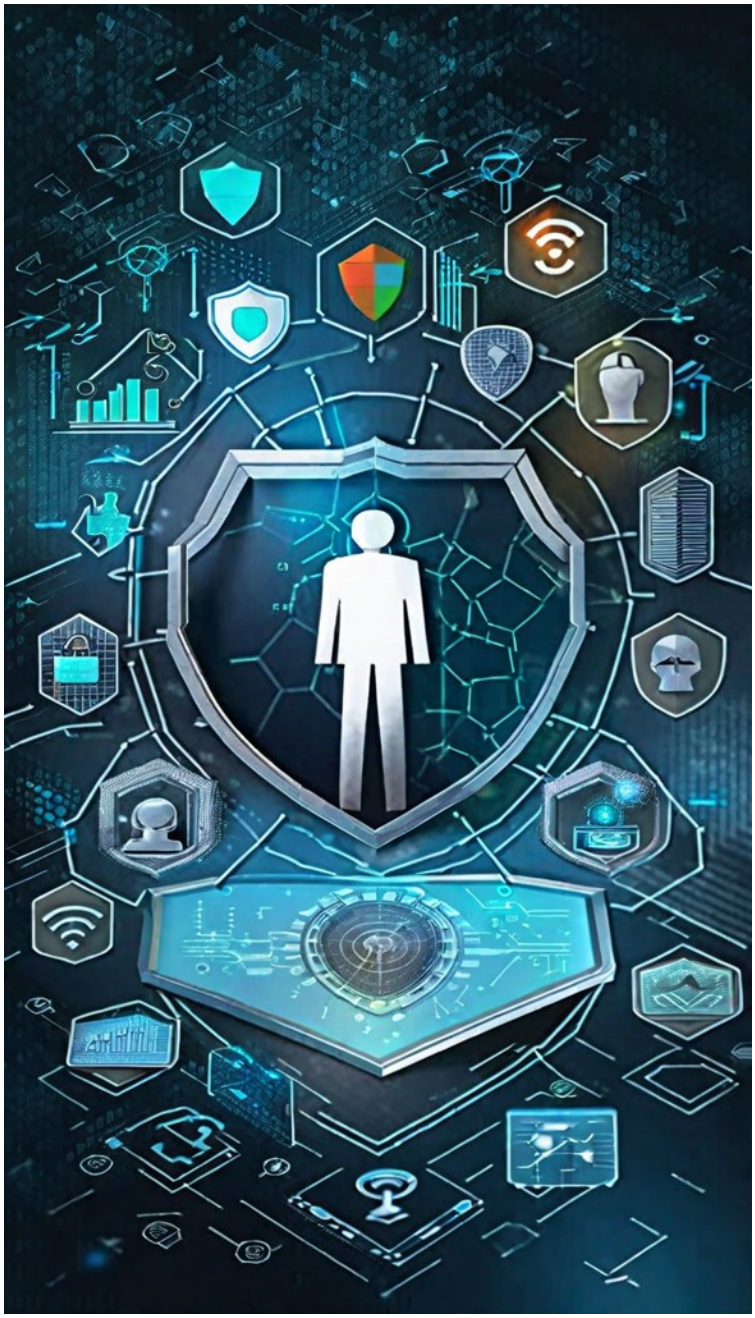
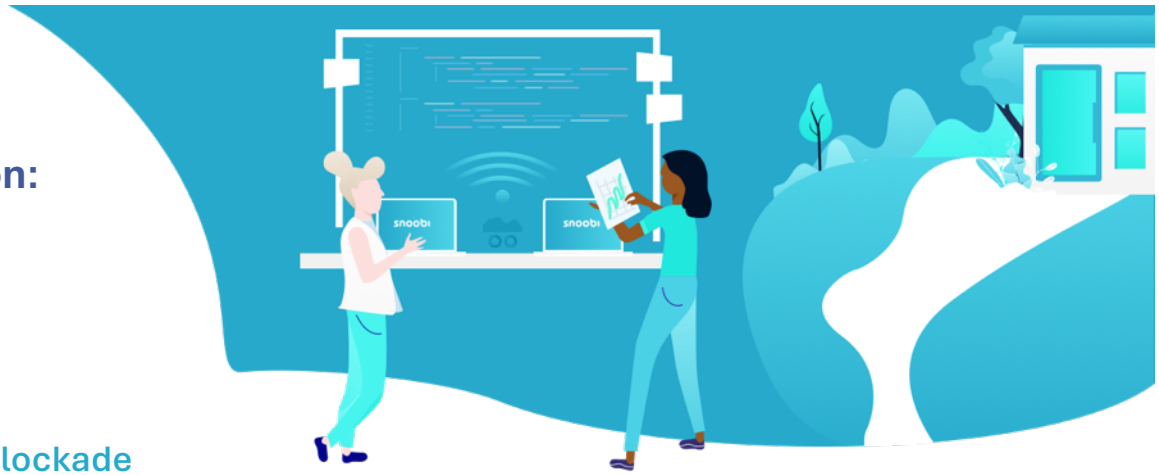
snoobi



White Paper

An overview of Privacy & Web Analytics

Introduction: cookies or cookieless



The cookie blockade

The 'cookie blockade' intensifies as privacy concerns reshape web analytics.
More browsers are blocking cookies by default, with an exception in Google Chrome, challenging marketers and data analysts' traditional tracking methods.
Third-party cookies or alternative storage solutions face increasing scrutiny, with privacy-conscious users mistrusting standard tracking approaches.
Consent managers attempt to bridge the data collection gap but often create 'consent fatigue' by overwhelming users with approval prompts. The analytics implementation demands a solution that balances valuable user insights with robust privacy protection. In general, it requires an innovative approach that respects user preferences while maintaining meaningful web analytics capabilities.

The rise of cookieless and hybrid analytics solutions

Emerging analytics solutions like Snoobi Analytics are approaching web data collection through a cookieless and hybrid approach. This overcomes traditional tracking limitations by collecting data without storing browser-based information. Aligned with data protection regulations, Snoobi Analytics offers flexible data collection methods that respect user privacy.

The Snoobi Analytics platform can leverage first-party data with user consent or operate entirely without cookies. This hybrid model enhances data accuracy and reliability, reducing vulnerability to browser privacy settings. By implementing such techniques, an organization can ensure comprehensive, compliant web analytics that balance detailed insights with stringent privacy standards.

Adapting to a changing environment: a strategic choice

The shift to cookieless and hybrid analytics models demands a fundamental redesign of data tracking strategies. Evaluating what data is truly essential and use ethical collection methods that respect user privacy is key. These emerging analytics solutions represent more than a technical update — they're a strategic transformation.

By proactively adapting to these changes, an organization can future-proof their data gathering approach while also building audience trust. The new analytics environment requires a detailed understanding of privacy-first methodologies, enabling organizations to select tools that can deliver robust insights within increasingly restricted data environments.

Staying informed and flexible remains crucial.
This white paper explains different ways to collect and analyze data while protecting privacy. It explores the available options, challenges, and how organizations can still benefit from analytics data.

Charles W.Odinot, Snoobi Technology, 2025

Index

About the Author

Charles Odinot is a specialist in privacy-friendly analytics technologies, dedicated to helping organizations navigate the evolving digital landscape while maintaining user trust and compliance. With deep expertise in privacy regulations, data analytics, and emerging tracking methodologies, Charles provides strategic insights into implementing ethical and effective data collection practices. As owner and CTO of Snoobi Technologies, his work focuses on developing solutions that balance business needs with privacy-first approaches, leveraging innovations such as cookieless tracking, differential privacy, and first-party data strategies.

Through his management of the developer team of Snoobi Analytics, research, consulting, and thought leadership, Charles contributes to shaping the future of analytics in a privacy-conscious world.

snoobi

Pseudo-anonymization vs. full anonymization

What is data anonymization

Data privacy is critical for website owners and users. Anonymization strategies are essential for protecting user information while enabling meaningful insights.

Web analytics tools employ different data handling techniques, including pseudo-anonymization and full anonymization, each offering distinct approaches to balancing user privacy, data analysis, and organizational compliance.

Pseudo-anonymization: a partial privacy shield

Pseudo-anonymization is viewed as a middle-ground approach to data protection. In this method, personally identifiable information is partially masked or replaced with artificial identifiers. While this technique appears protective, it leaves critical vulnerabilities that potentially could be exploited.

For instance, so called 'tracking cookies' still maintain a connection to the original user data. Websites using pseudo-anonymization may replace a user's direct identification with a randomly generated number. But the underlying potential to re-identify the user remains as the cookie or user information is still stored for future use.

Pseudo-anonymization provides only a low level of privacy protection that can be easily compromised by advanced data correlation techniques.

Full anonymization: the golden standard for user privacy

Full anonymization offers comprehensive user data protection by completely and unrecoverably removing individual identification possibilities.

Snoobi Analytics ensures data becomes truly depersonalized, enabling websites to gather insights without compromising privacy.

No tracking cookies are stored, and session data remains unique to a single session.

This approach fully aligns with GDPR and CCPA regulations. However, the trade-off is that subsequent user visits cannot be analytically linked, as individual user tracking is intentionally prevented.

Communicating privacy practices

Websites must communicate anonymization strategies transparently, clearly explaining data collection, processing, and protection.

By using plain language to describe privacy measures, organizations can build trust, meet legal requirements, and empower visitors as users of their website content to make informed privacy decisions.

Web analytics & browser cookie blocking

Web analytics has evolved significantly due to increasing privacy concerns and stricter regulations. Many browsers now actively block third-party cookies, and new tracking methods, such as first-party cookies and cookieless analytics, are gaining importance.

How browsers block cookies

- **Google Chrome:** Plans to phase out third-party cookies, replacing them with the Privacy Sandbox and topics-based targeting.
- **Safari (Apple):** Uses Intelligent Tracking Prevention (ITP) to block third-party cookies and limit first-party cookies to a short lifespan.
- **Firefox:** Enhanced Tracking Protection (ETP) blocks third-party cookies by default.
- **Microsoft Edge:** Includes tracking prevention settings that limit third-party cookies and other tracking mechanisms.
- Other browsers often use a similar mechanism, they block 3d party cookies.

Because of these changes, organizations should move towards privacy-friendly analytics solutions that rely less on traditional tracking methods.

What is lost when users block cookies

Marketing analysts lose critical insights: user journey mapping, attribution data, personalization, conversion rate optimization, and audience segmentation. Without cookies, understanding customer behavior, determining marketing channel effectiveness, serving tailored ads, and targeting specific user groups become significantly more challenging.

Types of cookies used in web analytics

Third-Party Cookies

- Can be set by domains or websites different from the one a user is visiting (e.g., advertising networks).
- The contents can be read by other tools than the analytics tool that placed the cookie.
- Are used for cross-site tracking, targeted advertising, and retargeting.
- Are increasingly blocked by browsers, reducing the effectiveness.

First-Party Cookies

- Are stored by the website a user visits (e.g., for login sessions, language preferences, and site analytics).
- Have less restrictions but are still impacted by privacy regulations and browser limitations.
- The lifespan is shortened in some browsers (e.g., Safari restricts them to 7 days or less).

Cookieless Analytics

- Uses server-side tracking, consent frameworks, fingerprinting, or anonymized first-party data.
- Relies on event tracking and aggregated data instead of individual user tracking.
- Is more compliant with privacy laws (e.g., GDPR, CCPA) but offers less detailed user insights.

Any method other than fully anonymized first-party data is still impacted by privacy regulations and needs user consent.

How a hybrid web analytics solution helps overcome the issues

A hybrid solution allows for (1st party) cookies to be set when the user gives consent. This can be done on a visit-by-visit basis. When a consent storage tool is used the user doesn't need to provide consent for every subsequent visit but should still be allowed to withdraw consent.

When the user doesn't consent, a web analytics tool such as Snoobi Analytics then does not store any cookie but fully anonymizes the user's session. *Retargeting and audience selection may not be possible, but the main metrics and page-by-page analysis of website traffic is fully enabled*.

Using 'Required Cookies'

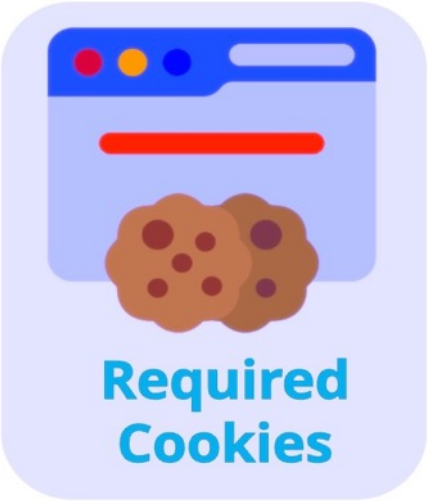
Required cookies, also known as essential cookies, are critical website components that ensure proper functionality and legal compliance. These mandatory cookies are automatically implemented without requiring user consent, serving fundamental technical and regulatory purposes for the website's optimal operation and performance.

When it comes to website analytics, below is some information on what should and should not be included in required cookies.

What should be included in required cookies for analytics

- **Session ID cookies:** These helps keep track of a user's session (e.g., remembering their login or keeping items in a shopping cart).
- **Load Balancing cookies:** These helps distribute traffic across servers for a speedy website response.
- **Security & Fraud Prevention Cookies:** These protect against attacks and unauthorized access.
- And any other cookie that the website needs to function properly.

These cookies are limited in scope and may 'live' only during the user's session.



What should NOT be included in required cookies for analytics

- **Personally Identifiable Information (PII):** Emails, names, phone numbers, or addresses.
- **Exact Location Data:** Unless explicitly required and with full user consent.
- **Health, Financial, or Legal Data:** Can lead to compliance violations.
- **User Tracking Cookies:** Cookies that track browsing behavior (e.g., what pages you visit or how you navigate over a page).
- **Advertising Cookies:** These store data about user preferences to show targeted ads.
- **Cross-Site Tracking identifiers:** These '3rd Party cookies' can track users across multiple websites for profiling or marketing and cannot be used without consent.

What text should be used for required cookies

Here is a sample text for a user message about essential cookies.

"We use essential cookies that are necessary for our website to function properly and to ensure the security of our services. These cookies enable core functionalities such as authentication, fraud detection, and security monitoring. They help us identify and prevent fraudulent activities, protect user accounts, and maintain the integrity of the website
These cookies do not collect personal data for marketing purposes and are not shared with third parties for advertising or any other purpose. They are strictly necessary for legal, regulatory, and security reasons. Because they are essential to the operation of our website, they cannot be disabled.
These cookies will also only be stored as long as legally required."

The key rule

If a cookie is necessary for the website to work properly (e.g., security, login, site stability), it can be considered "required."
If it's just (or also) used for tracking behavior, sales or marketing, it should not be in required cookies and must have full user consent.

Legitimate interest in analytics

In the world of website data management, "legitimate interest" is used as an important, but often misunderstood concept.

There is increasing scrutiny on how organizations manage user data. This makes correctly understanding and implementing legitimate interest crucial.

But what does it do exactly, and why is it not the overall simple solution for website analytics?

What exactly is legitimate interest?

Legitimate interest is one of the lawful bases for processing personal data under most privacy regulations such as the GDPR. Simplified, it allows organizations to process personal data without explicit consent if they have a genuine and legitimate reason, unless overridden by the right and freedom of the users involved.

How you can use legitimate interest?

There is a good example in the UK. The ICO in the UK (Information Commissioner Office) recommends a three-part test, called 'LIA'.

- **The purpose test:** determine if your purpose for processing data is legitimate.
- **The necessity test:** make sure that processing is necessary for the said purpose.
- **The balance test:** make sure that the individual's rights do not override your legitimate interest.

Using this test, you can identify if your use of legitimate interest is valid.
You can use their LIA template. It can be found on their website or under this link.

Determining legitimate interest in analytics requires a balance between your organizational needs and privacy rights. While you may argue that service improvement through analytics constitutes legitimate interest, this assessment must consider necessity and proportionality.

The key is to ensure organizational interests do not disproportionately infringe on user rights.
For example, a governmental organization using analytics to enhance public services might demonstrate more justifiable legitimate interest compared to sales-driven contact strategies. *Critically, users should always retain the option to opt-out and control their data usage.*

Legitimate interest may fall short

Legitimate interest involves a subjective interpretation that can easily create inconsistency in data handling practices. While legitimate interest provides a framework, it will not address complex analytics requirements.
Consent-based models offer a clearer, more concrete approach to data usage. Explicit user consent through opt-in systems provides stronger legal standing and enhanced transparency.
By prioritizing user consent, an organization can establish more robust compliance mechanisms, build trust, and ensure ethical data handling practices that align with privacy standards.

To summarize

Understanding legitimate interest requires a balanced approach. Privacy and business interests must be aligned. For organizations looking to harness the full power of analytics while maintaining compliance, integrating both legitimate interest assessments with solid consent processes and publication is the key.

While legitimate interest provides a baseline for analytics, tools like Snoobi Analytics demonstrate the need for robust consent frameworks. Managing legitimate interest requires continuous evaluation against evolving legal standards and user expectations.

Server-side tracking

Server-side tracking shifts data collection from the user's browser (client-side) to the website's own server before sending it to analytics tools like Google Analytics or other platforms. This approach can help with compliance, but it also comes with potential important privacy concerns.

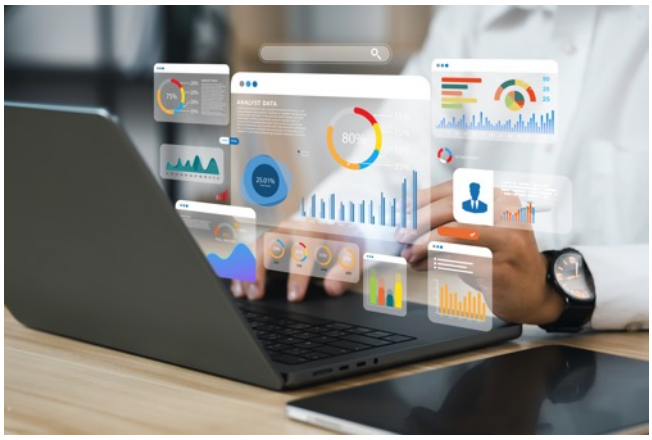
Server-Side tracking and privacy rules

There are three potential benefits

- Better Data Control: The website owner controls what data is sent to third parties, reducing reliance on cookies.
- Less reliance on user devices: Can bypass some browser restrictions like third-party cookie blocking.
- Security & Anonymization: Data can be anonymized or processed before sharing, aligning with GDPR, CCPA, and other regulations.

But there are also potential legal and privacy issues

- Still requires user consent: Even if tracking is server-side, personal data (e.g., IP addresses, user details. behavior) still requires consent in most countries.
- Transparency concerns: Users may not easily have access to stored data or control server-side tracking, raising ethical and legal issues.
- Misuse risk: Some organizations use server-side tracking to bypass privacy protections, which could lead to regulatory penalties.



Is Google Consent Manager a solution?

How it helps:

- Respects user preferences: If a user refuses tracking, Google Analytics and Google Ads adjust data collection accordingly.
- Supports GDPR & CCPA compliance: Works with cookie banners to control what data is sent.
- Enables limited data tracking: Even when users deny tracking, some limited aggregated data (without personal details) can still be collected for analytics.

Key limitations for usage in the EU:

- Not always fully GDPR-compliant as Google Consent Mode does not provide granular consent choices as required by GDPR (e.g., separate opt-ins for different cookie types).
- Primarily supports Google services (Google Analytics, Ads).
- Legitimate interest is not sufficiently covered as Google relies on legitimate interest for certain data processing, which is not valid under GDPR without explicit consent. Note that many EU regulators do not accept legitimate interest as a basis for analytics tracking without consent.
- Data transfer to the U.S. may be an issue as Google stores some data in the U.S., which raises GDPR concerns due to the "Schrems II ruling" on inadequate protection. Even with Google's EU Data Protection commitments, regulators may still view this as non-compliant.
- No automatic cookie blocking as Google Consent Mode does not block cookies automatically. Websites must properly implement Google's APIs to prevent data collection before consent is given.
- If incorrectly configured, Google services may collect partial data (e.g., using cookieless 'pings') before full consent is granted.
- Regulatory Differences Across EU Countries: Some EU Data Protection Authorities have stricter interpretations of consent rules than the standard GDPR, which Google Consent Mode may not fully satisfy.

Final words

Server-side tracking can improve compliance, but it does not remove the need for consent. Google Consent Manager helps manage tracking, but it doesn't solve all privacy concerns. And for full compliance, organizations must still ensure transparency, allow opt-outs, and process data lawfully.

Why consent managers alone are not enough

Browsers evolve continuously in the area of user's privacy, and the role of consent managers is changing. Their effectiveness is declining with new browser defaults rejecting all tracking. Consent managers, crucial for negotiating permissions and ensuring GDPR or CCPA compliance, must adapt as fewer consent pop-ups are required to align with user needs, content customization strategies and digital marketing.

Why you may still miss data even with consent managers

Many websites use consent management platforms (CMPs) such as Cookiebot® to comply with privacy laws. These platforms ask users for permission to track their data, allowing marketers to continue gathering insights only when consent is granted.
However, even with a CMP in place marketers may still face incomplete web analytics for several reasons.

(1) Users can reject tracking
Most consent banners allow users to opt out of one or more tracking options, meaning:

- No cookies (first-party or third-party) can be placed.
- No tracking scripts (any analytics, social media tracking, etc.) can run.
- No behavioral data (page views, clicks, conversions) is recorded for those users.

This leads to data gaps, making it harder to measure website performance accurately.

(2) Partial consent reduces data quality
Some users selectively allow tracking, meaning:

- Only essential cookies are allowed, while analytics and marketing cookies are blocked.
- Depending on implementation, it is also possible that consent is provided after multiple pages, impacting data quality.

Marketers and analysts get fragmented data, missing key actions like traffic source, bounce rates, or multi-session behavior.

For example, if a user only consents to necessary cookies, they may still browse the website, but their actions will not be tracked, leading to underreported visits.

(3) Browser & device restrictions still apply
Even if a user accepts cookies on the first page, modern browsers and privacy tools can still:

- Block tracking requests (e.g. Safari's Intelligent Tracking Prevention).
- Limit cookie lifespans (e.g., Safari and Firefox delete first-party cookies after 7 days).

As a result, analytics data will still be incomplete, even for users who consented.

However, as a marketer or analyst, if users do not consent to cookies, you can still gather insights while remaining GDPR-compliant by using cookieless tracking combined with the use of UTM Parameters. Staying transparent and offering clear opt-in options that make sense to the user. At the same time maximizing privacy-first analytics solutions such as Snoobi Analytics to maintain insight without violating GDPR is key.

Comprehensive analytics with Snoobi

When using a consent management tool such as Cookiebot®, which can be used together with Snoobi Analytics, it becomes possible to understand detailed visitor journeys by using 'hybrid' model, where consent behavior becomes an element in the web analytics metrics without infringement on GDPR- and other privacy regulations.

Analytics for portals or intranet

There is a potential to expose personal data like email addresses in website statistics. Although this issue is relevant for every website, since portals and intranets require login data for access control, there is a higher risk to include personal data in analytics.

Adding personal details to page URLs or allowing the portal to add these details, can lead to several risks concerning privacy, and here are some key risks and considerations.

Risk of exposing personal data in URLs

Personal data can find it's way into an URL that if the application needs this to function or is not properly configured. For instance, when sending an email such as

https://this.sample.com/usr?email=jdoe@this.com

This presents several risks

Most consent banners allow users to opt out of one or more tracking options, meaning:

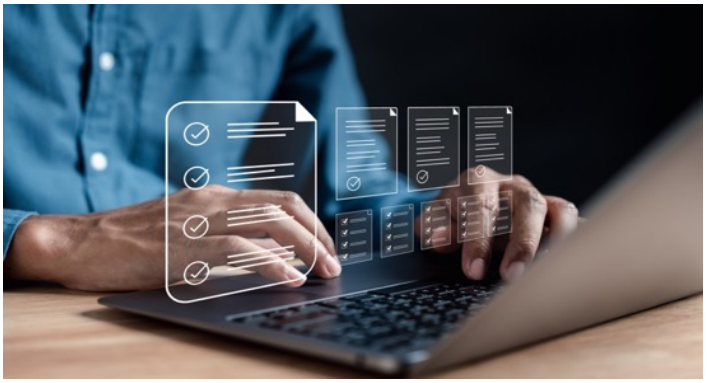
- **Data leakage:** URLs are logged in various places, including server and firewall logs as well as analytics tools.
- **Phishing & spam risks:** If email addresses are visible in URLs, they can be scraped and used for phishing attacks.
- **GDPR & compliance violations**: Under regulations like GDPR, exposing personal data in URLs is a data breach, as URLs are stored insecurely and outside user control.
- **Session Hijacking:** If authentication tokens or session information are embedded in the URL along with an email, attackers may gain access by capturing the URL.

What is allowed in portals or intranet?

For a company intranet, internal policies & employee agreements should clarify how analytics data is used. If external users or clients login than all standard privacy regulations are applicable.

So, can you automatically set cookies?

- **Yes**, for strictly necessary cookies. If cookies are essential for authentication, security, or core functions, they do not require consent.
- **No,** for analytics cookies without consent. Even on a logged-in intranet, GDPR still requires explicit consent for analytics cookies unless you can justify them under a legitimate interest basis (which is difficult for tracking).
- **Workaround:** Some organizations use cookieless analytics (fully anonymized) to bypass consent requirements while remaining compliant.



General Guidelines

Keep in mind that privacy regulations are still valid even when you have a closed employee-only portal.

Some guidelines:

- Use user IDs or hashed values instead of raw email addresses.
- Use session-based authentication instead of passing personal data in query parameters.
- Do not name personal folders with personal names.
- Avoid usernames, phone numbers or other personal identifiers in query strings.
- Do not include personal data in form entries visible in an URL.
- If a user needs to retrieve their information, fetch it from the server based on session authentication rather than embedding it in the URL.
- Configure logging systems (e.g., Apache, Nginx, IIS) to exclude sensitive query parameters.
- If you are using the Snoobi Portal Analytics solution, consult with Snoobi to exclude and obfuscate any personal data elements.
- If your intranet or portal runs on SharePoint Online, SharePoint Server, or Microsoft 365, best advice is to follow the Microsoft best practices.

Summary: Privacy friendly analytics

There are more aspects to privacy than we can cover in this white paper, but the main 'message' is that organizations have no option other than providing control to the user, be transparent, care about data protection, and handle security. Privacy-friendly analytics respects rights while enabling insights. When analytics and privacy are aligned, it creates an optimal situation for all parties involved. Where there is confidence that their data will not be misused, users are more willing to share their information.

Privacy and technology

When it comes to privacy, there are wide choices in terms of technology. Some protect privacy, while others do not. DuckDuckGo® is an example. This search engine and advertising platform does not collect personal data. Instead, DuckDuckGo provides visitors with contextual ads based on search terms. This approach avoids the privacy problems Google is increasingly running into.

Another option is an analytics platform that offers the possibility to collect data about users both with and without cookies. Personal data will only be collected if a user gives his or her consent. If the user does not consent, only anonymous data will be collected. Snoobi is using Cookiebot® settings and allows cookies to be set according to the user's preference

Here are the four important elements of privacy-friendly analytics

(1) Allow control over the use of personal data

- Consent is required for the processing of personal data. This consent must be free and non-dubious and there must be a clear, affirmative action. For example, clicking on a button "I agree". Just assuming that continuing on the website constitutes consent is only sufficient for 'essential cookies', these are required for the website to function.
- It is also important that only the consented date to share is collected and that this data is used only for the purpose for which it was collected. Personal data which have been registered for use by the first party may not, for example, be shared with partners or third parties at a later date.
- Organizations collecting data must clearly state their usage. (Not?) Surprisingly, many still gather extensive personal data without individuals' awareness. To be compliant, users must be informed of changes in data use and given opt-out options for new uses. They should also be allowed to request insight and deletion of personally linked data. Transparency and control are key in data collection practices.

(2) Transparent reporting and processing of data

- It must be clear if data is shared, how, with who, and for what purpose. Giving consent is easier if its use is clearly indicated. Organizations can then benefit from first-party data obtained directly from their users.
- Trust is essential; without it, users may use adblockers or other blocking tools, harming the ability of an organization to improve services. Storage location matters: "in the cloud" is insufficient as privacy protection depends on regional jurisdiction.
- Organizations processing personal data across countries must be aware of local privacy legislation. For data from EU citizens, keeping it within the EU is strongly recommended. Snoobi Analytics keeps all collected data on servers in Finland and within the EU. Transparency and compliance are key for both users and organizations.

(3) Data Privacy 'by design'

- Privacy-friendly analysis methods are grounded in "privacy by design" principles, emphasizing a proactive and preventive approach. The core philosophy is preventing privacy breaches rather than addressing them reactively.
- Two key proactive strategies include information minimization (using only essential data for specific purposes) and purpose limitation (transparently informing users about precise data usage before processing).
- After data processing, information must not be retained beyond the necessary timeframe. Implementation mechanisms vary by usage scenario, such as data anonymization or privacy-protecting analysis functions.

Snoobi Analytics enables complete data anonymization, ensuring robust privacy protection and compliance with modern data handling standards. Data is never shared outside the control of the website owner.

(4) Data security

Finally, data security and privacy are distinct but interconnected. Security involves protecting data from unauthorized access, theft, and corruption. It includes hardware protection, organizational procedures, and standard policies.

Privacy-friendly analytics solutions must prioritize robust security measures. Effective security helps organizations prevent reputational damage and potential financial losses. Critically, in a world where we almost daily are confronted with yet another data breach, users must trust that their personal data remains genuinely secure, or they may become reluctant to share information, even when potential benefits exist.

Is there such a thing as privacy-friendly analytics?

The short answer is that many major analytics platforms, are not designed with privacy in mind. They do some things well, such as data security, but fall short in other areas, especially in terms of transparency and providing full control to the user. After all, many parties benefit from analyzing the behavior or a specific user. Google's business model, for example, is based on maximizing data collection as their business model requires that.

The good news is that there are analytics tools such as Snoobi Analytics which are designed for privacy-friendly analytics while maintaining as much information about website behavior as is allowed.

Further reading

About Snoobi Analytics

- Snoobi Security measures
- Snoobi & Cookiebot
- Cookieless Analytics
- Snoobi Privacy-Secure Tracking
- Snoobi website
- Snoobi Knowledgebase
- Request a cookieless trial

About privacy and regulations

- Cookie Guidance Finland
- UK Information Commisioner's Office
- European ePrivacy Directive
- CNIL guidelines (in French)
- Data collection and cookies in NL
- German BfDI data protection page
- Wikipedia on 3rd party cookies