DATA PROCESSOR AGREEMENT

Eyworks Limited, a private limited company under the laws of England and Wales, with registration number 07939645 and registered address Acorn House, 381 Midsummer Boulevard, Milton Keynes, England, MK9 3HP provides a range of applications for nurseries to successfully manage their childcare business.

By using the eyworks applications, eyworks Ltd. might have access to personal data from data subjects for which the Customer is responsible. For the purposes of this Data Processing Agreement and with regards to data accessible through the eyworks services, the Customer acts as the "Controller" and eyworks Ltd. acts as the "Processor" as defined by the GDPR.

This Data Processing Agreement is not applicable to the processing of personal data by eyworks Ltd. through services or activities other than the applications as meant in this Data Processing Agreement. For personal data processed through other services or activities than the aforementioned application, eyworks Ltd. acts as the Data Controller as defined by the GDPR. For more information, please refer to our privacy policy, available here:

https://www.eyworks.co.uk/privacy-policy/.

You can contact us via dpo@eyworks.co.uk.

For the purposes of this Data Processing Agreement, the Customer shall be referred to as the "Controller" and eyworks shall be referred to as the "Processor". The Controller and the Processor together shall hereinafter be referred to as the "Parties"

WHEREAS:

(A) Under this data processing agreement, the Processor will process Personal Data; and

(B) The Controller and Processor wish to formalise the terms and conditions applicable to the processing of personal data in this Agreement.

THE PARTIES HAVE NOW AGREED AS FOLLOWS:

ARTICLE 1 DEFINITIONS

1.1 Terms with a capital in the Agreement are definitions and are set out in **Annex A**. All terms in the Agreement not defined in Annex A, but defined in the Data Protection Legislation will have the meaning as assigned thereto in the Data Protection Legislation.

ARTICLE 2 INSTRUCTIONS

2.1 The Processor will be considered as a data processor for the processing of Personal Data of the Controller.

2.2 The Processor will comply with the Data Protection Legislation in relation to the Personal Data of the Controller.

2.3 The Processor will only process Personal Data:

(a) for the provision of the Services;

(b) on written instructions from Controller, including, but not limited to, the instructions as set out in **Annex B**; or

(c) if required to do so by law to which the Processor is subject. In that case, the Processor will notify the Controller of that legal requirement before the processing, unless those laws prohibit such notification.

2.4 The Processor will as soon as reasonably possible inform the Controller if, in the Processor's opinion, an instruction of the Controller infringes the Agreement or the law.

ARTICLE 3 SECURITY

3.1 The Processor shall take appropriate technical and organisational measures to protect the Personal Data in accordance with the Data Protection Legislation. These measures are described in **Annex C**.

3.2 The Parties acknowledge that security measures need to be frequently updated in order to comply with the Data Protection Legislation. The Processor will therefore regularly evaluate and, if necessary, take any follow-up measures to maintain compliance with the Data Protection Legislation.

ARTICLE 4 SUBCONTRACTORS

4.1 The Controller gives a general authorisation for the use of Subcontractors. The Processor shall notify the Controller of any intended changes concerning the addition or replacement of relevant Subcontractors in advance, thereby giving the Controller the opportunity to object to

this change within 30 days after this notification. When Controller object to this change, Parties will negotiate any consequences and possibilities.

4.2 The Processor shall obligate all Subcontractors to comply with the same obligations the Processor has under the Agreement.

4.3 The Processor shall remain fully liable towards the Controller for any acts or omissions by Subcontractors on the processing of Personal Data of the Controller.

4.4 All Subcontractors are listed in Appendix I.

ARTICLE 5 CONFIDENTIALITY

5.1 The Processor will treat all Confidential Information confidential. The Processor will not disclose Confidential Information to any Third Party other than to Subcontractors, except if specifically approved in writing by the Controller or if this is otherwise permitted under the Agreement.

5.2 The Processor may disclose Confidential Information to its employees or Subcontractors insofar as this is necessary to perform the Services.

5.3 The Processor will ensure that its employees and Subcontractors are bound by the same confidentiality terms and conditions as the Processor under the Agreement.

5.4 This clause does not apply insofar as the relevant information has become part of the public domain without violation of the Agreement.

5.5 In the event of a conflict with other contractual arrangements between the Parties regarding confidentiality, the Agreement prevails.

ARTICLE 6 NOTIFICATION FOR PERSONAL DATA BREACH

6.1 In the event of a Personal Data Breach as further specified in Annex A, the Processor will notify the Controller without undue delay, but in any case within 48 hours after discovery. The Processor will cooperate with the Controller in order to enable the Controller to properly respond to a Personal Data Breach.

6.2 The Processor will not inform the affected data subjects nor a Regulator of a Personal Data Breach, unless this is required by Union or Member State law. In that case, the Processor will inform the Controller thereof as soon as possible (if not prohibited by Union or Member State law).

ARTICLE 7 ASSISTANCE

7.1 The Processor will assist Controller as much as possible to ensure that Controller is able to comply with any requests regarding:

(a) a complaint, inquiry or request from a natural person regarding the processing of Controller's Personal Data by Processor;
(b) an investigation or seizure of Controller Personal Data by authorised government officials;
(c) a Data Protection Impact Assessment by Controller as required under the Privacy Law, including updates thereof.

7.2 If the situations under Article 7.1 (a) and (b) arise, Processor will also notify Controller as soon as possible if this is not prohibited by law.

ARTICLE 8 INTERNATIONAL DATA TRANSFER

8.1 The Processor may transfer Personal Data between outside of the United Kingdom or to any country or territory outside the EEA with an adequate level of protection. When such an adequacy decision of the British Government is not in place, Processor may transfer Personal Data to a third country outside of the UK and the EEA and will take all necessary measures as set out in the Data Protection Regulation and inform the Controller of such transfer.

ARTICLE 9 RETENTION

9.1 The Processor will retain the Personal Data as long as necessary for providing the Services, as set out in more detail in **Annex B.**

9.2 Unless agreed otherwise in writing, Processor will delete all Personal Data of the Controller, and will confirm in writing to the Controller that all Personal Data have been deleted upon Controller's written request thereto.

9.3 If the Processor cannot return and/or delete all Personal Data of the Controller because of technical reasons, or because any applicable law requires longer storage of the Personal Data of the Controller, the Processor will inform the Controller as soon as possible. In that event, the Processor will still take all necessary steps to come closest to a complete and permanent return and/or deletion of the Personal Data of the Controller and make the Personal Data of the Controller unavailable for further processing.

9.4 The Controller is responsible for notifying the Processor of any data retention period coming to an end to enable the Processor to delete or anonymise this data before the end of the data retention period.

ARTICLE 10 LIABILITIES

10.1 To the extent permitted by applicable law, the Processor's total liability for damages relating to the Agreement will be limited to the amounts the Controller was required to pay for annually. In no event will either Party be liable for indirect damages, including loss of use, loss of profits or interruption of business, however caused or on any theory of liability in relation to the Agreement. The limitations to the Processor's total liability provided in this clause do not apply when arising out of gross negligence or willful misconduct of the Processor.

10.2 No limitation or exclusions will apply to liability arising out of either party's violation of theProcessor's intellectual property rights.

ARTICLE 11 AUDIT

11.1 Processor will cooperate as much as reasonable possible with Controller, or an external auditor engaged by Controller, to check compliance with the Agreement. Processor will cooperate as requested by Controller or the auditors engaged by Controller to perform the audit. At the request of Controller, Processor will make available all information concerning the facilities, locations, systems, data, certifications, relevant for the processing of Controller's Personal Data, to the extent relevant to this check, and on agreed date and time with Processor.

ARTICLE 12 FORCE MAJEURE

12.1 If, due to a Force Majeure Event, the Processor is unable to comply with its obligations under this Agreement, the Processor will inform the Controller thereof as soon as possible.

ARTICLE 13 TERM AND TERMINATION

13.1 This Agreement will be effective from the moment that the Controller uses Processor's services.

13.2 Unless terminated earlier in accordance with this Agreement, the Agreement will terminate by operation of law if the Processor no longer has access to or otherwise processes Personal Data for the Controller.

13.3 The Agreement may be terminated by either Party in writing with immediate effect in the event that the other Party:

(a) is declared bankrupt;

(b) has been granted suspension of payments.

13.4 Termination or expiration of the Agreement will not discharge the Processor from its confidentiality obligations under the Agreement nor any other obligations which by their nature are meant to survive termination.

ARTICLE 14 MISCELLANEOUS

14.1 Amendments and additions to the Agreement and the relevant annexes thereto will only be valid and binding if these amendments and additions have been made available to the Controller with at least 30 days written notice.

14.2 The Agreement is governed by the laws of England and Wales. The competent courts of London will have exclusive jurisdiction.

ANNEX A - DEFINITIONS

"Personal Data Breach"	A breach of security or confidentiality possibly leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, Confidential Information
"Personal Data"	Any personal data processed by Processor in connection with any Services
"Agreement"	This data processor agreement including any annex(es) thereto
"Confidential Information"	All Personal Data and other information about the processing, including the terms of this Agreement
"Data Protection Legislation"	Any legislation that applies to the processing of the Personal data, such as, but not limited to, the UK General Data Protection Regulation (UK GDPR), the Data Protection Act, and any code of conduct and/or any (non-)UK local laws applicable to the processing of the Personal data
"European Data Protection Legislation"	Any legislation that applies to the processing of the Personal data, such as, but not limited to, the EU General Data Protection Regulation (EU GDPR) and any code of conduct and/or any (non-)EU local laws applicable to the processing of the Personal data
"Force Majeure Event"	means any events or circumstances, or any combination of such events or circumstances, which are beyond the reasonable control of and not otherwise attributable to the affected party
"Regulator"	A supervisory authority such as the Dutch Data Protection Authority (*Autoriteit Persoonsgegevens)* or any other governmental body with supervisory authority over Controller
"Services"	Any services provided by Processor for Controller
"Subcontractor"	Any Third Party engaged by Processor for the processing of Personal Data
"Third Party"	All other parties and entities other than Controller or Processor itself, such as Subcontractors, agents, other clients, business partners or group members of Processor

“Member State law”	Any applicable law issued by a Member State of the European Union
“Union law”	Any applicable law issued by (institutions of) the European Union

ANNEX B - DETAILS ABOUT THE PROCESSING OF PERSONAL DATA

Instructions on the processing of the Controller's Personal Data (not limitative)

Category of data subjects	**Which Personal Data will the Processor process?**	**Which processing will Processor apply to the Controller personal data?**	**For which purposes will Processor process the Controller personal data?**	**How long will the Processor retain the Controller personal data?**
Children who frequent the nursery, where the nursery is the Controller	Name, last name Date of birth Address Ethnicity Religion Medical information Parent name, last name	Store Consult Combine Transfer Amend Delete	To provide the Controller with the services it pays for	As long as the contract with the Controller continues, save where legal retention periods apply
Employees of the Controller	Name, last name Email address Phone number	Store Consult Combine Transfer Amend Delete	To provide the Controller with the services it pays for; to create profiles for employees of Controller to use the application	As long as the contract with the Controller continues

CATEGORIES OF DATA

Processor will process special categories of data if the Controller uploads this data into the eyworks system. This data is about minors and includes:

- Images
- Video images
- Accident logs
- Medical information
- Religion
- Ethnicity

AUTHORISED SUBCONTRACTORS

AWS

Function	Website hosting, Email provider, Document storage service, Application hosting
Business process	Website, Email, Digital storage of documents, Administration, Software tools and applications
Data categories	Identification, Financial, Date of Birth, Educational and employment history, Copy of ID, Health, Location, Social Security Number, Contracts, Software tools and applications, Business data, Technical data
Data subjects	Customers, Employees, Contractors, Family members
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Google Workspace

Function	Email provider, Document storage service, Password manager, Appointment scheduling tool
Business process	Email, Digital storage of documents, Administration
Data categories	Identification, Financial, Date of Birth, Educational and employment history, Contracts, Business data
Data subjects	Employees, Contractors, Suppliers, Partners
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Jira (Atlassian)

Function	Task management or work planning

Business process	Software tools and applications
Data categories	Technical data
Data subjects	Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Mailchimp

Function	Email provider, Marketing tool
Business process	Email, Marketing
Data categories	Identification, Financial, Date of Birth, Educational and employment history, Location, Contracts, Software tools and applications, Business data, Technical data
Data subjects	Customers, Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

New Relic

Function	Other software suite
Business process	Software tools and applications
Data categories	Technical data
Data subjects	Customers, Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted

	according to national retention periods.

Slack

Function	Task management or work planning, Office software
Business process	Administration, Software tools and applications
Data categories	Software tools and applications, Business data
Data subjects	Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Trello

Function	Task management or work planning
Business process	Administration
Data categories	Technical data
Data subjects	Customers, Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Xero

Function	Accountancy software, Bookkeeping software, Payment processing software
Business process	Digital storage of documents, Administration
Data categories	Identification, Financial, Location, Business data
Data subjects	Customers, Employees, Suppliers

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Zoho

Function	CRM, Customer service software, Payment processing software, Password manager, Marketing tool, User management/authentication, Task management or work planning, Appointment scheduling tool, Office software
Business process	Administration, Marketing, Software tools and applications
Data categories	Identification, Location, Contracts, Business data
Data subjects	Customers, Employees, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Facebook Analytics

Function	Marketing tool
Business process	Marketing
Data categories	Location, Technical data
Data subjects	Customers, Employees, Suppliers, Partners
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

GoDaddy

Function	Website hosting
Business process	Software tools and applications
Data categories	Technical data
Data subjects	Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Google Analytics

Function	Marketing tool
Business process	Marketing
Data categories	Location, Technical data
Data subjects	Customers, Employees, Suppliers, Partners
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Stripe

Function	Payment software, Payment processing software
Business process	Software tools and applications
Data categories	Identification, Financial, Location
Data subjects	Customers, Employees

Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Google Firebase

Function	Other software suite
Business process	Software tools and applications
Data categories	Technical data
Data subjects	Customers, Employees
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

Wise

Function	Payment processing software
Business process	Administration
Data categories	Financial, Location
Data subjects	Employees, Suppliers
Security measures	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of unauthorised access on the basis of roles and strong authentication methods; All data is encrypted at rest and access is only permitted via encrypted channels (e.g. SSL); Data is minimised and regularly deleted according to national retention periods.

ANNEX C – DESCRIPTION OF THE SECURITY MEASURES

Physical and environmental security

Office security

The eyworks premises where its development and operations activities are carried out are secured to prevent unauthorised physical access, damage or interference to its offices.

There is 24x7 camera surveillance around the property, the recordings of which are saved to a centralised platform. All windows and doors are fitted with locks and all points of ingress are secured at all times.

Our office is secured and can only be entered with a dedicated keyset. The keys needed to enter the office can only be duplicated with a dedicated security code. Visitors are only allowed into the premises upon invitation from one of our staff members. We do not hold any form of personal data in our office.

Our office network router has been securely configured to remove the default network name and password as well as guest accounts, and its firmware is regularly patched.

Data centre security

The data that is stored in the eyworks application is hosted in AWS Data centres in the United Kingdom. AWS takes stringent security measures to ensure the security of its data centres. These data centres secure your data through encryption, back-up and strict location tracking and access controls. The physical security measures taken to secure these data centres range from secure perimeter defence systems, comprehensive camera coverage to biometric authentication.

To read more about Amazon's data centre security, please visit: Data and Security - Data Centres - Amazon Web Services.

The data you exchange with us via our website, email or other communication channels is stored on, and exchanged through, our eyworks Google Drive Environment. This data is hosted In Ireland, on Google's data centres. These data centres secure your data through encryption, back-up and strict location tracking and access controls. The physical security measures taken to secure these data centres range from secure perimeter defence systems, comprehensive camera coverage to biometric authentication.

To read more about Google's data centre security, please visit: Data and Security – Data Centres – Google.

Operational security policies and processes

Compliance with GDPR

eyworks complies with GDPR through security policies and processes. eyworks has carried out a Data Protection Impact Assessment and physical risk assessment to identify risks and the

necessary measures to remediate these. We further keep and regularly update the legally required policies and have strict retention periods for personal data in place.

Information Security Policy

eyworks requires all new staff to read and sign our extensive Information Security Policy, which details how staff are expected to keep your data safe and secure. This policy includes, but is not limited to, a secure remote working policy, requirements on passwords, multi-factor authentication, encryption of devices and stringent access controls.

Data Protection Officer and Information Security Officer

eyworks has appointed a Privacy Officer, who is responsible for ensuring adherence to all eyworks policies and procedures, regularly updating policies and procedures and ensuring that all staff is adequately trained on handling personal data under the GDPR and other relevant legislation.

eyworks has also appointed an external Information Security Officer, responsible for advising on all technical security measures and responding to a security incident within a reasonable time frame in accordance with our Incident Response Policy.

Security training for all employees

All eyworks employees undergo security training during their orientation phase and receive annual security training throughout their eyworks careers. This training covers, amongst others, how to handle personal data under GDPR; how to deal with Data Access Requests and Data Breach obligations.

Confidentiality

All eyworks Employees are required to sign a confidentiality agreement upon hiring, which ensures that all personal data owned by eyworks will not be made public to an unauthorised recipient. This confidentiality agreement is enforceable by a penalty clause.

Information security incident management

eyworks has defined an information security incident management policy which all members of staff are required to familiarise themselves with and sign. This policy is reviewed and updated at least once per year. At least once per year, a security incident or data breach is practised on the basis of a previously defined realistic scenario (e.g. ransomware, hack, phishing attack, or physical disaster event).

Data breach notification

Possible security incidents that could lead to a data breach are reported to eyworks customers in accordance with our formal data breach notification policy. eyworks always notifies our customers of a potential breach as soon as possible, allowing our customers to fulfil their data breach notification obligations under the GDPR.

Supply chain security

All third parties in the eyworks supply chain are evaluated on their level of security. Through signing processing agreements, we ensure that these third-party suppliers uphold the highest standards of security and compliance possible. eyworks regularly audits third-party suppliers and has ensured it can end the relationship immediately if the audit reveals inadequate levels of security and compliance.

Business Continuity

eyworks has a formal Business Continuity Management policy in place which requires the Business Continuity Plan to be updated at least once per annum and business continuity testing to take place at least annually. eyworks has Disaster Recovery plans in place to respond to disruption of the IT/Technology that provides services for our customers.

Hardware

All laptops and workstations are secured via full disk encryption. We update devices as soon as updates become available and monitor workstations for malware. eyworks has the ability to remotely wipe a machine.

Communications and data transfers

eyworks uses different communication tools for communications between teams and with our customers. eyworks has data processing agreements in place with all of these communication tool providers to ensure appropriate technical and organisational measures to protect personal data against unauthorised or unlawful processing and against accidental loss, destruction, damage, theft, alteration or disclosure are in place. In line with the GDPR, eyworks does not transfer data to countries outside of the UK without appropriate safeguards in place (in the meaning of art. 46 GDPR and Schrems II).

Security of our architecture

Application access and identity management

All eyworks users are required to set up an account with a combination of a unique username and strong and secure password (minimum 8 characters), complying with our access management policy and privacy by design requirements. Passwords are never stored unencrypted in any cache, file, database or access log.

User accounts are validated through email verification. If a wrong password is entered 5 times, the account will be locked for one hour.

Theeyworks app uses AWS Cognito to authenticate users and grant access to the app. Through AWS Cognito, eyworks has defined roles and mapped users to different roles so the eyworks app can access only the resources that are authorised for each user.

Amazon Cognito encrypts data at-rest and in-transit. Amazon Cognito is HIPAA eligible and PCI DSS, SOC, ISO/IEC 27001, ISO/IEC 27017, ISO/IEC 27018, and ISO 9001 compliant.

User authentication and data access controls

Access to the AWS development environment is strictly controlled via IAM roles. Separate IAM users are used for development and live environments. All access to the AWS platform is controlled by two-factor authentication.

eyworks follow the policy of 'least privilege' meaning that all users are given the minimum privileges required to perform their role. Any increase in privilege must be formally requested and is logged in an administrator tracking tool.

Data is strictly controlled via Data Access Controls to ensure confidentiality. To this end, eyworks uses the strong segregation mechanisms in AWS to segregate each user's data and encrypted and sandboxed S3 containers to store data. The back end is developed to enforce strict data segregation by checking and enforcing permissions for each network request.

Back-up and security of user data

eyworks uses Amazon Web Services (RDS & S3) to manage user data. The database is replicated synchronously so that we can quickly recover from a database failure. As an extra precaution, we take regular snapshots of the database and securely move them to a separate data centre so that we can restore them elsewhere as needed, even in the event of a regional Amazon failure. Backups are periodically tested to ensure they can be loaded quickly in the case of any incident. All S3 buckets are private by default and access to particular files is strictly managed through time-sensitive links.

All data is encrypted at rest using AES-256 encryption. eyworks hosts data in regions exclusively within the United Kingdom.

Monitoring

All access to the AWS environment and products built by eyworks are restricted to the responsible and authorised entities and alerts of suspicious activity are reported in real time.

Secure development practices

All software created by eyworks must be designed following the principles of Privacy by Design. The core definition of Privacy by Design is that privacy, and security, must be a primary focus throughout the entire software development lifecycle, from initial inception, through to design, development, testing, deployment, support and end-of-life.

Source code management and review

eyworks uses the Bitbucket revision control system. eyworks uses a third-party source code analysis software to check for any vulnerabilities or issues prior to manual testing being performed. There is then a round of manual review. When the code changes pass these tests, the changes are first pushed to a staging server wherein eyworks employees are able to test changes before an eventual push to production servers and our customer base.

All source code is backed up to a physically separate data centre where it is encrypted using the AES-256 encryption algorithm.

Data centre security

All personal data sourced from our architecture is stored in Amazon data centres. Amazon employs a robust physical security program and is accredited against multiple security industry certifications, including SSAE 16, ISO 27001 and SOC type II. For more information on Amazon's physical security processes, please visit: Cloud Security – Amazon Web Services (AWS).

Environment separation

All development of the application is performed within a dedicated development environment with completely separate architecture prior. Once functional and security tests have been performed, any configuration or source code is transferred to a separate live environment.

Patching

All applications, frameworks, libraries and operating systems are regularly patched. These patches environments are tested within the testing environment to ensure no issues or conflicts arise due to patches being applied.

Encrypted transactions

Web connections to the eyworks service are encrypted via TLS 1.1 and above. We support forward secrecy and AES-GCM, and prohibit insecure connections using TLS 1.0 and below or RC4.

Privacy Policy

Eyworks' privacy policy, which describes how we handle data throughout all of our business process, can be found here: https://www.eyworks.co.uk/privacy-policy

Want to report a security concern?

Email us at dpo@eyworks.com.