

Privacy Policy

TLDR (Too long, didn't read)

- We realize that many users and customers, like us, rarely read the entirety of a privacy policy. As such, we find it fitting to provide a quick overview.
- Our free services require no login, email or any other personal details to use.
- We usually will only ask you to give us your name and email to get access to our paid services. Anything beyond this is not required and will be directly given by you to us because you wish to communicate directly with us.
- We encrypt all your communications and do our best to store the least amount of data possible to protect you.
- We have no access to your conversations or communication sessions.
- We don't use cookies for our services, but some of our third-party providers do.
- All payments are accepted via Stripe, a secure payment provider.
- We do not collect or sell your personal information nor share it with any third-parties.
- If you need any specialized agreements, please reach out to legal@xroom.app
- We are here to help you maintain simple and secure communications and have no interest in obtaining your personal information. If you have any comments, concerns or suggestions please contact us at support@xroom.app.

Introduction – xroom.app

- We are dedicated and committed to safeguarding the privacy of our clients and users.
- In this policy, "We", "Us" and "Our" refer to xroom.app.
- In this policy, "Your", "User" and "Customer" refers to xroom.app's customer base and users.
- Everything we create will be done so with our users, their privacy and integrity in mind while ensuring our tools are simple-to-use. We keep no personal logs, nor store specific details about your private communications and will always gladly accept suggestions and criticisms on how we can improve our services. If you believe we are asking for more information than we require or you would like us to clear anything up, please contact us with your concerns.

What does this privacy policy cover?

- This privacy policy covers any and all the services xroom.app provides to any customer or user. If you decide to use any of our services, you will be asked to accept this privacy policy and it shall apply whether you are a paying customer, a free customer or a customer's guest.
- This policy describes what information we collect when you use xroom.app's sites, services, mobile applications, products, and content "Services". It also provides information about how we store, transfer, use, and delete that information, and what choices you have concerning the information.

- This policy applies to xroom's online video meeting tool, including the website and mobile applications, and other xroom.app websites "Websites", as well as other interaction (e.g. customer support, surveys, outreach etc.) you may have with xroom.app.
- This policy applies where we are acting as a Data Controller concerning the personal data of users of our Services; in other words, where we determine the purposes and means of the processing of that personal data. For content and data that you upload to or make available through the Service "User Content", you are responsible for ensuring this content is following our Terms of Service, and that the content is not violating other users' privacy.
- For customers on our free and non-enterprise plans, we decide what data we collect from users and the purpose of processing. This, according to the definitions in GDPR, defines us as a Data Controller, and not a Data Processor with regards to our Free and Pro users. It is therefore not relevant for us to offer a Data Processing Agreement to private-individual customers.
- This is clearly defined in GDPR Article 1 "Definitions"
 - Point 7: *'controller' means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data; where the purposes and means of such processing are determined by Union or Member State law, the controller or the specific criteria for its nomination may be provided for by Union or Member State law;*
 - Point 8: *processor' means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;*
- Since our free and non-enterprise plans are only intended for private and non-business use we do not enter into a corporate commercial agreement where your company instructs us to process personal information for you, every individual user of xroom.app will be the data subject in the case where they sign up for an account with us, the Data Controller. A Data Processor is someone who only processes data on the Data Controller's requests and instructions, and within strictly defined purposes, e.g. a hosting provider.

GDPR Compliance -

- On 25 May 2018, the EU General Data Protection Regulation (GDPR) came into force, highlighting the importance of data protection in an increasingly digital world. xroom.app is an Estonian-based organization that values integrity, privacy and protection of all personal data that both our customers and employees may generate.
- GDPR is set to replace diverse and growing directives and national legislation to introduce consistency to data protection in Europe. Additionally, GDPR sets a benchmark for many regions that are becoming ever increasingly digitized. GDPR core principles cover privacy, transparency, fairness and

introduce accountability. By introducing a risk-based approach, GDPR seeks to enable innovation within the global digital economy, while enabling the rights of individuals.

- In our view, the digital economy can only blossom when individuals can connect, store, process and share information across devices securely and ethically. At the same time, in general, we believe it is best to store the least data possible to lower your and our risk surrounding data integrity and privacy. That means creating our company and infrastructure in such a way where data and privacy is safeguarded and where we only keep what is legally required and or strictly business relevant.
- We will ensure to uphold all requirements and requests per GDPR. We will ensure to remain committed to helping our customers and partners by protecting and respecting their personal data.

GDPR readiness and updates

- Our GDPR readiness mission ensures that we meet our obligations relating to data protection.
- We are proud to say that we have taken precautions, during the creation of our mission and product, to only allow required data to flow in and be stored. As such, by minimizing the amount of data stored and kept, we have not needed to make significant changes as a result of our GDPR readiness preparations.
- xroom.app's products and services will continue to operate as intended and we will ensure to uphold efficient communication to our customers regarding any future changes to these measures. Any changes made will only benefit our stakeholders and improve our attention to security and data protection while remaining in compliance with legal requirements.
- Users will be informed via email and through GDPR articles on xroom.app's online communities and will be maintained and kept up to date as part of our regular communication to our stakeholders.
- Any users consenting to receive material such as via email or Newsletter, are already provided with the ability to change or withdraw consent, for example by adapting the frequency or relevance of emails and newsletters, or by unsubscribing. The notification data may be processed to send you relevant product information or newsletters. The legal basis for this processing is your consent cf. GDPR art. 6 (1) item a.
- As part of the ongoing evolution of the xroom.app products, we will constantly continue to review the business purpose for using personal information. We will never sell your data to any third party. We will also ensure to review all points of data transfer and adjust our collaborations based on any legal requirements and or our clients' needs. Transparency around these points shall be maintained and remain up to date. As such there may be future changes to our conditions or policies and potentially consent aspects. We remain committed to remaining transparent and in proactively making our customers aware of any and such changes.
- xroom.app guarantees to inform users when collecting their data (directly or indirectly) of their data processing and where required, we will collect consent from the data subject.

- As part of our GDPR readiness activities and as required by the regulations we have updated our records of processing activities as part of our continuous review of how personal information is handled across our business operations, products and services.
- Our data protection governance arrangements and privacy mindset ensure that our operations are subject to continuous review to maintain alignment with GDPR as we introduce new products and services.
- This policy may be updated from time to time by publishing a new version on our website. Users are encouraged to check our website privacy policy page occasionally to ensure they understand and agree with any updates.
- We will also notify users of changes to this policy by email, if possible, and in certain cases by communication via our social media channels.

Service and transactional notifications.

- If we send you emails about your account, service changes or new policies. You can't opt-out of this type of "service or transactional" emails (unless you delete your account) as they are necessary information for the Services.
- The legal grounds for processing this information is that it is required for performing our commitment about communicating changes in plans and pricing to you in the contract we entered into with you, at your request (our Terms of Service) cf. GDPR art. 6 (1) item b, and our legitimate interest of communicating important information about your account to you, cf. GDPR art. 6 (1) item f.

What kind of data does xroom.app store?

- We are proud to say this, but we store almost no data at xroom.app.
- We have no access to the video calls made via xroom.app's platform. The only persons that have access are the participants in the call. Therefore, we do not record or store your video calls, communications or files on our servers.
- Customers that choose to purchase a paid version of the Services provide xroom.app (and our payment processors) with limited billing details such as credit card information, billing email, name, address and the time of transaction.
- We store minimal payment info and the associated email account entered when you purchased our solutions, via Stripe. In general, this information is used to provide you access to our dashboard after you have purchased our products and to ensure ethical adherence regarding all legal requirements impacting our business, invoice and accounting activities. The transaction data may be processed to supply the purchased services and keep proper records of those transactions. This data may be used to deliver the Services to you.
- We will always focus on securing any data acquired with encryption, access control, anonymization or obfuscation.

- When using our solutions, we do not require names nor store any names you may enter. You do not even have to be logged into our dashboard if you do not require white-label or specialized solutions.
- We do not keep personal logs or any other details that could identify a user. We do not know what calls you have joined when they happened nor with whom. We do not save any personal data sets about visitors and their calls that could identify a user. This limits your vulnerability in case of a data breach.
- However, if you are to contact us, for example via email, we may store any data that you provide us to ensure we adequately process your request for up to 2 years. Any of these interactions will remain encrypted, via Zohomail, and if you wish to opt-out or have your information removed you may contact us at legal@xroom.app.
- The legal basis for this processing is your consent, cf. GDPR art. 6 (1) item a. The legal basis for the retention of transaction data is a legal requirement, cf. GDPR art. 6 (1) item c.

Detailed information on what xroom.app stores or processes?

- We do collect a minimal amount of data for analysis and statistics. The data on visitors to the xroom.app domain is fully anonymized and we do not pass it to any third party. We will never pass on any of your information to any third party or any similar platform, on contrary to almost 100% of other online services. The data we collect is only used to perform A/B tests and other experiments on marketing and design, ultimately improving your experience and interactivity with our services.
- Even though we do not store personal logs that can identify users, within our platform, we may keep minimal meta-data logs for up to 2 years. We do this entirely for analytical purposes and to ensure that we are constantly improving and building tools that our users make use of and enjoy.
- For example, we would like to be able to understand how many visitors we have had in a day, how many of those visitors are unique, how many unique visitors or users we have per month and how many unique rooms were created per month.
- Additionally, we keep logs that tell us when a room client has been added or removed when a room has been added or removed, if any room options, plugins or settings used have been enabled, set or removed. We may even store error network flags for troubleshooting reasons. This data cannot be used to identify you.
- The data that we collect is a result of [fingerprinting](#) analysis, but contrary to the name our methods cannot provide any information that could identify the user's name or personal details or who is who.
- What we know is mainly the session id, the language, the path used, the time, IP and domain and some general details about the users' browser. By limiting the amount of data we collect, we aim to limit your vulnerability in case of a data breach. However, sometimes these strict methods can also be slightly problematic for users and our developers. For example, if a user faces a technical problem it can be difficult to find their session and investigate further into what could have caused their particular problem.
- Further explanations can be found below:

Authentication	We may use local storage to identify you when you visit our website and to authenticate calls our web application makes to the backend servers on your behalf, if using a paid subscription. For example, if you're signed in to xroom.app, this helps us show you the right information and personalize your experience. (Local storage element used for this purpose is: "CredentialsStorage")
Analysis and statistics	We use cookies to help us analyze the usage patterns and performance of our website and services. We use services such as Google Analytics, and Sentry.io, for this purpose, see the cookie list for more details.
Payment and Fraud detection	We use cookies to enable easy payment processing and to detect fraud through our payment processor Stripe Payments Europe, Ltd. ("Stripe"). See the cookie list for cookies related to this.
Integrations	We may use cookies in your browser to access and share content from third-party Integration Services that you choose to activate in the Service. Some integrations will not work for users who have blocked third-party cookies in their browser, as it will then not be possible for us to open the content from the Integration Service for them. (Cookies used for this purpose depending on which Integration Services you have activated).
Advertising and Marketing	We may use cookies and similar tracking technologies of third parties, to learn whether someone who saw an ad in a marketing platform later visited our site and took an action (e.g. created an account or upgraded to a paid plan), and provide our advertising partners with information about how the ad performed. We may also work with advertising partners to show you an ad off xroom.app after you've visited our site or application.

Under no circumstance will we release any private or personal information to any of our providers, via cookies or any other form. The same goes for your private communications, we nor anyone else will have access to it, but you and your guests during the call.

Third-party service providers

- We check whether there is a lawful purpose for the processing of data, limit which data is shared with others and track the personal data shared with others (for example, our providers)
- Our Third-party service providers operate under the same regulatory frameworks that we do and we select and manage industry standard suppliers to ensure that we can deliver the best products and services
- xroom.app is based in the EU and our products make use of an industry-standard hosting and storage provider, named DigitalOcean, which operates in the EU.
 - More information about DigitalOcean's services may be discovered at the following links:
 - <https://www.digitalocean.com/legal/gdpr-faq/>

- <https://www.digitalocean.com/blog/gdpr-resources/>
- All payment details are stored by a third-party provider named Stripe, specifically Stripe Payments Europe, Ltd. Stripe is an extremely reliable, global payment processor that manages transactions for thousands of customers every day. Stripe is a PCI Service Provider Level 1, which is the strictest level of certification possible for a payment processor. They use high-level security to achieve this, and they are also GDPR compliant.
- To provide simplified purchase support, xroom.app administrative employees may have access to partial information about credit card transactions and any email associated with your purchase. All-access to this data will remain secure and logged per transaction. This transaction data is stored for 5 years and is strictly required for compliance, tax and business accountability. The legal basis for the retention of said transaction data is a legal requirement as stipulated in, cf. GDPR art. 6 (1) item c.
- If you have previously contacted us via our contact form and emailed us your name, email address, phone number or any other personal details, these details may be contained within your support history. Any personal data sent via our website's contact form is not sent to or connected with our platform's servers.
- The legal basis for the processing of all of the above is the performance of a contract, cf. GDPR art. 6 (1) item b as well as our legitimate interest of handling your requests cf. GDPR art. 6 (1) item f.
- - More information about Stripe's services may be discovered at the following links:
 - <https://stripe.com/en-se/guides/general-data-protection-regulation>
 - <https://stripe.com/privacy-center/legal>
- All corresponding email communications are stored and remain encrypted by a third-party provider named Zohomail.
- To end-to-end encrypt all xroom.app email interactions, to and from customers, employees and partners, we make use of services that limit access to the contents of said emails thanks to zero-access encryption. This limits your vulnerability in case of a data breach.
 - More information about Zohomail services may be discovered at the following links:
 - <https://www.zoho.com/mail/security/email-encryption.html>
 - <https://www.zoho.com/gdpr.html>
- To improve performance on our platform, we use Sentry.io which helps us to diagnose, fix errors, and optimize the product. Using this technology is a standard practice within the IT space and is used by giants such as Microsoft, GitHub and Cloudflare. Absolutely no personal information from your conversation is provided or passed to their platform.
 - More information about Sentry.io services may be discovered at the following links: <https://blog.sentry.io/2018/03/14/gdpr-sentry-and-you>
- If you require further additional information, a specific request for personal information, or a deletion request please submit this request using legal@xroom.app.

- We may need to authenticate your identity to ensure we handle any request securely.
- Existing legislation and GDPR requires organisations to respond to all data subject access requests. xroom.app can help our customers handle any of these requests.
- To bring you sequenced and constant technical updates we use a platform called <https://headwayapp.co>. It sets a cookie to provide you visual updates on our homepage, found next to the blog button. This is a common way to keep stakeholders updated.
 - More information about headway.app and their services can be found at:
 - <https://headwayapp.co/privacy>
- To market our products and to create retargeting we use SendinBlue. Using this technology is a common method for outreach and marketing.
 - More information about SendinBlue may be read at the following link:
 - <https://www.sendinblue.com/gdpr>

Cookies Policy

- xroom.app does not write any code that uses cookies at all because:
 - This is a rather old and poor practice originally developed in 1994.
 - We believe that most of the legal restrictions around data are due to cookies and as a result, LocalStorage regulations have become less strict because it's not possible to exchange that data cross-domain.
 - As a practice, our dev team has not created code using cookies, since 2010, and are not sure why they are still so active in use by so many of our partners.
 - This means that all the cookies on our site come from 3rd parties.
- Cookies are small files that store information on your computer, mobile phone and other devices. Through them, entities who put them on your device can sometimes recognise you across different websites, services, devices, or browsing sessions. Cookies can serve many purposes. Cookies also do things like remember your camera settings, prefill form fields and let you remain logged in. They allow us, amongst other things, to provide a better overall service by identifying which pages are the most popular, remembering user setting and preferences, identifying which of the users of our services engage more in and if some of our services and products need maintenance.
- Cookies are used to understand how effectively we can communicate to our customers what we are doing and which services we are offering, and we can understand that through Analytics, which requires cookies to provide us with that data.
- Users will be asked to consent to the use of cookies, per the terms of this policy, when you first visit our website. Users will need to give clear consent to our use of cookies by clicking "Accept, Okay, I confirm or Agree", after

reading a pop-up message informing them of our use of cookies and are given the chance to read more in detail about our cookie policy.

- Users always have the option to opt-out and disable cookies, but they should be aware that their experience using our service may be impacted negatively by doing so.
- You may elect to decline all cookies via your computer. Every computer can decline file downloads like cookies. Your browser has an option to enable the declining of cookies. If you do decline cookie downloads, you may be limited to certain areas of our site, as there are parts of our site that require cookies. The most effective way to do this is to disable cookies in your browser.
- We may use cookies and similar tracking technologies of third parties, to learn whether someone who saw an ad in a marketing platform later engaged with our site, and provide our advertising partners with information about how the ad performed. The advertising partners we may work with are Google, YouTube, Facebook, Instagram, Twitter and LinkedIn. We use and process limited data as part of these cookies based on your consent.
- You may also decline to accept cookies on our website. We suggest consulting the Help section of your browser or taking a look at [the About Cookies website](#) which offers guidance for all modern browsers.
 - Otherwise, you can also check the resources below:
 - Most cookies can be [disabled in your browser settings](#).
 - For more details about other popular browsers click below:
 - [Google Chrome](#)
 - [Microsoft Edge](#)
 - [Mozilla Firefox](#)
 - [Microsoft Internet Explorer](#)
 - [Opera](#)
 - [Apple Safari](#)
 - To opt-out of being tracked by Google Analytics across all websites, visit <http://tools.google.com/dlpage/gaoptout>.

Here's are some of the cookie you may notice while using our services:

Domain	Name	Description	Type
my.xroom.app	__stripe_mid	Data collected by xroom.app for our payment processor Stripe	First-party, persistent
my.xroom.app	__stripe_sid	Data collected by xroom.app for our payment processor Stripe	First-party, persistent
m.stripe.network	nsr	Data collected by our payment processor Stripe for fraud detection https://stripe.com/cookies-policy/legal	Third-party, persistent

xroom.app	_ga	Google Universal Analytics - This cookie is used to distinguish unique users by assigning a randomly generated number as a client identifier. It is included in each page request in a site and used to calculate visitor, session and campaign data for the sites analytics reports. Opt-out: https://tools.google.com/dlpage/gaoptout	First-party, persistent
xroom.app	_gat	Google Universal Analytics - it is used to throttle the request rate-limiting the collection of data on high traffic sites. Expires after 1 minute. Opt-out: https://tools.google.com/dlpage/gaoptout	First-party, session-based
xroom.app	goog_report_conversion	Ads conversion cookie for Google. Used on landing pages separate from xroom.app and used to track engagement with users directly acquired by marketing activities, if the user accepts.	Third-party, session-based
xroom.app	fr	Ads targeting cookie for Facebook. Used on landing pages separate from xroom.app and used to track engagement with users directly acquired by Facebook marketing activities, if the user accepts.	Third-party, session-based
xroom.app	HW_readItems	Headway uses browser's Local Storage to help Headway identify and track visitors, their usage of Headway website, and their website access preferences.	Third-party, session-based

Server locations

- We may operate a global infrastructure of video servers distributed across the world, and users will be automatically routed to the closest available one to them. This is solely done to improve our overall services. This means that e.g. users in a European country will automatically connect to a data centre physically located within the EEC. The video router servers and all of our infrastructure adhere to strict security measures, preventing any eavesdropping or interruption of the video/audio streams. The video router servers and all of xroom.app infrastructure adheres to strict security measures, preventing any eavesdropping or interruption of the video/audio streams. Media sent between participants in a room will not be stored. Hosting providers used to route video calls cannot access or control the data streams, nor is any transmission initiated by them, and data sent through xroom.app is initiated by the customer, the customer selects the receiver of the transmission and xroom.app or its subcontractors is not able to select or modify the information contained in the transmission, cf. GDPR Article 2 (4).

International transfers of data

- In some circumstances, your personal data may be transferred to countries outside the European Economic Area (EEA). You acknowledge that personal data that you submit for publication through our website or services may be available, via the internet, around the world. We cannot prevent the use (or misuse) of such personal data by others. For information about what types of content you as a user is responsible, see this Terms of Service.
- We have offices and facilities in Sweden and Estonia. The hosting facilities for Account information stored by xroom.app are based in Germany. The hosting facilities for Usage information are situated in Germany and the United States. Transfers to the United States will be protected by appropriate safeguards, namely the use of standard data protection clauses adopted or approved by the European Commission, a copy of which can be obtained from https://ec.europa.eu/info/law/law-topic/data-protection/data-transfers-outside-eu/model-contracts-transfer-personal-data-third-countries_en.

Integrations with external services

- You as a participant in a meeting may choose to open one of the integrations we provide (Slack, Telegram and others) in rooms where these have been enabled. We may store data from the use of integrations in local browser storage, and process this to enrich the user experience. This data can be deleted with the delete option in the integration settings or by deleting it from the cache of your browser. When using an integration, metadata like title, thumbnail, dates and share permissions about content selected may be fetched and displayed on the web page. We may store non-personal/non-restricted information (eg. content id and access date) in local browser storage to display lists of recently opened integrations. Restricted metadata is always stored by the services themselves and requires explicit consent given by the facing user to fetch it. The implementation complies with the services privacy policies: [Slack Privacy Policy](#), [Telegram Policy](#), [Random Word API](#), etc.
 - Additionally, we allow the possibility to login via linkedin per popular request. We do not access or request access to anything besides your

email address and we use it to validate your login in our dashboard. More details may be found on LinkedIn's site [here](#).

- The information may be used to operate our website and provide our services. This is required to deliver the Service to you as the user, by taking steps, at your request, to enter into and to fulfil such a contract (Terms of Service) cf. GDPR art. 6 (1) item b.

Encryption

- xroom.app lets you make video calls through a web browser on any modern web-enabled device and is best suited for video calls between a handful of individuals. Our platform provides video calls, communications and file transfers that are end-to-end encrypted.
- xroom.app is built using open source technology called WebRTC, and follows common industry standards, across its platform and API, for strong encryption by using AES and ECDH.
- End-to-end encryption means that only you and the person(s) you are speaking to can hear and see the conversation or review the files transferred and therefore makes it near possible for a third party to have access to it. This encryption makes it so that both you and your participants can engage in a confidential conversation that is protected and minimizes the risk that someone else could decrypt the contents of your communications, in real-time, as it's being transferred online.
- If a video conferencing software does not implement strong encryption through the entire connection between parties, then it will not fulfil the security standards, regulations, norms and best practices used today.

How is communication in xroom.app secured?

- Locking your room
 - The video and audio communication in an xroom.app room is only visible to participants inside a room. Another user can't listen in on room data unless they are present in the room themselves (which means they would be visible to everyone in the room). Because the room URL is public, it's possible for anyone who can guess a room name to enter an open room. If you want to prevent others from coming into the conversation, we recommend locking the room by clicking the Lock button in the room menu. If you are the owner of a room you can keep the room locked at all times, so no one else can enter it. After doing this no new participants will be able to enter the room without the owner's permission or without the owner providing them with the password.
- Chat and transfer files within a chat
 - Chat messages are not stored. They do not pass through our servers. Additionally, as each participant leaves the room the chat messages that were stored locally on their computer are deleted.
- End-to-end encryption
 - See "Encryption" paragraph
- User card
 - If you at any point add your name when you join a call, a photo (if you wish to show a picture instead of appearing via video) all added data

will be saved to a local user card and shall only be exchanged with the others in the room via the browser. We do not have access to this user card and this data never is stored by us on our servers. Additionally, as each participant leaves the room the user card info that was stored locally on their computer is deleted.

- Plugins that record audio and video
 - If you wish to record your video calls, you must be aware that there are many laws governing such types of recordings and whether or not you must acquire consent from all parties of your conversation. As a rule, please do not begin to record anyone without their knowledge and explicit consent. If you use the video or audio recorder plugin, in our platform, there will be clear feedback provided notifying everyone else that a recording is being made.

Intermediary media servers (aka "Boosters")

- It is a common practice to use intermediary media servers (selective forwarding units) within the video conferencing space. There are many legitimate purposes for using these types of servers, but when transmitting this data, the contents of the call will be unencrypted and read within the media server. Reasons for using a media server could be to strengthen the signal, by allocating extra bandwidth to it, to be used in streaming or webinar scenarios.
- xroom.app is made specifically for conferencing between individuals and due to the nature of WebRTC technology, is completely reliant on the conference initiator's internet connection (the "host" of the conference). As a solution, xroom.app offers "Boosters" should the host not have a reliable connection that supports a large number of participants.
- We realize that this can often pose a problem when it comes to security and integrity, on certain platforms, which is why we advocate for people to limit the use of intermediary media servers when privacy is required. Unlike many others, we provide an additional layer of End-to-end encryption to protect you on our platform ultimately making transfers through our "Boosters" safer.
- However, in full transparency, we plan to release all the code associated with our "Boosters" to our GitHub account soon, to ensure that our users know that we at xroom.app are not meddling with or reviewing their communications.

Statistics

- When you are a visitor to xroom.app we use Google Analytics to track your browsing on our websites. This is strictly done for marketing, sales and awareness. This also helps us improve our product, plans, and features. This places some cookies in your browser, and besides knowing which xroom.app pages you have visited, we also know:
 - The operating system you are using
 - The browser you are using to visit xroom.app
 - The page that linked to xroom.app if you clicked a link
 - Where you are located in the world (or the location of your IP address)
 - Which language your browser is set to

- We do not know who you are or have any personal information about you besides the above.
- We may even use this data to give you better support should you run into technical issues, and give better advice about how xroom.app will work for you.
- *The legal basis for this processing is your consent, cf. GDPR art. 6 (1) item a.*
- *Additionally, The legal basis for this processing is our legitimate interests cf. GDPR art. 6 (1) item f, namely using this data to ensure the proper administration of our website and business, analyze the use of the website and services, monitoring and improving our website and services, improving the user experience, preventing abuse, and assisting users with support inquiries. For information about cookies and how to opt-out of cookies, see our Cookie Policy section.*
- *You may decline accepting cookies on our page to avoid having these statistics are collected.*

Correspondence information.

- We may process information that you choose to share with us if you participate in a focus group, contest, activity or event, apply for a job, interact with our social media accounts or otherwise communicate with xroom.app.
- The correspondence data may be processed to communicate with you and record-keeping. The legal basis for this processing is our legitimate interests cf. GDPR art. 6 (1) item f, namely the proper administration of our website and business and communications with users.

Signing up for events or webinars

- If you fill out a form to order a guide or white paper, or if you attend a webinar or event, we may receive an email with the info you gave us in the form. This may include your:
 - Name
 - Address
 - Place of work
 - Email address
 - Phone number

We encourage you to provide as little data, as possible, that you feel comfortable with.

We will never require you to fill or provide anything we would not do and none of these fields will ever be mandatory.

- We may use Google Docs or the online Microsoft Suite and Typeform to collect signups and orders. This information is not stored anywhere tied to your browsing or behaviour mentioned above and is deleted after your order is sent or the event is over.
The legal basis for this processing is your consent, cf. GDPR art. 6 (1) item a.

Who else has access to your data?

- To make the tools we use for support, billing, and similar work as well as intended, it is often necessary to share some of your data with our third-party providers. We only share data when it is necessary, and we share as little as possible. We have strict data processing agreements with all our providers and control how they handle data. So, if you tell us to change or delete information, those changes will also be reflected in data they can access if these overlaps.
- In addition to the specific disclosures of personal data set out in this Section, we may disclose your data when legally obliged to by law.
- We retain your contact data as long as we have an active customer relationship with you. If the customer relationship ends, we keep your contact data for another 90 days before we delete it from our systems, except for invoices and transactions, that we are required to keep for 5 years.
-

Payment and billing

Service	Information	Why we use it	Where data is stored	Legal basis
Stripe	- Contact information - Financial info	We handle payments to xroom.app through Stripe	EU and US	GDPR 6.1.b

Support, communication marketing and sales

Service	Information	Why we use it	Where data is stored	Legal basis
Digital ocean	- Hosting provider	To bring you our services in a safe and efficient manner	EU and US	GDPR 6.1.b

Statistics

Service	Information	Why we use it	Where data is stored	Legal basis
Google Analytics	Cookies - How you use xroom.app	To see how you move around our website xroom.app (but not the video calling platform). Also useful for campaigns and attracting users to our website. Stores no identifying data, and your IP address is not collected. No personal data is passed along.	EU and US	GDPR 6.1.b
Sentry.io	Error reporting	To diagnose, fix errors, and optimize the product	EU and US	GDPR 6.1.b
Headway.app	Technical updates	We use it to provide our users with relevant technical updates and news about our product	EU and US	GDPR 6.1.b

User Rights: Changing, correcting or deleting your data

- We have firmly established that we do not aim to collect personal data about you. Nor will we ever sell it or use it for any other purposes than originally promised. Your personal data remains your own and under your control, so you have the right to tell us how to handle it. Contact us to request any changes in how we handle your data.
- You have the right to know exactly what data we have collected about you. If requested, we will provide a full overview within four weeks.
- You have the right to know who can access and alter your data.
- You have the right to data portability.
- You have the right to change, rectify and update your information if what we have is incorrect.
- You have the right to move your data to another provider. If requested, we will provide you with all your information in a file format (.json) readable by other web services.
- You have the right to object to and restriction of our processing of your personal data
- You have the right to be deleted and forgotten, with a small exception for billing and payment data, which we are lawfully required to keep.
- You have the right to complain to a government instance about how we use data. This complaint should be lodged with the Estonian Data Protection Inspectorate (Andmekaitse Inspektsioon). We would also appreciate it if you would contact our customer service if you find our use of data unethical or unlawful so we can correct it.
- If you have an xroom.app account, you can access, modify or export your personal information, or delete your account in settings. If you delete your account, your information and content will be unrecoverable after that time. You may instruct us at any time not to process your personal information for marketing purposes, by adjusting your settings, unsubscribing to our outgoing emails or contacting us directly. We may withhold personal information that you request to the extent permitted by law.
- If you have provided your consent to your processing of personal data, you may also withdraw your consent at any time, in our settings panel.
- We retain your contact data as long as we have an active customer relationship with you. If the customer relationship ends, we keep your contact data for another 90 days before we delete it from our systems, except for invoices and transactions, that we are required to keep for 5 years.
- The legal basis for the retention of transaction data is the legal requirement, cf. GDPR art. 6 (1) item c.
- The rights are not absolute, and you may read more about your rights in the EU general data protection regulation Chapter III, or at https://ec.europa.eu/info/law/law-topic/data-protection/reform/rights-citizens_en
- To exercise your rights or if you otherwise have any questions regarding our processing of your personal data, we encourage you to contact us as described below. However, we also notify you that you may raise a complaint to a data protection authority.
- Data Protection Officer: Haza Newman
Email: legal@xroom.app

Health providers EU/US

- In the EU, if a video conference involves the processing of personal data, then it is protected by the General Data Protection Regulation (GDPR). Additionally, your business must enter into a Data Processing Agreement (DPA) with xroom.app based on GDPR guidelines, Estonia's Personal Data Protection Act and Estonian eHealth Foundation standards. Please contact us with any questions or inquiries about these options at legal@xroom.app.
- We can exclude any remote third-party hosting or cloud storages, by installing our light-weight applications on any internal systems (your on-site premise) if needed. We have an open API that can also connect your needs directly to our core technology.
- In the United States, if a video call involves the exchange or processing of Protected Health Information (PHI), then it is legally protected by HIPAA. This means that your business must enter into a Business Associate Agreement (BAA) with xroom.app if you wish to use it for these purposes.
- The Health Insurance Portability and Accountability Act of 1996 (HIPAA) required the Secretary of the U.S. Department of Health and Human Services (HHS) to develop regulations protecting the privacy and security of certain health information. To fulfil this requirement, HHS published what are commonly known as the HIPAA Privacy Rule and the HIPAA Security Rule. The Privacy Rule, or *Standards for Privacy of Individually Identifiable Health Information*, establishes national standards for the protection of certain health information. The *Security Standards for the Protection of Electronic Protected Health Information* (the Security Rule) establish a national set of security standards for protecting certain health information that is held or transferred in electronic form. The Security Rule operationalizes the protections contained in the Privacy Rule by addressing the technical and non-technical safeguards that organizations called "covered entities" must put in place to secure individuals' "electronically protected health information" (e-PHI).
- xroom.app is an EU-based business that develops conferencing tools and is not a healthcare-focused solution. However, our tools are available for integration via our open API. In either case, we do not ourselves review, store nor distribute personally identifiable health information to covered entities, i.e. doctors, dentists, hospitals or health plans.
- We meet the requirements needed for HIPAA compliance because we encrypt data all and do not store any specific public health information or details about the private communications occurring on our platform.
- Because we do not store or collect any PHI, we are unable to provide backup measures, provide any PHI via notifications, emails or other channels and cannot provide updates about the safety or protection of any PHI.
- Identification security requirements - Should the healthcare professional know the patient; the video image of the patient may fulfil identification security

regulations. Additionally, checks can also be made visually through the use of other legal forms of documentation in countries that support telemedicine.

- We can exclude any remote third-party hosting or cloud storages that may or may not be HIPAA compliant, by installing our applications on any internal systems (your on-site premise) if needed. We have an open API that can also connect your needs directly to our core technology. We are even happy to set-up an audit or review if needed.

Need a BAA (business associate agreement) or a DPA (data processing agreement)?

- For our enterprise plan, we offer a Data Processing Agreement. These plans allow companies and organizations to set up accounts and add extra users and thus have the ability that an admin user can import emails of other employees when inviting them (which constitutes Personal Identifiable Information).
- We can also provide a Business Associate Agreement (BAA) for each xroom.app enterprise that operates within the American healthcare sector.
- The BAA protects the covered entity and requires that the business associate handle all Protected Health Information per the Privacy Rule.
- These types of agreements can be provided, as an addition to and for many customers. We can provide a suitable signed template for any of our commercial customers. Please contact us with any questions or inquiries about these options at legal@xroom.app.

Changes to this policy

- We can change these Terms at any time. We keep a historical record of all changes to our terms on [GitHub](#). If a change is materialized, we'll let you know before it takes effect. By using xroom.app on or after that effective date, you agree to the new Terms. If you don't agree to them, you should delete your account before they take effect, otherwise, your use of the Service and Content will be subject to the new Terms. Please contact us with any questions or concerns.

Any other questions or feedback?

- We hope that we have been fairly clear within our terms, but we understand you might have additional questions. You will find answers to the most frequently asked questions about the Service.
- However, feel free to reach out to support@xroom.app when the need arises and we'll always do our best to answer you as quickly as possible.
- For questions related to these Terms, or any legal concerns please contact legal@xroom.app.

Our details

- This website is owned and operated by NISDOS ESTONIA OÜ ()
- We are registered in Estonia, code (EE), 14349798, and our registered office is at Artur Lind Building Sepapaja 6 11415 Tallinn Estonia (Sepapaja tn 6 Lasnamäe linnaosa, Tallinn Harju maakond 15551)

Data protection officer

- Contact detail for our person responsible for data-related questions is:
legal@xroom.app

Versioning

- Version 1.0 of this document was created and released on 6 Sep 2020.