



Research report

DDMA 2025 Privacy Monitor

How Dutch consumers want to and must be informed about online privacy and data-sharing



Table of contents

Introduction	03
Management summary	04
Main conclusions of DDMA 2025 Privacy Monitor	09
Laws and regulations regarding online privacy and data sharing	22
Recommendations	32
Research methodology and colophon	33

Introduction

The 2023 edition of the DDMA Privacy Monitor revealed that the initial reaction of Dutch consumers to online privacy and data-sharing is to dig their heels in. However, consumers are certainly open to sharing data with organizations if provided with additional explanation, transparency and clarity, and this willingness is also growing with time.

Dutch regulation and legislation has not definitively specified the best manner for organizations to inform consumers about what happens to their data. The updated [Leidraad Bescherming Online Consument van Autoriteit Consument & Markt](#) (ACM, May 2024) provides slightly more guidance, but there is still ample room for organizations to shape their own interpretation. In this new edition of the DDMA Privacy Monitor, we take a closer look at how consumers prefer to be informed about their online privacy and data-sharing, including when this is utilised for AI purposes - and on the other hand: how the relevant Netherlands' regulation and legislation dictate the manner in which those organizations are obliged to inform consumers.

The manner in which consumers want to be informed

This year's DDMA Privacy Monitor consists of two parts: in the first part, we cover insights from qualitative research conducted through group discussions in different focus groups, which has provided us with valuable insights. To substantiate these insights in figures, we will occasionally refer back to the most recent quantitative Global Privacy Monitor study, from 2022.

We will address questions such as: how do consumers want to be informed about what happens to their data, what do they consider to be important and clear? What is the level of knowledge and sentiment of consumers about AI, and the use of their data for the purpose of AI? When do consumers experience their degree of control to be sufficient, and when does information become nudging?

The manner in which organisations are legally obliged to inform consumers

Conversely, in the second part, we explain how organisations are obliged to inform consumers about their online privacy and the sharing of data, in accordance with the applicable laws and legislation. The aim is to deliver concrete advice for organizations involved in data and marketing.

Management summary



Providing transparent information pays off and places your (potential) customer first

Transparent information about online privacy and data-sharing is not only a moral responsibility for organizations, but also a strategic opportunity to gain the trust of (potential) customers and increase their willingness to share data.

By providing insight into the whys and wherefores of data collection, clarifying the benefits for consumers, and tailoring communication to the knowledge level of the target group, you not only enhance the relationship with your customer as an organization, but you also contribute towards your own success.

Current situation shows resigned consumer acceptance of data-sharing

The experience of consumers is that they do not really have a choice when it comes to sharing data, and that it seems inevitable in today's digital way of living. While they seem to be slightly more knowledgeable about online privacy, the lack of deep understanding and complex cookie banners and privacy notices remains a barrier, resulting in the persistent negative associations concerning online privacy and data-sharing.

Additional knowledge and understanding about what happens to their data and what choices they have can ensure that consumers are less negative about sharing data.

More consumer awareness about the value of their data (consent or pay)

Consumers' preference for paying for an online service or product, or to be able to use it for free in exchange for sharing data or donating voluntarily is influenced by the type of service and perception of fairness.

Although awareness of data-sharing is growing, a sense of injustice still plays a role for a number of consumers, especially when they have to pay for online services that were previously free. People have a more positive attitude towards voluntarily donating for an online service, such as journalistic platforms or news media.

Cookie banners are often found to be disruptive and complex

Consumers would like to be more aware of their cookie preferences, but are limited in this sense by the disruptive effect of cookie banners and their complex and often misleading design. The lack of knowledge about the consequences of their choices, and the remaining belief that websites without cookies either do not work or do not work properly, cause a reduced sense of control.

How would consumers prefer to see cookie banners?

An easy-to-use cookie banner provides clear, concise information at a glance about what data is being collected, how this data is being used, what the benefit of accepting cookies is for consumers, and the potential downside of opting to reject. In addition, the configuration and layout of the buttons must be fair and simple, displaying matching-shaped data choices.

Effective methods for informing consumers about the privacy statement

Many consumers do not read privacy statements, mainly because of the complexity and interruption of their user experience. When consumers do actually look into a privacy statement more thoroughly, they prefer to see a scannable design with understandable wording, and a trustworthy tone of voice. Adding information about the benefits of data exchange for consumers can also contribute to a more positive experience.

Different expectations for different organizations

The expectations and trust of consumers regarding online privacy differ per organization type. Expectations are higher for major and more sensitive organizations, while consumers have less confidence in foreign organizations – especially Russian and Chinese ones.

The customer relationship also plays an important role in how willing consumers are to share their data. Loyalty and trust can increase the willingness to share data, while a lack of trust can actually reduce it.

The ideal way to deal with online privacy according to consumers

Consumers value clarity and transparency when dealing with online privacy. The desire for the standardisation of cookie banners and privacy statements, better consumer information about online privacy, and the use of a quality mark for online privacy, shows that consumers also want to share the responsibility with regulators, industry representatives and/or organisations in a sense. Meeting these needs can help the marketing industry build a more trustworthy image among their consumers.

No new consumer demands on AI yet due to lack of knowledge

Consumers do not have sufficient knowledge about AI, its impact on their online privacy, and possible privacy risks. People are especially enthusiastic about ChatGPT, but consumers hardly consider what happens to any data they share, and do not see the commercial applications of AI either. This lack of knowledge means that consumers currently do not feel that AI is making new demands on how to deal with their online privacy.

Trust and awareness needed for further AI adoption

AI is still in the adoption phase of the early majority, which entails that there are still many opportunities for further adoption and integration. Consumer trust and awareness are crucial to promote further adoption.

Organizations have an important role to play in this regard, not only by implementing AI, but also by being transparent about how they implement AI, what data they collect, and what risks and benefits it poses to consumers.



Research clarification: Three types of consumers

Consumers may have a pragmatic, unconcerned or sceptical attitude towards online privacy and data-sharing

In 2022, we already distinguished three types of consumers when assessing concerns about their online privacy on the one hand, and their willingness to share data on the other: the pragmatists, the unconcerned and the sceptics. When discussing the main conclusions, we use these group definitions to interpret the results.



The **pragmatist** is someone who is quite concerned (score >6) about their online privacy, but still reasonably willing to share data (score \geq 5).



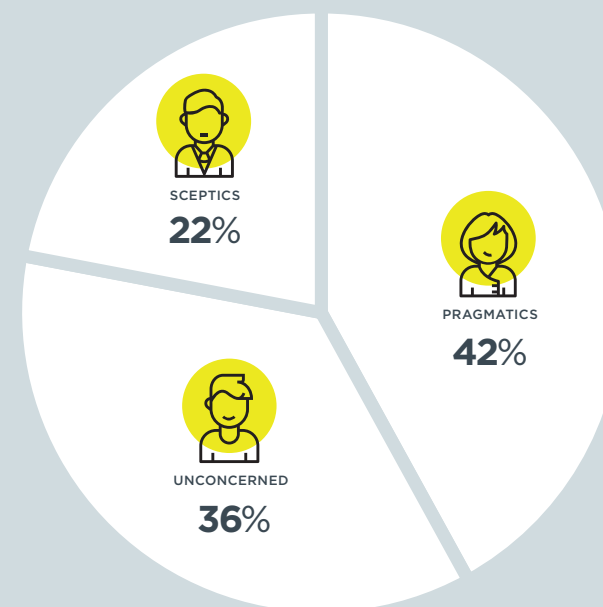
The **unconcerned** individual is not very concerned about their online privacy (score \leq 6).



The **sceptic** is very much concerned (score > 6) about their online privacy and unwilling to share data (score < 5).

The Dutch society consists mainly of pragmatists (42%) and unconcerned people (36%). A total of 1 in 5 Dutch people (22%) are sceptical about sharing data. The focus groups carried out were formed on the basis of these groups, with 1 group consisting of solely pragmatists, 1 group of unconcerned individuals and 1 group of sceptics.

Attitudes towards online privacy and data-sharing



Source: 2022 Global Privacy Monitor, selection: The Netherlands

Main conclusions of DDMA 2025 Privacy Monitor

How Dutch consumers want to be informed
about online privacy and data-sharing



Providing transparent information pays off, placing your (potential) customer first

At a time when online interaction and data collection is commonplace, the importance of transparent information provision is continuing to grow. Some 70% of Dutch consumers consider it (very) important for organizations to be transparent about how their personal data is collected and used, according to the 2022 Global Privacy Monitor. This demands attention from organizations: not only to meet consumer expectations, but also to support their own organizational goals.

The importance of transparency

Providing transparent information offers consumers a sense of control over their data. This not only has a positive effect on their trust, but also increases their willingness to share personal data. The key information that organizations can provide to increase that willingness is as follows:

- ▼ The reason for data collection (44%)
- ▼ The types of personal data collected (36%)
- ▼ The benefits for consumers (35%)
- ▼ And whether the data is shared with third parties (35%)

This applies to both the pragmatists and unconcerned group. For the sceptics, additional details are also important, such as the retention period of data, and the option to have it deleted upon request.

My willingness to share my personal information depends on...



Source: 2022 Global Privacy Monitor, selection: The Netherlands

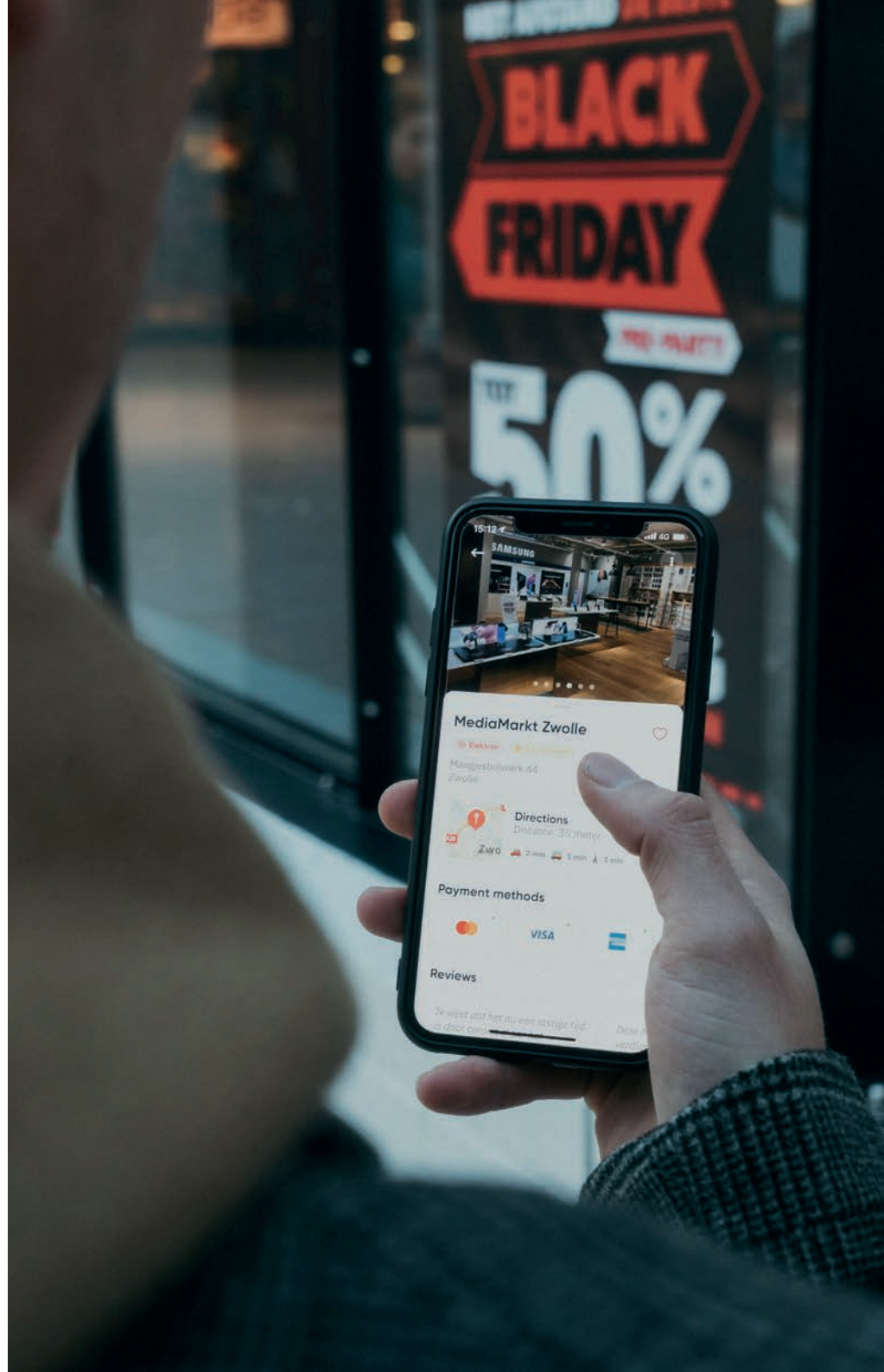
Trust as the key to willingness for sharing data

The central starting point for consumers is trust. According to the 2022 Global Privacy Monitor, 37% of Dutch people have stated that trust in an organization is the most important condition for sharing personal data. Trust is not only created by transparency, but also by placing the customer at the center when defining privacy and cookie policies.

At the same time, the **DDMA 2023 Privacy Monitor** already demonstrated that consumers mainly act out of their own interest when sharing data, and are willing to share data if they derive a direct benefit from doing so. This requires organizations to find out what their target group sees as the benefits of data exchange with the product or service in question.

Understanding encourages acceptance

The recent group discussions with Dutch consumers for this edition of the Privacy Monitor demonstrate that knowledge contributes towards a more positive attitude regarding data-sharing. That is why it is important for organizations to delve into the knowledge level of the (potential) customer. Consumers who understand why data is collected, what is done with it, and who experience a sense of control, are more pragmatic in this regard. This emphasizes the importance for organizations to not only be transparent, but also to tailor their communication to the knowledge level of their target group.



Current situation shows resigned consumer acceptance of data-sharing

During the recent group discussions about online privacy and data-sharing, the main associations among consumers were negative, with many consumers experiencing a feeling of resigned acceptance, because they feel they have no real choice in the matter. They believe that full participation in society, whereby texting, social media and online purchases play a major role, is intrinsically linked with the sharing of personal data.

This sentiment is substantiated in the 2022 Global Privacy Monitor, whereby 66% of consumers stated that sharing personal data is an increasingly important part of modern life. At 74%, this feeling is slightly stronger among pragmatists than among sceptics (57%) and the unconcerned (63%).

“It makes no difference to me how it’s communicated really, as I feel it’s something that needs to happen. I’ve never experienced any aspect of it as negative.”

Consumer from qualitative research

This resigned acceptance also stems from the limited sense of control, partly due to the frequency and complexity of cookie banners and privacy statements. Consumers say it is impossible to read these carefully for every website or app they use, and they therefore feel compelled to click ‘accept’.

Knowledge level remains limited, while this can lead to a more positive perception

Although the level of knowledge about online privacy seems to have increased compared to a few years ago, there is often still a lack of in-depth understanding. For example, consumers often still think that a website either cannot function or will not function properly without cookies, which perpetuates the negative associations surrounding online privacy and data-sharing.

At various stages of the group discussions with consumers, we noted that increased knowledge and awareness of online privacy and data-sharing can contribute to more positive perceptions. Consumers who understand how their data is used, and what choices they actually have, experience fewer negative feelings about the sharing of data.

More consumer awareness about the value of their data ('consent or pay')

There also seems to be slightly more awareness among consumers about the effect of marketing and the value of their personal data. Most realize that the use of free websites and apps, such as social media, news platforms, the weather or games, often involves the conscious or unwitting sharing of data, and advertisements.

This awareness brings mixed feelings: some consumers acknowledge that they have become dependent on these websites or apps, and understand that these organizations cannot continue to operate for free either. Others however have become so accustomed to certain services being available for free on the internet that the introduction of payment options, as in the case of Buienradar (Dutch weather forecasting website), leads to feelings of injustice, leaving pragmatists and sceptics in particular with a sense of grievance.

"That's the world turned upside down! You wish to have privacy, and yet you're made to pay for that privacy. That's just stupid, isn't it?!"

Consumer from qualitative research

"It means people with money are then able to skip adverts, so it will become a luxury, when really it should be a basic right for everyone."

Consumer from qualitative research



Bron: [Cookiebanner Buienradar](#), oktober 2024

Preferences for data-sharing or paying for online services

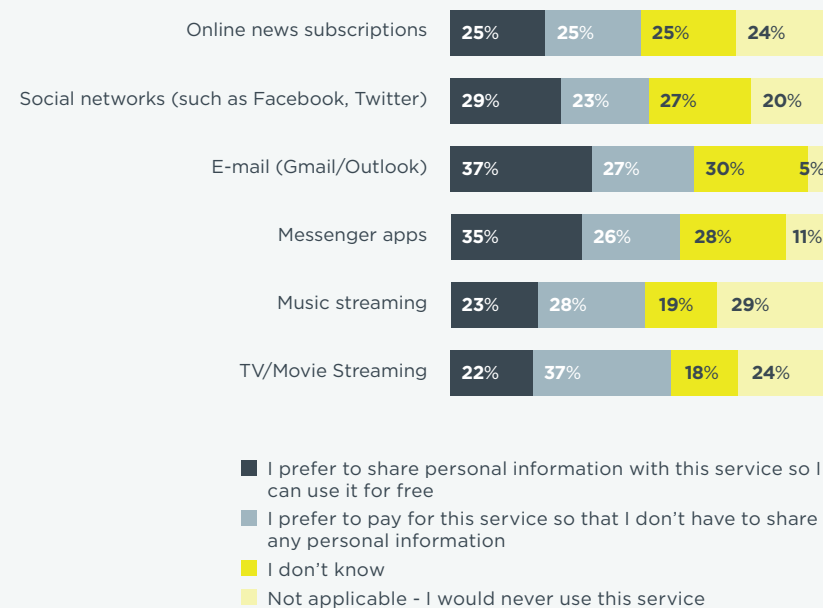
The 2022 Global Privacy Monitor already showed that Dutch consumers prefer to pay for online services that already required payment upon their introduction. For example, consumers of services such as music streaming (28%) and TV/movie streaming (37%) are more likely to opt to pay for the service over free use in exchange for data-sharing. By contrast, consumers prefer free use in exchange for sharing data when utilising social media (29%), email (37%) and messaging apps (35%).

Sceptics are more reluctant to share data, and state more often that they do not use these services at all. Those unconcerned individuals on the other hand, more often prefer free use in exchange for sharing data.

‘Willingness to donate’ category generates moderate propensity

A third option that is becoming increasingly common in addition to data-sharing or paying for online services, is a request to voluntarily donate personal data or money. Financial donation requests are used by journalistic platforms or news media (see The Guardian example). This category evokes less resistance from consumers, because it feels more understandable for quality journalism to cost money, and donations are voluntary.

Sharing data or paying for online services



Source: 2022 Global Privacy Monitor, selection: The Netherlands

“The Guardian provides insight in a clear manner, plus you are in control of things.”

Consumer from qualitative research

 **It's your choice**

When we make the Guardian available to you online, we and our partners may use cookies and similar technologies to help us to do this. Some are necessary to help our website work properly and can't be switched off, and some are optional but support the Guardian and your experience in other ways. To do this we work with a cross section of 156 [partners](#).

Cookies and other similar technologies may be used to access personal data, including page visits and your IP address. We use this information about you, your devices and your online interactions with us to provide, analyse and improve our services. Depending on your choice, we may also use your data to personalise content or advertising.

We use cookies and similar technologies for the following purposes:


- ✓ Store and/or access information on a device
- ✓ Personalised advertising and content, advertising and content measurement, audience research and services development

Learn more in our [privacy policy](#) and [cookie policy](#), and manage the choices available to you at any time by going to 'Privacy settings' at the bottom of any page.

Are you happy to accept cookies?
To manage your cookie choices now, or to opt out where our partners rely on legitimate interests to use your information, [click on manage cookies](#).

Yes, I accept No, thank you Manage cookies

The Guardian cookie banner, October 2024

Rejection hurts ... 

You've chosen to reject third-party cookies while browsing our site. **Not being able to use third party cookies means we make less from selling adverts to fund our journalism.**





We believe that access to trustworthy, factual information is in the public good, which is why we keep our website open to all, without a paywall.

If you don't want to receive personalised ads but would still like to help the Guardian produce great journalism 24/7, please support us today. It only takes a minute. Thank you.

One-time **Monthly** Annual

€4 per month **€12 per month**

Other

Continue →    

Not ready to support today? [Remind me later](#)

The Guardian

The Guardian cookie banner after clicking on 'No, thank you', October 2024

Cookie banners are often considered to be disruptive and complex

If we take a closer look at the control that consumers experience to safeguard their online privacy, they mention being aware of the use of cookies as the most obvious method within group discussions. Consumers state that you should actually be very aware when dealing with cookie banners, but find this difficult to put into practice. On the one hand, this has to do with the interruption of their online activities, and on the other, their experience of the information in cookie banners is that it is too complex or misleading. The 2022 Global Privacy Monitor already demonstrated that a mere 23% of Dutch people experience a sense of control when determining privacy settings. This percentage is the lowest among sceptics (11%), while pragmatists (33%) and the unconcerned (19%) feel slightly more in control.

"I have no control over it and it's confusing, but I don't read up on it all the time. You won't be able to function without cookies."

Consumer from qualitative research

Cookie banners have a disruptive effect

Consumers mention that cookie notifications distract them from their purpose on a website, such as searching for information or buying something. Each website uses a different cookie banner, which leads to irritation and time-consuming actions. This results in users often blindly accepting cookies, and opting for the most visually striking button, such as a colored or top-placed option, in order to be able to proceed quickly.

Cookie banners are too complex and misleading

In addition, the explanatory wording of cookie banners is often considered complex or misleading. Consumers often lack the marketing knowledge to properly understand concepts such as 'functional cookies' and 'marketing cookies'. And for example, when choosing between 'accept all cookies' and 'accept only required cookies', many consumers are uncertain about the consequences of their choice.

The misconception still prevails that websites will not function properly or at all if cookies are refused. As a result, consumers often choose to 'accept everything', which reduces the feeling of control, with in particular the way in which the options are presented reinforcing this pattern.

How do consumers prefer to see cookie banners?

Brief, clear information at a glance...

Consumers prefer short and understandable information in a cookie banner. At a glance, they want to see:

- ▶ **What data** is collected;
- ▶ **How** this data is **used**;
- ▶ What the **benefit of accepting** the cookies is for them as a consumer;
- ▶ Explaining the possible **disadvantage of not accepting** is also important, for example whether the website will still work properly afterwards.

The information must be simple and visible at a glance in the cookie banner, which also immediately displays a reference to a full privacy statement.



“This user experience is in line with our advice, and also in accordance with the Dutch Data Protection Authority (AP): use clear words in the buttons such as ‘allow’, ‘agree’ or ‘refuse’ and place different choices visibly on one layer. Website visitors should be able to refuse as easily as allow. This means that someone should not have to click through to refuse, if they do not have to do so to allow (all) either. It is also wise, when using ticks and sliders, not to have these automatically set to the ‘on’ mode. Read more about this in the paragraph [‘Cookies taste better with clear communication’](#)”

Isa Nieuwstad, Legal Counsel at DDMA

... This also applies to the button configuration and layout

In addition to the information in the banner, the layout of the options also plays an important role in a more positive user experience:

- ▶ Consumers want to **see clear, fair choices** for both the ‘accept’ and ‘reject’ options. The choices should be **immediately visible**, so that they are not forced to click through to continue navigating.

Only a few consumers who are more familiar with the concepts surrounding cookies would want to be able to turn different types of cookies on and off in some instances, for example via sliders. For the majority of consumers, this option is soon perceived as too complex and time-consuming.

“It depends on how much importance you attach to it. If you find it scary, you’ll want the maximum number of options for turning on and off. If you’re not really bothered, you won’t mind.”

Consumer from qualitative research

- ▶ It is important to use **terms that are understandable and consistent** for consumers when choosing cookies.
- ▶ **Options that are of matching designs** are viewed more positively. For example, if an ‘allow all’ button has a more striking color, it is perceived as deception.

What is effective when informing consumers about the privacy statement?

Consumers admitted that they rarely or never read privacy statements. Although some have read a privacy statement in the past, they generally experience this as too much effort. Just as with cookie banners, having to read privacy statements disrupts the initial purpose of visiting a website or app, and the process is perceived as too complex and long-winded.

If consumers take a more detailed look at the privacy statement, they prefer to see that:

- ▼ The text **can be scanned quickly**, for example by dividing it into clear chapters and using icons to visually clarify information;
- ▼ The text is written in **simple and understandable language**;
- ▼ The text has a **serious and reliable tone**. A tone that is too frivolous in nature is considered inappropriate for a privacy statement;
- ▼ A few consumers noted that privacy statements are often focused on what the organization can gain from the data, whilst they would also like to see **what benefits the data exchange generates for the consumer**.

“Sometimes you can have a connection with a company. I don’t mind what Rituals know about me for instance, it’s a give and take thing.”

Consumer from qualitative research

Different privacy expectations for different organizations

The group discussions show that consumers have different expectations in terms of how to deal with online privacy, depending on the size, sector and origin of the organization

- ▼ **Large organizations** are expected to have their online privacy matters in order, with a solid and well-thought-out privacy policy, partly because of the risk of image damage if data is handled carelessly. Consumers have fewer requirements when it comes to **smaller organizations**.
- ▼ There are different expectations and requirements from **commercial organizations** in comparison to **sensitive sectors such as banks, government or healthcare institutions** because of the difference in interests. In the case of banks, or governmental or healthcare institutions for example, there is more confidence that the handling of personal data will be carried out carefully and securely. This is due to the higher level of risk associated with the processing of sensitive data in these sectors.
- ▼ Consumers are generally less inclined to trust **foreign organizations**, and specifically mentioned Russian and Chinese organizations such as Temu and AliExpress. Moreover, this also shows that consumers have more confidence in Dutch regulators and legislation, and assume that scandals in the media will come to light if organizations do not comply with the rules.
- ▼ In addition, the relationship that consumers have with an organization also plays an important role in their willingness to share personal data. **Loyal and regularly returning** customers represent an advantage as an organization, as they are often willing to share more data than with organizations they land on by chance in an online setting.

Ideal handling of online privacy according to consumers

According to consumers, the key to a successful approach to online privacy is to provide clarity and transparency. They identify a number of sector-wide solutions for this purpose:

- For example, consumers state that they would prefer to see the **standardization of cookie banners and privacy statements**, as it would entail that informing and asking permission about online privacy and sharing data is always done using the same method, enabling consumers to more quickly and easily understand what they are accepting, without having to read up on the information every time they use it.



“Many organizations implement cookie banner generators (such as Cookiebot), but do not know exactly what it entails, and which rules must be complied with. Using standard bots is fine, but be critical of design choices. Choosing the ‘GDPR-compliant’ option does not automatically guarantee a compliant cookie banner. Always follow the rules of thumb when designing your cookie banner, which can be read in the paragraph ‘Standard cookie banner generators: what are the points of attention?’”

Isa Nieuwstad, Legal Counsel at DDMA

- Another point that consumers mentioned is the **importance of consumer information** about dealing with online privacy. They would like more information about what they can do themselves to safeguard their privacy when online. This should include reading privacy statements, the different types of cookies, and where and why data is collected.



“At the end of 2024, the AP (Dutch Data Protection Authority) took the initial step in its public campaign on the privacy risks of cookies, and in doing so, the regulator called upon organisations to take a closer look at their cookie policies.”

Isa Nieuwstad, Legal Counsel bij DDMA

- During the group discussions, all three groups spontaneously mentioned **the advantage of a quality mark**. This quality mark would show consumers at a glance whether their data is handled securely with a particular organization. They put forward a number of suggestions, such as displaying privacy levels, or traffic light colors that indicate privacy levels.

DDMA Privacy Quality Mark

An example of one such quality mark is the DDMA Privacy Quality Mark. This quality mark can be used internally at organizations for the processing of personal data for marketing purposes through self-audits. The DDMA Privacy Quality Mark offers an internal privacy and security check with which organisations can show consumers and partners that they respect privacy and handle personal data carefully and transparently. Organisations that carry the DDMA Privacy Quality Mark present a reliable image towards current and future consumers and parties to work with. Only members of DDMA are eligible for the Privacy Quality Mark. For more information, see: www.ddma.nl/privacy-waarborg

Lack of awareness deters new consumer demands on AI

There is still a lot of unfamiliarity among consumers when it comes to artificial intelligence (AI). When asked about their associations with AI, they mainly think of ChatGPT, an application that is now relatively well-known. Other applications are hardly mentioned, and in general, knowledge about the broader use of AI is limited.

General enthusiasm for ChatGPT, but lack of awareness concerning data use and future developments

Nevertheless, there is a degree of enthusiasm among consumers about the possibilities of ChatGPT. They use it for work or school assignments, generating texts, and getting answers to practical questions. What is striking, is that consumers hardly think about what happens to the data they share, and whether this is desirable. They often do not consider the information they share with ChatGPT to be privacy-sensitive either.

“It collects quite a lot of information. The more I use it, the better the answers it gives me.”

Consumer from qualitative research

However, that limited knowledge also generates concerns, with consumers wondering where the continuous development of AI will ultimately lead; for example whether AI will become smarter than humans in the future. There is also concern about possible abuse scenarios, such as deepfakes.

Commercial applications of AI are also not picked up on

The other noteworthy aspect, is that possible commercial applications of AI are hardly mentioned. The only application mentioned was the expectation that chatbots of organizations will become smarter in the future. Consumers assume that the data they share with these bots will be treated in the same way as information they share with a customer service team over the phone.

“I don’t care if it’s a robot or a human. People also learn from the conversations they have with one another. You don’t have to ask permission for that either.”

Consumer from qualitative research

The role of AI in processing and analyzing collected data is not spontaneously mentioned in any of the groups. Even when asked specifically about this subject, it turns out to be an elusive topic for most respondents. Due to the lack of knowledge about how AI is applied by organizations and how their data is processed by it, consumers currently do not feel that AI is making new demands in terms of how to deal with their online privacy.

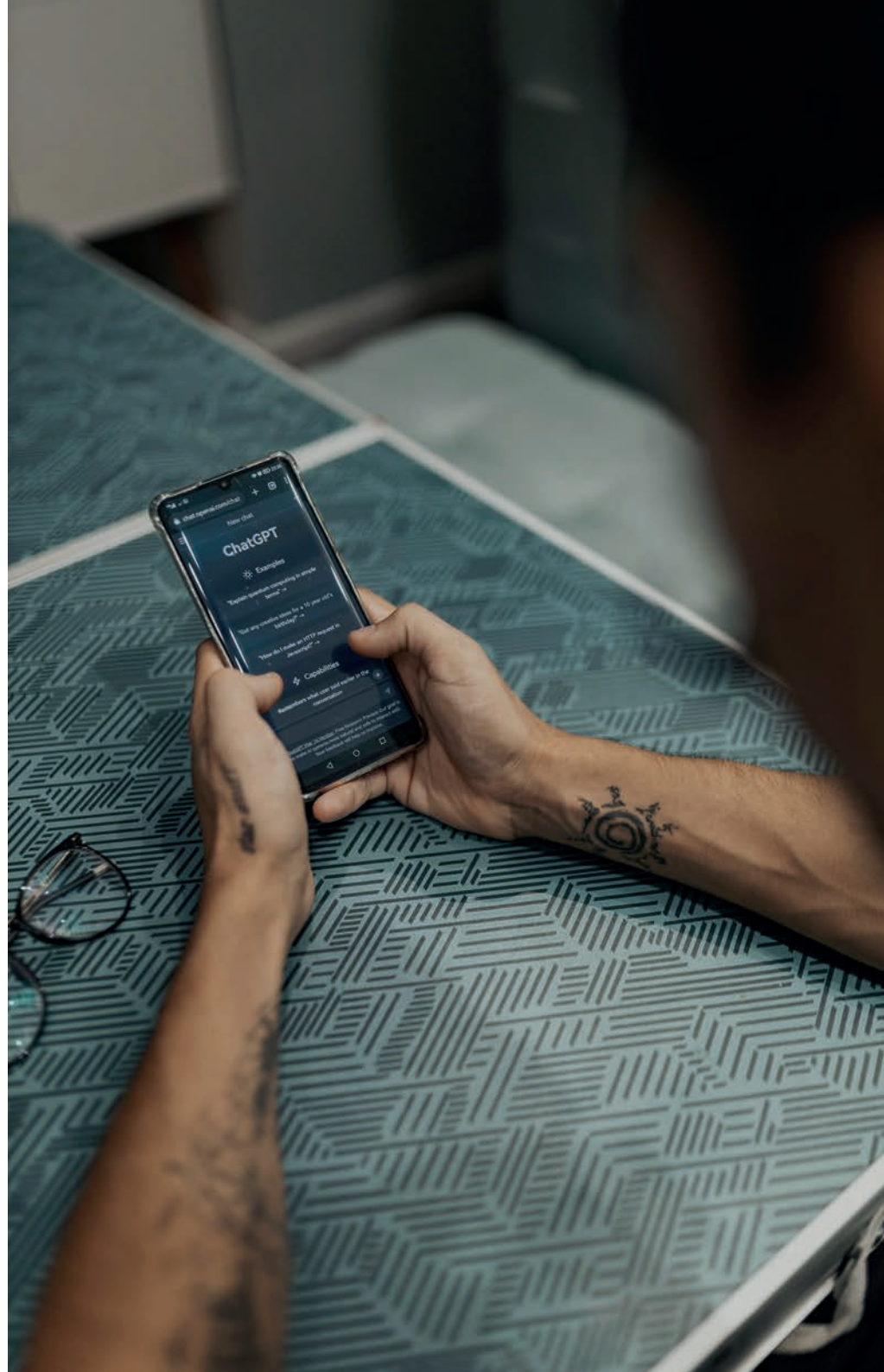
Trust and awareness needed for further AI adoption

AI adoption follows the pattern of Rogers' innovation adoption curve¹, which describes five phases of technology adoption. At present, AI is not yet fully integrated among the majority of users, but different groups are at varying stages of adoption:

- ▼ **Innovators:** The first group of users has fully embraced AI and have developed it further. They played a crucial role in making user-friendly AI tools accessible, and are often at the forefront of exploring new technologies.
- ▼ The **pioneers** (also known as the early adopters), often individuals and organizations interested in new technologies, also see the benefits of AI, and have now actively started to implement them, for example in the use of generative AI and automation possibilities.
- ▼ The **early majority** is showing an increased interest, especially for practical and accessible applications. This broader group of consumers and organizations is starting to open up to AI, but there are still hurdles to conquer, such as the lack of knowledge, and concerns about privacy and ethics, which can stand in the way of broader adoption.

There is an important task ahead for organizations to create trust and awareness among consumers in order to further promote AI acceptance. This can be done by being transparent about how AI is implemented, what data is collected, and what risks and benefits it holds for consumers.

¹ Rogers, E. M. (1962). *Diffusion of innovations*. Free Press of Glencoe.



Laws and regulations regarding online privacy and data sharing

How organizations should be informing consumers about online privacy and data-sharing



Introduction

A fine totalling 4.75 million euros was issued to **Netflix**. It sounds like a remarkable news item, but at the same time it represents a clear warning to every organization that processes personal data. The Dutch Data Protection Authority (AP) imposed the fine because Netflix did not comply with their legal obligation to provide information under the General Data Protection Regulation (GDPR). The regulator's stricter approach emphasizes how important it is to handle consumer privacy and communication surrounding this subject with due care.

The GDPR has been in force since 2018, and organizations have a legal obligation to be transparent about the use of personal data. Whether you collect email addresses for a newsletter, or use data to gain a better understanding of your target group: the rules of the GDPR are applicable in every instance. Providing clear and accessible information about how you process data is not only a legal requirement, but also a way to gain and maintain the trust of consumers.

As a responsible organization – or data controller in terms of the GDPR – you have a responsibility to provide visitors to your website with insight and control over their data. This demands clear communication, so that consumers can make an informed choice about the use of their personal data.

In this chapter, we will discuss the key legal requirements, and provide practical guidance on how to inform consumers in an effective manner. Through these recommendations, we are not only providing companies with tools for legal compliance, but also contributing towards promoting transparency, trust and an ethical approach to communication.

What obligations do organisations have to provide information?

According to the GDPR, organisations must inform consumers about the use of their personal data in a **clear and accessible** manner (GDPR Articles 12 and 13). This obligation is applicable **before** data is processed, and forms the basis for the transparent and fair handling of data. It means that you are required to communicate proactively and clearly about what data you are collecting, why you are collecting it, on what legal basis you are doing so, and the rights that consumers are entitled to.

This information must be easy to find, for example via a visible link on the website to a **privacy statement**. This document serves as a central point consumers can head to when seeking answers to their questions about data processing. It is important that the language and layout of the statement are in line with the target group, so that the content is both correct and comprehensible.

For marketing purposes, consent and legitimate interest are the most common bases for processing

If you are working on the basis of consent, which is most secure when obtained in the right way, make sure that it is given voluntarily, specifically, unambiguously and demonstrably. The process for this must be simple and transparent, so that consumers understand exactly what they are agreeing to. Legitimate interest offers more flexibility, and can in practice provide additional benefits for marketing purposes, but it requires a careful balance between the interests of the organization and the privacy of data subjects. It is essential to properly document this consideration, and to clearly inform the consumer about the basis used for this purpose.

If you're looking to know more, then read our article on [legitimate interest](#).

Some data processing, such as the provision of a service requested by the consumer, may be based on the **execution of a contract**. Please note that this basis is limited to what is strictly necessary for the provision of that particular service. In the case of marketing activities, processing may be necessary for an agreement, but in practice this is rare, because it is often difficult to substantiate this in a convincing manner.



Regardless of the basis: remember that you must always offer consumers an opt-out and actively inform them

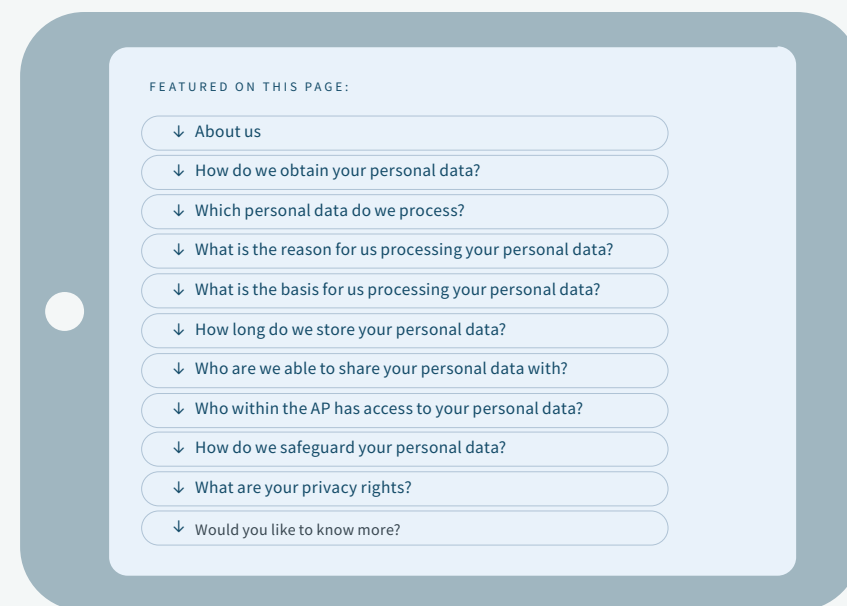
How do you inform the consumer about the processing of personal data?

It is therefore important to inform consumers about what happens to their data, which is also pointed out by the EDPB (European Data Protection Board). It may even be the case that there is an unfair commercial practice when consumers are not correctly informed about the use of their data by an organization, **ACM explained**. But how can you do this in the right way?

A privacy statement is one of the most commonly used means to provide this information. Although there are no strict requirements in terms of design, the content and structure must adhere to the principles of accessibility and comprehensiveness. The use of a layered structure is recommended for that purpose, in which you present the most important information, such as the identity of the organization and the key points of data processing, at least within the first layer.

A carefully drafted privacy statement can help to provide clarity to consumers on how their data is processed. **Beware, however: this statement must be easy to find**, for example via a prominent link on the homepage of your website or in your communication. This way, you not only create transparency, but also ensure that consumers feel they are both being heard and taken seriously.

The following is an example of a layout:



Source: *AP Privacy Statement / Dutch Data Protection Authority*

What does a privacy statement look like? Which elements should you incorporate?

You should not forget to include the following in your privacy statement:

- ▼ The identity and contact details of the organisation
- ▼ The contact details of any data protection officers (DPO)
- ▼ The purpose behind the processing of personal data, and the basis for doing so. If the basis is legitimate interest, make sure that the nature of the interest is stated (such as commercial interest).
- ▼ The (categories of) recipients of the personal data.
- ▼ Whether you intend to transfer the personal data outside the EEA or to an international organisation, and if so, state the legal basis for doing so.

Privacy statement, or privacy policy: what is actually the difference?

Privacy policy is for **internal** use: the rules and guidelines in the policy tell employees how to handle all personal data collected by an organization.

Privacy statement or general terms and conditions?

In a privacy statement, an organization explains which personal data is collected, for what purposes, how it is protected, and what rights data subjects have. In the general terms and conditions, you will find the rights and obligations of both the organization and the customer, such as liability and payment terms, but also more information related to the business activities.

In addition, it is good to mention, among other matters, the retention period of the data and rights of the data subjects.

An example

Suppose your organization is looking to offer transparency about building customer profiles, where will you place this information?

- ▼ Privacy statement: this is where you inform visitors about combining data to build a profile, and where you should state the following:
 - The fact that the organization builds customer profiles.
 - The purpose and legal basis for doing so (such as legitimate interest).
 - How customers can object (opt-out).
- ▼ Terms and conditions: If profiling is an essential part of your organisation's services, you can also include information about this in the terms and conditions.



Cookies taste better with clear communication

So, what if you use cookies as well? In addition to the privacy statement, it is also required that you inform consumers of this fact via a **cookie banner** and **cookie statement**.

A cookie banner specifically informs consumers about the use of cookies and other tracking technologies. Cookies often collect personal data, such as IP addresses or surfing behavior, and can therefore affect the privacy of the visitor to your web page. According to the 'Cookie Clause' (Article 11.7a of the Telecommunications Act), **the visitor's consent** is obligatory for the placement of non-essential cookies.

Did you know that (certain) analytical cookies are also considered essential in the Netherlands? This means that you **do not** need permission for privacy-friendly analytical cookies, which can be useful if you want to analyze how a website is being utilized, with a tool such as Google Analytics. **[Read more about the use of cookies here.](#)**

Visitors should also have the option to refuse non-essential cookies, **without incurring any adverse consequences**. This means that a web page must be available to visitors at all times, even if they refuse cookies.

It is important to avoid deceptive methods, also known as '**dark patterns**' when obtaining consent for cookies, such as making certain buttons less noticeable for instance: this prevents visitors from making an informed choice. In addition to being required by law, we also see a trend of stricter enforcement by the AP. Moreover, consumer confidence in an organization is increased when provided with honest and clear communication, which starts with their first look at the website: the cookie banner.

Important matters to know:

The following techniques are also subject to the rules for cookies: placing non-essential data on the user's device, for example via local storage, tracking pixels, web beacons and fingerprinting.

What is the proper way to configure a cookie banner?

The AP issued the following advice on this item:

- ▼ Provide information about the purpose
- ▼ Don't automatically check boxes
- ▼ Use clear wording
- ▼ Place different choices on one layer
- ▼ Don't hide certain choices
- ▼ Don't make someone have to use additional clicks
- ▼ Don't use an inconspicuous link in the text
- ▼ Be clear about withdrawing consent options
- ▼ Do not confuse consent with legitimate interest

Source: [Clear and misleading cookie banners | Dutch Data Protection Authority](#)

If you'd like to create your own compliant cookie banner, then check out our [Cookiebanner checklist](#).

Don't forget to refer to the cookie or privacy statement in the cookie banner!

Standard cookie banner generators: what are the points of attention?

Cookiebot, ConsentManager or Onetrust: if you've ever created a cookie banner, you'll undoubtedly be familiar with those platforms. They facilitate the availability of consent for categorized cookies (marketing, analytics, functional, etc.). Despite the fact that these are very useful tools with plenty of potential to create a good cookie banner, we often see that these types of cookie banners are not always set up correctly. Therefore, we always advise that you check the standard design of a 'GDPR-compliant' cookie banner yourself when you decide to use a CMP (Consent Management Platform). You can do this by going through the above rules of thumb.

If you're looking to find out more, you can read our article about [CMP's](#) here.

Also take a look at [Coolblue's cookie statement](#), which clearly emphasizes the benefits for the consumer.

DA maakt gebruik van cookies

We gebruiken cookies om content en advertenties te personaliseren, om functies voor social media te bieden en om ons websiteverkeer te analyseren. Ook delen we informatie over uw gebruik van onze site met onze partners voor social media, adverteren en analyse. Deze partners kunnen deze gegevens combineren met andere informatie die u aan ze heeft verstrekt of die ze hebben verzameld op basis van uw gebruik van hun services.

Cookiebot by Usercentrics

Noodzakelijk Voorkeuren Statistieken Marketing [Details tonen >](#)

Alle cookies toestaan

Selectie toestaan

Alleen noodzakelijke cookies

Source: [DA.nl | Personal health advice for you](#)

Deze website gebruikt cookies

We gebruiken cookies om inhoud en advertenties te personaliseren, om functies voor sociale media aan te bieden en om ons verkeer te analyseren. We delen ook informatie over uw gebruik van onze site met onze partners op het gebied van sociale media, reclame en analyse, die deze informatie kunnen combineren met andere informatie die u aan hen hebt verstrekt of die zij hebben verzameld via uw gebruik van hun diensten. U kunt deze accepteren, wijzigen of weigeren. Hier vindt u [Google's privacybeleid](#) en [LOAVIES privacybeleid](#).

ALLES ACCEPTEREN

Source: [LOAVIES | Shop Fashion Online](#)

Cookiebot by Usercentrics

Consent **Details** **About**

This website uses cookies

DDMA wants to make your visit to the website as easy and personalized as possible. To achieve this, we use cookies and similar technologies. This ensures that you see relevant DDMA advertisements on other websites, that we can create lookalikes on social media, and that we can map out behavior on our website. Prefer not to? In that case, we will only place essential and statistical cookies. These cookies do not collect any data about you as an individual. By clicking the 'clip' icon in the bottom left corner of the webpage you're visiting, it is possible to withdraw (or change) your consent. Want to know more? Then read our [Privacy Statement here](#).

No thanks **I agree**

Source: [DDMA](#)

AI & Privacy

In 2025, tools like ChatGPT have become indispensable in our daily lives. Whether it's drawing up a content plan or writing a newsletter: through a few simple prompts, you can conjure up an entire text in next to no time, often faster and better than you could have done yourself within that timeframe.

But don't let the convenience of these tools fool you: what at first appears to be a harmless application can harbor major risks. Take the free version of ChatGPT, for example: everything you enter is stored, and can be used for further training purposes for the tool. This means that personal data may be processed. And there are important obligations attached to this, such as having a legal basis, and complying with the obligation to provide information before processing data.

In other words, these tools are powerful, but certainly not without risks. As an organization, it is crucial to be aware of this fact, and to think carefully about how you use technology of that nature, especially if you work with customer data.

If you do decide to use personal data in a tool like ChatGPT, we have come up with a few tips:

- ▶ Provide a valid basis, such as consent or legitimate interest
- ▶ Avoid using sensitive data, such as medical data. Moreover, consider the following: would I post this prompt on a public platform? If the answer is no, then don't enter it as a prompt!
- ▶ Check the conditions of the tool thoroughly! The free version of ChatGPT uses automatically transmitted data for training purposes, while the business version, such as ChatGPT Enterprise, does not by default, to safeguard privacy.

If you're looking to find out more about the responsible use of AI in your organization's marketing strategies, then view the [Responsible AI Marketing Guide](#) here.

Consumer rights: what should you pay attention to?

One of the core principles of privacy legislation, such as the GDPR, is to enhance the level of control consumers have over their personal data. That sense of control, which also emerged from the group discussions with consumers for the study, arises in two instances: when an organization provides the correct information in a privacy statement or cookie banner, but also when consumers are able to actively exercise their rights. Transparency and offering genuine choices are key in this regard. These are the most important rights consumers have under the GDPR.

Firstly, consumers have the **right to access** their data. They can submit a request to find out what data an organisation processes about them, for what purpose this is done, and with whom this data is shared. In addition, they have the **right to rectification**, which allows them to request that any inaccurate or incomplete data be corrected. Consumers also have the **right to have their data deleted**, for example when it is no longer needed for the original purpose or if consent has been withdrawn. Furthermore, the GDPR provides consumers with the **right to data portability**, so that they can receive their data in a structured, commonly used format, and transfer it to another service provider. Finally, consumers have the **right to object** to specific processing of their data, such as for direct marketing, whereby organizations must always (!) stop any processing of that data.

Organizations are obliged to comply with the above requests within one month. It is essential to remember to inform consumers about this 'at the time of the first moment of contact at the latest', which must be included in the privacy statement.



Recommendations

- ▼ **Inform the consumer:** communicate clearly about the use of data by your organization in a privacy statement. Use the recommended 'layer structure', and ensure that the most important information is included in the first layer. Make privacy statements as simple as possible for consumers by using icons, symbols and fold-out sections.
- ▼ When **transparency is added to cookies, they taste better to consumers:** be critical when using standard cookie banners, also when deciding to make changes to the standard version of the cookie banner generators. Inform consumers in understandable language, and be comprehensive when wording your explanations, but take care to avoid information overload.
- ▼ Although it's a cliché, the **the customer comes first:** make sure that, in addition to the possible risks of sharing data, the benefits for the consumer are also clearly reflected in the information. That way you will have all areas covered, as well as also becoming more appealing to consumers with regard to them sharing their data.
- ▼ **Immerse yourself in your customer's level of knowledge:** extend a sense of control to potential customers. Research shows that consumers are willing to share more if there is clear communication.
- ▼ Consider the **overall look and branding** of your organization: research also shows that consumers are more likely to share information, or be more inclined to pay for certain matters when they trust an organization, and are attracted to the appeal of a company.
- ▼ **Do not create unnecessary barriers:** consumers should not be discouraged from exercising their rights, through complicated procedures or costs for example. In addition, act quickly: the law requires that privacy requests by consumers regarding their rights must be followed up within one month.
- ▼ **Stay up to date with the latest developments:** at DDMA, we regularly organize events, such as the monthly Legal Member Meet-up, and write articles that keep you informed of the latest trends and updates in the field of privacy. Members also know how to find us through our Legal Helpdesk, where all privacy and advertising law questions are quickly provided with practical advice. Want to stay informed? [Sign up here for our legal newsletter.](#)

Research methodology



The report contains results from two studies:

1. Group conversations with Dutch consumers

Method

Qualitative research, conducted through focus groups.

Research agency

Execution and analysis carried out in conjunction with qualitative research agency CO-efficient.

Target group and sample

The group conversations took place in the form of 3 focus groups on location: 1 group of pragmatists, 1 group of unconcerned individuals, 1 group of sceptics - a total of 24 respondents.

Fieldwork period

November 2024

2. Global Privacy Monitor

Method

Quantitative research, conducted by means of an online survey.

Research agency

Carried out by the GDMA (the umbrella organization of DDMA) in collaboration with Foresight Factory.

Target group and sample

For the 2022 Global Privacy Monitor, 20,626 respondents were questioned from 16 countries, including 1039 Dutch respondents representative of the Dutch population aged 18 and over (weighted afterwards by gender, age and region).

Fieldwork period

December 2021

Colophon

Publisher

DDMA
WG-plein 185
1054 SC Amsterdam
T: 020 452 8413
E: info@ddma.nl
W: www.ddma.nl

Authors

Nanda Appelman (Market Insights Specialist, DDMA)
Allisha Hosli (Legal Counsel, DDMA)
Isa Nieuwstad (Legal Counsel, DDMA)

Final editing

Bob Younge (Content and Communication Specialist, DDMA)

Do you have any questions or comments about this research?
If so, send an e-mail to info@ddma.nl.

About DDMA

DDMA is the largest trade association for marketing and data. We are a network of more than 360 brands, non-profits, publishers, agencies and tech suppliers who want to use data successfully and responsibly for marketing purposes. We identify developments in the field of technology, regulations and ethics and bring together marketers, data specialists and lawyers to help them grow in their profession. We also promote self-regulation, and are a discussion partner for policymakers and regulators.

For all DDMA studies, please visit: ddma.nl/research-insights