measured collective

We help you get GDPR right

5 privacy policy mistakes that can land you a fine

What you need to know and how to fix it (skip the fine), without a law degree.

The mistakes we'll cover:

1. Not making the distinction between UK GDPR vs EU GDPR
2. Yawn, still talking about the EU-US privacy shield
3. Limiting your policy to just your website
4. Missing out the people you share data with
5. Forgetting to make it clear how long you will retain data for

Is this exhaustive?

No. Privacy policies can be complex documents. This is a selection of some of the most common mistakes we see through our research.

What are the potential fines under GDPR?

UK GDPR Fines
Lower-tier violations can lead to a fine of up to £8.7 million or 2% of the organisation's worldwide annual turnover, whichever is higher. More serious violations can lead to a fine of up to £17.5 million or 4% of the organisation's worldwide annual turnover, whichever is higher.

EU GDPR Fines?
Lower-tier violations can lead to a fine of up to €10 million or 2% of the organisation's worldwide annual turnover, whichever is higher. More serious violations can lead to a fine of up to €20 million or 4% of the organisation's worldwide annual turnover, whichever is higher.

How are fines decided? ➔
Where does fine money go? ➔

Are fines increasing?

Yes. When we compare GDPR fines in 2020 to 2021, we are currently at a 612% increase in the total value of GDPR fines. Ouch.

MISTAKE 1

Not making the distinction between UK GDPR and EU GDPR

Let's not get into politics. Whether you're a remainer or a leaver, you'll need to update your privacy policy in the wake of Brexit.

When the UK completed the transition period, EU GDPR ceased to apply within the UK. In its place we have "UK GDPR".

Currently, UK GDPR differs only very slightly from the EU GDPR. But technically it is a different set of regulations.

This means that you should update your privacy policy text to reflect these changes.

If you process the personal data of UK residents and EEA (European Economic Area) residents then you should add disclosures for both different regulations.

You should identify how people may exercise their rights under each legislation and who they should complain to if they take issue with your data privacy practices. For example you can direct people covered by UK GDPR to the ICO, and people covered by EU GDPR to your EU Representative or to an appropriate data protection authority if you have a legal entity based in the EU.

Remember, this doesn't mean duplicating your entire privacy policy, it just means that you should take steps to make it clear which regulations apply and how people can exercise their rights.

MISTAKE 2

Still talking about the EU-US privacy shield

Some policies make reference to the EU-US privacy shield. They explain that data transfers to the US, like the ones you may make in order to use tools like Mailchimp and Google Analytics, are covered by the EU-US privacy shield.

The problem with this is that the EU-US privacy shield was ruled invalid by the in the Schrems II case issued by the European Court of Justice on Thursday 16 July 2020. It found that the Privacy Shield framework no longer provides adequate safeguards for the transfer of personal data to the United States from the EEA.

This issue is compounded further if you are processing data under UK GDPR. Even if the EU-US privacy shield was valid, it would not automatically apply to data from the UK.

If you are still talking about the EU-US privacy shield then you need to review all your "restricted transfers". These are data transfers that occur from the UK or EU to countries that are not covered by adequacy decisions.

The US is not covered by an adequacy decision but it's where the data of many popular SAAS tools are hosted.

For example:

- Mailchimp
- Slack
- AirTable
- Google Workspace
- Google Analytics

So it's probably where your focus should be first.

You will need to make a list of transfers, determine the appropriate transfer mechanism and then apply it. This may mean you have to sign SCCs with the SAAS tools that you are using.

MISTAKE 3

Limiting your policy to just your website

Many privacy policies use text which limits them to the website or app that they are present on.

For example they may say

“This policy applies to our website and users of our website”

This approach is fine, but what about all the other data processing activities you complete?

For many companies, their website is a focal point . But it’s not where ALL data processing happens.

You need to consider how you will provide adequate data privacy information for:

- Customers ordering directly via phone, or by email to a sales representative
- Suppliers whose details you store to issue payments
- Employees whose personal data is shared with payroll companies
- Prospects who have not yet visited your website, whose data is provided by third parties or social media platforms like LinkedIn

These are just some examples.

The point is that your data processing activities probably extend beyond your website, so limiting the scope of your privacy policy to just your website is a bad idea.

Under UK GDPR and EU GDPR you must make appropriate data privacy information available to all data subjects in order to help fulfil your obligations under the accountability principle.

So, you can either expand your privacy policy to give a more comprehensive overall of all the data processing activities you fulfil:

Covering at least:

- What data you collect
- For what purposes you collect it

- Under what legal basis you collect it
- How the data will be shared
- For how long the data will be processed

Or you can split this into smaller documents, for example you may issue an “employee privacy notice” to all staff.

MISTAKE 4

Missing out some of the people you share data with

Many privacy policies have very vague details about who data may be shared to, or haven't been updated since that fancy new email marketing tool or advertising platform was added...

It's important to get this section right and to disclose properly where people's data may be shared to.

You don't have to call out each individual organisation that you share data with by name, but you should make sure that every "type" is included.

You should provide detail about:

- what types of organisation you may share data to
- under what circumstances your may share the data to them
- the safeguards you have put in place to protect the data that you share to them

Frequently, people will miss out organisations that they never intended to share data with. For example you may in some cases be obliged to share data under a court order, to the police or a regulatory body as evidence.

You also may not have considered how you would handle customer data if it becomes difficult to reach your customer, for example you may then share data with a contact tracing company. Or in the case of missed payments, with a debt collection agency.

Make sure you consider every type of organisation that you may share data with and provide detailed information about it in your privacy policy.

MISTAKE 5

Not making it clear how long you will retain data for

Many privacy policies skip this section entirely or provide unreasonable periods of data retention.

Under the storage limitation principle of UK GDPR and EU GDPR you must retain data only for as long as you need it.

You cannot retain data indefinitely without a justified reason.

Your data retention periods can be flexible, for example they may extend each time a customer purchases from you again or logs back into your app. But they must be reasonable. This can be a difficult task to set properly. You want to get the right balance between practicality and adhering to the principle.

You should at least provide information on how long you intend to keep each type of data you collect, and some overview of the deletion process. Your privacy policy does not have to state exact time periods. However this would be best practice.

To minimise complaints you should clearly identify any areas where you may keep data for a long time, for example you may keep a “do not call” list of customers that have opted out of sales calls. Or you may keep basic details about customers such as their name, address and purchase history for many years in order to comply with your accounting requirements.

You will need to assess each type of data and purpose of processing individually to develop your complete policy.

Example

An employer receives several applications for a job vacancy. Unless there is a clear business reason for doing so, the employer should not keep recruitment records for unsuccessful applicants beyond the statutory period in which a claim arising from the recruitment process may be brought.

Example
A bank may need to retain images from a CCTV system installed to prevent fraud at an ATM machine for several weeks, since a suspicious transaction may not come to light until the victim gets their bank statement. In contrast, a pub may only need to retain images from their CCTV system for a short period because incidents will come to light very quickly. However, if a crime is reported to the police, the pub will need to retain images until the police have time to collect them.

A checklist you can use

Check your current privacy policy now and then run this checklist against your privacy policy each time you update it.

Requirement	Privacy Policy Version & Review Date Status	Privacy Policy Version & Review Date Status	Privacy Policy Version & Review Date Status	Privacy Policy Version & Review Date Status
	02/11/2021 V1.0 - Example (November 2021)			
The name and contact details of your organisation. Say who you are and how individuals can contact you. (Always)	Done			
The name and contact details of your representative. Say who your representative is and how to contact them. (If required).	N/A			
The contact details of your data protection officer. Say how to contact your data protection officer (DPO). (If required).	N/A			
The purposes of the processing (always)	Incomplete			
The lawful basis for the processing (always)	Incomplete			
The legitimate interests for the processing (always)	Incomplete			
The recipients, or categories of recipients of the personal data Say who you share people's personal data with. (always)	Incomplete			
The details of transfers of the personal data to any third countries or international organisation (always)	Incomplete			

The retention periods for the personal data (always)	Done			
The rights available to individuals in respect of the processing (always)	Done			
The right to lodge a complaint with a supervisory authority (Always)	Done			
The details of whether individuals are under a statutory or contractual obligation to provide the personal data (Always)	N/A			
The details of the existence of automated decision-making, including profiling (always)	N/A			

Download this as a Google Doc ➔

measured collective

We help you get GDPR right

Can we have your passport number, mother's maiden name and pin number?

Just kidding, but if you'd like to join our email list we'll need a first name and email address. You'll get practical GDPR compliance tips and news about incoming changes to data privacy law - on average once a week. You can apply what you learn straight away and reduce your risk of getting a fine. Of course if you don't like it you can unsubscribe at any time, we are quite obsessed with the rules.

Sign up ➔