Security measures and controls

- **Hosting:** Hoylu in Azure Cloud infrastructure meets a broad set of international and industry-specific compliance standards, such as ISO 27001, HIPAA, FedRAMP, SOC 1, SOC 2 and GDPR. They also meet country- or region-specific standards, including Australia IRAP, UK G-Cloud, and Singapore MTCS. Hoylu works strategically with Azure to deliver mission critical workloads and applications to our public sector clients

- **Authentication and Authorization:** Hoylu is a trusted platform when it comes to authentication and authentication services. Hoylu offers OIDC/SAML 2.0 compliant based B2B integrations with your on-prem or cloud Azure AD, Okta, PingIdentity, OneIdentity, OneLogin, etc…

- **Data Protection & Security**: Data protection is the protection, securing, and anonymizing the data as it is created, collected, or modified. We operate based on the Application of the Least Access Privileges model.

- **Infrastructure-As-Code:** Builds repeatable dynamic infrastructure securely and remotely at the push of a button in any region of Azure cloud. Keep track of the fingerprint of any changes done to the infrastructure in non-prod and prod. Facilitate collaboration between teams. Review and comment on plans prior to executing any change to infrastructure. Centralized teams codify policies enforcing security, compliance, and operational best practices across all cloud provisioning. Automated enforcement of policies ensuring the changes are complying without creating a manual review bottleneck.

- **Breach Notification**: Breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored, or otherwise processed will be notified to the client as soon as it is discovered.

- **Zero trust model:** Zero trust is a good proactive defense against cyberthreats because it is dynamic and hyper-vigilant in nature. Hoylu operate on Zero trust model security-first platform, which enables us to maintain and manage security and privacy at its core.

- **SEIM (Threat Intelligence):** Hoylu continuously and actively monitors data, devices, apps, appliances, and users inside or outside of the corporate network for any security risk that touch our boundary and flow into our system. Hoylu built security into the core design of our product. We believe security, privacy, and transparency go hand-in-hand. Data-Forensics / Audit-Trail / Monitoring is done actively.

- Data Protection:

- **Privacy Policies**: Details of the policies can be found at https://www.hoylu.com/privacy-policy/

- **Cookie Policies**:
  - On our https://www.hoylu.com site we have cookies with no personal information until a user login into the app. Post login we have email address attached in the cookie as part of the session data.
  - In our app (https://app.hoylu.com) we have the following cookie information stored in the cookie section. Each of them has their expiration date and time set on it.
    - Email Address: Email address of the user whose login is used to authenticate the system
    - Hoylu Token: Hoylu issued token post user login. This session management depends on the login type
    - Refresh Token: Token issued by our services to keep session alive if the user is active
    - Login Type: Azure AD / Okta / Basic

- **Protocol:** TLS v1.2

- **Ciphers:** ECDHE-ECDSA-AES128-GCM-SHA256: ECDHE-RSA-AES128-GCM-SHA256: ECDHE-ECDSA-AES256-GCM-SHA384: ECDHE-RSA-AES256-GCM-SHA384: DHE-RSA-AES128-GCM-SHA256: DHE-RSA-AES256-GCM-SHA384

- **Encryption**: All data stored in Azure Cloud is Encrypted. Both server-side encryption via the Transparent Data Encryption (TDE) feature and client-side encryption via the Always Encrypted feature https://docs.microsoft.com/en-us/azure/azure-sql/database/security-overview. Azure Storage is encrypted and decrypted transparently using 256-bit AES encryption, one of the strongest block ciphers available, and is FIPS 140-2 compliant. All data in transit to and from Hoylu services are encrypted using the TLS v. 1.2 protocol.

Compliance:

- **Data Controller (Controller):** A legal person assigned by Hoylu who determines the purposes and means of the processing of personal data.

- **Personal data and data subject:** Personal data relating to an identified or identifiable natural person (data subject); an identifiable natural person is one who can be identified, directly or indirectly is stored in the system. E.g., First name and Last name (Surname) along with email address is stored in the database.

- **Processor:** A natural or legal person, is assigned by the company to processes personal data on behalf of the controller.

- **Customer Data:** Data produced and stored in the day-to-day operations are stored in the DB owned and operated by Hoylu in the EU.

FedRAMP

- **FedRAMP and NIST 800-53:** FedRAMP and NIST 800-53 work together. Hoylu is pursuing the moderate certification initiatives in the Federal Risk and Authorization Management Program (FedRAMP). This certification will provide us a standard approach for assessing, authorizing and continuous monitoring of cloud products and services Hoylu offers. The certification will allow government agencies to realize the benefits of the Hoylu collaboration tools in Cloud and simplify the adoption of the Hoylu collaboration solutions at scale on the Azure Cloud. Hoylu is using NIST 800-53 framework which is considered the gold standard for all elements of compliance.

- **Security and Penetration Tests:** Our internal team runs their development process through security lifecycle management software to hunt for security bugs. We let the customer's conduct their penetration testing upon request. We do our own yearly penetration testing in parallel.