LAST UPDATED: 29 JANUARY, 2026

Privacy policy

KEY TAKEAWAYS

- The information we collect
- How we collect personal data
- Purposes and legal bases for processing
- Our disclosures of personal data to third parties
- Opt-Out Options
- Interest-Based Ads on Mobile Devices
- Overseas transfers
- Data retention
- Data Retention Policy
- Your rights and controlling your personal data
- Storage and security
- Incident Response Plan
- Notification of Personal Data Breaches
- Cookies

- Amendments

ApprovalMax Limited, a company registered in England and Wales, with company number 11326265 (**we, us, our** or **ApprovalMax**), understands that protecting your personal data is important. This Privacy Policy sets out our commitment to protecting the privacy of personal data provided to us, or otherwise collected by us when you visit www.approvalmax.com (the **Site**), use our mobile application or browser-based application at app.approvalmax.com (collectively, the **App**), contact us, or otherwise use any services offered through or associated with our Site or App (the **Services**) or when otherwise interacting with you. This Privacy Policy applies to all websites and online resources operated by ApprovalMax, including approvalmax.com and tothemax.online, as well as any other domains we may use to publish content or provide information about our services.

It is important that you read this Privacy Policy together with any other detailed privacy notices we may provide when we are collecting or processing personal data about you so that you understand our privacy practices in relation to your data.

ApprovalMax processes personal data as both a Data Controller and Data Processor, as defined in the UK General Data Protection Regulation and Data Protection Act 2018. We are a Data Controller with regard to the client information we collect and process for our own purposes, and we are a Data Processor with regard to all information clients upload to our systems, platforms or software. End users of our clients should consult the applicable client's privacy policy for information on how they handle your personal data. Clients may request a Data Processing Agreement (DPA) to govern our processing relationship by contacting us on approvalmax.com/hello. We also comply with the Australian Privacy Act 1988 (Cth) including the Australian Privacy Principles, and the New Zealand Privacy Act 2020 including the Information Privacy Principles, as applicable depending on your location and our relationship with you.

This Privacy Policy applies to:

ApprovalMax Limited, a company registered in England and Wales with company number 11326265; ("AML")

References to "we", "us", "our" or "ApprovalMax" in this Privacy Policy refer to AML as the specific entity that is collecting, using or disclosing your personal information regardless of your location and the Services you use.

1

The information we collect

below:

- **Identity Data** including first name and last name.
- **Contact Data** including billing address, email address, telephone number, Skype ID, and other social media usernames or profile links.
- **Financial Data** including credit card information or bank account information collected by our third-party payment processors on our behalf.
- **Transaction Data** including details about payments from you to us and other details of products and services you have purchased from us.
- **Technical and Usage Data** including internet protocol (IP) address, your login data, your browser session and geolocation data, device and network information, statistics on page views and sessions, acquisition sources, search queries and/or browsing behaviour, information about your access and use of our website, including through the use of cookies, your communications with our website, the type of browser and operating system you are using.
- We store certain referral and campaign parameters locally in your browser to understand how users discover our services. This information is used solely for internal analytics and attribution and is not shared for advertising purposes.
- **Profile Data** including your username and password for the App, support requests you have made, content you post, send, receive and share through our platform, feedback and survey responses.
- **Interaction Data** including information you provide to us when you participate in any interactive features of our Services, including surveys, contests, promotions, activities or events.
- **Marketing and Communications Data** including your preferences in receiving marketing from us and our third parties and your communication preferences.
- **Professional data** including where you are a worker of ours or applying for a role with us, your professional history such as your previous positions and professional experience.
- **Special Categories of Personal Data** is a special category of personal data that includes details about your race or ethnicity, religious or philosophical beliefs, sex life, sexual orientation, political opinions, trade union membership, information about your health and genetic and biometric data. We do not actively request special categories of data about you, nor do we collect any information about criminal convictions and offences. If at any time we need to collect special categories of data about you, we will only collect it and use it as required or authorised by law.

2

How we collect personal data

We collect personal data in a variety of ways, including:

- **Indirectly:** We may collect personal data which you indirectly provide to us while interacting with us, such as when you use our website, in emails, over the telephone and in your online enquiries.
- **From third parties:** We collect personal data from third parties, such as from your employer where they invite you to access our Services, from 2Checkout or other approved ApprovalMax resellers, and details of your use of our website from our analytics and cookie providers and marketing providers. See the "Cookies" section below for more detail on the use of cookies.
- **From publicly available sources:** We collect personal data from publicly available resources such as Companies House and professional networking sites such as LinkedIn.
- We also collect personal data when individuals visit or interact with our content hub at tothemax.online, which operates under the ApprovalMax brand and uses the same analytics and marketing tools as our main website.

Indirectly Obtained Business Contact Data

We may collect and process business contact information that is not provided to us directly by the individual.

- Source Categories: Source categories: This data may be obtained from (1) third-party B2B data and CRM enrichment providers (such as Cognism), (2) publicly available sources (such as Companies House and LinkedIn), and (3) company-level intent tools (such as Unify), which identify organisational interest based on website interactions where the use of cookies and similar technologies is permitted by your cookie choices.
- **Purposes of Processing:** We use this data for:
  - Targeted marketing and sales outreach
  - Maintaining suppression lists to ensure we respect opt-out requests and do not contact inappropriate audiences (for example existing customers or open opportunities)
  - Measuring and improving the effectiveness of our B2B engagement
- **Lawful basis:** We rely on legitimate interests for this processing. Our interest is to identify and communicate with relevant professional stakeholders who may benefit from our Services, in a proportionate way, and with suppression and opt-out controls in place.
- **How selection for outreach works:** Our selection for outreach may use:
  - Organisational intent signals from website activity
  - Matching against our ideal customer profile (for example industry and role)
  - Suppression rules (for example excluding opted-out contacts and other do not contact flags)

This may involve automated filtering to decide who should receive B2B communications. It does not produce legal or similarly significant effects for individuals.

International transfers: Business contact data may be transferred from the UK to the US for processing by our service providers. Where required, we use appropriate safeguards such as Standard Contractual

marketing emails, click the unsubscribe link in any email or contact us at privacy@approvalmax.com.

3

Purposes and legal bases for processing

We collect and process personal data about you only where we have legal bases for doing so under applicable laws. We have set out below, in a table format, a description of all the ways we plan to use your personal data, and which of the legal bases we rely on to do so. We have also identified what our legitimate interests are where appropriate. Note that we may process your personal data for more than one lawful ground depending on the specific purpose for which we are using your data. Please reach out to us if you need further details about the specific legal ground we are relying on to process your personal data where more than one ground has been set out in the table below.

Purpose of use / disclosure	Type of Data	Legal Basis for processing
To enable you to access and use our software, including to provide you with a login.	• Identity Data • Contact Data • Profile Data	• Performance of a contract with you
To contact and communicate with you about our Services, including in response to any support requests you lodge with us or other enquiries you make with us.	• Identity Data • Contact Data • Profile Data	• Performance of a contract with you
To contact and communicate with you about any enquiries you make with us via our website.	• Identity Data • Contact Data	• Legitimate interests: to ensure we provide the best client experience we can offer by answering all of your questions.
For internal record keeping, administrative, invoicing and billing purposes.	• Identity Data • Contact Data • Financial Data • Transaction Data	• Performance of a contract with you • To comply with a legal obligation

		to our terms of business and any other administrative points.
For analytics including profiling on our website, market research and business development, including to operate and improve our Services, associated applications and associated social media platforms.	• Profile Data • Technical and usage Data	• Legitimate interests: to keep our website updated and relevant, to develop our business, improve our Services and to inform our marketing strategy
For advertising and marketing, including to send you promotional information about our events and experiences and information that we consider may be of interest to you.	• Identity Data • Contact Data • Technical and usage Data • Profile Data • Marketing and communications Data	• Legitimate interests: to develop our Services and grow our business
If you have applied to work with us; to consider your application.	• Identity Data • Contact Data • Professional Data	• Legitimate interests: to consider your employment application
To comply with our legal obligations or if otherwise required or authorised by law.	All relevant Personal Data	• To comply with a legal obligation

If you have consented to our use of data about you for a specific purpose, you have the right to change your mind at any time, but this will not affect any processing that has already taken place. Where we are using your data because we or a third party have a legitimate interest to do so, you have the right to object to that use though, in some cases, this may mean no longer using our services. Further information about your rights is available below.

4

Our disclosures of personal data to third parties

the data we share with their platforms:

- marketing providers including HubSpot and Zoho Campaigns (to automate and manage our marketing emails and campaigns), Intercom (to deliver in-app messaging, product tours and live chat), Refiner (to gather information about customer satisfaction, such as our Net Promoter Score and other product feedback), Mailchimp and Mandrill (for systems notifications as part of our Service delivery), UserVoice (to gather customer feedback), Klenty (to support outbound sales engagement and cadence automation), Cognism (to enrich and validate business contact data for sales and marketing purposes). We also use Tilda as content management system;
- storage and security providers including Microsoft Azure (cloud storage) and Sentry and Stackify (to track user interface logs and errors);
- business process providers including Zoho Creator (for business process automation), Zoho CRM (for customer relationship management), Zoho Desk (for customer and sales lead support) and Zoom (for scheduling and running meetings and webinars) and Kickscale (for supporting and optimising sales development and performance processes);
- user experience software tools, such as where we track some user activity with a tool provided by Hotjar. This monitors all clicks made by trial users during the setup process in the product. Only the clicks on user interface controls are being tracked, we do not capture any financial data.

We may also disclose personal data to:

- our employees, contractors and/or related entities;
- other service providers who assist us to deliver our services;
- professional advisors, bankers, auditors, our insurers and insurance brokers;
- payment systems operators such as 2Checkout, Stripe;
- our existing or potential agents or business partners;
- sponsors or promoters of any promotions or competition we run;
- anyone to whom our business or assets (or any part of them) are, or may (in good faith) be, transferred;
- courts, tribunals and regulatory authorities, in the event you fail to pay for goods or services we have provided to you;
- courts, tribunals, regulatory authorities and law enforcement officers, as required or authorised by law, in connection with any actual or prospective legal proceedings, or in order to establish, exercise or defend our legal rights;
- third parties to collect and process data for analytics and measurement purposes, such as Google Analytics (to find out how Google uses data when you use third-party websites or applications, please see www.google.com/policies/privacy/partners/), Facebook Pixel, Microsoft Advertising (Bing Ads), G2 (which provides aggregated analytics based on browser-level identifiers when users who have consented to marketing or analytics cookies visit our website after viewing our G2 profile), or other relevant analytics providers. No personally identifiable information such as names or contact

We have enabled various Google Analytics Advertising Features to enhance our understanding of user interactions and improve our services. These features include, but are not limited to:

- **Remarketing Features**
- **Advertising Reporting Features**
- **Demographics and Interest Reports**
- **Store Visits**
- **Google Display Network Impression Reporting**

We, along with third-party vendors, utilise both first-party cookies (such as the Google Analytics cookie) and other first-party identifiers, as well as third-party cookies (such as Google advertising cookies) and other third-party identifiers. This combination allows us to gather comprehensive data to optimise our marketing efforts and user experience.

5

Opt-Out Options

We respect your privacy preferences and provide several options for you to control your data:

Google Analytics Opt-Out: You can opt-out of Google Analytics Advertising Features by installing the Google Analytics Opt-out Browser Add-on, which is available here.

Personalised Ads on Google Content Network: To opt-out of personalised ad delivery on the Google Content Network, please visit the Google Ads Preferences Manager here.

6

Interest-Based Ads on Mobile Devices:

Android Devices: Open the Google Settings app on your device, select “Ads”, and adjust your preferences.

iOS Devices (iOS 6 and above): Use Apple’s advertising identifier. To learn more about limiting ad tracking with this identifier, visit the settings menu on your device.

Other Analytics and Advertising Services

- Google Analytics GA4
- Google Ads
- Microsoft Advertising (Bing Ads)
- Microsoft Clarity
- G2 Pixel
- HubSpot
- ZOHO CRM
- Meta Ads (Facebook Ads)
- LinkedIn Ads
- HotJar
- Power BI
- Cognism
- Mailchimp
- Intercom
- Unify

These services help us understand user behaviour, track advertising effectiveness, and improve our marketing strategies. Each service adheres to its privacy policies and provides mechanisms for users to manage their privacy preferences.

7

Overseas transfers

Where we disclose personal data to the third parties listed above, these third parties may store, transfer or access personal data outside of the United Kingdom (or for Australian and New Zealand individuals outside Australia and New Zealand respectively). The level of data protection in countries outside of your home jurisdiction may be less comprehensive than what is offered in your home jurisdiction. When we transfer your personal data outside of your home jurisdictions, we will perform those transfers using appropriate safeguards in accordance with the requirements of applicable data protection laws and we will protect the transferred personal data in accordance with this Privacy Policy. This includes:

- only transferring your personal data to countries that have been deemed by applicable data protection laws to provide an adequate level of protection for personal data; or
- including standard contractual clauses in our agreements with third parties that are overseas.

8

We will only retain your personal data for as long as reasonably necessary to fulfil the purposes we collected it for, including for the purposes of satisfying any legal, regulatory, tax, accounting or reporting requirements. We may retain your personal data for a longer period in the event of a complaint or if we reasonably believe there is a prospect of litigation in respect to our relationship with you.

To determine the appropriate retention period for personal data, we consider the amount, nature and sensitivity of the personal data, the potential risk of harm from unauthorised use or disclosure of your personal data, the purposes for which we process your personal data and whether we can achieve those purposes through other means, and the applicable legal, regulatory, tax, accounting or other requirements.

9

Data Retention Policy

In accordance with the UK GDPR and other applicable laws, we will retain personal data associated with our payment products for a minimum of five (5) years following the termination of our relationship with you, unless a longer period is required or permitted by law. Our data retention practices adhere to the following principles:

- **Purpose Limitation:** Personal data is retained solely for the purposes for which it was collected and processed. We do not further process the personal data in a manner incompatible with those original purposes (unless you consent to another form of processing).
- **Data Minimisation:** We regularly review the personal data we hold and securely delete or anonymise personal data that is no longer necessary in relation to the purposes for which it was collected.
- **Security Measures:** We implement appropriate technical and organisational measures, such as encryption and access controls, to protect retained personal data from unauthorised access or processing, alteration, disclosure, accidental loss or damage.
- **Legal Compliance:** We ensure that all personal data retention and disposal practices comply with applicable laws and regulations, including UK GDPR, the Data Protection Act 2018 and any sector-specific requirements.

10

Your rights and controlling your personal data

Services to you and your use of our Services.

Information from third parties: If we receive personal data about you from a third party, we will protect it as set out in this Privacy Policy. If you are a third party providing personal data about somebody else, you represent and warrant that you have such person's consent to provide the personal data to us.

Access, correction, processing and portability: You may request details of the personal data that we hold about you and how we process it (commonly known as a "data subject request"). You may also have a right in accordance with applicable data protection law to have your personal data rectified or deleted, to restrict our processing of that information, to object to decisions being made based on automated processing where the decision will produce a legal effect or a similarly significant effect on you, to stop unauthorised transfers of your personal data to a third party and, in some circumstances, to have personal data relating to you transferred to you or another organisation.

Unsubscribe: To unsubscribe from our email database or opt-out of communications (including marketing communications), please contact us using the details below or opt-out using the opt-out facilities provided in the communication.

You can also object to our use of your data for direct marketing (including where we use profiling/segmentation to select recipients) by emailing privacy@approvalmax.com.

Withdraw consent: Where we are relying on consent to process your personal data, you have the right to withdraw your consent at any time. However, this will not affect the lawfulness of any processing carried out before you withdraw your consent. If you withdraw your consent, we may not be able to provide certain products or services to you. We will advise you if this is the case at the time you withdraw your consent.

Complaints: If you wish to make a complaint, please contact us using the details below and provide us with full details of the complaint. We will promptly investigate your complaint and respond to you, in writing, setting out the outcome of our investigation and the steps we will take to deal with your complaint. You have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

If you are in the UK, you have the right to make a complaint at any time to the Information Commissioner's Office (ICO), the UK regulator for data protection issues (www.ico.org.uk). If you are in Australia, you have a right to contact the Office of the Australian Information Commissioner (Phone: 1300 363 992, Website: www.oaic.gov.au). If you are in New Zealand, you may contact the Office of the New Zealand Privacy Commissioner. We would, however, appreciate the chance to deal with your concerns before you approach the ICO so please contact us in the first instance.

11

Storage and security

We are committed to ensuring that the personal data we collect is secure. In order to prevent unauthorised access or disclosure, we have put in place suitable physical, electronic and managerial procedures, to safeguard and secure personal data and protect it from misuse, interference, loss and unauthorised access, modification and disclosure.

While we are committed to security, we cannot guarantee the security of any information that is transmitted to or by us over the Internet. The transmission and exchange of information is carried out at your own risk.

12

Incident Response Plan

Our incident response plan, which is built upon our ISO 27001:2022 security management framework, is designed to effectively manage data breaches involving personal data. This plan includes:

- **Detection and Analysis:** Rapid identification and assessment of potential data breaches through continuous monitoring and alert systems, which will allow for prompt and thorough assessments of suspected incidents.
- **Containment and Mitigation:** Immediate steps to limit the impact of a breach and prevent further unauthorised access, including isolating affected systems.
- **Eradication and Recovery:** Identify and eliminate the root cause of the breach and restoring systems and data to full operational status, ensuring data integrity throughout the process.
- **Post-Incident Review:** Conducting a thorough analysis of the incident to implement enhanced security measures and update policies and procedures accordingly.

13

Notification of Personal Data Breaches

In compliance with the UK GDPR requirements, we adhere to the following protocols for notifying personal data breaches:

the breach, approximate number of individuals concerned, likely consequences, and measures taken.

- **Individual Notification:** Inform affected individuals without undue delay when the breach is likely to result in a high risk to their rights and freedom and provide clear and transparent information about the breach.
- **Information Provided:** Include details about the nature of the breach, the types of data involved, potential consequences, and the measures taken or proposed to address the breach and mitigate its effects.
- **Record Keeping:** Maintain detailed documentation of the breach, notifications made, and remedial actions taken, as required by GDPR Article 33(5).

14

Cookies

We use cookies and similar technologies on our website. For full details of what technologies we use, why we use them, which third parties are involved, and how long cookies last, please see our cookie notice at approvalmax.com/cookie. You can update your cookie preferences at any time via the cookie settings.

15

Links to other websites

Our website may contain links to other party's websites. We do not have any control over those websites and we are not responsible for the protection and privacy of any personal data which you provide whilst visiting those websites. Those websites are not governed by this Privacy Policy.

16

Personal data from social network accounts

If you connect your account with us to a social network account, such as Google or Microsoft, we will collect your personal data from the social network. We will do this in accordance with the privacy settings you have chosen on that social network.

The personal data that we may receive includes your name, ID, user name, handle, profile picture, gender, age, language, and any other personal data you choose to share.

interest you. We will not post to your social network without your permission.

17

Amendments

We may change this Privacy Policy from time to time. We will notify you if we make a significant change to this Privacy Policy, by contacting you through the contact details you have provided to us and by publishing an updated version on our website.

For any questions or notices, please contact us:

ApprovalMax Limited, a company registered in England and Wales, with company number 11326265.
Contact: support@approvalmax.com
Last update: 29 January 2026

To review the previous Privacy Policy, click here.

ApprovalMax

Stay updated with ApprovalMax

Subscribe to newsletter

Get our app

GET IT ON Google Play Downlo App

INTEGRATIONS

All integrations
Xero
QuickBooks Online
Oracle NetSuite

FEATURES

Accounts payable
Multi-level approvals
Approval channels
Bill-to-PO matching

Certain payment services for ApprovalMax are provided by The Currency Cloud Limited. Registered in England No. 06323311. Registered Office: 1 Sheldon Square, London, W2 6TT, United Kingdom.The Currency Cloud Limited is authorised by the Financial Conduct Authority under the Electronic Money Regulations 2011 for the issuing of electronic money (FRN: 900199)

For business

Platform security

ApprovalMax Pay

ApprovalMax Capture

ABOUT

Pricing

Contact sales

Support

Partner enquiry

About us

Careers

RESOURCES

Product demos

Webinars

Customer stories

How to videos

Knowledge base

News

Feature releases

Data privacy request

Currency Cloud safeguards your funds. For more information click here

To make a complaint, please refer to our complaints page.

All testimonials, reviews, opinions, or case studies presented on the website may not be representative of all customers. Results may vary and customers agree to proceed at their own risk.



Add as a preferred source

Legal Agreements Security Terms & Conditions Privacy Policy

Do not sell or share my personal information

© 2026 ApprovalMax. All rights reserved.