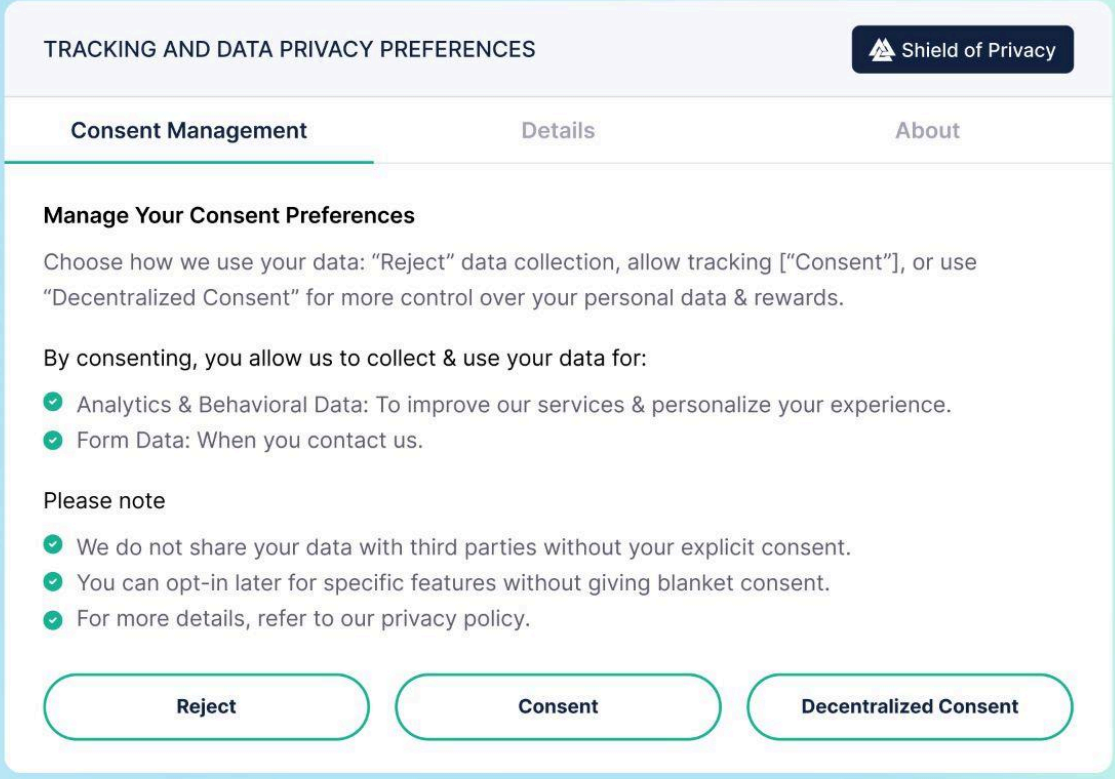
AESIRX

ENHANCING PRIVACY AND COMPLIANCE IN THE DIGITAL AGE:

A Comprehensive Analysis of AesirX's Unified Consent & Analytics Platform and Consent Model.



By Ronni K. Gothard Christiansen
Creator, AesirX.io

Table of Contents

Introduction

In this comprehensive document, we aim to explore the privacy and compliance implications of user interactions on the AesirX platform, both before and after user consent is obtained. Understanding the data flows and third-party interactions that occur during these stages is necessary for ensuring compliance with regulations such as the General Data Protection Regulation (GDPR) and the ePrivacy Directive.

We will provide an in-depth analysis of our consent models, decentralized consent mechanisms, and the integration of our solutions within various platforms, including WordPress. Through the examination of HTTP Archive (HAR) files, we will identify all first-party and third-party hosts involved in user data exchanges, offering a detailed overview of the current state of privacy management on the AesirX platform.

Additionally, this documentation will cover the technical requirements and legitimate interest considerations, ensuring that our consent models are not only compliant but also practical and user-friendly. The inclusion of conditional consent for specific features, the AesirX First-Party Foundation WP Plugin, and our innovative approaches to integrating Web3 technologies will illustrate our commitment to safeguarding user privacy.

Our goal is to provide clear, actionable insights and guidelines for implementing and maintaining compliant data handling practices, while also embracing the advancements of Web3. By the end of this document, readers will have a thorough understanding of how AesirX enables users and businesses to manage the complexities of data privacy in a decentralized digital ecosystem.

Ronni K. Gothard Christiansen
Creator, AesirX.io

Introduction to Data Privacy and Compliance

Understanding Data Privacy

Data privacy is the protection of personal data from unauthorized access, use, disclosure, disruption, modification, or destruction. Ensuring it maintains trust and complies with laws protecting individuals' rights and freedoms.

Key Legal Frameworks

1. General Data Protection Regulation (GDPR)

- **What it covers:** Applies to any organization processing personal data of individuals within the European Union (EU).
- **Principles:** Includes principles such as lawfulness, fairness, transparency, purpose limitation, data minimization, accuracy, storage limitation, integrity, and confidentiality.
- **Rights:** Provides individuals with rights such as access, rectification, erasure, restriction of processing, data portability, and the right to object.
- **Example**: A company operating in the EU must ensure they only collect data necessary for their services and allow users to access and correct their personal data.

2. ePrivacy Directive

- **What it covers:** Focuses on the confidentiality of communications and the rules of online tracking and monitoring.
- **Article 5(3):** Requires explicit consent before storing or accessing information on a user’s device, such as cookies and other tracking technologies.
- **Example**: Websites must get user consent before placing cookies that track online behavior for targeted advertising.

3. European Data Protection Board (EDPB) Guidelines

- **Guidelines 02/2023:** Stresses the need for clear, informed, and unambiguous consent for using cookies and similar technologies.
- **Example**: An app must provide clear information about its data collection practices and obtain explicit user consent before accessing personal data.

Basics of Consent

1. Definition

- **GDPR Article 4(11):** Consent is defined as any freely given, specific, informed, and unambiguous indication of the data subject's wishes.

2. Conditions for Consent

- **Explicit Consent:** Users must provide a clear affirmative action to agree to the processing of their personal data.
- **Informed Consent:** Users must receive detailed information about data processing activities, including purposes and any third parties involved.
- **Example**: A subscription service must inform users about data usage and get their clear agreement before processing their data.

3. Transparency

- Organizations must ensure that information provided to data subjects is concise, transparent, and easily accessible. This includes the identities of data controllers, the purposes of processing, and the rights of the data subjects.
- **Example**: A social media platform should clearly explain how it uses data and what rights users have over it.

4. Data Minimization

- **GDPR Article 5(1)(c):** Data processing should be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.
- **Example**: An online retailer should only collect data needed to fulfill orders and not request unnecessary personal information.

Overview of AesirX's Approach to Data Privacy

AesirX is committed to ensuring compliance with data privacy regulations and protecting user data through transparent and reliable consent mechanisms. The following chapters explore specific aspects of AesirX's approach, including legitimate interest, technical requirements, and consent before data collection.

Legitimate Interest

First-Party and Third-Party under ePrivacy Directive 5(3) and GDPR

1. Understanding Legitimate Interest

First-Party Context:

- **GDPR**: Legitimate interest can be invoked by first-party data collectors when processing is necessary for purposes like improving services, security, or analytics. However, this must be balanced against the individual's rights and freedoms. Users should be informed about such processing, and mechanisms put in place to opt out.
- **ePrivacy Directive 5(3)**: This requires explicit consent for storing or accessing information on a user's device. First-party cookies or trackers used solely for technical purposes (e.g., remembering shopping cart contents) might fall under exceptions where consent isn't mandatory, but transparency and opt-out options are crucial.

Third-Party Context:

- **GDPR**: Third-party data processing under legitimate interest is more complex due to additional risks. It involves entities other than the original service provider and often requires explicit user consent to comply with GDPR's principles of transparency and data minimization.
- **ePrivacy Directive 5(3)**: Explicit user consent is necessary before any third-party can store or access information on a user's device. This applies broadly to cookies and trackers used for advertising or detailed analytics.

2. Consent Requirements

First-Party:

- **Consent**: Explicit, informed consent is necessary before collecting or processing personal data for purposes beyond essential functionalities. This includes analytics and marketing purposes.
- **Transparency**: Websites must provide clear information about data collection practices and allow users to opt out easily. Implementing robust consent management platforms (CMPs) is essential to ensure compliance.

Third-Party:

- **Consent**: Explicit consent is required before third-party trackers can be activated. This includes detailed disclosures about data sharing and the specific purposes of processing.
- **Control**: Users must have granular control over their data, allowing them to accept or reject specific types of data processing, particularly those involving third-party services.

Technical Requirement

First-Party and Third-Party under ePrivacy Directive 5(3) and GDPR

1. Understanding Technical Need

First-Party Context:

- **GDPR**: First-party data collectors can process data under technical need when it is essential for the operation of a service requested by the user. This includes activities necessary to maintain security, provide core functionality, and improve service performance. However, transparency about such processing is necessary, and users should have the ability to opt-out where feasible.
- **ePrivacy Directive 5(3)**: Consent may not be required for storing or accessing information if it is strictly necessary to provide an information society service explicitly requested by the user. This includes first-party cookies or trackers essential for technical purposes, such as session management or user authentication. Clear disclosure about these activities is essential, along with providing opt-out options where appropriate.

Third-Party Context:

- **GDPR**: Third-party data processing under technical need is complex and generally requires explicit user consent due to the higher risk associated with involving external

entities. This is crucial for ensuring transparency and adherence to GDPR principles of data minimization and security.

- **ePrivacy Directive 5(3)**: Explicit user consent is required before any third-party can store or access information on a user's device, even for technical purposes. This ensures users are aware of third-party involvement and can control their data processing preferences.

2. Consent Requirements

First-Party:

- **Consent**: Explicit, informed consent is necessary before collecting or processing personal data for any purpose beyond essential technical functionalities. This includes activities such as advanced analytics or enhanced user experience features.
- **Transparency**: Websites must provide clear information about data collection practices and allow users to opt-out easily. Implementing robust consent management platforms (CMPs) is needed to ensure compliance and maintain user trust.

Third-Party:

- **Consent**: Explicit consent is a prerequisite before any third-party trackers or cookies can be activated, even for technical needs. This involves detailed disclosures about the nature of data sharing, the specific technical purposes of processing, and the identities of third-party entities involved.
- **Control**: Users must have granular control over their data, allowing them to accept or reject specific types of data processing, particularly those involving third-party services. Providing clear opt-out mechanisms and maintaining transparency about data handling practices is vital for compliance.

Consent Before Data Collection

AesirX emphasizes the importance of obtaining explicit user consent before any data collection, whether by first-party or third-party entities, even for legitimate interest or technical needs. This approach aligns with both GDPR and ePrivacy Directive 5(3) requirements. Here are key aspects of AesirX's approach:

1. **Comprehensive Consent Mechanisms**: AesirX advocates for transparent consent mechanisms ensuring users are fully informed about data collection activities, including those necessary for technical purposes or under legitimate interest. This builds trust

and establishes compliance with legal requirements.

2. **First-Party Solutions**: AesirX promotes the use of first-party data solutions to minimize reliance on third-party data processors. This approach enhances user privacy and enables better control over data processing practices.

3. **Privacy-First Tools**: Using tools like AesirX Analytics, which offer robust insights without relying on traditional third-party cookies or trackers, enables compliance with privacy regulations while still providing valuable technical insights.

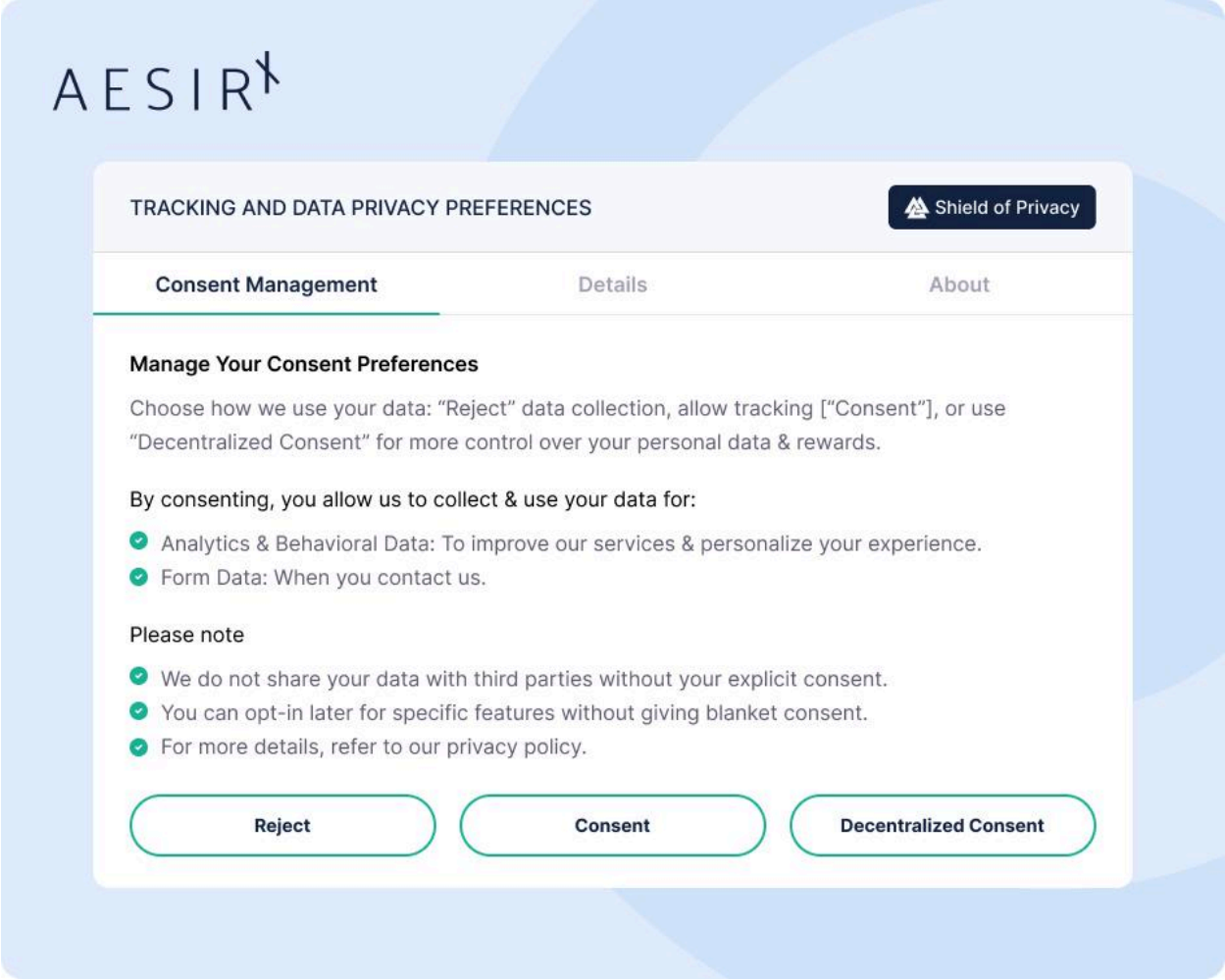
4. **Consent Solution Implementation:** The consent solution is loaded from first-party servers (e.g., api.analytics.aesirx.io and storage.aesirx.io) to ask the user for consent before any data collection. This means no personal data is collected before explicit consent is obtained, adhering to GDPR and ePrivacy Directive requirements. Note: The first-party server is self-hosted by the user and not connected to AesirX APIs, ensuring that IP addresses and other personal data remain under the user's control, maintaining the first-party perspective.

By emphasizing these aspects, AesirX promotes a reliable framework for data privacy and compliance, fostering user trust and adhering to stringent legal standards.

How AesirX Consent Model Works

AesirX Consent Model contains 3 options that are presented to the website visitor.

- Reject
- Consent
- Decentralized Consent

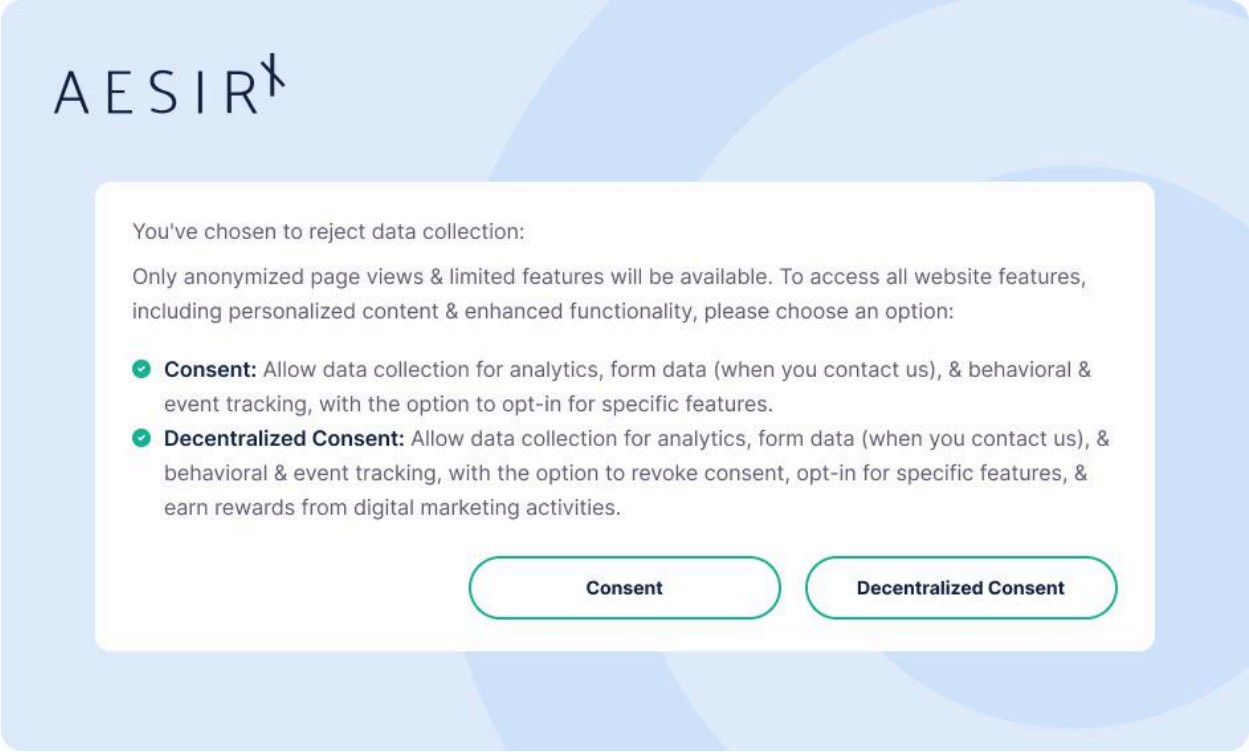


AesirX Consent Model - user chooses from 3 options

Reject

- **Tracking**: No cookies, scripts, or trackers are loaded onto the user's device.
- **General Data Collection**: Only basic information (total number of page views and the fact that consent was rejected) is recorded. This information is not linked to the visitor's identity and is used only to understand overall site usage and consent choices.
- **User Data Collection**: Nothing is collected from the user.

- **Consent Notice**: If the site is configured, it can display a notice prompting the user to activate consent for certain features to work at a later time, e.g. payment software.



AesirX Consent Model - user has rejected data collection

Consent

- **Tracking**:
    - Consent and tracking are activated.
    - 1st Party tracking data is loaded.
    - 3rd Party tracking data is loaded.
- **User Data Collection**: All consented data is collected.

Decentralized Consent

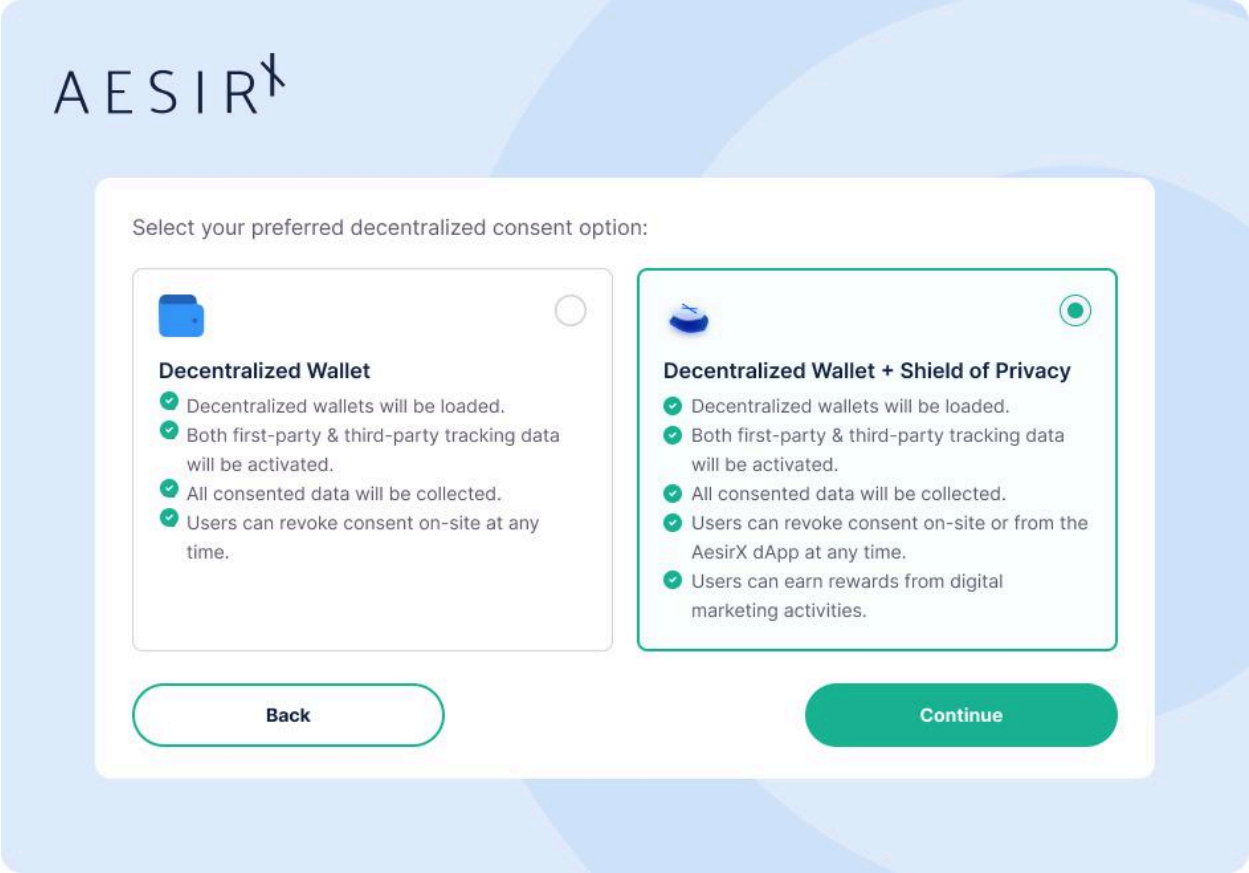
Wallet

- **Tracking**:
    - Consent and tracking are activated.
    - 1st Party tracking data is loaded.
    - 3rd Party tracking data is loaded.
    - Decentralized Wallets are loaded.
- **User Data Collection**: All consented data is collected.
- **Revoke Consent**: Users can revoke consent on site.

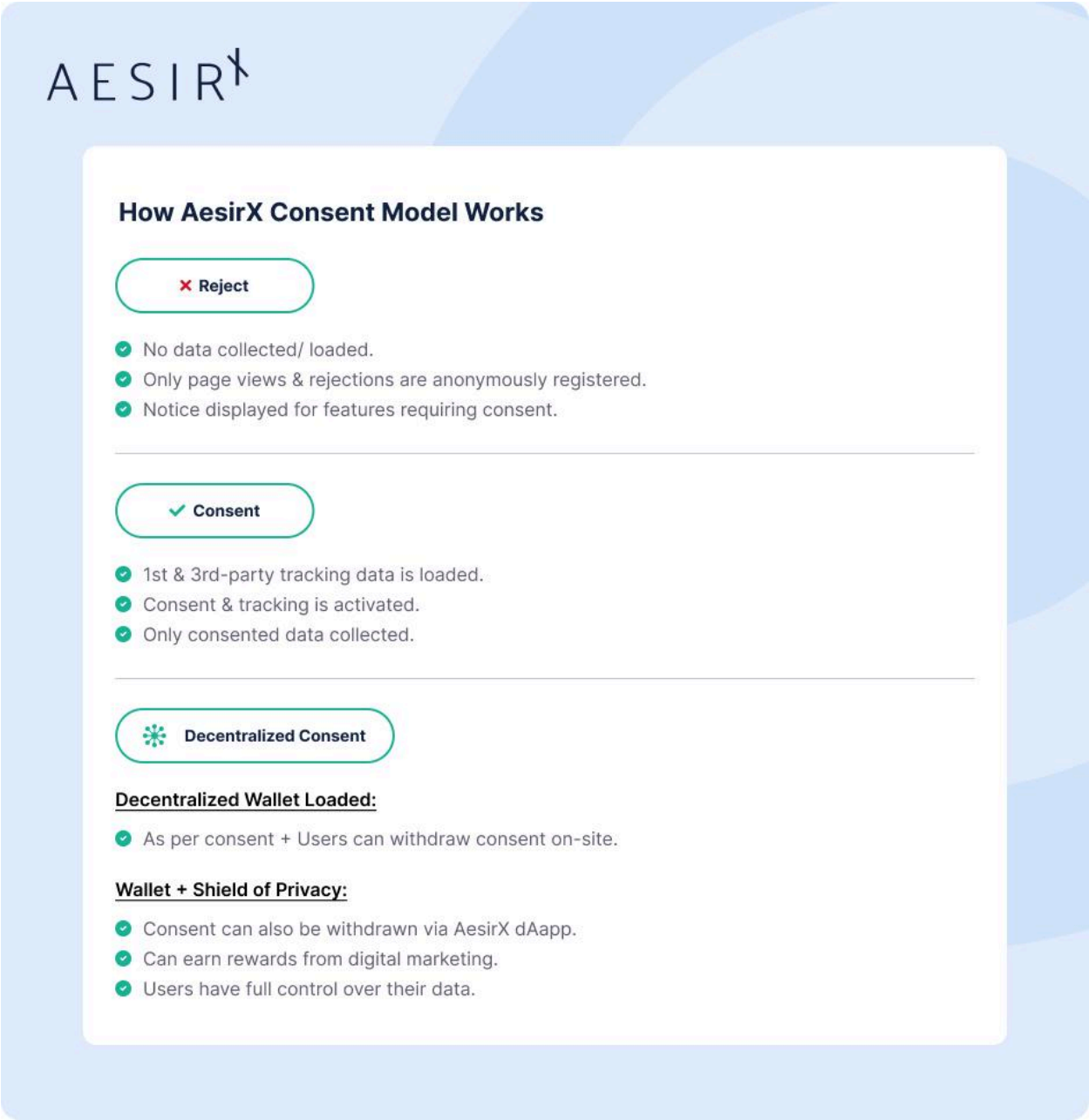
Wallet + Shield of Privacy

- **Tracking**:
  - Consent and tracking are activated.
  - 1st Party tracking data is loaded.
  - 3rd Party tracking data is loaded.
  - Decentralized Wallets are loaded.
- **User Data Collection**: All consented data is collected.
- **Revoke Consent**:
  - Users can revoke consent on site.
  - Users can revoke consent from the AesirX Decentralized Application (dApp, giving full data control.
- **User Rewards**: Users can earn rewards from digital marketing in the AesirX dApp.

Decentralized Consent configuration depends on the site owner. AesirX allows site owners to configure whether both first-party and third-party tracking data are loaded. This includes support for opt-in consent, allowing site owners to load only first-party consent if preferred.



AesirX Consent Model - User selects Decentralized Consent, then can add Shield of Privacy



Overview of how the AesirX Consent Model works

How AesirX Decentralized Consent Works

AesirX's decentralized consent mechanism empowers users by providing control over their data through decentralized technologies. This approach ensures that users can manage their consent across various platforms securely and transparently, aligning with the principles of GDPR and the ePrivacy Directive.

The Shield of Privacy: Pseudonymization Layer

- **Pseudonymization**:
    - **User Data**: User's email, social media account, or wallet address is masked through the Shield of Privacy.
    - **Anonymized Interaction**: Allows users to interact with websites and e-commerce platforms without revealing their actual identity, protecting their privacy.
- **Decentralized Data Ownership**:
    - **Control**: Users retain control over their data, ensuring that their interactions are based on decentralized ownership rather than centralized databases.
    - **Privacy**: The pseudonymization layer ensures that users' personal information is not directly accessible by websites or businesses, enhancing privacy.

Consent Process through Wallet Signing Request

- **User Action**:
    - **Click on Decentralized Consent**: The user clicks on the "decentralized consent" option on the website.
- **Wallet Interaction**:
    - **Signing Request**: A signing request is generated and sent to the user's wallet. This request contains details about the user's consent.
    - **User Review and Sign**: The user reviews the consent details and signs the request in their wallet, providing explicit and informed consent.
- **Consent Activation**:
    - **Legal Audit-Trail**: Once the user signs the request, the consent is recorded through the signing request in the wallet.
    - **Decentralized Subscription Model**:
        - The business owner can then activate the consent and the consent is recorded on the blockchain, creating an immutable and transparent audit trail.

        - The business then gets access to the decentralized subscription data model, collecting first-party data only from the specific sites where the user has given consent.

User Control and Revocation

- **Revoking Consent**:
    - **Specific Site**: Users can revoke their consent directly on the specific site where they had previously granted it using the same wallet they gave consent with.
    - **AesirX Decentralized Application**:
        - **Consent Dashboard**: Users can access the AesirX decentralized application to see a comprehensive list of all decentralized consents they have granted across various sites.
        - **Wallet Requests and Registered Consents**: The application combines the wallet requests with the registered consents through the Shield of Privacy, providing a clear and manageable overview, based on decentralized data.
- **Managing Consents**:
    - **Revoke or Update**: Users can revoke or update their consents at any time, ensuring continuous control over their data and how it is used.

Summary

The AesirX decentralized consent mechanism, combined with the Shield of Privacy, offers a robust, user-centric approach to data privacy. Leveraging blockchain technology and pseudonymization, this system ensures users can interact with digital platforms securely and privately, maintaining control over their data. For small business owners, the process is straightforward and tailored to performance and specific needs (additional clarity would be provided to better differentiate options.) This system not only meets legal requirements but also empowers users to manage their consents transparently and effectively, fostering trust and compliance in the digital ecosystem.

How Activation of Consent Works

AesirX's decentralized consent mechanism not only ensures user control and transparency but also provides a robust system for businesses to activate and manage consents. Here's a detailed explanation of how the activation of consent works, particularly focusing on the decentralized consent process:

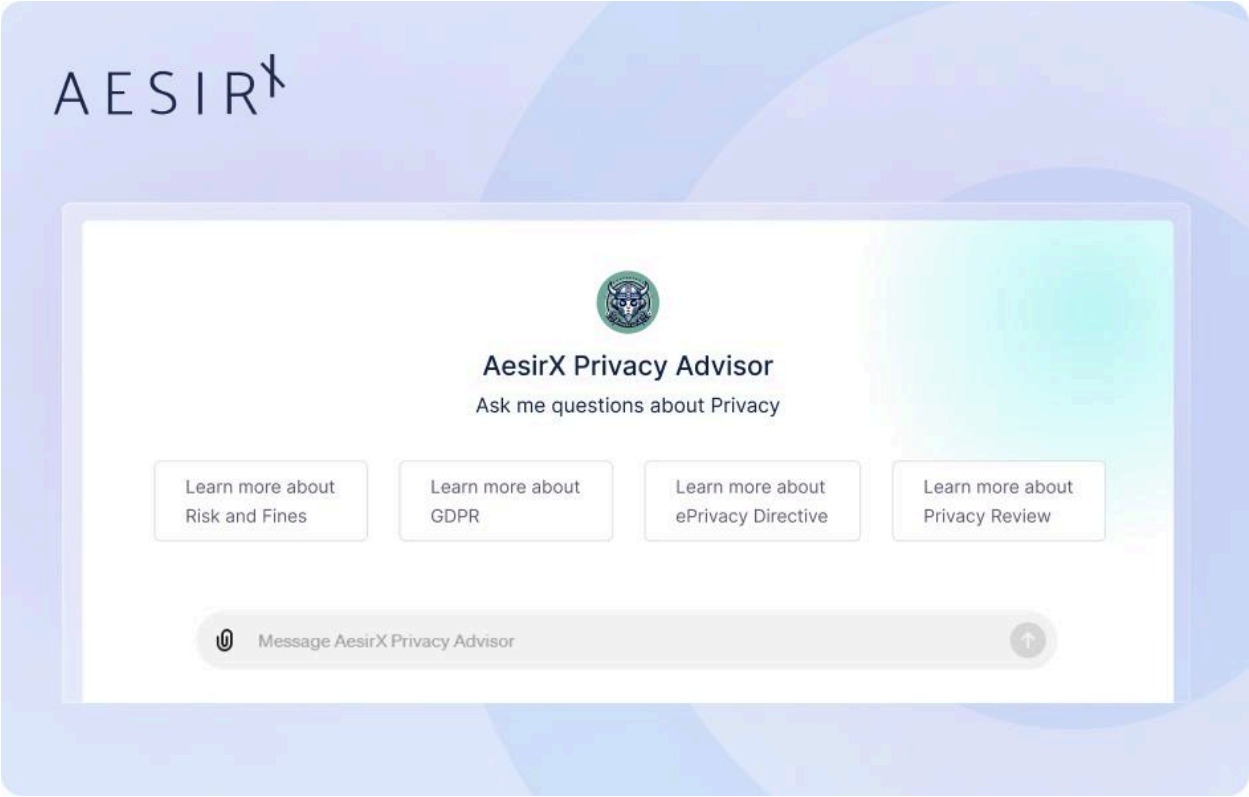
Activation Process for Decentralized Consent:

1. **User Interaction and Consent**:
    - The user visits the website and is presented with the consent options.
    - If the user selects the "Decentralized Consent" option, a signing request is generated and sent to the user's wallet.
    - The user reviews the consent details and signs the request in their wallet, providing explicit and informed consent.
2. **Consent Registration**:
    - Once the user signs the consent request, the consent is temporarily stored and visible in the Business Intelligence (BI) dashboard of the business owner.
3. **Business Owner Activation**:
    - The business owner accesses the BI dashboard and reviews the consents.
    - The business owner can see all consents, including decentralized consents.
    - The business owner selects the decentralized consents that need to be activated.
4. **Bulk Transaction and Legal Audit-Trail**:
    - Upon selection, the business owner activates the consents.
    - This activation triggers a bulk transaction process where each selected consent is formally recorded on the blockchain.
    - This transaction registers the legal audit trail, creating an immutable and transparent record of the user's consent and its activation by the business.
5. **Data Use and Compliance**:
    - Once activated, the business can legally use the consented data as specified in the consent agreement.
    - The blockchain record ensures that the use of consent is documented, providing a verifiable audit trail that aligns with compliance requirements.

Summary

- **Decentralized Consent Only**: This activation process is specific to decentralized consents, which leverage blockchain technology to ensure transparency and security.
- **User Control**: Users have full control over their consents and can revoke them at any time, either on-site or through the AesirX decentralized application.
- **Business Intelligence Dashboard**: The BI dashboard provides the business owner with a comprehensive view of all consents, facilitating easy management and activation.
- **Legal Compliance**: The bulk transaction process ensures that all consents are recorded on the blockchain, providing a robust legal audit trail that meets regulatory requirements.

This process ensures that both users and businesses benefit from a transparent, secure, and compliant consent management system, leveraging the power of decentralized technologies to uphold privacy and trust.



Support for Decentralized Consent

Decentralized Consent Mechanism

The use of third-party hosts like WalletConnect and Concordium services is essential for enabling decentralized consent and supporting decentralized data ownership. Here's how this approach aligns with the legal requirements and technological needs:

1. **User-Triggered Interaction**:
    - **User Action**: The decentralized consent mechanism is triggered by a user action, specifically by clicking "decentralized consent" on the website. This ensures that the user is actively involved in the consent process, aligning with GDPR's requirement for explicit consent.
    - **Informed Decision**: Users are informed about the nature of the decentralized consent process, the third parties involved, and the purpose of data sharing, meeting the transparency obligations under GDPR.
2. **Decentralized Data Ownership**:
    - **Blockchain Technology**: Utilizing blockchain technology for consent ensures that data ownership remains decentralized. This approach prevents any single entity from having control over the data, thereby adhering to the principle of data minimization and purpose limitation.
    - **Immutable Records**: Blockchain's immutable ledger provides a transparent and verifiable record of consent, ensuring compliance with GDPR's requirements for accountability and proof of consent.
3. **No Centralized Provider**:
    - **Elimination of Centralized Control**: By leveraging WalletConnect and Concordium, AesirX.io avoids relying on centralized data processors. This method ensures that user data is not controlled or stored by any central authority, enhancing data security and user trust.
    - **Enhanced Security**: Decentralized systems reduce the risk of data breaches and unauthorized access, thereby aligning with GDPR's principles of integrity and confidentiality (Article 5(1)(f)).

Technical Compliance Details

AesirX's approach aligns with the legal foundations of GDPR and the ePrivacy Directive, ensuring comprehensive compliance through its innovative consent and data processing mechanisms:

- **Consent Mechanisms**:
    - AesirX ensures explicit and informed consent, complying with GDPR's requirements. Users are informed about data collection and provide consent before any data is processed. This includes options for rejecting, consenting, or opting for decentralized consent, with clear communication about what each option entails.
    - The decentralized consent mechanism allows users to manage their consent securely across various platforms, with the ability to revoke consent at any time through the AesirX decentralized application or directly on the site where consent was given.
- **Data Processing Activities**:
    - AesirX scrutinizes personal data collection, storage, and sharing, ensuring all activities are lawful, transparent, and aligned with user consent. The pseudonymization layer (Shield of Privacy) masks identifiable information, allowing users to interact with websites and e-commerce platforms without revealing their actual identities, thus enhancing privacy.
    - All consented data, whether collected through standard or decentralized consent, is processed in accordance with GDPR principles, ensuring that user data is handled responsibly and securely.
- **Tracker and Beacon Compliance**:
    - Website owners must configure their sites to ensure that third-party trackers, beacons, and similar technologies are loaded only after obtaining user consent. AesirX provides the necessary tools and guidance to facilitate this process, helping site owners implement compliance measures effectively.
    - For decentralized consent, tracking activities are managed through a secure wallet signing process, ensuring that all tracking activities are consented to and transparent. Users are presented with clear options to accept or reject these tracking technologies, and their preferences are respected and documented.

AesirX's platform is designed to empower users with control over their data, ensuring that all consent and data processing activities comply with legal requirements while maintaining transparency and trust.

Technological Necessity

The integration of third-party hosts like WalletConnect and Concordium is not merely a convenience but a technological necessity for achieving true decentralized consent. Here's why:

1. **Interoperability**:
    - **Seamless Integration**: These third-party services enable seamless integration of decentralized technologies into the user consent process. Without them, achieving the same level of security, transparency, and user control would be challenging.
2. **Decentralized Identity Verification**:
    - **Verified ID**: Concordium provides identity verification through blockchain, ensuring that each consent instance is linked to a verifiable and authenticated user identity without compromising privacy.
3. **Secure Communication**:
    - **WalletConnect**: Facilitates secure communication between the user's device and the blockchain network, ensuring that consent transactions are securely transmitted and recorded.

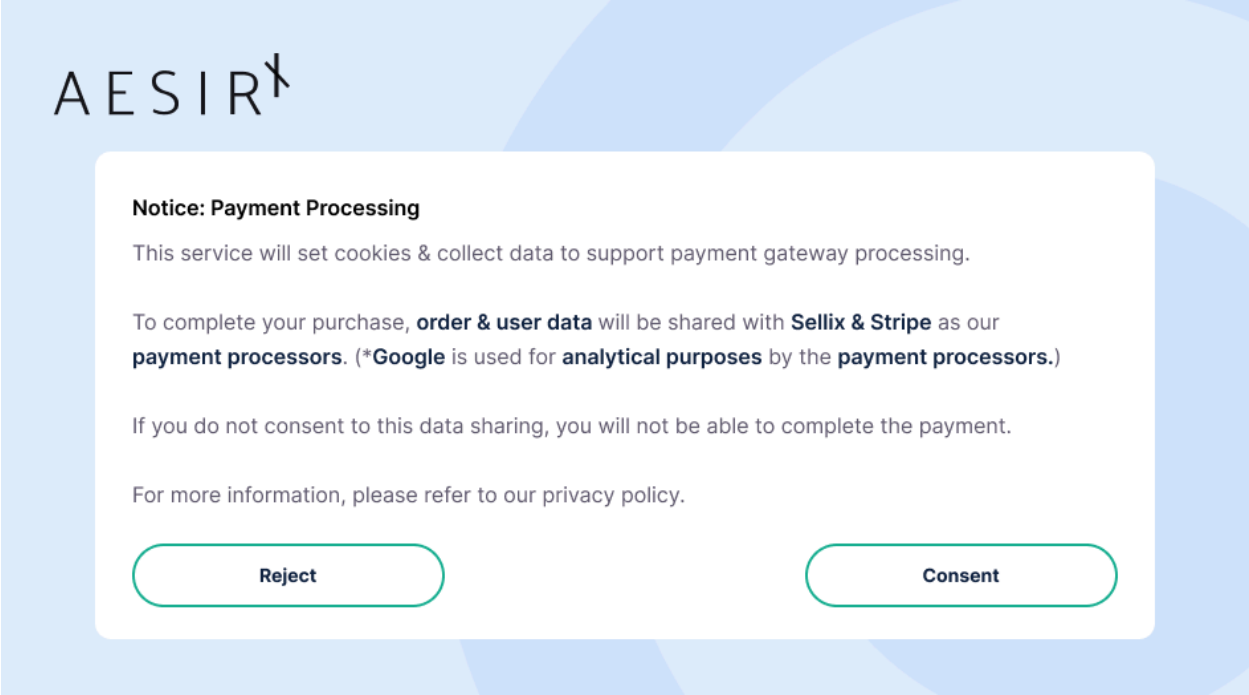
Summary

The loading of third-party hosts such as WalletConnect and Concordium after user consent is fully compliant with GDPR and the ePrivacy Directive. It supports the decentralized consent mechanism, ensuring that user consent is informed, explicit, and verifiable. This approach enhances user trust and data security while aligning with legal requirements and the technological imperatives of decentralized data ownership. By avoiding centralized providers, AesirX.io prioritizes keeping user data secure and under the users' control, reinforcing the principles of privacy and data protection.

Conditional Consent for Specific Features

Introduction to Conditional Consent

AesirX offers a flexible consent model that respects user choices and ensures essential functions like payment processing.This model enables users who reject general consent to still opt-in for specific features without providing blanket consent for the entire site.



Key Aspects of AesirX's Conditional Consent Approach

Specific Feature Consent Mechanism:

- **Tailored Consent**: Users can specifically consent to load third-party elements necessary for particular functionalities, such as payment processors, without having to give general consent for all site activities.
- **Transparency**: Provide clear information about the specific third-party service being activated and why it is necessary, ensuring users are fully informed about their choices.

Granular Control for Users:

- **Opt-In for Specific Actions**:

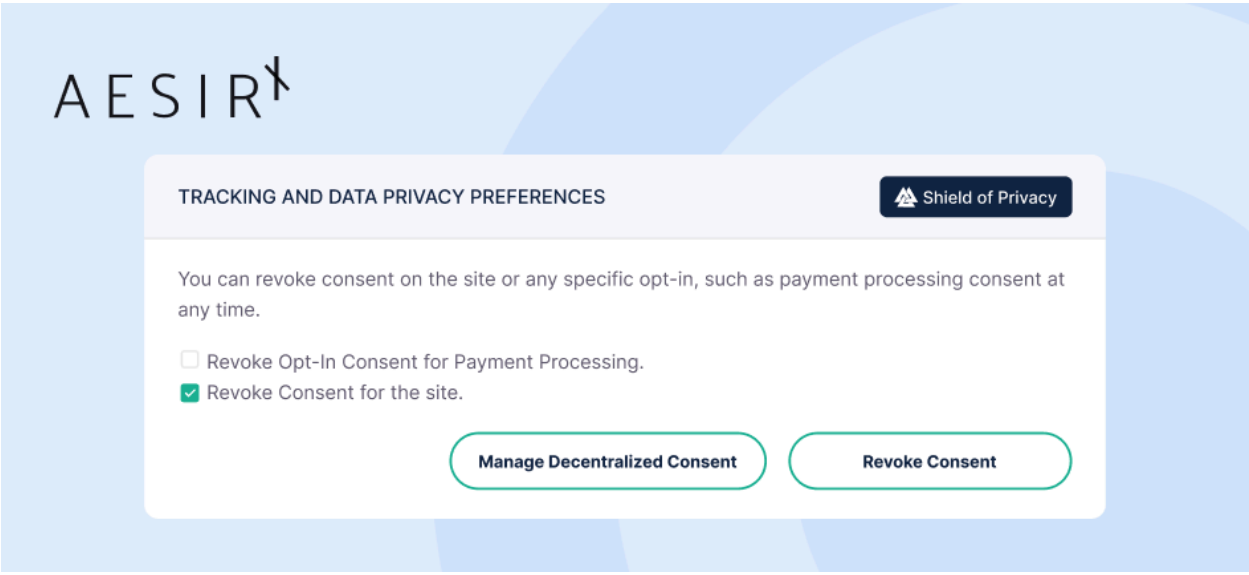
- Allow users to opt-in for specific site functions case-by-case, such as enabling payment processing only when making a payment.
- **Persistent General Rejection**: Maintain the user's general consent rejection for other site activities, ensuring their broader privacy preferences are respected.

Potential Applications:

- **General Site Consent**: The same logic can be applied to general site consent, allowing users to opt-out of specific third-party processing parts of the site.
- **Opt-Out Mechanism**: Users can opt-out in a granular way, selecting which specific third-party services they do not consent to, even after initially opting in. This provides greater control and flexibility, enhancing user trust and compliance.
- **Legitimate Interest Documentation**: Legitimate interest for data processing must be clearly documented, detailing purpose and necessity. Inform users about these interests and provide an easy opt-out option.

Comprehensive Opt-Out Model:

- **Granular Opt-Out Options**: Users can opt-out of specific third-party services and processing activities at a granular level, ensuring control over their privacy.
- **Seamless Opt-Out Experience**: The user interface should provide clear and simple options for users to opt-out, ensuring transparency and ease of use.
- **Documentation of Legitimate Interests**: Data processing based on legitimate interests must be thoroughly documented. Users should be clearly informed about interests and provided with an option to opt-out if they do not agree with the processing.



Developer Support:

- **Comprehensive Guides**: AesirX provides guides for WordPress, Joomla! and Drupal plugin and theme /template developers on implementing consent, opt-in, and opt-out mechanisms to enable seamless integration with AesirX Analytics and compliance without additional setup by site developers.
- **Best Practices for Consent Management**: These guides cover best practices for managing consent, ensuring transparency, and maintaining regulatory compliance.

This approach allows AesirX.io to achieve optimal data minimization and compliance, offering a user-friendly experience while respecting privacy and regulations. The opt-in, opt-out, and legitimate interest documentation create a strong framework for managing user consent and building trust.

AesirX First-Party Foundation WP Plugin

Overview

The AesirX First-Party Foundation WP Plugin is designed to enhance data privacy compliance by utilizing the internal WordPress database (WP DB) for data storage and processing. In its default configuration, this setup means that no external third-party hosts are involved, as all data handling is managed within the main site's database infrastructure. This approach aligns with stringent data privacy regulations, providing a secure and compliant environment for data handling.

Functionality

1. **Internal WordPress Database Utilization:**
    - The plugin defaults to using the internal WP DB for all data storage and processing tasks. This means that all data remains within the confines of the main site's database infrastructure, avoiding the need for external API calls.
2. **First-Party Server Option:**
    - For WordPress site owners who require enhanced performance, there is an option to use their own first-party server. In this case, they would configure their setup to use domains such as api.analytics.theirdomain.com and storage.theirdomain.com. This allows for scalable performance while maintaining first-party data handling.

Impact on Consent Modes

The use of the AesirX First-Party Foundation WP Plugin impacts the analysis and findings of different consent modes. Here is a summary based on the two configurations: using the internal WP DB (default) and using a first-party server.

Using Internal WordPress Database (Default)

1. Before Consent:

- **First-Party Hosts:** theirdomain.com
- **Third-Party Hosts:** None

2. After Consent:

- **First-Party Hosts:** theirdomain.com
- **Third-Party Hosts:** None

3. After Decentralized Consent:

- **First-Party Hosts:** theirdomain.com
- **Third-Party Hosts:** explorer-api.walletconnect.com, grpc.mainnet.concordium.software:20000, relay.walletconnect.com, verify.walletconnect.com

4. After Revoke Consent:

- **First-Party Hosts:** theirdomain.com
- **Third-Party Hosts:** None

5. After Reject Consent:

- **First-Party Hosts:** theirdomain.com
- **Third-Party Hosts:** None

Using First-Party Server

1. Before Consent:

- **First-Party Hosts:** theirdomain.com, api.analytics.theirdomain.com

- **Third-Party Hosts:** None

2. After Consent:

- **First-Party Hosts:** theirdomain.com, api.analytics.theirdomain.com, storage.theirdomain.com
- **Third-Party Hosts:** None

3. After Decentralized Consent:

- **First-Party Hosts:** theirdomain.com, api.analytics.theirdomain.com, storage.theirdomain.com
- **Third-Party Hosts:** explorer-api.walletconnect.com, grpc.mainnet.concordium.software:20000, relay.walletconnect.com, verify.walletconnect.com

4. After Revoke Consent:

- **First-Party Hosts:** theirdomain.com, api.analytics.theirdomain.com, storage.theirdomain.com
- **Third-Party Hosts:** None

5. After Reject Consent:

- **First-Party Hosts:** theirdomain.com, api.analytics.theirdomain.com
- **Third-Party Hosts:** None

Compliance and Findings

The default configuration of the AesirX First-Party Foundation WP Plugin enhances compliance with GDPR and ePrivacy Directive 5(3) by ensuring that no third-party hosts are loaded in any consent mode. This includes the period after consent is revoked, where typically, external third-party servers might still be contacted.

Key Compliance Points:

1. **No Third-Party Data Sharing:**
    - The absence of third-party hosts means that user data is not shared externally, maintaining strict adherence to data minimization and purpose limitation principles outlined in GDPR.

2. **Enhanced User Control and Transparency:**
    - Users are assured that their data remains within the primary site's control, enhancing transparency and trust. The lack of external data processing after consent revocation underscores the plugin's commitment to respecting user choices.
3. **Simplified Data Management:**
    - By using the internal WP DB, the plugin simplifies data management processes, ensuring that data processing is efficient and localized. This reduces the complexity of managing consent and data withdrawal processes, thereby improving overall compliance.

Summary

The AesirX First-Party Foundation WP Plugin's default use of the internal WordPress database represents a robust approach to data privacy and compliance. By avoiding external third-party interactions, data processing remains secure, transparent, and fully compliant with regulatory requirements. This configuration not only simplifies data management but also builds greater user trust through enhanced privacy protections.

For site owners who opt to use their own first-party servers for improved performance, the setup remains compliant as long as it adheres to the same principles of data handling and user consent management. In this scenario, site owners would use their own domains, such as api.analytics.theirdomain.com and storage.theirdomain.com, ensuring that all data processing remains first-party.

Ensuring Compliance for Third-Party Integrations in WordPress

Overview

While the AesirX First-Party Foundation WP Plugin significantly enhances data privacy compliance by primarily using the internal WordPress database (WP DB) or the site owner's first-party server, WordPress site owners must also ensure that any potential loads of other third-party or first-party services that collect user data through their devices are clearly informed in the consent modal. This chapter provides guidance on how to configure consent handling for third-party integrations correctly.

Importance of Transparency and Informed Consent

Under GDPR and the ePrivacy Directive, it is essential to provide users with clear and comprehensive information about any data collection and processing activities. This includes:

1. **Transparency:**
    - Users must be informed about all entities collecting their data, including both first-party and third-party services.
    - The purposes of data collection and processing must be clearly stated.
2. **Informed Consent:**
    - Users must give explicit consent before any data collection or processing occurs.
    - The consent modal must present options to accept or reject data collection from all services, ensuring no use of dark patterns.

Configuring Consent Handling for Third-Party Integrations

1. **Identify Third-Party Services:**
    - Conduct a thorough audit of all third-party services integrated into the WordPress site.
    - Identify all potential third-party hosts that may load on user devices and collect data.
2. **Update Consent Modal:**
    - Ensure that the consent modal includes clear information about all third-party and first-party services that will collect user data.

    - Include details on the types of data being collected, the purposes of the collection, and the entities involved.
3. **General Site Consent or Granular Consent Options:**
    - **General Site Consent:** Configure the consent modal to allow users to provide overall consent for data collection that includes third-party services.
    - **Granular Consent:** Provide users with the option to opt-in or opt-out of data collection for each third-party service individually. This is particularly important for services with varying legal requirements and data collection practices.
4. **Consent Revocation:**
    - Implement easy-to-use mechanisms for users to revoke consent at any time.
    - Ensure that revoking consent for third-party services ceases all related data collection and processing activities immediately.
5. **Regular Audits and Updates:**
    - Regularly audit the site to ensure that no new third-party services have been added without updating the consent modal.
    - Keep the consent modal updated with any changes to third-party integrations or data processing activities.

Summary

WordPress site owners using the AesirX First-Party Foundation WP Plugin must take additional steps to ensure compliance with GDPR and the ePrivacy Directive when integrating third-party services. By providing clear and comprehensive information in the consent modal and offering either general site consent or granular consent options, site owners can build trust with their users and maintain compliance with data privacy regulations. Regular audits and updates to the consent handling processes are key to ongoing compliance and transparency.

Blockchain Use in AesirX Model and Privacy Preservation

AesirX leverages blockchain technology to facilitate decentralized consent and data ownership without compromising user privacy. Here's a detailed explanation of how this model works:

Privacy-Preserving Mechanisms

No Personal Information on the Blockchain:

- **Anonymous Interactions**: The AesirX model ensures that no personal information about the user is stored on the blockchain. Instead, the model relies on pseudonymous interactions through the user's wallet.
- **Decentralized Identifiers (DIDs)**: When users engage with their wallet, they use decentralized identifiers (DIDs) which do not reveal personal details. These identifiers are unique and secure, enabling private interactions.

Wallet Signatures and Domain Specificity:

- **Engaging Wallet**: Users provide consent by interacting with their wallet. The wallet signature confirms their consent but does not store or expose personal data.
- **Domain-Specific Interaction**: The consent provided by the user is linked to a specific domain. This ensures that the consent is context-specific and relevant only to the interactions with that particular site.

Matching On-Chain Transactions:

- **Business Owner Activation**: AesirX matches the activation of decentralized consent with an on-chain transaction made by the business owner. This transaction is recorded on the blockchain.
- **Audit Trail**: The on-chain transaction provides an immutable and transparent audit trail without revealing any user-specific data. It only indicates that a consent-related transaction occurred between the user's wallet and the business.

Ensuring User Control and Revocability

Control Over Data:

- **User Empowerment**: Users maintain full control over their data. They can manage their consents through their wallet and the AesirX decentralized application.
- **Revocation Rights**: Users can revoke consent at any time. When consent is revoked, the link between the activated consent and the user's wallet or Shield of Privacy (SoP) is broken, ensuring that the consent is no longer valid. This action maintains the audit trail while respecting user privacy.

Audit Trail without Personal Data:

- **Pseudonymous Records**: The blockchain stores pseudonymous records of consent transactions. These records do not contain personal data but serve as verifiable proof of consent actions.
- **Transparency and Accountability**: The audit trail ensures transparency and accountability for both users and businesses. Users can see when and where they provided consent, and businesses can demonstrate compliance.

Future Roadmap for Automatic Deletion

Automatic Deletion:

- **Planned Feature**: AesirX is planning to implement a feature for automatic deletion of data based on consent revocation. This will further enhance user control, allowing users to ensure their data is not only inaccessible but also deleted when consent is revoked for any website, ecommerce solution, app or dApp.
- **Enhanced Privacy**: This feature will mean that once consent is revoked, any associated data is automatically removed from the business's systems, thereby maintaining user privacy and complying with data protection regulations.

Summary

The AesirX model uses blockchain to create a decentralized, privacy-preserving consent mechanism. Users engage through their wallets, with no personal data stored on the blockchain. This provides a transparent audit trail, giving users full control over their data and the ability to revoke consent at any time by breaking the link between the activated consent and the user's wallet or SoP. A future feature for automatic data deletion will further reinforce this privacy-first approach, user empowerment, and compliance with data protection laws.

AesirX Single Sign On, Shield of Privacy and Concordium Wallet

The AesirX SSO and Shield of Privacy, integrated with the Concordium Wallet, offer a privacy-preserving solution for verifying credentials without sharing personal data. Using Concordium blockchain and zero-knowledge proofs, it meets legal and compliance requirements like age and country verification, ensuring cross-border data compliance.

Key Components and Processes

1. **Concordium Wallet and Base ID Credentials**:
    - **Base ID Credentials**: Users create a Base ID on the Concordium blockchain, which includes their verified identity attributes like age, country, and other necessary compliance information.
    - **Zero-Knowledge Proofs (ZKPs)**: These credentials are verified using zero-knowledge proofs, which allow the user to prove certain information (e.g., age or country) without revealing their actual personal data.
2. **AesirX Single Sign On (SSO)**:

- **Secure Authentication**: Users can authenticate themselves across various services using AesirX SSO. This system uses the Concordium Wallet to securely manage and verify user credentials.
- **Privacy Protection**: Through ZKPs, the SSO process verifies the necessary attributes (like age and country) without sharing the underlying personal data.

3. **Shield of Privacy**:
   - **Pseudonymization Layer**: The Shield of Privacy acts as a layer that masks the user's identifiable information during interactions with websites and e-commerce platforms.
   - **Data Ownership**: This ensures that users maintain decentralized ownership of their data, interacting with services without compromising their privacy.

Zero-Knowledge Proofs in Practice

ZKPs are cryptographic protocols that enable one party (the prover) to prove to another party (the verifier) that they know a value without disclosing any information about the value itself. In the context of AesirX and the Concordium Wallet, ZKPs are implemented as follows:

- **Generation of Proofs**: When a user needs to verify an attribute (e.g., age), the Concordium Wallet generates a cryptographic proof that confirms the attribute without revealing the actual data.
- **Verification Process**: The service requesting the verification sends a challenge to the Concordium Wallet. The wallet responds with the proof, which the service can verify without accessing the underlying personal data.

This process ensures that user attributes are confirmed without any data being exposed, maintaining user privacy and compliance with data protection regulations.

How It Works

1. **User Authentication**:
   - **Concordium Wallet Login**: The user logs into a service using their Concordium Wallet via AesirX SSO. The wallet provides a secure and encrypted way to access the user's Base ID credentials.
   - **Zero-Knowledge Proof Generation**: For specific compliance requirements, the wallet generates zero-knowledge proofs to verify attributes e.g age and country.
2. Verification Process:
   - **Compliance Check**: The service receives the proof and confirms compliance with legal requirements without accessing personal data.

- **Indirect Verification**: The service requesting the verification sends a challenge to the Concordium Wallet. The wallet responds with a proof that confirms the attribute (e.g., age above 18) without revealing the actual age.

3. **Privacy-Preserving Interaction**:
   - **Pseudonymized Data Use**: During the interaction, the Shield of Privacy ensures that all user data remains pseudonymized. For instance, while shopping on an e-commerce site, the site can verify the user's eligibility for a specific product (e.g., age-restricted items) without accessing personal information.
   - **Cross-Border Compliance**: This model complies with cross-border data protection regulations, ensuring no personal data is transmitted or stored outside user's control, adhering to GDPR and other international privacy laws.
4. **Data Control and Revocation**:
   - **User Control**: Users maintain full control over their data through their Concordium Wallet. They can manage, and revoke consents via AesirX dApp.
   - **Audit and Revocation**: Any consent given can be audited and revoked at any time, ensuring that users can always withdraw their data-sharing permissions, which are also logged on the blockchain for transparency and accountability.

Benefits and Compliance

1. **Enhanced Privacy**:
   - **Zero Personal Data Sharing**: Using zero-knowledge proofs, no personal data is shared during the verification process.
   - **Pseudonymization**: The Shield of Privacy ensures that users' interactions are pseudonymized, maintaining anonymity and privacy.
2. **Regulatory Compliance**:
   - **GDPR and International Laws**: This model adheres to GDPR and other international data protection laws by ensuring that personal data is neither shared nor stored unnecessarily.
   - **Cross-Border Compliance**: By leveraging the decentralized Concordium blockchain and ZKPs, the AesirX model ensures data encryption and anonymization, preventing unauthorized access and ensuring compliance with cross-border data transfer regulations.
3. **User Empowerment**:
   - **Data Ownership**: Users have complete control over their data, managing consents and interactions securely through their wallet.

- **Transparent Audit Trail**: Blockchain provides an immutable audit trail, allowing users and businesses to verify consent and compliance actions transparently.

Summary

The integration of AesirX SSO and Shield of Privacy with the Concordium Wallet offers a privacy-preserving solution for verifying user credentials. Using ZKPs and decentralized data ownership, legal and compliance requirements are met without compromising privacy, adhering to international data protection regulations and empowering users.

Methodology

Overview

The methodology section outlines the systematic approach used to analyze the HAR files and assess the legal implications of data interactions on the AesirX platform. This section aims to provide transparency and reproducibility for the analysis conducted, ensuring that the findings are based on rigorous and standardized procedures.

HAR File Analysis

1. **Data Collection**:
    - **HAR Files**: HTTP Archive (HAR) files were collected from the AesirX platform at two stages: before user consent and after user consent.
    - **Tools and Software**: HAR files were analyzed using industry-standard tools and software capable of parsing and interpreting network traffic data.
2. **Steps of Analysis**:
    - **Initial Examination**: A preliminary examination of the HAR files was conducted to understand the overall data structure and the types of requests and responses captured.
    - **Host Identification**: All hosts (both first-party and third-party) involved in data exchanges were identified and categorized.
        - **First-Party Hosts**: Hosts directly associated with the AesirX domain and its subdomains.
        - **Third-Party Hosts**: External hosts that interact with the user's data through the AesirX platform.
    - **Data Points Analyzed**:

        - **Request URLs**: URLs requested by the client (user's browser) to understand the data flow.
        - **Request Headers**: Analyzed for metadata and any potential personal data transmission.
        - **Response Headers and Content**: Assessed to determine what data is being sent back to the client.
        - **Cookies and Storage**: Evaluated to see what information is stored on the user's device and under what conditions.
3. **Comparative Analysis**:
    - **Before vs. After Consent**: A comparative analysis was conducted to identify differences in data exchanges and third-party interactions before and after user consent.
    - **Key Metrics**:
        - **Number of Requests**: Comparing volume of requests to third-party hosts.
        - **Types of Data**: Assessing changes in the types of data being transmitted and received.
        - **Privacy and Security Measures**: Evaluating the implementation of privacy and security measures such as encryption and pseudonymization.

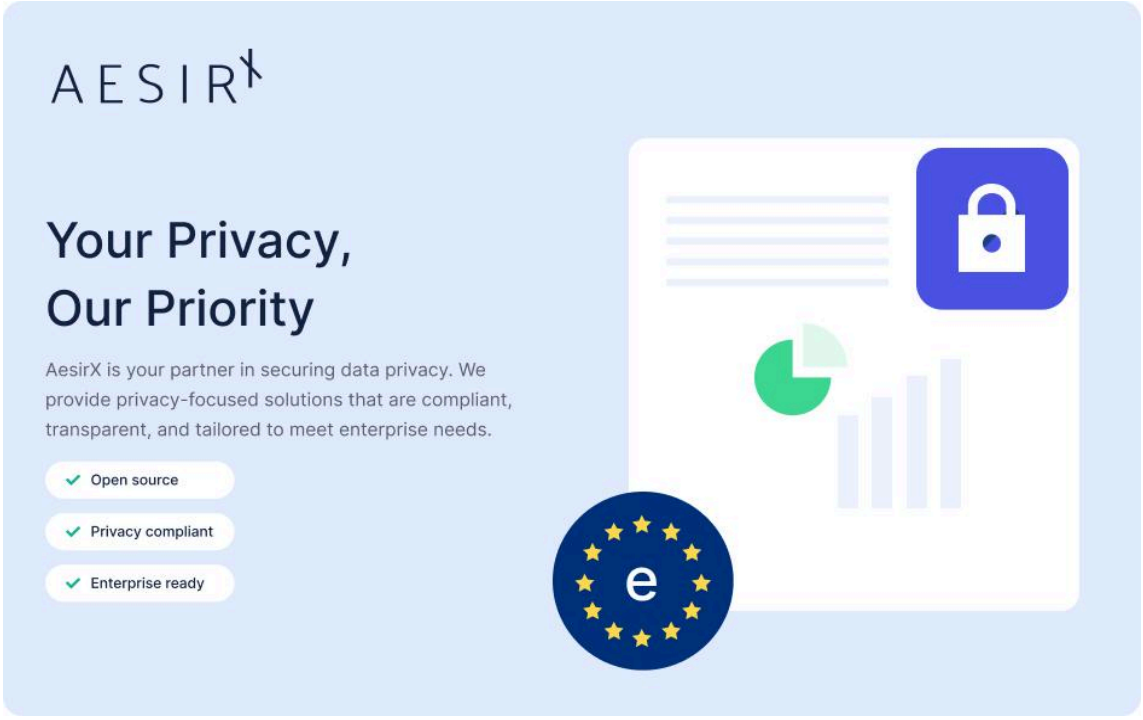
Legal Perspectives

1. **Regulatory Frameworks**:
    - **GDPR Compliance**: Analyzed the data interactions against the requirements of the General Data Protection Regulation (GDPR), focusing on:
        - **Consent**: Ensuring that user consent is informed, explicit, and freely given.
        - **Data Minimization**: Assessing whether only necessary data is collected and processed.
        - **Transparency and Information**: Evaluating if users are adequately informed about data processing activities.
    - **ePrivacy Directive**: Examined compliance with the ePrivacy Directive, particularly regarding:
        - **Cookies and Trackers**: Ensuring proper consent mechanisms for cookies and similar technologies.
        - **Electronic Communications**: Analyzing the confidentiality of communications and data integrity.

2. **Compliance Checks**:
    - **Explicit Consent Documentation**: Verifying that consent documentation meets legal standards and provides a clear audit trail.
    - **Third-Party Interactions**: Ensuring that third-party data interactions are compliant with GDPR and ePrivacy Directive requirements, including:
        - **Data Sharing Agreements**: Confirming that appropriate agreements are in place with third-party hosts.
        - **User Rights**: Assessing mechanisms for users to exercise their rights, such as data access, rectification, and deletion.
3. **Technological Implementations**:
    - **Decentralized Consent Mechanisms**: Reviewing the technical implementation of decentralized consent to enable compliance and security.
    - **Pseudonymization Techniques**: Analyzing the use of pseudonymization to protect user identities while enabling necessary data processing.

Summary

This methodology ensures a comprehensive analysis of the AesirX platform's data interactions and legal compliance. By detailing the steps and tools, we provide a clear framework for assessing privacy and compliance in digital platforms. This approach highlights strengths and areas for improvement and sets a standard for future evaluations.



Analysis of AesirX.io Consent Model

Impact on Consent Modes

The use of the AesirX consent model impacts the analysis and findings of different consent modes. Here is a summary based on the configurations using a first-party server, with an additional opt-in granular consent for payment processing based on the HAR file analysis.

Using First-Party Server

1. Before Consent:

- **First-Party Hosts:** aesirx.io, api.analytics.aesirx.io
- **Third-Party Hosts:** None

2. After Consent:

- **First-Party Hosts:** aesirx.io, api.analytics.aesirx.io, storage.aesirx.io
- **Third-Party Hosts:** None

3. After Decentralized Consent:

- **First-Party Hosts:** aesirx.io, api.analytics.aesirx.io, storage.aesirx.io
- **Third-Party Hosts:** explorer-api.walletconnect.com, grpc.mainnet.concordium.software:20000, relay.walletconnect.com, verify.walletconnect.com

4. After Revoke Consent:

- **First-Party Hosts:** aesirx.io, api.analytics.aesirx.io, storage.aesirx.io
- **Third-Party Hosts:** None

5. After Reject Consent:

- **First-Party Hosts:** aesirx.io, api.analytics.aesirx.io
- **Third-Party Hosts:** None

Opt-In Granular Consent for Payment Processing:

When a user initiates a payment by clicking "Pay," they are presented with an explicit and informed granular opt-in consent for payment processing. This consent is separate from the general site consent and includes the following third-party hosts:

- **Third-Party Hosts for Payment Processing:**
  - sellix.io
  - stripe.com
  - google.com (reCaptcha)

Compliance and Findings

By analyzing the consent modes, we see that the AesirX consent model, when using a first-party server configuration, ensures that no third-party hosts are involved before or after consent is revoked, with all data handling managed within the main site's infrastructure. The introduction of an opt-in granular consent for payment processing provides users with explicit choices regarding third-party interactions for specific purposes, such as payments.

This approach aligns with GDPR and ePrivacy Directive requirements by ensuring informed and explicit consent for all data processing activities, including those involving third-party hosts for payment processing. It demonstrates AesirX's commitment to safeguarding user privacy through transparent and user-centric consent processes.

Legal Analysis of First-Party Hosts Loaded After Consent

Context and Frameworks

The loading of first-party hosts on AesirX.io after user consent is a critical aspect of ensuring compliance with various legal frameworks, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive. These frameworks emphasize the need for transparency, user consent, and data protection when processing personal data and interacting with first-party services.

GDPR Compliance

Consent:

- **Article 4(11):** Defines consent as any freely given, specific, informed, and unambiguous indication of the data subject's wishes.
- **Article 7:** Details the conditions for consent, including the requirement that consent be distinguishable and provided with clear information about data processing activities.

Transparency and Information:

- **Article 12:** Mandates that information provided to data subjects must be concise, transparent, and easily accessible.
- **Article 13:** Specifies the information that must be provided when personal data is collected, including recipients of the data and the existence of automated decision-making.

Data Minimization and Purpose Limitation:

- **Article 5(1)(c) and (1)(b):** Requires data processing to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

ePrivacy Directive

Consent for Cookies and Similar Technologies:

- **Article 5(3):** Requires consent before storing information or gaining access to information stored on a user's terminal equipment.

First-Party Hosts Analysis

First-Party Servers for Consent

The integration of first-party servers such as api.analytics.aesirx.io and storage.aesirx.io is essential for the AesirX consent model. These servers are involved in the collection and processing of user data within the AesirX infrastructure. The first-party consent solution is loaded immediately to ask the user for consent before any other data is collected.

GDPR Compliance for First-Party Servers:

- **Consent:** The initial loading of first-party servers like api.analytics.aesirx.io and storage.aesirx.io to present the consent modal does not collect personal data but rather sets up the environment for consent collection. Once the user gives consent, these servers can then handle user data as per the consent provided.
- **Transparency:** The consent modal must clearly state the purposes of data collection and the involvement of these first-party servers. Users should be informed about what data will be collected and how it will be used once they provide consent.
- **Data Minimization:** Only the necessary data for the specified purposes should be processed by the first-party servers after consent is given. The data collection should be limited to what is required for analytics, storage, and other operational purposes.

ePrivacy Directive Compliance for First-Party Servers:

- **Consent:** Explicit consent must be obtained before any first-party servers store or access information on the user's device, aside from the initial consent modal setup. This includes the use of cookies and other tracking technologies after consent is given.

Summary

Ensuring compliance with GDPR and the ePrivacy Directive involves obtaining explicit and informed user consent for all first-party data interactions. For AesirX.io, this includes:

1. **First-Party Consent Solution:** The initial load of api.analytics.aesirx.io and storage.aesirx.io to display the consent modal means that no personal data is collected before user consent. This setup aligns with GDPR and ePrivacy Directive requirements by ensuring transparency and adhering to data minimization principles.
2. **Post-Consent Data Handling:** Once consent is provided, first-party servers can handle user data in compliance with the informed consent given by the user.

By adhering to these legal requirements, AesirX.io demonstrates a strong commitment to safeguarding user privacy and maintaining compliance with relevant data protection regulations for both first-party and third-party data interactions.

Legal Analysis of Third-Party Hosts Loaded After Consent

Context and Frameworks

The loading of third-party hosts on AesirX.io after user consent is a critical aspect of ensuring compliance with various legal frameworks, including the General Data Protection Regulation (GDPR) and the ePrivacy Directive. These frameworks emphasize the need for transparency, user consent, and data protection when processing personal data and interacting with third-party services.

GDPR Compliance

Consent:

- **Article 4(11):** Defines consent as any freely given, specific, informed, and unambiguous indication of the data subject's wishes.
- **Article 7:** Details the conditions for consent, including the requirement that consent be distinguishable and provided with clear information about data processing activities.

Transparency and Information:

- **Article 12:** Mandates that information provided to data subjects must be concise, transparent, and easily accessible.

- **Article 13:** Specifies the information that must be provided when personal data is collected, including the recipients of the data and the existence of automated decision-making.

Data Minimization and Purpose Limitation:

- **Article 5(1)(c) and (1)(b):** Requires data processing to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

ePrivacy Directive

Consent for Cookies and Similar Technologies:

- **Article 5(3):** Requires consent before storing information or gaining access to information stored on a user's terminal equipment.

Third-Party Hosts Analysis

Wallet SDKs

The integration of Wallet SDKs such as explorer-api.walletconnect.com, grpc.mainnet.concordium.software:20000, relay.walletconnect.com, and verify.walletconnect.com requires explicit user consent. These services enable decentralized consent mechanisms and facilitate interactions with blockchain networks.

GDPR Compliance for Wallet SDKs:

- **Consent:** Users must provide explicit, informed consent before any interaction with these third-party hosts.
- **Transparency:** The consent modal must clearly state the purposes of data collection and the involvement of these SDKs.
- **Data Minimization:** Only the necessary data for enabling wallet interactions should be processed.

ePrivacy Directive Compliance for Wallet SDKs:

- **Consent:** Explicit consent must be obtained before any Wallet SDKs store or access information on the user's device.

Payment Processors

For payment processing, third-party hosts such as sellix.io and stripe.com are involved. These hosts are only loaded when the user initiates a payment by clicking "Pay," at which point a granular opt-in consent is presented.

GDPR Compliance for Payment Processors:

- **Consent:** Users must provide explicit, informed consent specifically for payment processing activities involving sellix.io and stripe.com.
- **Transparency:** The consent modal must include detailed information about the data processing activities and the role of these payment processors.
- **Data Minimization:** The data collected should be limited to what is necessary for processing payments.

ePrivacy Directive Compliance for Payment Processors:

- **Consent:** Before sellix.io and stripe.com can store or access any information on the user's device, explicit consent must be obtained through a granular opt-in mechanism.

Summary

Ensuring compliance with GDPR and the ePrivacy Directive involves obtaining explicit and informed user consent for all third-party data interactions. For AesirX.io, this includes Wallet SDKs and payment processors. By adhering to these legal requirements, AesirX.io demonstrates a strong commitment to safeguarding user privacy and maintaining compliance with relevant data protection regulations.

Legal Analysis: Loading the Consent Solution First-Party vs. Third-Party

Context and Frameworks

Loading the consent solution, whether first-party or third-party, has significant implications under legal frameworks like GDPR and the ePrivacy Directive. This examines the legal differences, particularly regarding ePrivacy Directive Article 5(3) and EDPB Guidelines 02/2023.

GDPR Compliance

Consent:

- **Article 4(11):** Defines consent as any freely given, specific, informed, and unambiguous indication of the data subject's wishes.
- **Article 7:** Details the conditions for consent, including the requirement that consent be distinguishable and provided with clear information about data processing activities.

Transparency and Information:

- **Article 12:** Mandates that information provided to data subjects must be concise, transparent, and easily accessible.
- **Article 13:** Specifies required information when personal data is collected, including data recipients and the existence of automated decision-making.

Data Minimization and Purpose Limitation:

- **Article 5(1)(c) and (1)(b):** Requires data processing to be adequate, relevant, and limited to what is necessary in relation to the purposes for which they are processed.

ePrivacy Directive Compliance

Consent for Cookies and Similar Technologies:

- **Article 5(3):** Requires consent before storing information or gaining access to information stored on a user’s terminal equipment.

EDPB Guidelines 02/2023

These guidelines emphasize the importance of clear, informed, and unambiguous consent for any data processing activities involving cookies and similar technologies. They stress the need for transparency and the avoidance of dark patterns that may influence user consent.

Legal Analysis: First-Party vs. Third-Party Consent Solution

First-Party Consent Solution

Description:

- The consent solution is loaded directly from the first-party server (e.g., api.analytics.aesirx.io and storage.aesirx.io).
- The user is presented with the consent modal immediately upon visiting the site, before any other data is collected.

GDPR Compliance:

- **Transparency:** The first-party approach ensures that users are fully informed by the entity directly responsible for the site they are visiting. This aligns with Article 12 and Article 13, providing clear and concise information about data processing activities.
- **Control and Trust:** Users may have greater trust in the consent solution as it is presented by the site they are directly interacting with, enhancing their control over their data.

ePrivacy Directive Compliance:

- **Initial Load:** The initial load of the consent solution from first-party servers does not involve storing or accessing personal data. This complies with Article 5(3), as no consent is needed for merely setting up the environment to request consent.
- **Post-Consent:** Once consent is obtained, any data storage or access complies with the given consent, ensuring full adherence to Article 5(3).

EDPB Guidelines Compliance:

- **Avoidance of Dark Patterns:** The first-party approach can be designed to avoid any misleading or manipulative practices, ensuring that consent is freely given, informed, and unambiguous.

Third-Party Consent Solution

Description:

- The consent solution is loaded from a third-party server.
- The user is presented with the consent modal, which is served by a third-party service provider.

GDPR Compliance:

- **Transparency:** While the third-party consent solution must also comply with transparency requirements, there may be challenges in ensuring that users understand the relationship between the site they are visiting and the third-party provider. This could complicate compliance with Articles 12 and 13.
- **Trust Issues:** Users may be less trusting of third-party consent solutions, potentially affecting their willingness to provide consent.

ePrivacy Directive Compliance:

- **Initial Load:** The initial loading of a third-party consent solution may involve accessing information on the user's device, potentially requiring prior consent under Article 5(3). This complicates the compliance process as consent is needed before the consent modal is even displayed.
- **Post-Consent:** Managing and ensuring that the third-party provider adheres to the user's consent preferences adds an additional layer of complexity and potential compliance risk.

EDPB Guidelines Compliance:

- **Transparency and Clarity:** Ensuring that third-party consent solutions provide clear and understandable information without dark patterns is crucial. However, the involvement of a third-party may inherently complicate this process, potentially affecting the quality of consent obtained.

Summary

From a legal perspective, loading the consent solution from a first-party server (e.g., api.analytics.aesirx.io and storage.aesirx.io) is generally more compliant with GDPR and the ePrivacy Directive requirements. It ensures greater transparency, user trust, and easier

compliance with the stringent requirements set forth by the GDPR and ePrivacy Directive Article 5(3), as well as the EDPB's Guidelines 02/2023.

In contrast, loading the consent solution from a third-party server introduces additional complexities and potential compliance risks. It may require prior consent before even displaying the consent modal, complicating adherence to legal requirements and potentially affecting user trust and the quality of consent obtained.

The Competitive Landscape

How AesirX First-Party Foundation compares to other solutions on the market.

Features/USPs	AESIR First-Party Foundation	Plausible	matomo	PIWIK PRO COOKIE INFORMATION	Cookiebot by Usercentrics	Google Analytics 4
Open-Source	✓	✓	✓	×	×	×
Decentralized Data Model	✓	×	×	×	×	×
Cookieless Tracking	✓	✓	✓	✓	×	Possible
First-Party Data	✓	Possible	Possible	×	×	×
First-Party Consent	✓	×	×	×	×	×
First-Party Leads (Coming Soon)	✓	×	×	×	×	×
Cross-Site Marketing	✓	×	✓	✓	✓	✓
Compliance (GDPR, CCPA, HIPAA)	Seamless	✓	Possible	Possible	Possible	Possible
Consent Requirement (ePD 5.3)	Seamless	×	Possible	×	×	×

AESIR

447 Broadway,
2nd Floor Suite #1305, New York, New York 10013, United States.
https://aesirx.io/
solutions@aesirx.io