	Yes
Appointments	If required to do so, have you appointed a: ● Data Protection Officer ● EU Representative	Yes
Data processing records	If required to do so, have you begun **documenting** your data processing activities?	Yes
International transfers	Have you considered which **safeguards** you'll be employing for **international transfers**?	Yes
Security	Have you implemented **security measures** into your data processing where applicable, for example: ● Pseudonymization ● Encryption ● Anonymization ● TLS/SSL ● Firewalls	Yes

Table 10. GDPR Compliance Checklist

TermsFeed