



# Privacy Policy

Protecting your privacy is extremely important to us. The following information will help you understand the purposes for which we collect, store and use your information. We will keep your information confidential and will only share it if we are legally required to do so, or if we must do so in order to fulfill our agreement with you, or if you have given your consent.

We have tried to make this notice as clear as possible, but if there is something we have not explained well, please contact us at [info@ReserTrac.com](mailto:info@ReserTrac.com).

## 1. What is this notice about.

We want you to understand who we are, what kind of personal information (“PI”) we collect, and what we do with it. This notice is part of our contract with you, and it may change from time to time.

1.1 In your day-to-day dealings with us we obtain PI about you. We want you to understand who you are sharing your PI with, what kind of information we are collecting and how we use it.

1.2 PI does not include any anonymous, de-identified, or statistical information – provided that it cannot be linked back to you.

1.3 This privacy notice forms part of our contract with you. You should read it along with the terms applicable to any ReserTrac services you use.

1.4 From time to time we may have to amend this notice to accommodate changes in our services, or if legal requirements change.

1.5 By using any of our products, you agree to our information practices, including the collection, use, processing, and sharing of your information as described in this Privacy notice. As well as the transfer and processing of your information to our data facilities in either Canada or the United States where we have, or use, facilities, service providers, or partners, depending on where you are based while using our services. You acknowledge that ReserTrac will abide by the laws, regulations, and standards of the country in which your information is stored or processed.



## 2. Who are you sharing your information with?

You are sharing your information with ReserTrac. Sometimes we may need to share your PI with others in order to provide our services to you or if we are legally required to.

2.1 ReserTrac is a North American company. When you share information with ReserTrac, the information can be accessed by any of our subsidiaries. ReserTrac's head office is in Mississauga, Ontario, Canada.

2.2 We do not sell or otherwise share your information with third parties aside from the sharing described in this section. In particular, we do not share information with third parties for their direct marketing purposes, unless you have given us explicit consent. This consent is not given by means of accepting our standard terms and conditions and/or our privacy policy.

2.3 In order to deliver our services we will have to share information with other communications service providers to enable them to transmit your communications. We only do so on your instruction and we will only share the information which is needed to fulfill our service obligation to you.

2.4 We also make use of third-party service providers or consultants who need access to information in order to do their jobs. An example of this is when we share information with service providers so they can store the data in either of our data processing facilities at IBM Cloud Object Storage Canada or IBM Cloud Object Storage USA. These service providers are not entitled to use the information for any other purposes, must keep it confidential and have given us reasonable assurances that the information is safe.

2.5 Sometimes we may need to disclose your information to a third party:

2.5.1 if we believe that disclosure is reasonably necessary to comply with any applicable law, regulation, legal process or a government request,

2.5.2 to enforce our contracts and policies,

2.5.3 to protect the security and integrity of our services,

2.5.4 to fulfill our legal obligation in connection with data subject requests,

2.5.5 to protect ourselves, our other customers, and the public from illegal activities; or

2.5.6 to respond to an emergency which we believe in good faith requires us to disclose information.

2.6 If we go through a corporate sale, merger, reorganization, dissolution or similar event, your information may be part of the assets transferred or shared in connection with the due diligence for any such transaction. Any acquirer or successor of the ReserTrac companies may continue to use the information as explained in this notice.

2.7 We will require anyone that we share your PI with to honour this policy in terms of applicable law.



### 3. Where is the information going?

3.1 ReserTrac maintains primary data locations in our two main areas of operations:

- 3.1.1 Canada; and
- 3.1.2 The United States of America (USA).

3.2 ReserTrac's operations are in various locations in the world. Currently our primary locations of our staff are in USA and Canada. ReserTrac does not store copies of production data in these operational locations, but for some services such as support tickets and finance services, we may process some of your data in the operational locations where the applicable staff attending to the matter is working.

3.3 ReserTrac makes use of service providers that process some of the data that forms part of the fulfillment of our services to you. Some of the data related to this third-party processing may be transferred from ReserTrac to the service provider. However, ReserTrac stores all information within IBM Cloud Object Storage with separate regional facilities for Canadian and American users.

3.4 ReserTrac makes use of vendors such as legal firms to perform operational tasks, which may require access to some PI. The sharing of information with vendors will always be limited to what is necessary for ReserTrac to deliver its services.

3.5 You consent to us processing your personal information in a foreign country with less stringent data protection laws than the country in which it was collected, to the extent allowed by applicable law.

3.6 ReserTrac does not sell any customer data to any third parties.

3.7 ReserTrac collects data from its customers in the following manner:

- Customer sends data to ReserTrac using mobile phone/device, via a mobile service provider or third party or by using a website belong or operated by ReserTrac.
- ReserTrac may transit the data to sub-processors to participate in the transit of this data. During this transit, only the minimum required information is shared to fulfill the obligation to our customers.
- During fulfillment of some transactions ReserTrac is only facilitating the transmission of content or categories of information, while doing so ReserTrac does not look at the content of the information itself. It is possible that the content our customers request us to transit is highly sensitive information; however, we do not collect any of these sensitive categories of information in our own capacity.
- ReserTrac collects information in its own capacity in the event of a customer registration.



## 4. What information we collect and why.

We collect personal information when you set up your account with us. We also pick up some information during the course of our interactions with you. Some personal information is generated and collected through your use of our services and sometimes we will collect personal information from another source. We also use cookies on our website.

\*Please note: Certain ReserTrac's service(s) and/or products(s) inherently retain items of information submitted by the user(s) during use. There are instances where such information will be of a nature to fall within the scope of PI (as defined herein). The continued use of these services accepts on the part of the user that such submitted PI will be retained for period(s) longer than the standard stated retention period for such PI, as without such data being present, the efficacy of the service requested is materially undermined. Be that as it may, ReserTrac is actively working on the wider implementation of shorter retention periods for such products (without degradation of the service) and these initiatives will be rolled out in due course. Should you be concerned in this respect, kindly reach out to us for more information.

4.1 When you set up your account with us, we collect the following information directly from you:

- 4.1.1 Company names and names of your affiliates\*, employees, account users and contact persons,
- 4.1.2 Identifiers such as registration numbers, identity numbers and
- 4.1.3 Contact details such as e-mail addresses, telephone numbers and fax numbers,
- 4.1.4 Location information such as your country of incorporation and physical address,
- 4.1.5 Financial information such as information held by credit bureaus, credit references, banking details, date of fiscal year end, the name of your auditor, date of last audit, payment method; and
- 4.1.6 Your username, password, and any other applicable authentication detail

\*When we say 'affiliate' we mean an entity or person that controls you, is controlled by you, or under common control with you, such as a subsidiary, parent company, employee, etc.

## 4.2 We collect this information for all the obvious reasons:

- 4.2.1 We want to provide our services to you,
- 4.2.2 Bill you,
- 4.2.3 Communicate with you about your account,
- 4.2.4 Recognize you when you communicate with us or want access to your account,
- 4.2.5 Comply with any legislation or regulation which requires us to collect the information,
- 4.2.6 We may also verify the information which you provided about your company for purposes of fraud prevention and to ensure the accuracy of the information you provided to us.
- 4.2.7 We need some of the information (for instance the location of your vehicle) to provide our services.
- 4.2.8 We use the data to manage and route traffic, to analyze and improve our services and to identify and solve problems.
- 4.2.9 From time to time, we gather publicly available information about companies that are our customers, such as where they are located, their website URL, their industry, and their size. We do this to understand our customer base better and to tailor the information which we send to you.
- 4.2.10 We make use of cookies on our website to identify your web browser, to analyze how our website and online services perform and are used and to make improvements to ensure that our website is useful, effective and efficient.
- 4.2.11 For some of our services we will require additional information. For instance, when you want to make use of one of our apps, we need additional information about your vehicle and whether you have been licensed by a client airport authority. Another example is when you apply for credit with ReserTrac.
- 4.2.12 When you interact with our support, sales, and account management teams, we pick up personal information in order to effectively assist you.

## 5. Your rights and preferences

We support all the required data subject rights, such as knowing what information we have and accessing, changing, or erasing it (to name a few).

5.1 You have various rights in terms of applicable law, including (but not limited to) the right to:

- 5.1.1 Ask what PI we hold about you,
- 5.1.2 Ask us to update, correct or delete any information we hold about you,
- 5.1.3 Unsubscribe from any direct marketing communications we may send you,
- 5.1.4 Object to the processing of your personal information,
- 5.1.5 To not receive discriminatory treatment by the business for the exercise of your privacy rights,
- 5.1.6 Designate an Authorized Agent to submit any data privacy request on your behalf,
- 5.1.7 Ask us any questions on the business' privacy policies and practices by emailing [info@ReserTrac.com](mailto:info@ReserTrac.com) . Please call our main Mississauga, ON office +1 (905) 267-8540 – simply ask for the Data Protection officer, or notify the service desk of your query.

We will do our best to keep your PI that we collect accurate, complete, and up to date and may ask you to update it yourself from time to time.

To exercise any of your rights, please email [info@ReserTrac.com](mailto:info@ReserTrac.com) . We will ensure our response and resolution align with timelines as prescribed by various data protection legislation. We may require you to go through an authentication process to confirm you are truly the owner of the PI. Our default process is as follows:

- You send us the request to [info@ReserTrac.com](mailto:info@ReserTrac.com)
- We send you a document to complete where we require information about you that can identify the data, we hold on you.
- In some cases, we will authenticate you through a “one-time pin” sent to your registered email account or mobile number.
- We then action your request and start the process.
- We resolve all requests within the guidelines prescribed by various privacy laws.

## 6. Data protection

ReserTrac fulfills the role as data processor for our customers and we adhere to privacy requirements as required by law.

6.1 ReserTrac has implemented multiple policies, processes, and procedures to support our and our customers' requirements to adhere to various privacy laws.

6.2 ReserTrac guides product decision with the concept of privacy by design in mind and we implement data retention policies for all PI.

6.3 ReserTrac is able to support all data subject rights as prescribed by various privacy laws. Any data subject request can be sent to [info@ReserTrac.com](mailto:info@ReserTrac.com).

6.4 ReserTrac has implemented multiple security protocols to ensure the safety of data. We offer different services to different customers.

6.4.1 We process data at IBM Cloud Object Storage in Canada and the USA based on the client's location.

6.4.2 Information related to IBM Cloud Object Storage (IBM Cloud):

IBM Cloud services provide ReserTrac with the capability to implement security measures in the ways needed to enable ReserTrac's compliance with the GDPR, including specific measures such as:

- encryption of personal data,
- ability to ensure the ongoing confidentiality, integrity, availability, and resilience of processing systems and services,
- ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident; processes for regularly testing, assessing, and evaluating the effectiveness of technical and organizational measures for ensuring the security of processing.

ReserTrac's virtual instances are solely controlled by ReserTrac. ReserTrac has full root access and administrative control over accounts, services, and applications. IBM Cloud personnel do not have the ability to log into ReserTrac instances. Formal policies and procedures delineating standards for logical access to the IBM Cloud infrastructure and hosts serve as a baseline for secure engagement with IBM Cloud.

6.4.3 Security management

- ReserTrac has dedicated security professionals that are responsible for various components of security.
- ReserTrac's services offer various encryptions and secure transfer options to our customers.
- ReserTrac has multiple vulnerability and penetration test exercises per year. Some of these also include independent third-party scans.
- ReserTrac makes use of Web Application Firewall (WAF) to protect websites against all Open Web Application Security Project (OWASP) threats, including SQL injections, Cross-site scripting (XSS) and remote file inclusions. This includes Distributed Denial of Service (DDoS) protection, as well as utilizing Content Delivery Networks (CDNs) to decrease page load times.



Digital Security: ReserTrac implemented multiple digital security controls such as unstructured data discovery, password protection, device encryption, MFA, CAB processes, threat detection, endpoint protection, port blocking, email protection, antivirus, software updates, vulnerability scans and penetration tests to name a few.

Operational security: ReserTrac implemented multiple operational security controls such as incident response teams, security officers, tailgating awareness, social engineering awareness, phishing awareness, training, workstation monitoring, onboarding and exit automation, etc. ReserTrac also conducts multiple security reviews per month on various security platforms and systems.

Administrative security: ReserTrac implemented multiple administrative security controls such as leadership awareness, infosec frameworks, privacy policy, incident policy, information security policy, password policy, audit controls, etc.

#### 6.4.4 Incident management

ReserTrac has an incident management response team that are responsible to handle any breach or incident related to PI.

#### 6.4.5 Data management and data classification

ReserTrac has implemented strict role-based security protocols for all data in ReserTrac. ReserTrac has started data classification processes to ensure sensitive data is identified and classified to assign the appropriate access and retention of data.

#### 6.4.6 Board awareness

ReserTrac has a dedicated compliance management committee to oversee all data protection matters. The compliance management committee reports directly into senior management through the audit committee to ensure awareness of IT strategies, policies, risk, and security.

#### 6.4.7 Business Continuity and disaster recovery

ReserTrac has a BCP and DR plan to ensure we are able to protect our data and our ability to sustain the services we offer to our customers. During the Covid-19 pandemic, ReserTrac managed to get all staff 100% operational within 24h of the various lock-down protocols implemented by various governments. All our internal and external services are 100% available to all staff.



## 7. GDPR

The General Data Protection Regulation (GDPR) is a Regulation by the European Commission with the intention of making data protection stronger for people and organizations in the European Union. To the extent applicable, ReserTrac processes personal data of European Union residents within the EU (on behalf of our Controllers), the regulation applies to our organization.

Although ReserTrac specifically references GDPR, the information also relates to the California Consumer Privacy Act and multiple other privacy laws.

### 7.1 What approach did ReserTrac take to comply with GDPR?

- We've invested significant time and resources into our data protection compliance projects.
- We planned our compliance efforts carefully by:
  - Consulting with data protection professionals.
  - Educating our staff and contractors through face-to-face workshops and online training; and
  - Identifying actions to comply with GDPR.

### 7.2 Where is ReserTrac's data infrastructure hosted?

A of December 2019 ReserTrac moved its data infrastructure to IBM Cloud Object Storage (IBM Cloud) in Canada and the USA. Data (including personal data) gathered by ReserTrac is hosted and processed wholly within the respective IBM Cloud Network of each country. IBM Cloud maintains an information security program that is certified under ISO 27001. ISO 27001 is the international best practice standard for information security. IBM Cloud also makes provision for GDPR compliance.

### 7.3 Where do we process data?

#### Products and Services:

ReserTrac only processes personal information within the respective IBM Cloud Object Storage (IBM Cloud) of either Canada, or the USA based on the country of residence of the system user e.g., a given livery company or driver.

#### CRM and Account management:

ReserTrac manages our customers through various cloud-based services. These services are hosted in IBM Cloud Object Storage, Canada, and USA respectively.

We have staff located at USA, Canada and Europe that might serve our customers.

Please reference the section above (Section 4: What information we collect and why) for more information.

## 7.4 Sub-Processors

ReserTrac uses various sub-processors to perform part of the services to our customers. We require any sub-processor that processes personal information to sign a data processing agreement and we started an audit process on vendors in Q4 2022.

## 7.5 Data processing agreement

ReserTrac has a standard data processing agreement that we make available to both customers and vendors. Kindly request a copy from [info@ReserTrac.com](mailto:info@ReserTrac.com).

## 7.6 Data security

Please refer to the section above – “Section 6: Data Protection”.

## 7.7 Privacy by design

ReserTrac has ensured that data protection is a topic that is addressed on all levels of the business. We have implemented (among others) key requirements as follows:

- Privacy governance and policies
- Data impact assessments
- Incident management
- Privacy training
- Data minimization
- Change management
- Access controls (physical and logical)
- Data retention policy
- Disposal and destruction of data processes
- Purpose collection and data maintenance
- Data subject right facilitation and technical solutions.

## 7.8 Data subject rights

We are able to process any data subject right. To exercise any of your data subject rights:

- Please send an email to [servicedesk@ReserTrac.com](mailto:servicedesk@ReserTrac.com). You will get an automated ticket and reference number as a response.
- ReserTrac will send an authentication form that has to be completed. It is our role to ensure that any request we get is indeed a legitimate request.
- Once we receive the completed authentication form, we start the process to action the request from the data subject.
- If we receive a request from our customer (on behalf of a data subject) – we follow the same process above.

## 7.9 Data protection officer

ReserTrac has appointed a data protection officer, who can be contacted on [info@ReserTrac.com](mailto:info@ReserTrac.com). Otherwise, you can call our main Mississauga, ON office +1 (905) 267-8540



## 8. The Personal Information Protection and Electronic Documents Act (PIPEDA)

ReserTrac needs to collect and use certain types of information about people with whom it deals in order to operate. These include: current, past and prospective clients; service providers and their appointed staff members; ReserTrac's own employees; suppliers and others with whom ReserTrac conducts business.

In addition to carrying out our own statutory functions, ReserTrac may occasionally be required to collect and use certain types of information of this kind to comply with the requirements of other legislations.

ReserTrac regards the lawful and correct use of personal information as important to the achievement of our objectives, to the success of our operations and to maintaining confidence between those with whom we deal and ourselves. We therefore aim to ensure that our organization treats personal information lawfully and correctly.

ReserTrac is obligated that personal information is collected, used, and maintained for its intended purpose in a manner that a reasonable person would consider appropriate in the circumstances.

The last time this notice was updated: February 2023