

Privacy Policy 1.0

Version	Date	Description of Changes	Classification
1.0	12.02.2023	Initial creation of Privacy Policy	Public

Effective Date: February 12, 2023

The company group of Xtreme Software Solutions d.o.o. and Nirvana d.o.o. (collectively referred to as "we," "us," or "our") operates the <https://www.playnirvana.com> website (the "Service"). This Privacy Policy describes how we collect, use, disclose, and protect your Personal Data when you use our Service and outlines the choices you have associated with that data.

We are committed to protecting the privacy and security of your Personal Data in accordance with GDPR, ISO 27001:2022, and other relevant information security standards. By using the Service, you agree to the collection and use of information in accordance with this Privacy Policy and our Information Security Policy.

Information We Collect

Device Information: When you visit our website, our analytics tools collect certain information about your device, including information about your web browser, IP address, time zone, and some of the cookies that are installed on your device. Additionally, as you browse the Service, we collect information about the individual web pages or products that you view, what websites or search terms referred you to the Service, and information about how you interact with the Service. We refer to this automatically collected information as "Device Information."

We collect Device Information using the following technologies:

- **Cookies:** Data files that are placed on your device or computer and often include an anonymous unique identifier. For more information about cookies and how to disable cookies, visit [All About Cookies](#).
- **Log Files:** Track actions occurring on the Service and collect data including your IP address, browser type, Internet service provider, referring/exit pages, and date/time stamps.

- **Web Beacons, Tags, and Pixels:** Electronic files used to record information about how you browse the Service.

When we talk about "Personal Information" in this Privacy Policy, we are referring to both Device Information and other information that can identify you as an individual.

Privacy Policy Statement

This Privacy Policy outlines our commitment to protecting the personal data of individuals and ensuring compliance with the General Data Protection Regulation (GDPR). Below are the key principles and rights we uphold:

1. Consent for Processing of Personal Data:

- We will obtain explicit consent from individuals before processing their personal data. This consent must be freely given, specific, informed, and unambiguous. Individuals have the right to withdraw their consent at any time.

2. Right to be Forgotten:

- Individuals have the right to request the deletion of their personal data when it is no longer necessary for the purposes for which it was collected or if they withdraw their consent. We will comply with such requests in accordance with GDPR requirements.

3. Right to Decline:

- Individuals have the right to decline the processing of their personal data. They can object to processing based on legitimate interests or for direct marketing purposes. We will respect such objections and cease processing as required.

4. Information on Collected/Processed Personal Data:

- We will provide clear and transparent information about what personal data is collected, how it is processed, the purposes of processing, and the legal basis for processing. This information will be made readily available to individuals.

5. Data Access and Portability:

- Individuals have the right to access their personal data and request a copy in a structured, commonly used, and machine-readable format. They can also request the transfer of their data to another controller.

6. Data Accuracy:

- Individuals have the right to request the correction or update of inaccurate or incomplete personal data. We will ensure that personal data is accurate and kept up to date.

7. Data Processing Restrictions:

- Individuals can request the restriction of processing of their personal data under certain conditions, such as when they contest the accuracy of the data or object to the processing. We will limit processing as requested in accordance with GDPR.

8. Breach Notification:

- In the event of a data breach that poses a risk to individuals' rights and freedoms, we will notify the affected individuals and the relevant supervisory authority within 72 hours of becoming aware of the breach.

9. Supervisory Authority Contact Information:

- Individuals can lodge complaints with the relevant data protection supervisory authority. Contact information for the supervisory authority will be provided upon request.

10. Data Protection Officer (DPO):

- Our Data Protection Officer oversees compliance with GDPR requirements and acts as a point of contact for data protection matters. You can reach our DPO at dpo@playnirvana.com.

Contact Us

If you have any questions about this Privacy Policy or our privacy practices, or if you would like to make a request regarding your personal data, please contact us at dpo@playnirvana.com

Policy Statement on Transfer of Data

Your information, including Personal Data, may be transferred to and maintained on computers located outside of your state, province, country, or other governmental jurisdiction where the data protection laws may differ from those of your jurisdiction. If you are located

outside the EEA and choose to provide information to us, please note that we transfer the data, including Personal Data, to the EEA and process it there.

We will take all necessary steps to ensure that your data is treated securely and in accordance with this Privacy Policy. No transfer of your Personal Data will take place to an organization or a country unless there are adequate controls in place, including the security of your data and other personal information.

For any transfers of data outside the EEA, we implement Standard Contractual Clauses approved by the European Commission or obtain your explicit consent to ensure your data remains protected.

Disclosure of Data - Legal Requirements

Xtreme Software Solutions d.o.o. and Nirvana d.o.o. are committed to protecting your Personal Data. In certain circumstances, we may be required to disclose your Personal Data in accordance with GDPR and applicable laws. These circumstances include, but are not limited to:

1. **Compliance with Legal Obligations:** We may disclose your Personal Data to comply with a legal obligation, including but not limited to, court orders, legal processes, or requests from regulatory authorities.
2. **Protection of Rights and Property:** We may disclose your Personal Data to protect and defend the rights, property, or safety of Xtreme Software Solutions d.o.o., Nirvana d.o.o., our employees, or others. This includes enforcing our agreements, policies, and terms of use.
3. **Investigation of Wrongdoing:** We may disclose your Personal Data to prevent, detect, or investigate possible wrongdoing in connection with our services. This includes sharing information with law enforcement agencies for the purpose of crime prevention and investigation.
4. **Protection of Personal Safety:** We may disclose your Personal Data to protect the personal safety of users of our services or the general public. This may include responding to emergency situations or threats to public safety.

5. **Legal Liability:** We may disclose your Personal Data as necessary to protect against legal liability, including pursuing available remedies or limiting the damages that we may sustain.

All disclosures of Personal Data will be conducted in accordance with GDPR requirements, ensuring that such disclosures are lawful, necessary, and proportionate. We will ensure appropriate safeguards are in place to protect your Personal Data during such disclosures.

Security of Data

We are committed to protecting the security of your Personal Information and maintaining its confidentiality in accordance with ISO 27001:2022, GDPR, and other relevant information security standards. To safeguard your Personal Information against unauthorized access, disclosure, alteration, or destruction, we implement appropriate technical and organizational measures, including but not limited to:

1. **Regular Vulnerability Scanning and Security Assessments:** Conducting routine vulnerability scanning and comprehensive security assessments of our systems and website to identify and remediate potential security vulnerabilities.
2. **Access Controls and Authentication Mechanisms:** Enforcing stringent access controls and authentication mechanisms to restrict access to Personal Information to authorized personnel only. This includes role-based access controls, multi-factor authentication, and regular access reviews.
3. **Data Encryption:** Employing industry-standard encryption technologies to protect Personal Information during transmission and while stored.
4. **Employee Training:** Providing continuous training to our employees on data security best practices, protocols, and policies to ensure they are well-informed about their roles and responsibilities in safeguarding Personal Information.
5. **Incident Response Plan:** Maintaining a robust incident response plan to swiftly address and mitigate any data security breaches or incidents.

Despite our rigorous efforts to protect your Personal Information, please be aware that no method of transmission over the Internet or method of electronic storage is completely secure. While we strive to use commercially acceptable means to protect your Personal Information, we cannot guarantee its absolute security.

If you have reason to believe that your interaction with us is no longer secure, please immediately notify us of the problem by contacting us in accordance with the "Contact Us" section below.

Service Providers

We may employ third-party companies and individuals ("Service Providers") to facilitate our Service, provide the Service on our behalf, perform Service-related tasks, or assist us in analyzing how our Service is used. These third parties have access to your Personal Data solely to perform these tasks on our behalf and are obligated to comply with strict data protection and confidentiality measures.

Specifically, our arrangements with Service Providers include the following safeguards to ensure compliance with GDPR and ISO 27001:2022:

1. **Data Processing Agreements:** We enter into data processing agreements with all Service Providers that outline their responsibilities and obligations regarding the protection of Personal Data. These agreements ensure that Service Providers process Personal Data in accordance with our instructions and applicable data protection laws.
2. **Access Controls and Security Measures:** Service Providers are required to implement appropriate technical and organizational measures to protect Personal Data against unauthorized access, disclosure, alteration, or destruction. This includes the use of encryption, access controls, and regular security assessments.
3. **Data Minimization and Purpose Limitation:** Service Providers are granted access to only the minimum amount of Personal Data necessary to perform their tasks. They are prohibited from using Personal Data for any purpose other than providing the agreed-upon services.
4. **Regular Audits and Assessments:** We conduct regular audits and assessments of our Service Providers to ensure ongoing compliance with GDPR, ISO 27001:2022, and our internal security policies.
5. **Breach Notification:** Service Providers are required to promptly notify us of any data breaches or security incidents involving Personal Data. This allows us to take immediate action to mitigate any potential harm and comply with our legal obligations.

By employing these measures, we strive to ensure that your Personal Data is handled with the utmost care and in full compliance with GDPR and ISO 27001:2022 standards.

Google Analytics

Our website uses Google Analytics, a web analytics service provided by Google, Inc. ("Google"). Google Analytics uses "cookies," which are text files placed on your computer, to help the website analyze how users interact with the site. The information generated by the cookie about your use of the website (including your IP address) will be transmitted to and stored by Google on servers in the United States and other countries.

We use Google Analytics to track and report website traffic, understand user interactions with the website, and improve our website's performance and user experience. The data collected is anonymized and aggregated to provide insights without identifying individual users.

Google may transfer this information to third parties where required to do so by law or where such third parties process the information on Google's behalf. Google will not associate your IP address with any other data held by Google.

To comply with GDPR, we have implemented the following measures:

1. **Data Processing Agreement:** We have entered into a Data Processing Agreement with Google, which outlines the responsibilities and obligations of both parties regarding the processing of personal data.
2. **Data Minimization:** We ensure that only the necessary data is collected and processed by Google Analytics.
3. **IP Anonymization:** We use IP anonymization, where Google truncates/anonymizes the last octet of the IP address for Member States of the European Union and other parties to the Agreement on the European Economic Area.
4. **User Controls:** You may refuse the use of cookies by selecting the appropriate settings on your browser. However, please note that if you do this, you may not be able to use the full functionality of this website.

For more information on Google's privacy practices and how Google Analytics handles your data, please see the [Google Privacy & Terms](#) page.

Contact Us

If you have any questions about this Privacy Policy or our privacy practices, or if you would like to make a complaint or request regarding your personal information, please contact us at info@playnirvana.com