Privacy Policy

Version History

Date	Version	Reason for Change	Author
02/11/2023	1.0.0	Initial Release	Naq
02/11/2023	1.1.0	Business name	Naq
02/11/2023	1.2.0	Other third party suppliers	Naq
02/11/2023	1.3.0	Business name	Naq
09/01/2024	2.0.0	Document structure changed	Rebecca Cort

Privacy policy

Introduction

eyworks Limited respects the privacy of its customers, suppliers and partners. We have therefore formulated and implemented a policy on complete transparency regarding the processing of personal data, its purpose(s) and the possibilities to exercise your legal rights in the best possible way. For employees, we have formulated a separate privacy policy, available upon employment and upon request.

This privacy policy pertains to processing by eyworks Limited by means other than through the use of cookies. eyworks Limited has formulated a separate cookie policy, which can be found on our eyworks Limited's websites: https://eyworks.co.uk

Definitions

- Party responsible for processing personal data: eyworks Limited; with registered address at Acorn House, 381 Midsummer Boulevard, in United Kingdom; company registration number 07939645 and Data Protection Officer Rachit Chawla who can be reached at rachit.chawla@eyworks.co.uk (the “Controller”).
- Data Protection Authority: The Data Protection Authority of United Kingdom.
- Data Protection laws:
  - For European citizens or residents, the EU GDPR 2018; the EU e-privacy directive 2002 (soon to be replaced by the EU e-privacy regulation);
  - For UK citizens or residents, the UK GDPR 2020 and the UK Data Protection Act 2018
  - and the national laws of the countries where we operate.

Collection of data

- Your personal data will be collected by eyworks Limited and its data processors.
- Personal data means any information relating to an identified or identifiable natural person (‘data subject’).
- An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

The types of personal data we may process:

Business process	Type	Data subject	Legal basis
Website	Business data, Contracts, Copy of ID, Date of Birth, Educational and Employment History, Financial, Health, Identification, Location, Photographs, Social Security Number, Software, Tools, and Applications, Technical data (e.g. source code)	Contractors, Customers, Employees, Family Members	Consent
Email	Business data, Contracts, Copy of ID, Date of Birth, Educational and Employment History, Financial, Health, Identification, Location, Social Security Number, Software, Tools, and Applications,	Contractors, Customers, Employees, Family Members, Partners,	Legitimate interest

	Technical data (e.g. source code)	Suppliers	
Storage and exchange of documents	Not applicable	Not applicable	Legitimate interest
Delivery of goods and services	Business data, Date of Birth, Educational and Employment History, Identification, Location, Photographs	Customers, Employees	Performance of a contract
Financial and business administration	Business data, Contracts, Copy of ID, Date of Birth, Educational and Employment History, Financial, Health, Identification, Location, Social Security Number, Software, Tools, and Applications, Technical data (e.g. source code)	Contractors, Customers, Employees, Family Members, Partners, Suppliers	Legitimate interest
Marketing	Business data, Contracts, Date of Birth, Educational and Employment History, Financial, Identification, Location, Software, Tools, and Applications, Technical data (e.g. source code)	Customers, Employees, Partners, Suppliers	Consent

Purposes

eyworks Limited processes personal data for one or more of the following purposes:

- Customer, employee, contractor, partner or supplier management
- Business and financial administration
- Direct marketing
- Delivery of goods or services
- Work planning

How we collect, store or otherwise process your data:

The following business processes describe how we may collect, store or otherwise process the types of personal information set out in the table above:

- Collection of cookies, subscription to newsletter or filling out the contact form on the website(s);
- Analyse trends and profiles, for our legitimate interest to aim to enhance, modify, personalise and improve our services and communications for the benefit of our customers;
- Process and respond to support requests, enquiries and complaints received from you through use of business email;
- Provide services and products requested and/or purchased by you and to communicate with you about such services and/or products. We do this as necessary in order to carry out a contract with you and in accordance with our legitimate interest to operate a business;
- Carry out administrative activities such as invoicing and collecting payments either locally on devices or using cloud-services;
- Store and exchange personal information contained in documents through email and cloud-services;
- Marketing and customer acquisition through email or using cloud-services.

Sharing data with third parties

We may have to share your data with third parties, including third-party service providers. We require third parties to respect the security of your data and to treat it in accordance with the law.

We may transfer your Personal Data outside United Kingdom. If we do, you can expect a similar degree of protection in respect of your Personal Data.

We will only share your Personal Data with third parties in accordance with the GDPR and as outlined in the legal justification table above.

We share your personal data with the following enterprise third parties. We also share your data with SME third parties, details of which are available upon request. You will be notified when we have engaged with a new third party recipient of your personal data.

AWS

Function	Application Hosting, Document Storage Service, Email Provider, Website Hosting
Business process	Administration, Email, Software, Tools, and Applications, Storage of Digital Documents, Website

Data categories	Financial, Copy of ID, Business data, Technical data (e.g. source code), Software, Tools, and Applications, Date of Birth, Identification, Health, Contracts, Location, Social Security Number, Educational and Employment History
Data subjects	Contractors, Customers, Employees, 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 minimized and regularly deleted according to national retention periods.

Google Workspace

Function	Appointment Scheduling Tool, Document Storage Service, Email Provider, Password Manager
Business process	Administration, Email, Storage of Digital Documents
Data categories	Business data, Contracts, Date of Birth, Educational and Employment History, Financial, Identification
Data subjects	Contractors, Employees, Partners, 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 minimized and regularly deleted according to national retention periods.

Jira (Atlassian)

Function	Task Management/Work Planning
Business process	Software, Tools, and Applications
Data categories	Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

Mailchimp

Function	Email Provider, Marketing Tool
Business process	Email, Marketing
Data categories	Business data, Contracts, Date of Birth, Educational and Employment History, Financial, Identification, Location, Software, Tools, and Applications, Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

New Relic

Function	Other Software Suite
Business process	Software, Tools, and Applications

Data categories	Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

Trello

Function	Task Management/Work Planning
Business process	Administration
Data categories	Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

Xero

Function	Accountancy, Bookkeeping, Payment Processing
Business process	Administration, Storage of Digital Documents
Data categories	Business data, Financial, Identification, Location
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 minimized and regularly deleted according to national retention periods.

Zoho

Function	Appointment Scheduling Tool, CRM, Customer Service, Marketing Tool, Office, Password Manager, Payment Processing, Task Management/Work Planning, User Management/Authentication
Business process	Administration, Marketing, Software, Tools, and Applications
Data categories	Business data, Contracts, Identification, Location
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 minimized and regularly deleted according to national retention periods.

Facebook Analytics

Function	Marketing Tool
Business process	Marketing
Data categories	Location, Technical data (e.g. source code)
Data subjects	Customers, Employees, Partners, Suppliers
	Physical security such as access controls, clean desk policy and CCTV; Access controls and prevention of

Security measures	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 minimized and regularly deleted according to national retention periods.

GoDaddy

Function	Website Hosting
Business process	Software, Tools, and Applications
Data categories	Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

Google Analytics

Function	Marketing Tool
Business process	Marketing
Data categories	Location, Technical data (e.g. source code)
Data subjects	Customers, Employees, Partners, 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 minimized and regularly deleted according to national retention periods.

Stripe

Function	Payment, Payment Processing
Business process	Software, Tools, and Applications
Data categories	Financial, Identification, 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 minimized and regularly deleted according to national retention periods.

Google Firebase

Function	Other Software Suite
Business process	Software, Tools, and Applications
Data categories	Technical data (e.g. source code)
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 minimized and regularly deleted according to national retention periods.

Wise

Function	Payment Processing
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 minimized and regularly deleted according to national retention periods.

International data transfers

The third parties we have engaged for the abovementioned business process may transfer your personal information to outside of your jurisdiction. eyworks Limited's third party processors take all necessary measures to ensure the confidentiality, availability and integrity of personal data and to comply with the GDPR with regards to international data transfers. The international nature of its compliance certifications, as well as far-reaching technical security measures (including but not limited to encryption of the personal data, making the data illegible to an unauthorised recipient) are sufficient to ensure that the data subjects continue to benefit from the fundamental rights they are entitled to under the GDPR.

Where eyworks Limited transfers data to third countries, it relies on the following legal grounds for international data transfers:

- An Adequacy Decision in accordance with article 45 of the GDPR
- In the absence of an Adequacy Decision, appropriate safeguards in the form of Standard Contractual Clauses or Binding Corporate Rules.

In the event that eyworks Limited is reliant on Standard Contractual Clauses for the legality of its international data transfer, it ensures that the Processor or Subprocessor takes supplementary security measures to safeguard the international data transfer with one or more of the following measures:

- Encryption;
- Anonymisation;
- Pseudonymisation.

Storage and protection of data

Your data is protected by eyworks Limited and its processors in pursuance to all legal requirements set by the relevant data processing laws. eyworks Limited has taken technical and organizational security measures to protect your data and requires its data processors to meet the same requirements. eyworks Limited has signed processing agreements with its processors to ensure an adequate level of data protection.

The following security measures are taken by eyworks Limited to protect your personal data in the course of the listed business processes:

Organisational security measures

Staff

eyworks Limited staff members are required to conduct themselves in a manner consistent with eyworks Limited's guidelines regarding confidentiality, business ethics, appropriate usage, and professional standards. All staff members undergo appropriate background checks prior to hiring and sign a confidentiality agreement outlining their responsibility in protecting customer data.

We continuously train staff members on best security practices, including how to identify social hacks, phishing scams, and hackers.

Access controls

eyworks Limited maintains your data privacy by allowing only authorized individuals access to information when it is critical to complete tasks for you. eyworks Limited staff members will not process customer data without authorization.

Data hosting

As a rule, data is hosted within countries and areas that provide a substantially similar level of protection as data subjects have under the GDPR. To ensure this, we rely on Adequacy Decisions as a legal basis for our international data transfers. In exceptional circumstances, where data is transferred to a country or area not subject to an Adequacy Decision, we rely on Standard Contractual Clauses with the recipient and take supplementary security measures to secure this data transfer, such as anonymisation.

Physical security

The data centres on which personal data is hosted are secured and monitored 24/7 and physical access to facilities is strictly limited to select staff.

Technical security measures

All devices which are used to access personal data for which we are responsible are secured with antivirus software, firewalls, encryption and access management. We regularly update operating systems and software to ensure vulnerabilities cannot be exploited.

We carry out regular vulnerability scanning of our website and have engaged credentialed external auditors to verify the adequacy of our security and privacy measures.

Your rights regarding information

Each data subject has the right to information on and access to, and rectification, erasure and restriction of processing of their personal data, as well as the right to object to the processing and the right to data portability.You also have the right to request that you are not made subject to decision making based solely on automated processes, including profiling, if these decisions would have a significant effect on you.

You can exercise these rights by contacting us at the following email address: hello@eyworks.co.uk. If we have any doubts as to your identity, we may request you to provide us with proof of identification, such as through sending us a copy of your valid ID. Ensure that you write “Data Request” in the subject line of your email.

Within one month of the submitted request, you will receive an answer from us. We will not charge you for submitting your request unless the request is manifestly unfounded or otherwise unreasonable in its nature. Depending on the complexity and the number of the requests this period may be extended to two months.

Marketing

- You may receive commercial offers from eyworks Limited. If you do not wish to receive them (anymore), please send us an email to the following address: hello@eyworks.co.uk and ensure that you write “Data Opt-Out” in the subject line of your email.
- Your personal data will not be used by our partners for commercial purposes.
- If you encounter any personal data from other data subjects while visiting our website, you are to refrain from collection, any unauthorized use or any other act that constitutes an infringement of the privacy of the data subject(s) in question. The collector is not responsible in these circumstances.

Data retention

The collected data are used and retained for the duration determined by law. You may, at any time, request your data to be deleted from any eyworks Limited account, system or other data processing medium in accordance with the process described above.

Applicable law

These conditions are governed by the laws and regulations of the country where we are headquartered. The court in the district where we are headquartered has the sole jurisdiction if any dispute regarding these conditions may arise, save when a legal exception applies.

Children's Data

We do not knowingly process children's data, unless specifically stated in this Privacy Policy. If you have concerns about or knowledge of a child using our services, products, websites or apps without parental consent, please contact our DPO via rachit.chawla@eyworks.co.uk to ensure we can take appropriate action as soon as possible.

Contact

For questions about this privacy policy, product information or information about the website itself, please contact: hello@eyworks.co.uk.

International data transfers

Third Party Applications

AWS

Third party headquarter address	410 Terry Ave. North, Seattle, WA, 98109-5210, United States of America
The primary location of processing is the United States of America.	Personal data collected by AWS may be stored and processed in any country where AWS or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see AWS's Privacy Policy	https://aws.amazon.com/privacy/

Google Workspace

Third party headquarter address	1602 Amphitheatre Parkway, Mountain View, CA, 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Workspace may be stored and processed in any country where Google Workspace or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Workspace's Privacy Policy	https://policies.google.com/privacy?hl=en-US

Jira (Atlassian)

Third party headquarter address	Level 6, 341 George Street, Sydney, Australia
The primary location of processing is the Australia.	Personal data collected by Jira (Atlassian) may be stored and processed in any country where Jira (Atlassian) or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Jira (Atlassian)'s Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Mailchimp

Third party headquarter address	675 Ponce De Leon Ave NE #5000, Atlanta, GA 30308, United States of America
The primary location of processing is the United States of America.	Personal data collected by Mailchimp may be stored and processed in any country where Mailchimp or its affiliates, subsidiaries, or service providers operate

	facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Mailchimp's Privacy Policy	https://www.intuit.com/privacy/statement/

New Relic

Third party headquarter address	188 Spear Street, Suite 1200, San Francisco, CA 94105,, United States of America
The primary location of processing is the United States of America.	Personal data collected by New Relic may be stored and processed in any country where New Relic or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see New Relic's Privacy Policy	https://newrelic.com/termsandconditions/privacy

Trello

Third party headquarter address	55 Broadway 25th Floor New York, NY 10006 , United States of America
The primary location of processing is the United States of America.	Personal data collected by Trello may be stored and processed in any country where Trello or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Trello's Privacy Policy	https://www.atlassian.com/legal/privacy-policy

Zoho

Third party headquarter address	Beneluxlaan 4B, 3527 HT Utrecht, Nederland, The Netherlands
The primary location of processing is the The Netherlands.	Personal data collected by Zoho may be stored and processed in any country where Zoho or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and The Netherlands
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Zoho's Privacy Policy	https://www.zoho.com/privacy.html

Facebook Analytics

Third party headquarter address	1601 Willow Rd, Menlo Park, California, 94025, United States of America
The primary location of processing is the United States of America.	Personal data collected by Facebook Analytics may be stored and processed in any country where Facebook Analytics or its affiliates, subsidiaries, or service

	providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Facebook Analytics's Privacy Policy	https://www.facebook.com/privacy/explanation/

GoDaddy

Third party headquarter address	2155 E. GoDaddy Way, Tempe, AZ 85284, United States of America
The primary location of processing is the United States of America.	Personal data collected by GoDaddy may be stored and processed in any country where GoDaddy or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see GoDaddy's Privacy Policy	https://www.godaddy.com/en-uk/legal/agreements/privacy-policy

Google Analytics

Third party headquarter address	1601 Amphitheatre Parkway, Mountain View, CA 94043, United States of America
The primary location of processing is the United States of America.	Personal data collected by Google Analytics may be stored and processed in any country where Google Analytics or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Analytics's Privacy Policy	www.google.com/policies/privacy/partners/,

Stripe

Third party headquarter address	510 Townsend Street San Francisco, CA 94103, United States of America
The primary location of processing is the United States of America.	Personal data collected by Stripe may be stored and processed in any country where Stripe or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Stripe's Privacy Policy	https://stripe.com/en-gb-nl/privacy

Google Firebase

Third party headquarter address	1600 Amphitheatre Parkway in Mountain View, CA 94043, United States of America
	Personal data collected by Google Firebase may be

The primary location of processing is the United States of America.	stored and processed in any country where Google Firebase or its affiliates, subsidiaries, or service providers operate facilities.
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible
For more information, see Google Firebase's Privacy Policy	https://firebase.google.com/support/privacy

Suppliers

MetaDesign Solutions

Country where data is processed or sent to	India
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible

Orange Tree Software Pvt Ltd.

Country where data is processed or sent to	India
Safeguards (art. 45 GDPR)	Standard Contractual Clauses
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible

Smart Job Board

Country where data is processed or sent to	United States of America
Safeguards (art. 45 GDPR)	Adequacy decision exists between United Kingdom and United States of America
Additional safeguards	• Encryption • Anonymisation where possible • Pseudonymisation where possible