EU PHARMACY WEBSHOPS: HOW GDPR VIOLATIONS PUT CUSTOMER TRUST AT RISK

USERCENTRICS

KEY INSIGHTS

Our website scans show that EU residents are being tracked without consent when visiting online pharmacies. This sharing of sensitive personal data with commercial third parties is in clear breach of the EU's General Data Protection Regulation (GDPR) and its cookie consent requirements.

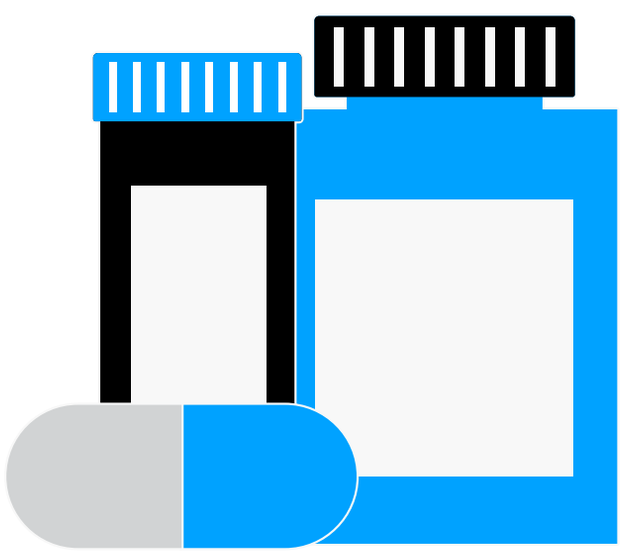
89% OF THE 150 MOST POPULAR ONLINE PHARMACIES IN THE EU FAIL GDPR COMPLIANCE BY SETTING A MINIMUM OF ONE NON-NECESSARY COOKIE WITHOUT END-USER CONSENT.

55% OF ALL NON-NECESSARY COOKIES WERE ACTIVATED AND IN USE ON THE WEBSITE'S LANDING PAGE WITHOUT ANY USER CONSENT.

62% OF COOKIES SET WITHOUT THE USER'S CONSENT ARE THIRD-PARTY MARKETING COOKIES.

The Cookiebot CMP scanner is able to detect whether cookies and trackers are being set prior to any type of user consent (i.e. activated and in use on a website's landing page despite no consent from end users). It does this by performing fully rendered user simulations to discover, locate and identify all cookies and trackers that are active on all subpages of any given website.

For this report, deep domain scans were performed on all subpages of each pharmacy webshop domain. Up to 10,000 pages were analyzed for each domain - corresponding to a total scan of 1,089,438 pages, an average of 7,078 pages per domain. All scans were performed in February 2022.



INTRODUCTION

In February 2022 we scanned pharmacy webshops in the EU to check the degree of GDPR cookie consent compliance on commercial websites that process sensitive personal data of European residents, including data about mental health medications, diabetes treatment, sexual health ailments and contraceptives, COVID-19 tests, addiction treatments, and much more.

Our scan research was conducted on the 150 most popular online pharmacies and medical webshops across 10 EU member states, selected from the top results on Google, with an average size of 7,078 subpages and an average monthly traffic of 495,000 visits.

The results paint a grim picture: 89% of the 150 websites were not compliant with the GDPR requirements for obtaining end-user consent before processing any personal data via cookies.

More than half (55%) of all cookies in use on the most popular online pharmacies in the EU are operating without end-user consent. Out of the total number of cookies set without end-users' consent, 62% are third-party marketing cookies.

The results of our latest report reveal worrying GDPR compliance failures across a major privacy-sensitive sector in the EU. This can be attributed to the fragmented market, which offers a multitude of consent management solutions, but also to the difficulty of living up to data privacy regulations while running an online business that is dependent on data to drive revenue. Therefore, solutions are needed that help balance data privacy with data-driven business for companies in the fast-developing consent-centric internet economy.

Since the GDPR came into force in 2018, data privacy has evolved from an obscure legal requirement into a strong consumer demand and metric of brand reputation. Respecting end-user consent through transparent and compliant use of cookies and trackers is therefore vital for any online business wishing to build consumer trust.

Tilman Harmelin
Usercentrics Entrepreneur in Residence

LACK OF TRANSPARENCY IN HANDLING SENSITIVE DATA

Almost all of the 150 most popular online pharmacies in the EU fail at GDPR compliance — i.e. set a minimum of one non-necessary cookie without end-user consent, allowing sensitive personal data to be collected and shared by third parties when EU residents browse and buy pharmaceutical products.

What kind of data is being collected?

Personal data generated and processed when EU residents visit these 150 online pharmacies can include:

- **User purchases**
- **Search and browsing history**
- **On-site behavior (such as scrolling speed and how their mouse moves)**
- **Sites they visited before**
- **Previous web searches**
- **IP addresses and other identifiers**

All this data can be combined into detailed profiles about each individual user, revealing information about who they are and their physical and mental health.

Privacy-sensitive products sold on the 150 EU online pharmacies include: antidepressants and anti-anxiety medicines, diabetes medicines, products related to reproductive health, (such as menstrual and menopausal products), products related to sexual health and sexual orientation, (such as pregnancy tests, contraceptives and LGBTQIA+ products), products related to high blood pressure and heart disease, and products for smoking cessation and other addiction treatments.

The market for pharmaceutical products is one of the fastest growing sectors in European e-commerce. Between 2020 and 2024, growth in this area is expected to reach nearly EUR 9.5 billion*.

Consumers are spoiled for choice when it comes to choosing among providers of largely equal quality, so the issue of data protection is playing an increasingly important role in their choice.

CONSUMERS DEMAND MORE DATA PROTECTION

In contrast to the staggering rates of noncompliance found in this scan research, consumers are increasingly demanding enhanced data privacy based on transparency and consent from the companies and brands they do business with. A 2021 study by CISCO shows that the effect of losing customer trust, and the accompanying long-term reputation damage, should not be underestimated as risks to loss of sales and revenue.

79% **OF CONSUMERS SAY THAT DATA PRIVACY IS A BUYING FACTOR FOR THEM.**

47% **OF CONSUMERS SAY THEY HAVE SWITCHED COMPANIES OVER THE COMPANY'S DATA POLICIES OR DATA SHARING PRACTICES.**

19% **OF CONSUMERS SAY THEY HAVE TERMINATED A RELATIONSHIP WITH A RETAILER, E-COMMERCE WEBSITE, AND/OR ONLINE BUSINESS OVER THEIR DATA POLICIES OR DATA SHARING PRACTICES.**

USER CONSENT IS KEY TO SUCCESSFUL DATA-DRIVEN BUSINESS

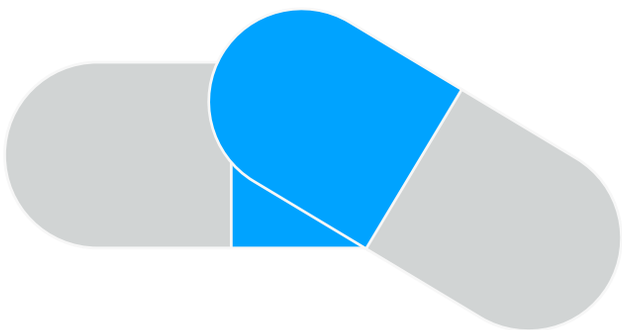
The figures from the Cisco study paint a clear picture: **data privacy has become a consumer demand and a metric of brand reputation**, influencing customer choices in ways similar to how "sustainability" and "being organic" now adds value to brand image.

Consumers welcome data protection laws and regulations such as the EU's GDPR, with 60% saying that they have a positive impact on the protection of personal data (53% more than in 2020, according to the study).

As an e-commerce website, to take data privacy legislations seriously is to take customer demand seriously.

Building consumer trust through compliance with global privacy regulations is a must for online businesses in the coming years, considering the steady increase in the numbers of consumers who are willing to act to protect their data privacy.

In the post-cookie era, **data-driven business models will only be successful if they function on the basis of valid user consent**, and companies that already rely on a user-centric and transparent data processing strategy will ultimately have a decisive competitive advantage.



WHAT CAN COMPANIES DO NOW?

With this special scan report, we at Usercentrics wish to create awareness about non-compliance across an important privacy-sensitive industry in the EU in order to help companies achieve a better balance between data privacy and data-driven business.

If you already have a consent management platform (CMP) implemented on your website, we suggest that you reach out to your provider to determine whether any non-necessary cookies and trackers are being activated without end-user consent on your website, as this is the crux of cookie compliance under the EU's GDPR.

If you do not currently have a consent management platform for your website, or are looking to switch, we would be happy to arrange an appointment with the right contact person at your company. Cookiebot CMP and Usercentrics have recently merged, and we can therefore offer a wide range of different compliance solutions that meet your company's specific requirements.

ABOUT US

Usercentrics is a global market leader in the field of consent management platforms (CMP). Cookiebot CMP and Usercentrics have recently joined forces, allowing us to offer a wide range of compliance solutions to meet your company's specific requirements. We enable businesses to collect, manage and document user consents on websites and apps in order to achieve compliance with global privacy regulations, while facilitating high consent rates and building trust with their customers.

We believe in creating a healthy balance between data privacy and data-driven business, delivering solutions for every size of enterprise. Cookiebot CMP is our plug-and-play SaaS for smaller businesses and organizations, App CMP handles user consent on mobile apps, and Usercentrics CMP serves companies with enterprise-grade custom requirements for unifying consent and data from capture to processing.

VISIT USERCENTRICS.COM AND COOKIEBOT.COM TO LEARN MORE.

EXTERNAL RESOURCES

2021 CISCO STUDY: BUILDING CONSUMER CONFIDENCE IN THE AGE OF PRIVACY THROUGH TRANSPARENCY AND CONTROL

EU PHARMA E-COMMERCE MARKET TO GROW BY USD 10.69 BN DURING 2020-2024

BEYOND THE FRONT PAGE: MEASURING THIRD PARTY DYNAMICS IN THE FIELD

APPENDIX

USERCENTRICS

SCAN DATA

Method: The Cookiebot CMP scanner was used to perform deep domain scans of all subpages of each pharmacy webshop domain. Up to 10,000 pages were analyzed for each domain, corresponding to a total scan of 1,089,438 pages, an average of 7,078 pages per domain. All scans were performed in February 2022.

COUNTRY	PERCENTAGE OF SCANNED DOMAINS SETTING AT LEAST ONE NON-NECESSARY COOKIE WITHOUT ANY USER CONSENT	AVERAGE NUMBER OF NON-NECESSARY COOKIES SET WITHOUT ANY USER CONSENT
Germany	100%	14.3
Austria	94%	11.5
Switzerland	78.5%	20.2
France	91%	16.5
Italy	82.5%	23
Spain	86%	21.3
Netherlands	100%	23.3
Denmark	89%	15.4
Sweden	87.5%	26.3
Norway	84%	22

Further access: As the sample for this report is anonymized, we cannot share a direct link to the individual scan results per domain. However, should you have any additional questions regarding the report, please feel free to send us an email at research@usercentrics.com. We will reply to your request as soon as possible.

MOST COMMON REASONS FOR GDPR NON-COMPLIANCE ON WEBSITES

- Website does not have a Consent Management Platform (CMP) implemented that can control cookies and handle end-user consent.
- Website employs a custom CMP that does not meet the requirements of the EU's GDPR for controlling all cookies based on end-user consent.
- Website employs a CMP that is incapable of detecting all known cookies and trackers across all subpages. (The website owner/operator may not have realized the limitations of the CMP.)
- The CMP has been incorrectly implemented or lacks the most recent updates, making it unable to detect and control all known cookies across all its subpages.
- Website operator has chosen not to employ the CMP correctly so as not to lose data that is valuable for revenue and analytics.

METHODOLOGY

HOW DID WE SELECT THE TOP EU 150 ONLINE PHARMACY WEBSHOPS?

In this investigation, we used the scanning technology of our consent management platform Cookiebot CMP to **scan the top 150 online pharmacy websites in the EU and detected a total of 6,606 cookies.**

Selected from the **top results on Google** in ten EU member states — with an average size of 7,078 subpages and average monthly traffic of 495,000 visits — the 150 EU webshops are some of the most popular websites in the online pharmacy industry in the region.

These websites are **important EU digital infrastructure** that not only deliver large quantities of medications and pharmaceutical products to EU residents (especially during a pandemic, where more people than ever have been shopping online), but also process significant amounts of sensitive personal data from their end users every day.

HOW DOES THE COOKIEBOT CMP SCANNER WORK?

The Cookiebot CMP scanner is **able to detect whether cookies and trackers are being set prior to any type of user consent** (i.e. activated and in use on the website's landing page despite no consent from end users).

The Cookiebot CMP scanner performs **fully rendered user simulations** to discover, locate and identify all cookies and trackers that are active on all subpages of any given website.

The Cookiebot CMP scanner **simulates multiple users** (7-8 on average) visiting a website simultaneously and performs all actions that real users potentially would. The simulated users will scroll through up to 10,000 subpages, clicking all links, menu items and buttons. They will move their cursors around and play and pause embedded video or audio content. During these simulated sessions, the scanner monitors all network traffic between the website and the "browsers" of the simulated users, as well as any traffic sent to other websites. The scanner uses this data to **identify all cookies and trackers** that are activated as a result of the simulated users and their on-site behavior.
The Cookiebot CMP scanner detects all cookies and trackers and catalogs all technical properties, such as name, type, duration/expiry period, its exact location within the source code of the website, as well as monitoring domain data to determine if third parties are controlling the cookie. All of the information that the Cookiebot CMP scanner finds is automatically logged in a global repository, which consists of millions of trackers that the scanner has encountered across the web.

HOW DOES COOKIEBOT CMP DETERMINE COMPLIANCE/NON-COMPLIANCE?

Important to know: The Cookiebot CMP scanning technology **does not state compliance, but only detects non-compliance.**

Cookiebot CMP detects any cookies that are being activated without end-user consent, and if any of these cookies can be classified as non-necessary (e.g. by being from a third-party provider or for the purpose of running analytics or marketing services), Cookiebot CMP can determine that the website **does not meet the compliance requirements of the EU's GDPR.**

It classifies unclassified cookies as necessary and does not state non-compliance for cookies set when imitating users, e.g. in the possible event of implied consent, despite not being best practice and specifically non-compliant according to several EU data protection authorities.

The Cookiebot CMP scanning technology does not find cookies properly withheld across all subpages nor cookies in use behind logins or restricted areas. It also does not find cookies that are set behind login or cookies properly withheld before end-user consent across all subpages on a website.

TERMINOLOGY EXPLAINER

WHAT IS A 'NECESSARY/NON-NECESSARY COOKIE'?

A 'non-necessary cookie' is any kind of cookie that is not strictly necessary for the most basic functions of a website. Necessary cookies are one of four categories of cookies (along with preference cookies, statistics cookies and marketing cookies). Common examples include cookies that handle user logins or shopping cart contents on a domain. Any cookie that tracks personal data from end users for the purposes of, for example, remembering language or currency preferences across visits, performing analytics services or engaging in marketing and digital advertising, cannot be classified as a non-necessary cookie.

HOW DO COOKIES WORK?

Cookies are usually small files that get set on an end user's browser when they arrive on a website. Here they will collect, process and share information (often personal data) about the end user in order to run analytics services about the website's performance or run marketing campaigns on the domain. Some cookies, like third-party marketing cookies, track personal data, including IP addresses, search and browser history and can stay active on user browsers for years. Since tracking cookies are often loaded in combination with other statistical and marketing cookies, it is almost impossible to detect and control them without the deep scanning technology of a Consent Management Platform (CMP).

WHAT IS A 'THIRD-PARTY PROVIDER'?

A 'third-party provider' simply means that the cookies and trackers on a website are not of the domain's own origin (first-party cookies) but are placed on the website and operated by third parties, usually through the use of analytics services (such as Google Analytics), social media plugins (such as Facebook or Twitter) or marketing services (such as HubSpot). The use of third-party services on a website is the most common way for third-party cookies to become embedded on a domain, e.g. featuring YouTube videos on a website.

WHAT IS A 'FIRST-PARTY COOKIE'?

'First-party cookies' are cookies that are hosted entirely on the website that users visit. Unlike third-party cookies that are operated by third-party providers, first-party cookies live entirely on the domain in question. However, first-party cookies are not always privacy-safe either, as they have also been known to transmit personal data to third parties through a complex set of tracking structures, e.g. pixel trackers that transmit end-user data to third parties, effectively bypassing the first-party concept, and therefore needing end-user consent to operate legally.

WHAT DOES 'COOKIE COMPLIANCE' MEAN ACCORDING TO THE EU'S GDPR?

In the EU, the GDPR and ePrivacy Directive form the overall data privacy regime that comes with specific requirements for how websites are allowed to use cookies and process the personal data of users inside the EU. Any processing of personal data of users inside the EU must be done on a legal basis, and the most common is 'with the consent of the end user'. If a website intends to use cookies that will process personal data from EU users, the website is required to inform its users with full transparency about such operations. Then the website must ask for and obtain the explicit consent from the end users before any activation of such cookies is legally allowed to take place.

'Cookie compliance' refers to this mechanism, in which a website must first ensure that its end users have given explicit consent before running cookies that will process their personal data. Any website that processes personal data from users located inside the EU is obligated to comply with the EU's GDPR, regardless of where in the world the company or website itself is located ('extra-territorial scope').

WEBSITES MUST COMPLY WITH THE FOLLOWING GDPR COOKIE COMPLIANCE REQUIREMENTS:

- Prior and explicit consent must be obtained before any activation of cookies (apart from whitelisted, necessary cookies).
- Consents must be granular, i.e. users must be able to activate some categories of cookies rather than others and not be forced to consent to either all or none.
- Consent must be freely given, i.e. not allowed to be forced.
- Consents must be as easily withdrawn as they are given.
- Consents must be securely stored as legal documentation.
- Consent must be renewed regularly, best practice is at least once per year.
- Some national data protection guidelines recommend more frequent renewal, e.g. every 6 months. Check your local data protection guidelines for compliance requirements.

WHAT IS A 'SUBPAGE'?

A subpage is any page on a website that is not the home page, e.g. a blog post, contact page or pricing page. A subpage can host its own variety of cookies that might differ from other subpages or the front page.

WHAT IS 'PERSONAL DATA' AND 'SENSITIVE PERSONAL DATA' UNDER THE EU'S GDPR?

Under the EU's GDPR, 'personal data' is any kind of information that relates to or can in any way be related to an identified or identifiable natural living person (known in the GDPR as a "data subject"). This can include IP addresses, search and browser history, location data (such as geolocation through a phone), email addresses, home addresses and names. 'Sensitive personal data' is a subcategory of personal data under the EU's GDPR that includes information revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation.