HansRoslinger

Yubi

Technical Report: Privacy

Table of contents

1 Report Scope

This report will examine the privacy policies and practices that Yubi must implement to protect the data of its end user. Specifically, compliance requirements outlined in legislation from different countries such as the European Union (GDPR), Australia (1988 Privacy Act) and America (COPPA) will be identified and explored.

Building on this, all user data that is collected will be identified and potential breaches of user privacy and legislation will be explored.

Finally, this report will provide recommendations to address privacy and legislation issues within the project. Ensuring that Yubi fulfills its legal responsibilities and protects the privacy of its users.

2 Executive Summary

This report identifies key privacy risks in Yubi's handling of user data and aligns them with relevant policies and legislation. Yubi collects emails, passwords, names, and uploaded assets, creating several risks.

First, **data minimisation** is not fully observed, as collection of full names may exceed necessity. The associated mitigation measures are to minimise data collection by making full name optional

Second, **storage security** is a concern: while passwords are hashed, emails and assets remain in plaintext, raising exposure risks if the database is breached. Mitigation will include applying field-level encryption & RBAC for emails and names. Secure asset uploading via using bucket policies and session checks

Third, **transparency and user awareness** are insufficient. Users are not adequately informed about webcam/biometric processing via MediaPipe or how their data is used. This is to be addressed via a dashboard for access, correction, and deletion, with a manual fallback in the short term to avoid delivery delays.

Finally, **user rights** are limited, with no mechanism for account deletion or data correction. Publishing a privacy policy & onboarding notice is the associated mitigation measure.

3 Research & List Privacy Policies

3.1 Australia

The biggest privacy policy in Australia is the 1988 Privacy Act [1] which regulates the handling and personal information including collection, use, disclosure and storage. The Privacy Act contains 13 main privacy principles [2]. These principles are known as **Australian Privacy Principles (APP)** and all policies must be adhered to but the ones most relevant to Yubi include:

- **Australian Privacy Principle 1 - Open and transparent management of personal information**
  Yubi must have a clearly expressed, up-to-date privacy policy outlining how personal information is collected, used, stored, and disclosed.

- **Australian Privacy Principle 2 - Anonymity and pseudonymity**
  Users must have the option of not identifying themselves, or of using a pseudonym, when dealing with an organisation.

- **Australian Privacy Principle 3 - Collection of [solicited personal information**
  Yubi may only collect personal information that is reasonably necessary for its functions or activities, and must do so by lawful and fair means.

- **Australian Privacy Principle 6 - Use or disclose personal information**
  Yubi may only use or disclose personal information for the primary purpose it was collected, unless the individual has consented to another use/disclosure, or an exception applies.

- **Australian Privacy Principle 11 - Security of personal information**
  Yubi must take reasonable steps to protect personal information from misuse, interference, loss, unauthorised access, modification, or disclosure. Once information is no longer needed (e.g., account deletion), it must be securely destroyed or de-identified.

There is also the notifiable data breaches (NDB) scheme [3] which is a part of the Privacy Act. This requires Yubi to notify affected customers and the Office of the Australian Information Commissioner (OAIC) if a data breach is likely to cause serious harm. This does not directly affect the build of the software but is important to be aware of.

3.2 Europe

Yubi is subject to the General Data Protection Regulation (GDPR) (EU) 2016/679 [4] when offering services to individuals within the EU based on the information collected from the user (name, email and images).

Key legal obligations include:

- **Article 5 - Data Processing Principles**
  Personal data must be processed lawfully, fairly, and transparently, collected for specific purposes, minimised, kept accurate, and stored securely.

- **Article 6 - Lawful Basis**
  Yubi must have a valid legal basis for processing data, typically user consent or necessity for account creation and image storage.

- **Articles 13–14 - Transparency Requirements**
  Yubi must inform users at the point of collection about how their data will be used, stored, and their rights.

- **Article 17 - Right to Erasure**
  Users can request the deletion of their data, which must be honoured unless a legal exemption applies.

- **Article 32 - Data Security**
  Yubi must apply appropriate technical and organisational measures to protect personal data from loss, unauthorised access, or misuse.

- **Articles 33–34 - Data Breach Notification**
  If a breach poses a risk to individuals, Yubi must notify the relevant supervisory authority within 72 hours and inform affected users promptly.

In addition, Yubi must comply with the ePrivacy Directive (2002/58/EC) for the use of cookies and similar technologies, requiring informed consent for any non-essential tracking.

Further national laws, such as Germany’s BDSG or France’s Loi Informatique et Libertés, may also apply depending on user location.

By complying with these regulations, Yubi ensures strong data protection standards and allows for operation within the European market.

3.3 America

Unlike Europe and Australia, America does not have an overarching privacy law. Regulations to be considered include federal, state and sector-specific regulations.

Federal regulations to be considered include:

- **Children's Online Privacy Protection Act [COPPA]**
  This applies to users under 13 years of age and states that parental consent is required to obtain private information [5].

Sector-specific regulations to be aware of include:

- **HIPAA**
  There are special regulations around Health Data [6]. A disclaimer will be needed that states sensitive information should not be uploaded so that HIPAA privacy regulations do not apply.

- **FERPA**
  There are special regulations around student data in educational settings [7]. A disclaimer will be needed that states sensitive information should not be uploaded so that FERPA privacy regulations do not apply.

State regulations to be considered include:

- **California Consumer Privacy Act (CCPA)**
  Applies if you handle data of Californian residents and meet certain thresholds such as having an annual gross revenue of more than 25 million USD [8].

Similar policies apply in states across America such as Virginia (VCDPA), Colorado (CPA), Connecticut (CTDPA) and Utah (UCPA). These should be considered and monitored as the company grows but are not yet relevant.

4 Identify Types of Collected Information

Data Collected	Usage	Stored
Email	Each user's email is collected in order to identify them in the app. The value is stored as a plain text. The email is not hashed and anonymized as Yubi can also serve as a content storage app which means we must comply with audit purposes if one of our users was found to be storing illegal content. Furthermore an email is not hashed because as part of a future feature we may need to send emails to users for a password reset for example, this would not be possible if we hashed the email. Furthermore an email on its own does not consitute as PII (https://www.oaic.gov.au/privacy/privacy-guidance-for-organisations-and-government-agencies/handling-personal-information/what-is-personal-information) as it alone cannot identify an individual, a user may have an email FIT3170@gmail.com, this email does not uniquely identify a person however since Yubi also stores the name of the user it stores PII as the combination constitutes PII [2].	Stored in the prisma database which has restricted access to only select developers through a gmail verification system.
Password	The passwords stored in Yubi are hashed using SHA256 meaning they cannot be reversed and a user's password can never be used or viewed by someone who has access to the database. This ensures users' passwords are kept private.	Stored in the prisma database which has restricted access to only select developers through a gmail verification system.
Visual Assets	Users select or add visual assets (e.g., PNG images or Vega-Lite JSON specifications) to place on the canvas, move, resize, and interact with. The app renders assets in the KonvaOverlay and tracks position, size, and hover state to support	The files themselves are stored externally (e.g., public assets for demos or user-specific S3 buckets referenced by s3BucketUrl). Within the app, only selection state

	interaction and layout. To provide users with a consistent experience, only lightweight selection metadata is persisted to the client-side.	and layout metadata are stored in the browser's localStorage under the key selectedUploadKey.
Name	The user's name is collected to personalise the UI and, if present, to label user-owned visual assets or S3 buckets for easier identification. It is not used for authentication or authorisation decisions.	Stored in the Prisma database's User table with restricted access to select developers via an email verification system.

5 Identify & Prioritise Privacy Issues

5.1 Issue 1: Collection of personal information

- Issue: The Yubi collects and stores key personal information from users, including full name, email address, and password. While these data are necessary for user authentication, the way in which this information is collected raises potential privacy concerns. Specifically, the application does not provide a clear privacy notice outlining why the data is collected, how it will be used, or whether users have the option to limit disclosure. Additionally, the collection of full names may not always be essential for the system's core functionality, which could potentially exceed the principle of data minimization.
- Policies:
  - **APP 1: Open and transparent management of personal information [2]**
    Requires the web application to manage personal information in an open and transparent way, typically by providing a clear and accessible privacy policy.
  - **APP 3: Collection of solicited personal information [2]**
    Personal information should only be collected if it is reasonably necessary for the application's functions. Collecting unnecessary details (e.g., requiring full names) may be excessive.
- Address:
  - **Clarify Collection Purpose**: Update the registration process and privacy policy to clearly state the purpose of collecting each data type (e.g., email for login, password for authentication, name for personalization). This ensures users understand why their data is being collected.

    - **Minimize Data Collection**: Review whether collecting full names is strictly necessary. For certain cases, allowing pseudonyms or optional name entry could still satisfy business needs while improving compliance.
- Recommendation:
    - Publish an updated privacy policy that explicitly explains the collection, purpose, and use of personal data.
    - Implement a transparent consent mechanism during registration, requiring users to acknowledge the terms before proceeding.
    - Minimise data collection, making non essential fields optional (eg. full name). Review forms and features to avoid capturing any unnecessary data
    - Provide user control, allow users to easily manage their personal information in profile settings (eg. update, delete)

5.2 Issue 2: Storage and security of personal information

Personal Information:

- Issue: While Yubi stores user passwords using hashing, other forms of personal information such as names, email addresses, and uploaded assets are stored in plaintext within the Prisma database. This is common practice since emails are required for account identification, audit trails, and potential features such as password resets. However, under the Australian Privacy Act, an email address constitutes personal information when it is collected together with other identifiers such as a full name. Storing these values in plaintext means that if the database is compromised, personal information could be exposed.
- Policy: **APP 11 - Security of Personal Information [2]**
  Organisations are obliged to protect personal information against unauthorised access.
  Policy: **APP 2 - Anonymity and Pseudonymity [2]**
  While a single email may not uniquely identify an individual, in combination with other data, such as a full name, it does. This allows a user to be reasonably identifiable.
- Address:
    - **Tighten Access Controls:** Maintain plaintext storage, but strengthen role based access control.
    - **Field-Level Encryption:** We can encrypt email addresses and names using AES-256, decrypting only when required. This supports features like password resets while adding an extra layer of security.

  - **Tokenisation/Pseudonymisation:** Store tokenised email addresses, and resolve through a mapping service. This is a higher level of privacy but adds more complexity.
- Recommendation:
  - Keep the current approach but add field-level encryption for emails and names. This keeps features like password resets working while improving compliance with [2]. Encryption plus stricter access controls will make it much harder for emails to be exposed if the database is compromised.

5.3 Issue 3: Security of uploaded assets

Uploaded Assets:

- Issue: Yubi allows users to upload assets in the form of visuals (e.g. PNGs or JSONs) to their dashboard to be used during presentations, which may contain personally identifiable information (PII), such as names and addresses, or private and confidential information, such as employee record or health record. If these visuals are stored without strict access control and the database gets compromised, these files are at high risk of being accessed or downloaded by unauthorised users. Uncontrolled download or external access could lead to data and privacy regulatory breaches, as well as significant reputational damage and loss of user trust.
- Policy:
  - **APP 11 - Security of personal information [2] -** Reasonable steps should be taken to protect personal information from unauthorised access.
- Address:
  - **Bucket Policy:** Applying a set of permissions at the storage bucket level to prevent public access to uploaded files.
  - **Authenticated Session Access:** Implement a session-based authentication where the server creates a unique session for the user after their log-in details are verified. This ensures that only logged in and authenticated users can access uploaded assets during active sessions, enabling controlled access to the private assets.
- Recommendations:
  - Implement access control using bucket policies. This prevents unauthorised users from downloading artifacts outside the application, thus protecting user data.
  - Enforce authenticated session checks to control who can access the uploaded files.

5.4 Issue 4: Transparency and User Awareness

- Issues: Yubi uses MediaPipe to process real-time video for gesture detection, which involves sensitive biometric data (e.g., hand position, face, body movement). Even if processed locally, this data may be stored or reused for debugging or analytics. Without clear disclosure, this breaches APP5 and PDPA requirements [2] for informed consent and user notification.
- Policy:
    - **APP 1 - Open and Transparent Management of Personal Information [2]**
      Explanation:
      Organisations must clearly explain how they collect, use, and store personal data. This should be written in a public privacy policy that's easy for users to find and understand. For Yubi, this means being upfront about using things like camera and gesture data.
    - **APP 5 - Notification of the Collection of Personal Information [2]**
      Explanation:
      Users must be told what data is being collected, why it's needed, and how it will be used before or while it's being collected. In Yubi's case, users should know right away that their webcam and microphone are used for gesture and voice input.

- Address:
    - To address this issue, Yubi should implement the following steps:
        - Create and publish a comprehensive privacy policy that details:
            - The types of data collected (e.g., uploaded images, data, etc)
            - Technologies used (e.g., MediaPipe)
            - Whether and how data is stored or reused
            - Data retention period and access rights
        - Add an onboarding popup or modal at first use that includes a brief summary of these details, such as:
            - “This application uses your webcam and microphone to enable gesture and voice-based interaction. Your data may be processed locally and stored temporarily to improve system performance.’
- Recommendation
  The team recommends implementing both the privacy policy and onboarding popup immediately, as they are low-efforts, non-technical changes that significantly improve legal compliance and user trusts. These steps address APP1 and APP 5 obligations [2] without impacting system performance or requiring changes to core functionality.

5.5 Issue 5: User data access and correction

- Issue: As mentioned in the previous section, Yubi collects and stores personal information such as usernames, emails, passwords, and uploaded assets. Under APP 12 and APP 13 [2], users must be provided with access to their personal information and the ability to modify or delete it. Currently, the application does not allow users to update or delete their personal information, nor does it provide an option to delete their account. This represents a compliance issue and a breach of the APPs.
- Policy:
    - APP 12: Access to personal information
      Users have the right to access their personal data. Yubi must ensure that users are properly verified before accessing their data and that no information is disclosed to unauthorized personnel.

    - APP 13: correction of personal information
      Users have the right to modify or delete their personal data. Yubi should ensure that users are logged in and authorized before making any changes to their information.

- Address:
    - Developing a user management page
        - Develop a dedicated user management page.
        - Display the user's personal information, including their email and username.
        - Allow users to update or change their personal information with proper verification.
        - Provide an option for users to delete their account and all associated data.
        - Implement strict security measures to ensure only verified users can access this page.
        - Ensure only data linked to the verified user is displayed.
    - Management of uploaded assets:
        - Allow users to edit or permanently delete their uploaded assets.
        - Ensure all deleted files are completely removed from the database and are not retained in any backups.
- Recommendation:
    - In the short term, implement a manual process that allows users to request changes or deletions of their personal information through email support. While simple to implement, this approach is not ideal for the long term, as a high volume of requests could overwhelm support and lead to delays in response times.
    - Begin the design and development of a secure user management page to allow users to manage their data independently. This will be

the preferred long-term solution, streamlining the process by eliminating the need for users to call or email support.

  - Additionally, provide support team contact details as a backup channel for users. While the dashboard will typically be sufficient, this ensures users can still receive assistance if they are unable to manage their data through the platform.

6 Analyse impact

6.1 Issue 1: Collection of personal information

- Impact on delivery: Low
- Reasoning: Updating forms, such as full name, optional and adding clear purposes in the privacy policy are light changes as these are more about policy updates, UX adjustments and text revisions rather than deep technical implementations.
- Recommendation effect: Can be implemented quickly with minimal delay or effect on the timeline of development.

6.2 Issue 2: Storage and security of personal information

- Impact on delivery: Moderate
- Reasoning: Adding field level encryption such as AES-256 for emails or names can and strengthening access controls would require updating schemas, implementing encryption and decryption logic and key management. Additional engineering effort is required in coding, testing and performance considerations therefore this must be planned into the project timeline.
- Recommendation effect: If not planned and scoped early, this may slightly delay development timeline but can be staged (eg. initial access controls then encryption)

6.3 Issue 3: Security of uploaded assets

- Impact on delivery: Moderate
- Reasoning: Adding strict access control to uploaded assets is more involved than a simple configuration. Bucket policies are straightforward, but enforcing session-based authentication requires backend changes to link file access with active user sessions. This increases coding and testing effort and may affect development timelines if not properly planned.

- Recommendation effect: Apply bucket-level restrictions first for quick compliance, then roll out session-based access in later stages. This staged approach limits delivery delays while still addressing [2] obligations.

6.4 Issue 4: Transparency and User Awareness

- Impact on delivery: Low
- Reasoning: Publishing a privacy policy and adding an onboarding modal are simple and quick changes as it is mostly content and frontend work that is unlikely to affect the system's functionality.
- Recommendation effect: Easy to deliver, no impact on project delivery timelines.

6.5 Issue 5: User data access and correction

- Impact on delivery: High
- Reasoning: Developing a user management page with secure access, deleting and deletion workflows is an essential and significant feature, not just a minor adjustment to the user data configuration background. This requires integrating backend APIs, implementing strict and strong authentication and authorization checks, and ensuring full compliance with deletion requests. While a manual support-driven process would reduce immediate delivery impact, it is not sustainable in the long run.
- Recommendation effect: Use a short-term manual process to reduce delivery risk, while planning a full user management module for future milestones.

References

[1] Australian Government, Privacy Act 1988 (Cth), Act No. 119 of 1988. [Online]. Available: https://www.legislation.gov.au/Series/C2004A03712. [Accessed: Aug. 29, 2025].

[2] Office of the Australian Information Commissioner, “Australian Privacy Principles guidelines,” Dec. 2022. [Online]. Available: https://www.oaic.gov.au/__data/assets/pdf_file/0030/40989/app-guidelines-combined-December-2022.pdf. [Accessed: Aug. 29, 2025].

[3] Office of the Australian Information Commissioner, “About the Notifiable Data Breaches scheme,” 2024. [Online]. Available: https://www.oaic.gov.au/privacy/notifiable-data-breaches/about-the-notifiable-data-breaches-scheme. [Accessed: Aug. 29, 2025].

[4] European Union, Regulation (EU) 2016/679 (General Data Protection Regulation), Apr. 27, 2016. [Online]. Available: https://eur-lex.europa.eu/eli/reg/2016/679/oj. [Accessed: Aug. 29, 2025].

[5] Federal Trade Commission, “Children’s Online Privacy Protection Rule (COPPA),” [Online]. Available: https://www.ftc.gov/legal-library/browse/rules/childrens-online-privacy-protection-rule-coppa. [Accessed: Aug. 29, 2025].

[6] U.S. Department of Health & Human Services, “HIPAA for professionals,” Jul. 19, 2024. [Online]. Available: https://www.hhs.gov/hipaa/for-professionals/index.html. [Accessed: Aug. 29, 2025].

[7] U.S. Department of Education, “FERPA | Protecting Student Privacy,” 2024. [Online]. Available: https://studentprivacy.ed.gov/ferpa. [Accessed: Aug. 29, 2025].

[8] State of California Department of Justice, “California Consumer Privacy Act (CCPA),” Mar. 13, 2024. [Online]. Available: https://oag.ca.gov/privacy/ccpa. [Accessed: Aug. 29, 2025].

Work Breakdown Structure

https://docs.google.com/spreadsheets/d/1qFBX1AaNtHvk8-L3razTz6iEm6tFvXUX6ORZfjKmCBI/edit?usp=sharing