THEO Technologies Privacy and Security Policy

THEO Technologies (hereinafter "THEO") is the leading provider of universal video playback technologies for online media companies and enterprises worldwide. THEO takes your privacy very seriously. This policy explains the type of data that we collect, how we collect it and the ways in which we use it.

A. Privacy Policy

As the provider of the website www.theoplayer.com (hereinafter "Website"), software and services (hereafter "Services") we at THEO are Controller as defined in applicable data protection law, more specifically the General Data Protection Regulation (EU) 2016/679 (hereinafter "GDPR"), and are therefore responsible for the Personal Data of the Website user. As a user of the Website and Services you consent to THEO use of your Personal Data and Customer Data under this privacy policy and you acknowledge, accept and consent that THEO uses your Personal Data and Customer Data as necessary for THEO to provide the Services to you. Your privacy is important to THEO and THEO is committed to protecting your privacy. This privacy policy explains how THEO collects and uses Personal Data, what Personal Data THEO uses and for what purposes such data is used.

Personal Data means personal information about you as defined in the GDPR.

Customer Data means all information provided by you to THEO which is not Personal Data.

1. Date Controller vs. Data Processor?

THEO is considered to be a "Data Controller" in accordance with the GDPR. THEO is not a "Data Processor" as its Services do not involve activities which make THEO "processing Personal Data on behalf of you" as defined in the GDPR. In case that you or THEO become a Data Processor, we may enter into a separate data processing agreement. THEO shall ensure that (a) in its role as Data Controller, it only uses the Personal Data and Customer Data for the purpose of providing its Services and in accordance with the GDPR; (b) its personnel and subcontractors that are involved in the fulfilment of the Services have committed themselves to confidentiality and comply with the GDPR, (c) it takes appropriate technical and organisational measures, insofar as this is possible and required for the fulfilment of the GDPR, (d) upon reasonable request, it makes available to the other Party all information necessary to demonstrate compliance with the obligations under GDPR.

2. What Personal Data and other Customer Data does THEO collect?

Website visit – Customer Data only: When you access the Website, THEO collects Customer Data information that includes the type and version of browser that you are using, the browser language, the operating system and platform, the date and time of access, the time zone setting, your access status/http status code and the data volume transferred, cookies, how you used our Website, the services you searched for, page response times, download errors, length of visits, page interaction information.

Website forms – Personal Data as provided by you: When using THEO's webforms and the THEO platform, the Personal Data THEO collects may include names, surnames, e-mail addresses, postal addresses, phone numbers, payment details, user specific settings, your preferences in receiving marketing information from us, your communication preferences and other Personal Data provided by you when you sign up for the Services and when you use the Services. THEO will only use your Personal Data to the extent necessary to fulfil the Services and for purposes which are compatible with providing the Services, such as directing advertisement regarding the Services to you.

Business contacts: When you engage with THEO through emails, negotiations, telephone calls, contractual documents, THEO will maintain a copy of your contact details in order to be able to contact you and as such provide the Services as required.

THEO software products: THEO uses Customer Data and Personal Data in accordance with "Product Data Sheets" that can be requested by you from THEO.

When using Personal Data, THEO complies with all applicable data protection laws and regulations, in particular (but not limited to) GDPR.

3. Cookies

THEO also uses cookie files to improve and personalize your use of the Services. When you use THEO Services, THEO saves cookie files on your computer. Cookies are small text files that, unless you have adjusted your browser setting to refuse cookies, our system will send your device when you visit the Website. Cookies collect standard internet log information and visitor behaviour information. The cookie files help with the functionality of the Website and allow the Website to identify your browser and to recognize what preferences you have and what settings you have made. Users of THEO Services and visitors of the Website may always choose to accept or decline THEO use of cookies. If you block cookies, this may affect your ability to use our Website. You can access more information about cookies at www.allaboutcookies.org.

THEO uses the following Cookies:

- Functional and Required Cookies. We use necessary cookies which allow visitors to navigate the key features on the Website.
- Analytics and Performance Cookies. We use analytics and performance cookies to collect information about how visitors interact with the Website.
- Session Cookies. We use session cookies to operate our Services.
- Preference Cookies. We use preference cookies to remember your preferences and various settings.
- Security Cookies. We use security cookies for security purposes.
- (Re)marketing Cookies. We use these cookies to serve more relevant content to you on third-party websites, based on your expressed preferences.

4. How do we collect Personal Data and Customer Data?

THEO may use information from you when you use our Services or register on our Website, place an order, subscribe to a newsletter, respond to a survey, fill out a form, use live chat, open a support ticket or enter information on our Website and when you provide feedback to us on our site.

THEO may also use Personal Data and Customer Data you provide directly to THEO via Websites, e-mail, EDI, and other interactions such as your registration on THEO systems and platforms as a customer, partner or supplier, your purchase orders, and participation in THEO events.

5. How does THEO use your Personal Data and Customer Data?

THEO only uses Personal Data and Customer Data to the extent necessary to provide the Services and for purposes which are compatible with providing the Services, such as directing periodic emails to you regarding your order and advertisement regarding Services and/or other products offered by THEO. Customer Data is only used in order to provide the Services to you.

Unless otherwise provided, THEO stores Personal Data and Customer Data collected directly by THEO in a secured database within Europe and locally in Belgium. Personal Data and Customer Data is used to contact you and to manage your account. THEO may also follow up after you have had contact with THEO through live chat, email of phone inquiries.

THEO may use automated decision making in using your information when providing its Services.

When THEO uses Personal Data and Customer Data, THEO complies with all applicable data protection laws as well as any laws and regulations applicable to the Services provided to you.

When Personal Data and Customer Data is collected or used directly by THEO, it will be stored on servers or cloud service platforms within the EU. Should Personal Data be submitted to or stored by any third party in so called Third Countries, countries outside the EU, then you acknowledge that THEO cannot guarantee that the same level of protection can be offered as that provided for by the GDPR.

6. How long does THEO store Personal Data and Customer Data?

THEO will only store Personal Data and Customer Data for a limited period. THEO ensures that Personal Data and Customer Data will be deleted when it is no longer necessary to retain it to provide the Services, or for purposes which are compatible with providing the Services.

Personal Data and Customer Data provided by you to THEO is retained for the duration of your subscription of the Services and for a longer period if it is required by applicable laws, for example for any legal, accounting, or reporting requirements or purposes.

7. Direct marketing and the right to opt-out

By accepting this policy, you authorize THEO to use your Personal Data for providing information regarding THEO Services to you as a Website user, including regular electronic newsletters, webinar invitations, product updates. . You have the right to object to THEO use of your Personal Data for direct marketing under applicable data protection laws. If you wish to object to direct marketing, please contact THEO by sending an e-mail to contact@theoplayer.com or click or the unsubscribe link provided with the respective communication.

8. Subject Access Requests

You are entitled to additional information regarding the use of your Personal Data. In case you want to know what Personal Data THEO stores about you and how your Personal Data is used, please contact THEO by sending an e-mail to contact@theoplayer.com ("Subject Access Request"). If you make a Subject Access Request by electronic means, THEO will provide information regarding the use of your Personal Data in a commonly used electronic form. The information provided by THEO shall include the following:

(1) the purposes of the use;

(2) the categories of Personal Data concerned;

(3) the recipients or categories of recipients to whom your Personal Data has been or will be disclosed, in particular recipients in third countries or international organizations;

(4) where possible, the envisaged period for which your Personal Data will be stored;

(5) whether you are entitled to request rectification or erasure of Personal Data or restriction of Personal Data or to object to the use or to lodge a complaint with a supervisory authority;

(6) where Personal Data is not collected from you, available information as to the source of the Personal Data;

(7) the existence of automated decision-making, including profiling;

(8) where Personal Data is transferred to a third country or to an international organization, information regarding the appropriate safeguards relating to the transfer;

(9) a copy of the Personal Data undergoing usage.

9. Rights relating to Personal Data

You are entitled to request rectification or erasure of your Personal Data and to object to the use of your Personal Data. You may also request restriction of the use of your Personal Data. THEO is required to update or rectify your Personal Data if the Personal Data THEO holds on you is inaccurate. THEO may also be required to delete your Personal Data, for example if you withdraw your consent to its use or if the Personal Data THEO stores about you is incorrect or irrelevant. Deletion may not be required for data that must be retained as required by applicable laws.

THEO undertakes to respond to requests regarding rectification, erasure or restriction of Personal Data, as well as to objections to the use of Personal Data, in a timely manner. When THEO receives a request, which is justified according to applicable data protection laws, THEO shall comply with the request and delete or rectify the Personal Data or restrict or cease the use of such data.

You have the right to receive the Personal Data, which has been provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit such data to another controller without hindrance from the controller to which the Personal Data have been provided. You also have the right to lodge a complaint with a supervisory authority.

Requests under this paragraph shall be sent to THEO by e-mail to contact@theoplayer.com.

10. User responsibility

As a Website and Service user it is important that you are aware of your responsibility for the related risks. You are responsible for protecting and updating your account information to prevent unauthorized access to your account.

You are also responsible to abide by all applicable laws and regulations. Where you process your own Customer and Personal Data you act as the Data Controller, hence you are responsible for compliance with applicable data protection laws. This entails ensuring the rights of the data subjects and in particular to erase your Customer Data and Personal Data when you no longer need it for the purposes specified by you. If you use free text fields, you are responsible for ensuring that free text fields do not generate processing of excessive or irrelevant Personal Data. You are further responsible for your sharing of your Customer Data and Personal Data, for example when providing access to third parties.

11. Is THEO using Customer Data and Personal Data with Third Party Tools, Subcontractors and Authorities?

THEO uses your Personal Data and Customer Data confidentially. THEO does not sell or trade your data. THEO does not, without your consent, transfer or share it with third parties.

THEO may use subcontractors for the purpose of performing its Services to you. THEO has subcontractors such as cloud service providers, infrastructure providers, content delivery networks, customer service, email delivery, banking operation, credit card networks, website hosting and consultants including for IT-support and accounting. THEO ensures that its subcontractors are liable to keep your Personal Data and Customer Data confidential by signing confidentiality agreements or data privacy agreements with such subcontractors.

In order to be able to provide Services and products to you, THEO uses the third-party programs and tools of subcontractors (“Third Party Tools”).

While using such Third-Party Tools be advised that your access and use of such Third Party Tools are governed solely by the terms and conditions of their providers including their privacy terms and conditions, and that THEO is not liable for, and makes no representations as to such other services and products provided by the Third Party Tools, including, without limitation, their content or the manner in which they handle data (including your data) or any interaction between you and the Third Party Tools provider(s). A list of most relevant Third Part Tool’s own privacy statement is attached in Annex 1 which apply to THEO and you directly.

THEO may further reveal your Personal Data and Customer Data to third parties, including the competent supervisory authority, if it is required by applicable data protection laws or other applicable laws and regulations.

THEO ensures that access to your Personal Data and Customer Data is limited to the personnel and subcontractors who require such access to perform the Services and other activities which are compatible with providing the Services.

B. Security Policy

1. General

Your privacy is important to THEO and THEO is committed to protecting your Personal Data and your Customer Data. THEO ensures that THEO will take all reasonable measures to protect your Personal Data and Customer Data and in particular to prevent unauthorized access to such data.

THEO wants to make you aware of the risks which are inherent in data transmissions over the Internet since such transmissions are never completely secure. When you provide your Personal Data and Customer Data to THEO over the Internet you are responsible for the risks of unauthorized access and loss of data which the transmission entails.

THEO has implemented and maintains a number of technical and organizational security measures to keep your Personal Data and Customer Data safe when stored by THEO. Such security measures include encryption, firewalls, antivirus and security monitoring which can reasonably be expected in accordance with applicable market standards.

In the event that the security of the Website, Services and the Personal Data and Customer Data be compromised, THEO reserves the right to take any appropriate action as set out in the relevant data protection laws, including notifying you and the appropriate regulator of such a breach where required by law.

The Website may carry links to other websites that are not affiliated to nor controlled by the THEO. Should you access these sites from the Website, THEO accepts no liability or responsibility over the content, privacy policies, data handling or practices of these sites.

2. What are the security measures and means?

Agreements: With its customers, subcontractors and partners THEO puts non-disclosure agreements and commitments with regards to data privacy and security in place.

Devices: All devices used by THEO employees are encrypted and secured by password. As a general company policy, all company devices, including peripherals such as USB drives and hosted services run on encrypted systems. No data is to be copied outside of these systems on third party devices. This policy is enforced and controlled by the THEO's operations team.

VPN: All remote access to THEOs systems is VPN secured and protected by a password.

Firewall: All servers and software are protected by secured connection and firewalls.

Office access: THEO's office is only accessible via registered badge and not open to the public.

Training: THEO has implemented a yearly Data Privacy training for its employees.

Background checks: All employees were hired after having carefully assessed their relevant background and proof of sufficient education.

Endpoint security: All employee devices are encrypted with a TPM based AES-128 encryption algorithm. THEO uses a permission-based authorization, network-based authorization and geographical based authorization. If a user fails to authenticate in any way or uses services outside of the correct networks or devices, or if he is outside of the approved geographical areas, access will be denied.

Network security: All network traffic is separated and segregated based on user access level. Any offsite traffic that will be tunnelled through AES-256 encrypted VPN tunnels. Network access rules are enforced by firewalls and are in place to stop users from using services they are not privileged to. Every service has been provided with its own access control systems as a tertiary backup. Any and all traffic to any private service is logged.

Data integrity: All company data that is stored in any way is stored on encrypted media. Daily and weekly backups are performed, stored and tested. These backups ensure the integrity of THEO's data and the continuity of THEO's Services.

Information security: Personnel is made aware of their responsibility of keeping THEO's company data secure. They are made aware of the dangers of data loss or leaks. Use of external storage devices (USB keys, drives, etc.) is not allowed or discouraged at the very least.

C. Changes, Contact and Complaints

1. Changes to our Privacy and Security Policy

THEO continues to develop its Website and Services. THEO keeps its Privacy and Security Policy under regular review and places any updates on this page. This Privacy and Security Policy was last updated: April 2022.

2. Contact

If you have any questions about THEO's Privacy and Security Policy, the data we hold on you, or would like to exercise one of your data protection rights, please do not hesitate to contact THEO.

THEO Technologies NV
Philipssite 5 Bus 1
3001 Leuven
Belgium
E-mail: contact@theoplayer.com

https://www.theoplayer.com/

3. Complaints

Should you wish to report a complaint or if you feel that THEO has not addressed your concern in a satisfactory manner, you may contact THEO at contact@theoplayer.com.

Annex 1

Applicable Data Privacy terms of Third Part Tools

THEO Technologies cannot guarantee that the links and content below is up to date.

Hubspot: https://legal.hubspot.com/legal-stuff

Jira: https://www.atlassian.com/trust

Stripe: https://stripe.com/en-se/privacy

DocuSign: https://www.docusign.com/company/privacy-policy

LinkedIn: https://www.linkedin.com/legal/privacy-policy?trk=homepage-basic_footer-privacy-policy

Outlook (Office 365): https://privacy.microsoft.com/en-gb/privacystatement

Google Services: https://policies.google.com/privacy?hl=en&gl=US

Auth0: https://auth0.com/docs/compliance/gdpr

Intercom: https://www.intercom.com/legal/privacy

Slack: https://a.slack-edge.com/bed7/marketing/img/legal/pdf/slack_data_processing_addendum.pdf

Odoo: https://www.odoo.com/fr_FR/privacy

Fastly: https://www.fastly.com/privacy/

Readme.com: https ://readme.com/privacy

AWS: https://aws.amazon.com/blogs/security/aws-gdpr-data-processing-addendum/