acorn

Privacy Policy

As at May 2026

ACORN PLMS
ACN 600 787 139

Privacy at a glance

This short summary covers the main things to know. Our full privacy policy starts on the next page. It has more detail and the legal specifics you may need.

What we collect	The things you give us (like your name or email), what happens when you use our platform (like logins and pages viewed) and information from your employer if they set up your account.
Why we use it	To run the service, keep it safe, help you when you ask, and improve it. We only use your information for the reasons we explain in this policy.
Who we share it with	Trusted suppliers that help us run the service, your organisation if it set up your account, and others when the law requires it. We do not sell your personal information.
Your rights	You can ask to see, correct or delete your information, opt out of marketing, and complain if something's gone wrong. Some extra rights apply in Europe, the UK, Canada and the United States.
How to contact us	Email privacy@acorn.works or call +61 (0)2 6269 3330 and ask for the Privacy Team.

→ Turn the page for the full policy, including your legal rights, how we handle different audiences, and regional information for Europe, the UK, Canada and the United States.

1. About this policy

IN PLAIN ENGLISH

This policy tells you how Acorn handles your personal information. It covers people who visit our website, buy from us, use our platform, apply for a job with us, or work for us.

Acorn PLMS Pty Ltd (ABN 47 600 787 139) (we, us or our) looks after your privacy. This policy explains how we collect, use and protect your personal information, whether we deal with you through our website, our platform, our services or any other interaction.

It applies to:

- People who visit our website or hear from us about Acorn
- Customers, suppliers and partners
- People who use the Acorn platform (including users signed up by a client organisation like an employer)
- Job applicants and people who work for us (employees, contractors, consultants, interns and similar)

This is a general policy. Depending on your relationship with us, we may give you extra notices at the time we collect information — for example, a recruitment notice, a cookie notice or a client-specific notice. If something in this policy conflicts with a law that applies to your situation, we follow the law.

REGIONAL NOTE

If you are in the EEA, UK or Switzerland, extra rights under GDPR / UK GDPR apply — see Appendix 1. If you are in Canada, see Appendix 2. If you are in the United States, see Appendix 3.

Our approach to privacy is based on these principles:

PRINCIPLE	WHAT IT MEANS
Only what we need	We collect the minimum information needed to do what we've said we'll do, or to meet a legal duty.
Open about it	We explain how we handle your information in this policy or at the point we collect it — no surprises.
Kept safe	We protect your information with appropriate technical and organisational measures.
You're in control	We give you tools and options to manage your information and preferences.
We're accountable	We follow the privacy laws that apply to us and keep improving our practices — including for new things like AI transparency.

2. Acorn's role

IN PLAIN ENGLISH

Acorn plays different roles depending on who you are. For our own customers and website visitors, we decide how your information is used. For people who use the platform through an employer or school, that organisation is usually in charge of the information — we run the platform for them.

Acorn's role is not the same in every situation. The table below shows the main ones. In legal terms, Acorn is sometimes a controller (the party that decides what information is used for and how) and sometimes a processor (the party that handles information on behalf of another organisation). That distinction matters because it affects who you go to for requests about your information.

AUDIENCE / SITUATION	ACORN'S USUAL ROLE	WHAT THIS MEANS FOR YOU
Website visitors, marketing contacts, prospects, direct customers, suppliers and partners	Controller	Acorn decides what the information is used for — things like running the website, sales, support, events and running our business.
Users of the Acorn platform who got their account through a client organisation (for example, an employer, school or other tenant customer)	Processor / service provider for the client organisation; controller only for things Acorn is responsible for itself (like platform security and legal compliance)	Your organisation decides what the platform is used for, and its own privacy notice may also apply. Requests about your content in the platform may need to go through your organisation. Acorn will help where the contract or law requires it.
Job applicants and people who work for Acorn	Controller	Acorn decides how this information is handled — for recruitment, managing the working relationship, payroll, benefits, workplace health and safety, access management, security logging and legal compliance.

REGIONAL NOTE

EEA/UK: Where Acorn is a controller, we are responsible for showing a lawful basis under GDPR (see Appendix 1). Where we are a processor, the client organisation is the controller and sets the lawful basis.

3. What personal information we collect

IN PLAIN ENGLISH

We collect different things depending on how you deal with us — your contact details, what you do on the platform, information your employer or school gives us, and technical things like your IP address. We don't usually collect sensitive things like health or religion unless there's a clear reason.

The table below lists the main categories, with examples and who each relates to.

CATEGORY	EXAMPLES	WHO THIS RELATES TO
Identity and contact details	Name, email address, phone number, address, job title, organisation, account credentials.	Everyone
Profile and preferences	Profile photo, display name, settings, preferences, support requests, feedback and survey answers.	Platform users, customers
Service and account information	Information needed to set up, manage and support an account or business relationship.	Customers, partners, suppliers
Content you put in the platform	Things you upload or create through the platform — training modules, assignments, forum posts and similar.	Platform users
Recruitment and working relationship information	CVs, employment history, references, screening results, payroll setup, tax forms, emergency contacts, performance and engagement records.	Applicants, workforce members

Payment and billing	Payment, billing or reimbursement details.	Customers, suppliers, workforce
Usage, device and technical data	IP address, browser or device type, operating system, sign-in events, timestamps, diagnostic data and product usage data.	Anyone using our platform or website
Security and operational logs	Sign-in events, access changes, email security metadata, device security information for company-issued devices, and application and network security logs.	Platform users, workforce
Cookies and similar	Session identifiers, security tokens and analytics identifiers — see Section 8.	Website visitors, platform users

Sensitive information. We don't usually collect sensitive things — for example information about your health, race, religion, sexuality or biometric identifiers — from customers or platform users. There are limited exceptions: for instance, an accessibility adjustment in a learning module or optional demographic information for diversity reporting with your clear consent. For workforce members, we sometimes collect sensitive information where it's necessary and lawful (for example, health information for a workplace adjustment). Where a stricter legal standard applies, we meet it.

REGIONAL NOTE

EEA/UK: We only process special-category data where we have an explicit lawful basis under Article 9 GDPR, such as explicit consent, employment-law obligations or vital interests.

Children's data. Our services are for adults, or for minors under the supervision of an adult client such as a school or employer. We don't knowingly collect personal information from children below the age required by law without the right consent. For school deployments involving minors, the school or institution is responsible for getting any parental consents. Where a school or similar client asks for our help with a verified request about a minor's information — including deletion — we will support that request in line with the client's instructions and the law.

How we collect information

- Directly from you (sign-up forms, support requests, onboarding forms, HR and payroll forms).
- Automatically when you use our platform, website or a company-issued device.
- From client organisations or administrators that sign users up or set up integrations.
- From SSO or identity providers, integration partners, payment providers and other suppliers.
- From referees, screening providers and public sources where it's lawful and appropriate.

4. How we use personal information

IN PLAIN ENGLISH

We use your information to run the service, keep it safe, talk to you when we need to, improve it, and run our business. We only use it for the reasons in this table — not for something different without telling you.

We only use personal information for clear and lawful business reasons. The lawful basis we rely on depends on your relationship with us, where you are, and the situation. The table below sets out the main reasons.

WHAT WE USE IT FOR	EXAMPLES	LAWFUL BASIS WE RELY ON
Running and supporting the service	Setting up and verifying your account, delivering content, answering support questions, managing the relationship, billing and sending service messages.	Contract (we need it to deliver what you or your organisation signed up for); pre-contract steps; legitimate interests in supporting the service.
Running and improving our platform and website	Product analytics, reliability monitoring, debugging, planning, quality assurance and improving the user experience.	Legitimate interests in running and improving the service; consent where the law needs us to get it — for example, for non-essential cookies.
Security, fraud prevention and keeping things running	Spotting threats, controlling access, preventing abuse, patching vulnerabilities, responding to incidents, keeping audit logs and restoring from backups.	Legitimate interests in keeping systems and users safe; legal duties where a law or contract requires it.

Sending service messages	Service notices (like password resets, enrolment confirmations, platform updates), satisfaction surveys and important service announcements.	Legitimate interests; contract for service messages you need in order to use the product.
Marketing, events and business development	Answering enquiries, sending updates about products and services, event invitations, measuring campaigns and managing your preferences.	Legitimate interests for business-to-business outreach to existing or likely prospects; consent where a direct-marketing or electronic-communications law requires it.
Recruitment and managing the workforce	Assessing applicants, onboarding, payroll, tax, benefits, training, performance management, adjustments, device and access management and offboarding.	Pre-contract and contract steps; legal duty; legitimate interests; consent for sensitive or optional things.
Legal, compliance and corporate matters	Keeping records, responding to lawful requests, protecting legal rights, compliance, internal investigations, insurance and corporate transactions.	Legal duty; legitimate interests in running and protecting the business.

Where Acorn handles information on behalf of a client organisation, we follow the client's instructions, our contract with them, and any laws that apply to us directly.

We won't use your personal information for reasons that don't fit with the list above. If we plan a new use, we will update this policy and, if required, let you know or ask for consent.

REGIONAL NOTE

EEA/UK: For a full breakdown of lawful bases by purpose, see Appendix 1. You can object to processing based on legitimate interests — see Section 11.

REGIONAL NOTE

Canada: Where Canadian law applies, we collect, use and disclose personal information only where it's reasonably required, and we give you notice or ask for consent where that's needed. See Appendix 2.

5. How we share personal information

IN PLAIN ENGLISH

We don't sell your personal information. We share it only with trusted suppliers that help us run the service, your organisation if it set up your account, our advisers where needed, and authorities when the law requires it.

We do not sell personal information. We share it only in these situations:

- Service providers and contractors that help us run the business or the service — for example, hosting, identity, communications, support, payroll, security, analytics, screening and professional service providers. We require them to protect your information and use it only for the job we've given them.
- Client organisations and their administrators where an account is provided through that organisation's subscription. Your organisation's own privacy notice may also apply once it has the data.
- Affiliates, advisers, auditors, insurers, bankers or transaction counterparties where it's reasonably needed for our operations, governance or corporate activity.

- Courts, regulators, law enforcement and other third parties where disclosure is required or allowed by law, or necessary to protect rights, safety, systems or users.
- Anyone else with your consent or at your direction, such as integrations you turn on or agents you appoint.

If Acorn goes through a merger, acquisition, reorganisation or asset sale, personal information may transfer as part of that, subject to appropriate confidentiality and transition protections.

REGIONAL NOTE

US: We don't sell personal information and haven't done so in the last 12 months. We don't share it for cross-context behavioural advertising. See Appendix 3.

6. International transfers

IN PLAIN ENGLISH

Acorn is based in Australia and our main infrastructure is in Sydney. Some customer deployments use regions in the US, UK or Canada. When your information moves across borders, we use contracts and other safeguards to keep it protected.

Acorn is an Australian company. Our primary infrastructure runs on Amazon Web Services in Sydney (the ap-southeast-2 region), with additional regions available in the United States (us-east-1), the United Kingdom (eu-west-2) and Canada (ca-central-1). Depending on how your client organisation is set up, and who supports you, your information may be accessed from or transferred to locations outside your own country.

When this happens:

- We only transfer what's needed for the specific purpose.
- We require recipients to protect your information through contractual
- commitments and through vendor risk assessments that match the sensitivity of the data.
- We use reputable providers with strong security certifications and try to keep data in the region most appropriate for you where we can.

REGIONAL NOTE

Australia: Under APP 8, we take reasonable steps to make sure overseas recipients handle personal information consistently with the Australian Privacy Principles. For Australian government customers we offer dedicated deployment options (our gov1 and slgov1 clusters in Sydney).

REGIONAL NOTE

EEA/UK: We rely on adequacy decisions, Standard Contractual Clauses (SCCs) or other approved transfer mechanisms. See Appendix 1.

REGIONAL NOTE

Canada: We remain accountable for personal information transferred to service providers outside Canada through due diligence, contractual safeguards and proportionate security measures. See Appendix 2.

7. Security

IN PLAIN ENGLISH

We put a lot of effort into keeping your information safe. Our platform is independently audited (IRAP/SOC 2), we encrypt data, require strong sign-in controls, run daily backups and train our people. If something goes wrong, we'll tell you and the right authorities when we need to.

We apply administrative, technical and physical safeguards to protect personal information from loss, theft, misuse and unauthorised access or disclosure.

SAFEGUARD AREA	WHAT WE DO
Independent audit	Acorn holds IRAP and SOC 2 reports covering our production environment, with continuous monitoring through automated evidence collection. We also maintain alignment with the Australian Government's Information Security Manual (ISM) for our government customers.
Encryption	External connections use HTTPS/TLS. Personal information stored in our primary databases, object storage and file systems is encrypted at rest using AES-256 with managed keys.
Access controls	Access is role-based and granted on a need-to-know basis. Single sign-on with multi-factor authentication is required for staff and administrators accessing production systems.
Logging and audit	We maintain logging and audit trails appropriate to the sensitivity of the data. Administrative actions on sensitive systems are logged. Logs are treated with the same protection as the most sensitive data they contain.

Security monitoring	We run continuous security monitoring across our infrastructure, including threat detection, configuration monitoring and centralised audit logging. High-priority alerts are investigated by our security team.
Security testing	We carry out regular vulnerability scans, periodic third-party penetration testing, and code reviews. We track findings against defined service levels.
Backups and recovery	We run automated daily backups, with cross-region copies where appropriate. We test our recovery processes.
People and vendors	Our staff are trained on data protection and are contractually bound to protect personal information. We carry out vendor security assessments before giving suppliers access to personal data.
Data minimisation and disposal	We minimise personal information in logs where we can, and securely delete, anonymise or cryptographically erase data we no longer need. For higher-sensitivity data, we log evidence of destruction.

No system is 100% secure. We continuously improve our security. If a breach were to affect your personal information, we will notify you and the relevant authorities as required by law.

REGIONAL NOTE

Australia: Where an incident is an eligible data breach under the Notifiable Data Breaches scheme, we notify affected individuals and the OAIC.

REGIONAL NOTE

Canada: Under PIPEDA, if a breach creates a real risk of significant harm, we notify affected individuals and report to the OPC. Under Québec law, we notify the CAI where a confidentiality incident presents a risk of serious injury. See Appendix 2.

8. Cookies and similar technologies

IN PLAIN ENGLISH

Cookies are small files that help our site and platform work. We use them mainly to keep you signed in, keep the service secure, and see how things are used. We don't run third-party advertising cookies inside the Acorn platform.

We use cookies and similar technologies to run our websites and services, keep sessions secure, remember preferences, understand performance and improve the user experience. Some are strictly necessary. Others are optional and depend on the context.

Inside the Acorn platform

We mainly use cookies for sign-in, session management, security, reliability and limited-service improvement. We do not use third-party advertising cookies or cross-site tracking cookies on the Acorn platform. Where we use optional analytics or similar technologies, we give you any consent choices required by law.

On our public website and marketing channels

Our public website or marketing channels may use analytics, measurement or advertising-related technologies. Where a technology is not strictly necessary, we ask for consent where the law requires it and explain the choices. You can find more detail in any separate cookie notice or preference tool we provide.

Your choices

You can manage cookies through your browser settings and any preference tools we provide. Blocking some cookies may affect parts of our sites or services.

9. System monitoring and security logging

IN PLAIN ENGLISH

We keep security logs so we can detect and respond to threats. We don't run productivity monitoring or behavioural surveillance on our workforce. Access to logs is restricted to the people who need it.

To protect our services and your information, we maintain security and operational monitoring. Acorn does not operate dedicated workforce monitoring for productivity scoring or behavioural surveillance. We do maintain standard security and operational logging that's necessary to run, secure and support our systems.

Examples of monitoring and logs that may include personal information (minimised where possible):

- Identity and access logs (sign-in events, MFA events, access changes). Administrative activity logs on systems that manage workforce or sensitive data.
- Endpoint and device security information for company-managed devices (device identifiers, IP address, security status, threat detection events).
- Collaboration and email security logs (anti-malware and phishing scanning outcomes, limited metadata needed for security).
- Network and application security logs used to detect abuse, intrusion or data loss.

Access to monitoring data is restricted to authorised people (usually IT and Security, and when needed HR and Legal) on a need-to-know basis, and used for security operations, incident investigation, legal compliance and audit.

REGIONAL NOTE

Australia: If Acorn introduces significant new workforce monitoring, we provide notice and any required signage under state or territory workplace surveillance laws.

REGIONAL NOTE

EEA/UK: Any monitoring is subject to a necessity and proportionality assessment under GDPR. Workforce members have the right to be informed about monitoring and, in some situations, to object. See Appendix 1.

10. How long we keep your information

IN PLAIN ENGLISH

We keep your information only as long as we need it. Here are the typical periods we follow, unless a law or contract makes us keep it longer.

We keep personal information only as long as we need it for the reasons we collected it, or as required by law. The table below shows the typical retention periods, unless a longer period is required by law or contract.

DATA CATEGORY	TYPICAL RETENTION PERIOD	TRIGGER / NOTES
Account and service data	For as long as the relationship lasts, plus up to 12 months	To allow for wind-down and re-activation after closure.
Billing and financial records	7 years from the end of the relevant financial year	Australian tax law baseline; other jurisdictions may differ.
Security and operational logs	Up to 12 months	Unless an investigation or legal hold needs longer.
Analytics and cookie data	Up to 13 months from collection	Aligned with analytics tool defaults.
Marketing contacts	Until you unsubscribe or withdraw consent	A suppression-list entry is kept indefinitely so we can honour the opt-out.
Recruitment data	12–24 months after the recruitment process ends	Unless you consent to us keeping it longer for future opportunities.
Workforce records	7+ years after the end of the engagement	Or longer where workplace, tax or superannuation law requires it.
Support communications	As long as needed to resolve the issue, then up to 2 years	Unless deletion is requested earlier.

When we no longer need your information, we securely delete, de-identify or destroy it using appropriate methods. If a legal hold applies, deletion is paused until the hold is lifted (and the reason is documented).

11. Your rights and choices

IN PLAIN ENGLISH

You can ask to see, correct or delete your personal information, opt out of marketing, and complain. The full set of rights depends on where you live. If your account was set up by an employer or school, some requests may need to go through them.

You have control over your personal information. You can choose whether to provide personal information to us, but if you don't provide certain details, we may not be able to give you some services. Tell us if you don't want to provide something and we'll let you know whether it's required or optional.

The exact rights available to you in respect of your personal information depend on where you live and our relationship with you, but we extend many core rights to everyone as a global baseline.

RIGHT	WHAT IT MEANS	HOW TO EXERCISE IT
Access	Ask to confirm whether we process your personal information and get a copy.	Email privacy@acorn.works
Correction	Ask us to correct information that is inaccurate, out of date or incomplete.	Email us, or update directly in your account settings where available.
Deletion	Ask us to delete your information where we no longer need it for a legal, contractual or documented business reason.	Email privacy@acorn.works
Marketing opt-out	Stop getting marketing emails at any time.	Use the unsubscribe link in any marketing email, or contact us.

Withdraw consent	Where we rely on consent, you can withdraw it at any time. Anything we did before you withdrew stays lawful.	Email privacy@acorn.works
Complain	Raise a concern about how your information is handled.	See Section 12.

REGIONAL NOTE

EEA/UK: You also have the right to data portability, the right to restrict processing, the right to object to processing based on legitimate interests, and the right not to be subject to a decision based only on automated processing that has legal effect. See Appendix 1.

REGIONAL NOTE

US: Depending on your state, you may have additional rights — including the right to know, the right to opt out of sale or sharing (we don't sell personal information), and the right to non-discrimination. See Appendix 3.

REGIONAL NOTE

Canada: You have the right to access, correction, and to withdraw consent, subject to legal or contractual constraints. See Appendix 2.

Enterprise and tenant accounts: If your account is set up and managed by a client organisation, that organisation's administrator may control certain account actions (like suspension, export and deletion) inside the tenant. Requests about the content you put in the platform may need to go through your organisation. Acorn will help where the contract or law requires it.

12. Contact us, complaints and escalation

IN PLAIN ENGLISH

Contact the Privacy Team by email, phone or post. We'll respond within 30 days — sometimes less, depending on the law that applies. If you're not happy with our response, you can raise it with senior management or the privacy regulator in your region.

Step 1: Contact our Privacy Officer

METHOD	DETAILS
Email	privacy@acorn.works
Phone	+61 (0)2 6269 3330 (ask for the Privacy Team)
Post	Privacy Officer, Acorn PLMS Pty Ltd, Level 6/1 Farrell Pl, Canberra ACT 2601, Australia

Please include your full name, contact details, a clear description of your request or complaint, and any relevant dates or reference numbers. We verify your identity before acting on a request.

Step 2: Our response

We respond in writing, usually within 30 days (or within the time required by the law that applies, which can be shorter). We explain what we'll do and keep you updated on progress.

Step 3: If you're not satisfied (complaints only)

If you're not satisfied with our response, you can ask our senior management to review it, or contact the relevant external regulator:

WHERE YOU ARE	REGULATOR AND CONTACT
Australia	Office of the Australian Information Commissioner (OAIC) — www.oaic.gov.au — 1300 363 992
EEA	Your local Data Protection Authority (contacts at edpb.europa.eu)
United Kingdom	Information Commissioner's Office (ICO) — ico.org.uk — 0303 123 1113
Canada	Office of the Privacy Commissioner (OPC) — priv.gc.ca — 1-800-282-1376; or the relevant provincial regulator (BC, Alberta, Québec)
California, USA	California Privacy Protection Agency (CPPA) — cppa.ca.gov; or the Attorney General

13. Artificial intelligence and automated processing

IN PLAIN ENGLISH

We use AI in some parts of the platform, but we don't use your data to train outside AI models unless your organisation has chosen to allow it. Important decisions aren't made by AI alone — a person is always involved.

We use artificial intelligence and machine learning in parts of our business and services. We're committed to using these technologies responsibly, transparently and in a way that respects your privacy.

How we use AI

- AI-assisted content creation and editing tools inside the platform (for example, writing assistance and content improvement), where your client organisation has enabled them.
- Product analytics, reliability monitoring and service improvement.
- Personalised learning recommendations (where the platform is configured to
- provide them).
- Internal workflows like support triage and code assistance.
- Detecting security threats and unusual activity.

Data boundaries and safeguards

We don't use customer or user data to train third-party AI models unless the client organisation has explicitly opted in. When we work with third-party AI providers, we require contractual commitments that they won't use customer / PII data for training, will process data in line with applicable privacy laws and will meet our security standards. Where AI features are enabled, platform content may be processed by our AI infrastructure to deliver the feature. We keep AI prompts, outputs and related logs only as long as we need them for the reasons in this policy.

Human review and transparency

We don't make decisions that have legal or similarly significant effects on you by AI alone without meaningful human involvement. Where AI is used in a context that could significantly affect you, we provide appropriate transparency and a way to ask for human review where the law requires it. Client organisations control whether AI features are turned on for their users.

REGIONAL NOTE

EEA/UK: You have the right not to be subject to a decision based only on automated processing that produces legal effects or similarly significantly affects you. Where we use automated decision-making, we explain the logic involved and provide the right to human intervention. See Appendix 1.

14. Updates to this policy

IN PLAIN ENGLISH

We review this policy at least once a year, and more often when something important changes. If we make a material change, we'll tell you — for example, by email or a notice on our website.

We may update this policy from time to time by posting the revised version on our website. We review it at least once a year, and more often when laws, technology or our practices change. Where changes are material, we take reasonable steps to notify affected individuals (for example, by email or a prominent notice on our website).

Effective date: May 2026 | **Last updated:** May 2026 | **Next review:** May 2027

Appendix 1: Additional information for individuals in the EEA, UK and Switzerland

Under the General Data Protection Regulation (EU) 2016/679 (GDPR) and, for UK residents, the UK GDPR and the Data Protection Act 2018 (together, European Data Protection Laws), you have additional rights. This appendix supplements the main policy — the main body (including the Regional notes throughout) remains the primary reference.

Lawful bases for processing

European Data Protection Law requires us to have a lawful basis for processing your personal data. Section 4 sets out the typical basis for each purpose. The full bases we rely on are:

PURPOSE	LAWFUL BASIS	DATA CATEGORIES
Business operations and service delivery	Contract performance; legitimate interests	Identity and contact; service information; digital information
Communication and support	Legitimate interests; contract performance	Identity and contact; digital information
Service improvement	Legitimate interests	Digital information; usage data
Marketing and promotions	Legitimate interests (existing or likely B2B relationships); consent (where required)	Identity and contact; digital information
Employment purposes	Contract performance; legal duty; legitimate interests; consent (for sensitive or optional processing)	Identity and contact; professional data; sensitive data where applicable
Legal and compliance	Legal duty; legitimate interests	All relevant personal information

Where we rely on legitimate interests, we have carried out balancing tests to make sure our interests don't override your fundamental rights and freedoms.

International transfers

When we transfer personal data outside the EEA or UK, we ensure it receives appropriate protection by transferring only to countries recognised as providing adequate protection, putting in place contracts (such as EU-approved SCCs) that require the recipient to protect personal data to the same standards, or relying on other approved mechanisms.

Additional rights

In addition to the rights in Section 11, you have:

- Right to erasure: Request deletion of personal data where it is no longer necessary, has been unlawfully processed, or where you withdraw consent.
- Right to restrict processing: Ask us to pause processing where you contest accuracy, processing is unlawful, we no longer need the data but you need it for legal claims, or you have objected pending verification.
- Right to data portability: Receive your personal data in a structured, commonly used format or have it transmitted to another controller where processing is based on consent or contract and is automated.
- Right to object: Object to processing based on legitimate interests or for direct marketing. We will stop unless we can show compelling legitimate grounds.
- Right to withdraw consent: Where processing is based on consent, withdraw it at any time without affecting the lawfulness of prior processing.
- Automated decision-making: You have the right not to be subject to decisions based only on automated processing that produce legal effects or similarly significantly affect you, with the right to human intervention and to contest the decision.

Contact for GDPR matters: Privacy Officer, Acorn PLMS Pty Ltd, privacy@acorn.works, +61 (0)2 6269 3330, Level 6/1 Farrell Pl, Canberra ACT 2601, Australia.

Appendix 2: Additional information for individuals in Canada

Canada's privacy requirements may be federal and/or provincial, depending on your location, the nature of the relationship and Acorn's operating context. This appendix applies to all individuals in Canada — customers, website visitors, platform users and workforce members alike.

Applicable laws and regulators

- PIPEDA (federal): Applies in relevant circumstances, including employees of federally regulated organisations. Regulator: Office of the Privacy Commissioner of Canada (OPC).
- Provincial private-sector laws: May apply in some provinces, commonly including BC PIPA, Alberta PIPA and Québec's private-sector law.

Our approach: we apply the policy baseline globally and meet any stricter applicable Canadian federal or provincial requirements.

Consent and reasonableness

Where Canadian laws apply, we collect, use and disclose personal information only as reasonably required, and give you notice at or before collection. For workforce personal information, we collect only what's reasonably required to establish, manage or end the working relationship.

Cross-border processing

We may process personal information outside Canada where service providers host or support systems internationally. We remain accountable through vendor due diligence, contractual safeguards and security measures proportionate to data sensitivity.

Individual rights and request handling

We handle access, correction and other privacy requests in line with applicable Canadian law and document any lawful basis to refuse, limit or defer a request. Decisions are applied across relevant systems and service providers.

Complaints

You may raise concerns through our internal privacy complaint process (see Section 12) and also complain to the OPC (federal) or the relevant provincial regulator (for example, in BC, Alberta or Québec).

Appendix 3: Additional information for individuals in the United States

Several US states have comprehensive privacy laws, including the California Consumer Privacy Act as amended by the California Privacy Rights Act (CCPA/CPRA), and similar laws in Virginia, Colorado, Connecticut, Utah, Texas, Oregon and other states. This appendix provides additional disclosures for residents of states with applicable privacy legislation.

Categories of personal information we collect (CCPA terminology)

As described in the main body of this policy, we may collect: identifiers (such as name, email address, IP address); commercial information (such as service subscriptions and billing records); internet or electronic network activity (such as interaction with our services and device information); professional or employment-related information (for workforce members and applicants); geolocation data (inferred from IP address); and inferences drawn from the above.

Use and disclosure

The purposes for which we collect and use personal information are described in the main body. We do not sell personal information and have not done so in the preceding 12 months. We do not share personal information for cross-context behavioural advertising. We do not use or disclose sensitive personal information for purposes other than those permitted under applicable US state privacy laws.

Your rights under US state privacy laws

- Right to know: Request that we disclose the categories and specific pieces of personal information collected, the sources, purposes and categories of third parties to whom we have disclosed it.
- Right to delete: Request deletion of personal information, subject to exceptions
- such as legal obligations or completing a transaction.
- Right to correct: Request correction of inaccurate personal information.
- Right to opt out of sale/sharing: We do not currently sell or share personal information for cross-context behavioural advertising.
- Right to non-discrimination: We will not discriminate against you for exercising your privacy rights.

How to exercise your rights

Contact our Privacy Officer using the details in Section 12. We verify your identity and respond within the time required by applicable law (generally 45 days for CCPA/CPRA requests, extendable by a further 45 days). You may appoint an authorised agent to make a request on your behalf.

Metrics

Where required by applicable law, we will publish annual metrics on the number and nature of privacy rights requests received and our response rates.