Canada Aviation Dispute Resolution (CADR) Privacy Policy

EFFECTIVE FROM: March 2026

1. Introduction
    1. Canada Aviation Dispute Resolution (CADR) is an alternative dispute resolution (ADR) provider operating in Canada. CADR is dedicated to protecting your privacy and handling your personal information in a responsible and transparent manner.
    2. CADR's role is to help resolve disputes between consumers (passengers) and participating organizations (airlines) that have entered into formal agreements to use our ADR services.
    3. This Privacy Policy, along with our Cookies Policy, explains how we collect, use, disclose, and protect your personal information when you access our website or use our ADR services. It is intended to comply with the Personal Information Protection and Electronic Documents Act (PIPEDA), Quebec's Act to Modernize the Protection of Personal Information (Law 25), and any other applicable privacy laws.
    4. Please read this Privacy Policy carefully. By using our website or services, you acknowledge that you have read and understood this Privacy Policy. Where required by law, we will obtain your express consent for the collection, use, or disclosure of your personal information.
    5. We may update this Policy from time to time, so please check back regularly for the latest version.
2. Scope
    1. This Policy applies to:
        - Individuals using CADR's website or Application (APP)
        - Parties (individuals or organizations) involved in a dispute submitted to CADR
        - Authorized representatives of those parties
        - Job applicants submitting applications to CADR
        - Any other individual/organization who interacts with us and whose personal information we collect
    2. This Policy applies exclusively to our website, APP and services (under the CADR brand) and does not extend to other third-party websites that may be linked to from our website. We encourage you to review the privacy policies of any such websites before providing them with personal information.

3. Who is responsible for your personal information
    1. CADR is responsible for the personal information in its custody or under its control and is committed to ensuring its protection in line with the PIPEDA and, where applicable, Law 25.
    2. CADR has appointed a designated Privacy Officer responsible for
        - Overseeing CADR's compliance with applicable privacy laws
        - Managing privacy related inquiries, complaints and access requests
        - Ensuring appropriate policies, safeguards, and training are in place
        - Coordinating responses to privacy incidents and breaches
        - Acting as the point of contact for regulators or affected individuals
    3. The Privacy Officer holds sufficient authority and autonomy within our organization to fulfill their responsibilities and ensure accountability.
    4. The Privacy Officer's contact information is:
        - Name: Sophie Gustave
        - Email: privacy@cadr.ca
        - Postal Address: Canada Aviation Dispute Resolution, 2482 Yonge St #4131 Toronto, ON M4P 2H5
    5. If you require an alternative method of contact for accessibility reasons, please let us know and we will work with you to accommodate your request.
4. What personal information we collect
    1. We only collect personal information necessary to deliver our ADR services, operate our website, and meet our legal obligations. The specific types of information we collect depends on your relationship with CADR.

Role / Data Subject	**Types of personal information collected**
Complainants (passengers)	Full name, Postal address, Email address, Phone number, Identification documentation, Nature and details of the dispute, Supporting documentation, Technical information from your device or software. Please refer to “website users” in this table and our Cookies Policy for further details
Respondent organizations (airlines)	Names and contact details of staff or individuals related to the complaint, Information provided to CADR about the complainant(s) and their dispute

Website/App users	IP address, Browser type and settings, Pages visited and referring URLs, Data regarding access, Cookie/device identifiers Please refer to our Cookies Policy for further details
Job applicants	Full name, Postal address, Email address, Phone number, Resume/CV and cover letter, Employment and education history, References, Other information submitted during the hiring process

5. How we collect personal information

We collect personal information from a variety of sources, depending on your relationship with us and the way you interact CADR. This includes:

1. Directly from complainants (passengers): We collect the following information you provide to us voluntarily when you: Submit a complaint to CADR, Contact us by email, telephone or post,Complete a webform
2. From authorized representatives: We may receive personal information from someone acting on your behalf, such as a legal or professional representative, where you have provided consent for them to represent you.
3. From organizations involved in a dispute: We may receive personal information about you from the organization that is the subject of your complaint (also referred to as the respondent organization). For example, a respondent organization may provide us with relevant information about you and your dispute. Respondent organizations may also provide us with personal information about their staff or representatives, where necessary.
4. From your use of our website or APP: We automatically collect certain technical information when you visit our website. This may include the use of cookies or analytics tools, as described in our Cookie Policy.

6. How we use your personal information

We use your personal information only for purposes that are specific, explicit and legitimate. These purposes include:

1. To deliver our ADR services, Submitting and administering complaints lodged with CADR , Communicating with complainants, respondent organizations, and their authorized representatives (if applicable). We generally use the contact information you provide to notify you of updates about your complaint, so you can stay informed about its progress, For in-scope complaints, informing the respondent organization about the complaint and requesting relevant information from them about you and the matters related to the dispute , Facilitating the ADR process, Sharing relevant information with the CADR staff and the opposing party, Maintaining accurate records in compliance with our internal retention policy
2. For recruitment and employment with CADR, Evaluating qualifications, experience and suitability of applications , Contacting references for verification (where lawful), Communicating with candidates throughout the recruitment process , Maintaining application records in compliance with our internal retention policy

3. To comply with our legal and regulatory obligations , Fulfilling obligations under the applicable data protection, dispute resolution, and employment laws, Verifying the identity of parties involved in a complaint (where necessary) , Maintaining impartiality, transparency and fairness in dispute proceedings, Responding to requests from regulatory authorities or comply with legal processes
4. To enable us to improve our services , Evaluating and improve the quality and effectiveness of our ADR services, Developing internal training materials and anonymized case studies, Producing statistical and performance reports, using de-identified or anonymized data, in line with applicable privacy laws, Some calls may be used for internal training, quality assurance, or service improvement purposes

Note: when anonymizing data, we follow standards set out under Law 25, which requires that information be irreversibly de-identified and no longer re-identifiable.

7. Legal grounds for collection and use

CADR collects, uses and discloses personal information in line with the applicable Canadian privacy laws, including PIPEDA and, where applicable, Law 25.

We rely on the following grounds to collect, use and disclose personal information:

1. Consent: We primarily rely on your consent for the collection, use, and disclosure of your personal information in accordance with our Privacy Policy. Consent may be express (e.g. signing a form, checking a tick-box), or implied (e.g. providing your personal information voluntarily and authorising us to inform the respondent organization of your complaint). The type of consent we seek depends on:, The sensitivity of the information , The context of the collection of personal information , Any legal or contractual obligations that apply You may withdraw your consent at any time by emailing privacy@cadr.ca, subject to legal or operational limitations. If you withdraw your consent, we will explain any consequences and inform you whether we must retain or continue to use certain information as required by law.
2. Compliance with legal and regulatory obligations: In certain circumstances, CADR may be required to collect, use, or disclose personal information, such as:, Where laws regarding consumer protection, data protection, or dispute resolution apply, Responding to lawful requests from regulatory authorities, including the Office of Privacy Commissioner of Canada (OPC) and the Commission d'accès à l'information (CAI), Disclosing information pursuant to a subpoena, warrant, court order, or legal proceedings In these cases, we limit our use and disclosure of your personal information to what is strictly necessary to meet these obligations.
3. Contractual necessity: When an organization engages with CADR under an agreement (e.g. an airline contracting with us to handle consumer disputes or a third-party service provider that helps support CADR to deliver its operations), we may need to handle personal information to fulfill our obligations under that contract. In such cases, personal data is used strictly for delivering the agreed upon ADR services.
4. Exceptions to consent: In limited circumstances permitted by law, we may collect, use, or disclose personal information without your consent. These situations may include:, It is clearly in the individual's interest and consent cannot be obtained in a timely manner, The

information is publicly available as defined by law, It is required to investigate or prevent fraud, or to comply with regulatory inquiries or legal proceedings In these instances, we only handle your personal information to the extent necessary to meet our legal obligations or protect our services and users.

8. Disclosure of your personal information

We may disclose your personal information in limited and defined circumstances, in line with applicable privacy laws. Disclosures are made only to the extent necessary to fulfill the purposes described in this Policy and with appropriate safeguards in place, as follows:

Disclosures to parties involved in the dispute: We may disclose your information to the following parties to administer, facilitate, and arbitrate upon disputes:, The other party involved in the dispute, referred to as the respondent organization, to allow for a fair and transparent ADR process, Authorized representatives, including relatives, friends, legal or professional advisors appointed by the complainant or the respondent organization , Internal CADR staff with a legitimate need to know, who require the information to facilitate our ADR services

1. Disclosures to third-party service providers: We may share your personal information with trusted third-party service providers who assist us in delivering our services. These providers are not parties to the dispute, but rather support CADR's administrative, operational, or technical functions. Examples of such providers include:, Web developers who maintain our systems, Telephone system providers, Cybersecurity and data protection service providers, Printing and mailing services (if paper correspondence is requested) , Website hosting and IT infrastructure providers All our nominated service providers are contractually bound to:, Maintain appropriate technical and organizational safeguards, Use the personal information only for the purposes we specify, Refrain from any unauthorized use or disclosure. See section 12 below (cross-border transfers) for information about service providers located outside of Canada.
2. Legal and regulatory disclosures: We may disclose personal information where required or permitted by law in accordance with clause 7.2 above.
3. General safeguards applicable to disclosures: All disclosures are limited to the minimum amount of personal information necessary to achieve the stated purpose. CADR maintains strict controls over access and ensures that:, All recipients understand their confidentiality obligations, Information shared is relevant, accurate and up-to-date, Data subjects are informed of key disclosures unless prohibited by law

9. Data transparency summary

To help you better understand how we use your personal information, we have prepared the following summary:

Data subject	**Purpose of collection**	**Legal basis**	**Retention period**	**Information shared with**
Complainants (passengers)	Accept and administer the complaint,	(i) Consent, and (ii) Contractual	Retained in accordance with	Opposing party (or their representative

	and arbitrate upon the dispute	necessity where we have formal agreements in place with third-parties for the use of our ADR services	regulatory requirements (please refer to section 14 of this Policy)	where applicable) / CADR internal staff / third-party service provider (where strictly necessary)
Authorized representatives	Communicate about the complaint with the authorized party representative	Same as above	Same as above	Same as above
Respondent organizations (e.g. airlines)	Verify and respond to complaints	Contractual necessity	Same as above	Same as above
Website/App users	Improve website performance and functionality (via Cookies in line with Cookie Policy)	Consent (for non-essential cookies)	Please refer to our Cookie Policy	Website analytics vendors (if applicable) / CADR internal IT team / hosting vendors
Job applicants	Assess and manage applications, and make hiring decisions	Consent	6 months	CADR internal senior staff and HR

10. Disclosure of your personal information

    1. We are committed to ensuring that personal information is only accessed and used by individuals within CADR who have a clear and documented need to do so.

        - Administration: to assess and facilitate the complaint through the ADR process, and to provide operational support where required;

- Arbitrators: to review the case file and issue an arbitral award;
- IT personnel: to maintain secure systems, troubleshoot IT issues, and implement technical safeguards;
- Privacy Officer: to oversee CADR's compliance with applicable privacy laws and respond to privacy related inquiries and requests; and

2. Access to your personal information is strictly limited to personnel whose duties require it. This includes:
3. All CADR staff, contractors, and external professionals (including service providers) are subject to binding confidentiality agreements.
4. CADR applies the principle of data minimization, meaning that personal information is accessed only when necessary, in accordance with this Policy. We regularly review access permissions and perform audits to ensure compliance.
    - HR staff and senior personnel: for job applicants, only for recruitment and personnel management purposes.
    - HR staff and senior personnel: for job applicants, only for recruitment and personnel management purposes.
5. CADR maintains internal policies and technical controls to monitor and manage access to personal information. These are designed to prevent unauthorised access and to ensure that access is limited to individuals with a legitimate operational need.

11. Automated decision-making

1. CADR uses limited forms of automation to support the efficient administration of its ADR services. These include:
    - Automated triage functions to assess whether a complaint falls within CADR's jurisdiction
    - Workflow automation to identify and request missing information from the parties to the dispute
    - Automated routing of cases between parties for responses, and
    - Systems that organise and present information in a structured format for arbitrator review.
    - Submit the required information
2. CADR also uses automation to assist arbitrators in preparing draft determinations. These tools may include the use of templates, guided frameworks, or system-generated suggestions. However, no final decision on the outcome of a complaint is made solely by automated means. All decisions are reviewed and issued by a qualified human decision-maker following a full assessment of the case file.
3. In some cases, automated procedural actions may occur, for example where a file is automatically closed due to prolonged inactivity or failure to provide required information.

These actions are initiated based on pre-defined system rules and may not involve prior human review.

4. Where an automated action could significantly affect your ability to access or continue with the ADR process, you will be notified in advance and given an opportunity to:
    - Ask for human review of the proposed action
    - Submit the required information

5. If you are a resident of Quebec, these rights are provided in line with section 12.1 of Law 25. CADR extends these protections to all users, regardless of their location, as part of its commitment to privacy best practices.

12. Cross-border transfers of personal information

    1. All personal information collected by CADR is stored and used on servers located within Canada. While our online portal may be accessible internationally via the internet, CADR does not host or disclose personal information to servers located outside of Canada.
    2. CADR ensures any service providers we work with handle personal information in line with Canadian privacy laws.

13. How we safeguard your personal information

    1. CADR is committed to protecting personal information under its control through appropriate physical, organizational, and technological measures, as required by law. We apply a risk-based approach to safeguarding personal information, taking into account the sensitivity of the information, the purpose for which it is used, and the potential impact of unauthorized access or disclosure.
    2. Physical safeguards: Where personal information is held in physical form, we use appropriate controls such as restricted access to the premises and file storage areas, secure storage cabinets for sensitive materials, and controlled shredding and disposal of physical documents.
    3. Organizational safeguards: Our internal practices are designed to promote responsible data handling and reduce the risk of human error and misuse. These include:
        - Documented privacy and security policies
        - Role-based access to personal information based on operational need
        - Privacy training for staff with access to personal information
        - Confidentiality obligations in contracts
        - PIA's where required for new projects or technologies involving personal information
    4. Technical safeguards: We implement reasonable and proportionate technical security measures to protect personal information in electronic form, including:
        - Encryption of data at rest – ensures stored personal information is protected if storage media is lost or stolen.

- Multi-factor authentication (MFA) – adds an extra layer of identity verification for system access.
- Endpoint protection and anti-malware software – protects devices from viruses, ransomware, and other threats.
- Regular software updates and patch management – keeps systems protected against known vulnerabilities.
- Role-based access control (RBAC) – ensures users only access the data necessary for their role.
- Audit logging and monitoring – records access to personal information and flags unusual or unauthorized activity.
- Intrusion detection and prevention systems (IDPS) – monitors network traffic for suspicious activity.
- Secure coding practices and code reviews – reduces the risk of introducing vulnerabilities into software.
- Security incident response mechanisms – ensures rapid response to breaches or suspected intrusions.
- Protection against Denial-of-Service (DoS) and Distributed DoS (DDoS) attacks using traffic filtering and rate-limiting technologies.
- High availability architecture and automated failover systems for service continuity.

5. CADR monitors its privacy and security controls to ensure they remain effective. We review risks, lessons learned from audits or incidents, regulatory changes, and technical advancements regularly. Where required, we update our policies and procedures in response.

14. Retention and deletion

1. We retain personal information only as long as is reasonably necessary to fulfill the purposes for which it was collected, including:
    - Delivering our ADR services
    - Complying with our legal and regulatory obligations
    - Maintaining operational integrity
    - Handling complaints, appeals, or legal disputes
    - Enabling quality assurance, training, or reporting using anonymized data
2. We apply a tiered retention schedule based on the type of information and its purpose, as outlined below:

Category	Typical retention period	Justification
CADR complaint files and data held on associated systems (e.g. CADR controlled mailboxes / support ticket systems)	For complaints accepted as in-scope, 6 years from closure of CADR complaint file.	Regulatory compliance, potential legal claims, service auditing.
	For complaints deemed out-of-scope, the retention period is shortened to 3 years from the date of rejection.	Record of initial decision to reject claim.
General inquiries made in writing / sent electronically (not associated to a CADR case)	Up to 12 months.	Limited follow-up window, low legal risk and minimal retention required.
Website/App user data	As per cookie lifespan.	Performance and user analytics.
Job application data	For unsuccessful applicants, 6 months from our last contact.	Employment law compliance.
Anonymized data for training, statistics and reporting	Indefinite.	Used only when irreversibly anonymized as per applicable data protection standards.

3. When personal information is no longer required, we either:
    - Securely destroy it; or
    - Anonymize it in accordance with applicable standards. Anonymized data may be retained for statistical analysis, service improvement, quality insurance, and/or public reporting, but it will contain no personal data.
4. We periodically review our retention practices to ensure they remain:
    - Legally compliant
    - Proportionate to the risks involved
    - Aligned with our operational needs and contractual obligations

15. Your privacy rights (including right of access)

    1. Under Canadian privacy law, you have rights including:

        - The right to be informed about how your personal information is used (as outlined in this Policy).
        - The right to access the personal information we hold about you.
        - The right to request that we correct inaccurate or incomplete information.
        - The right to withdraw consent or request deletion of your information in certain circumstances.
        - The right to file a complaint with our Privacy Officer about how your personal information is handled by CADR.
        - The right to escalate the complaint with the OPC, or where applicable for Quebec residents the CAI.

    2. If you wish to exercise any of these rights, please contact the Privacy Officer using the contact details provided at clause 3.4. You may also do so verbally or in writing.

    3. If you have any concerns about how we have handled your personal information, or you believe we have not complied with our privacy obligations, you have the right to submit a complaint directly to us. You may do so by contacting our Privacy Officer using the details above. Please include as much information as possible about the nature of your concern. Our Privacy Officer will investigate your concerns and respond within 30 days of receiving your complaint. If you are not satisfied with our response, or if you prefer, you may also file a complaint with the OPC or, if applicable, the CAI.

    4. For rights of access to personal information we hold about you, we aim to respond within 30 days of the request. In most cases, we will supply a copy of your personal information to you free of charge. However, we reserve the right to charge a reasonable administrative fee where a request is:

        - Clearly unfounded
        - Excessive or repetitive, or
        - Involves significant administrative, transcription, reproduction, or transmission costs.

If a fee applies, you will be informed of the estimated cost in advance and given the opportunity to modify or withdraw your request before any changes are incurred.

CADR will not charge fees for the exercise of your privacy rights where no justification exists for doing so. Any fee imposed will reflect only the actual cost of responding to the request.

16. Data breach and incident response

    1. CADR has established internal procedures to defect, assess, and respond to potential data breaches and privacy incidents. In the event of a security incident involving personal information, we will:

- Promptly investigate the incident and assess whether it constitutes a privacy breach
- Determine whether the breach creates a real risk of significant harm (as defined under PIPEDA) or a risk of serious injury (as defined under Law 25 applicable to residents of Quebec).
- Notify affected individuals as required by law, providing details of:
    - The nature of the breach
    - The type of personal information involved
    - Steps taken or planned to reduce the risk of harm
    - Contact details for any questions or requests for additional information.

2. If a serious data breach occurs that poses a real risk of significant harm to individuals, we will notify the OPC, or the CAI.
3. All breaches are documented internally in our Data Breach Log in line with our obligations under the applicable privacy laws.

17. Cookies and website tracking

1. Our website uses cookies and similar technologies to enhance your browsing experience, improve our services, and understand how visitors use our website. We use:
    - Essential cookies to enable basic website functionality
    - Analytics cookies to monitor website traffic and performance (e.g. page visits)
    - Preference cookies to remember your settings (e.g. language, accessibility)
2. Some of these cookies may collect device identifiers, IP addresses, or location data. Under applicable privacy laws, we are required to obtain your explicit consent before placing non-essential cookies that identify or locate you.
3. You may manage your cookie preferences through the cookie banner on our website. For more information about the cookies we use and your options, please refer to our separate Cookies Policy.

18. Changes to this Privacy Policy

Any updates to this Policy will be posted on our website. When we make update, we will update the Effective From date at the top of this Policy. We encourage you to check back regularly to stay informed of any changes.