Privacy Policy

## Introduction

**Armour Cybersecurity**

At **Armour Cybersecurity** (“us”, “we”, “our” or the “Company”) we value your privacy and the importance of safeguarding your data. This Privacy Policy ("Privacy Policy") describes our privacy practices for the activities set out below. As per you rights, we inform you how we collect, store, access, and otherwise process information relating to individuals. In this Policy, "Personal Data" refers to any information that on its own, or in combination with other available information, can distinguish an individual, or any information with a high risk of harm that is linked directly to an individual (eg financial, medical, government).

The office locations of **Armour Cybersecurity** can be found [here](https://armourcyber.ca/contact-us/).

## Scope

This policy applies to all **Armour Cybersecurity** websites, domains, applications, services, and products.

This Policy does not apply to third-party applications, websites, products, services or platforms that may be accessed through (non **Armour Cybersecurity**) links that we may provide to you. These sites are owned and operated independently from us, and they have their own separate privacy and data collection practices. Any personal data that you provide to these websites will be governed by the third-party’s own privacy policy. We cannot accept liability for the actions or policies of these independent sites, and we are not responsible for the content or privacy practices of such sites.

## Processing Activities

This Privacy Policy applies when you interact with us by doing any of the following:

* Make use of our application and services as an authorized user
* Visit any of our websites that link to this Privacy Statement
* Visit any of our branded social media pages
* Visit our physical offices
* Attend any of our branded or sponsored events
* Receive any communication from us including newsletters, emails, calls, or texts
* Register for, attend and/or take part in our events, webinars, or contests

## Personal Data We Collect

### Data you provide

Personal data we collect includes:

* *Account information* such as your name, company, email address, and password
* *Payment information* such as your billing address, credit card, debit card or other payment method

Note that we do not request, gather, or store the following information:

* *Mobile device specific identifiers* such as make and model, IMEI and phone number
* *Government Identifiers* such as driver’s license numbers, SSN, passport numbers
* *Biometrics* such as finger prints, face scans, voice prints
* *Location Data*
* *Other information* such as your occupation, employment details, or residential address

If you provide us, or our service providers, with any Personal Data relating to other individuals, you represent that you have the authority to do so and acknowledge that it will be used in accordance with this Privacy Statement. If you believe that your Personal Data has been provided to us improperly, or to otherwise exercise your rights relating to your Personal Data, please contact us by using the information set out in the “Contacting us” section below.

### Device and Usage Data

When you visit an **Armour Cybersecur**ity website, we automatically collect and store information about your visit using browser cookies (files which are sent by us to your computer), or similar technology. You can instruct your browser to refuse all cookies or to indicate when a cookie is being sent. The Help feature on most browsers provide information on how to accept cookies, disable cookies or to notify you when receiving a new cookie. If you do not accept cookies, you may not be able to use some features of our Service and we recommend that you leave them turned on.

We also process information when you use our services and products. This information includes IP addresses, login information, time stamps, authentication records, and other operational data.

### Data we collect from third parties

We may receive your personal data from third parties such as companies subscribing to **Armour Cybersecurity** services, partners and other sources. This information is not collected by us but by a third party and is subject to the relevant third party’s own separate privacy and data collection policies. We do not have any control or input on how your personal data is handled by third parties. As always, you have the right to review and rectify this information. If you have any questions you should first contact the relevant third party for further information about your personal data. Where that third party is unresponsive to your rights, you may contact the Data Protection Officer at **Armour Cybersecurity** (contact details below) and we can assist you.

Our websites and services may contain links to other websites, applications and services maintained by third parties. The information practices of such other services, or of social media networks that host our branded social media pages, are governed by third parties’ privacy statements, which you should review to better understand those third parties’ privacy practices.

## Purpose and Legal Basis for the Processing of Personal Data

We collect and use personal data about you with your consent to provide, maintain, and develop our products and services and understand how to improve them.

These purposes include:

* *Building a Safe and Secure Environment*
  + To Verify or authenticate your identity; and
  + Investigate and prevent security incidents such as breaches, attacks and hacks.
* *Providing, Developing, and Improving our Products and Services* 
  + Deliver, maintain, debug and improve our products and services.
  + Enable you to access **Armour Cybersecurity** services and set up accounts.
  + Provide cloud services to enable the user and administrator to access their assessments and reports.
* *Provide you with technical and customer support.*
* *Organize and Deliver Advertising and Marketing*
  + Aggregate your information in an anonymized form to generate usage statistics
  + Send you newsletters and other marketing communications about current and future products, programs and services, events, competitions, surveys and promotions held by us or hosted on our behalf; and
  + Organize events or register attendees and schedule meetings for events.

Where we process your personal data to provide a product or service, we do so because it is necessary to perform contractual obligations. All of the above processing is necessary in our legitimate interests to provide products and services and to maintain our relationship with you and to protect our business for example against fraud. Consent will be required to initiate services with you. New consent will be required If any changes are made to the type of data collected. Within our contract, if you fail to provide consent, some services may not be available to you.

## International Data Transfer and Storage

We store and process data on servers in the general geographical region you reside within, note this may not be within the country in which you reside. However, your personal data may also be transferred to, and maintained on, servers residing outside of your state, province, country or other governmental jurisdiction where the data laws may differ from those in your jurisdiction. We will take appropriate steps to ensure that your personal data is treated securely and in accordance with this Privacy Policy as well as applicable data protection law. We will enter into EU standard contractual clauses (or equivalent measures) with parties outside the EEA and ensure adequate controls are in place for the security of your data.

## Sharing and Disclosure

We will share your personal data with third parties only in the ways set out in this Policy or set out at the point when the personal data is collected. We consider your personal data to be a vital part of our relationship with you. **We do not sell your personal data to third parties, including to third-party advertisers**.

## Legal Requirement

We may use or disclose your personal data in order to comply with a legal obligation, in connection with a request from a public or government authority, or in connection with court or tribunal proceedings, to prevent loss of life or injury, or to protect our rights or property. Where possible and practical to do so, we will tell you in advance of such disclosure.

## Service Providers and Other Third Parties

We my use a third party service provider, independent contractors, agencies, or consultants to deliver and help us improve our products and services. Service providers may be within or located outside the EEA. We may share your personal data with marketing agencies, database service providers, backup and disaster recovery service providers, email service providers and others but only to maintain and improve our products and services. For further information on the recipients of your Personal Data, please contact us by using the information in the “Contacting us” section below.

## Data Aggregation and Analytics

We may collate your personal data you provide to us or we collect and use it anonymously for analytics, benchmarking, and to effectively monitor our service and improve your user experience.

## Merger or Acquisition

If we are involved in a merger, acquisition or asset sale, your personal information may be transferred. We will provide notice before your personal information is transferred and becomes subject to a different Privacy Policy.

Under certain circumstances, we may be required to disclose your personal information if required to do so by law or in response to valid requests by public authorities (e.g. a court or a government agency).

## Security

We are constantly deploying and updating our technical and organizational security measures to protect against loss, misuse or alteration of personal data that we have collected or received from a third party.

To the extent permitted by law, **Armour Cybersecurity** may review, scan or analyze communications for fraud prevention, investigation, regulatory compliance, risk assessment, research, product development, and customer support purposes.

We use industry-standard encryption technologies when transferring and receiving personal data, and network access control technology to limit access to the systems on which personal data is stored, and we monitor for possible vulnerabilities and attacks.

If you become aware that there has been a breach in security of any of the personal data that we store or that is stored by our third-party service providers, please contact us via the instructions provided in the Contact Us section below.

## Retention & Deletion

We will only retain your personal data for as long as necessary for the purpose for which that data was collected and to the extent required by applicable law. When we no longer need personal data, we will remove it from our systems and / or take steps to anonymize it.

## Children’s Privacy

We will not knowingly collect personal data from children under the age of 16 years.

## Your Rights for Your Personal Data

Depending on your geographical location and citizenship, your rights are subject to local data privacy regulations. These rights may include:

**Right to Access** (GDPR Article 15, CCPA)

You have the right to request a copy of the personal data we are processing about you.

**Right to Rectification** (GDPR Article 16)

You have the right to have incomplete or inaccurate personal data that we process about you rectified.

**Right to be Forgotten** (right to erasure) (GDPR Article 17, CCPA)

You have the right to request that we delete personal data that we process about you, except we are not obliged to do so if we need to retain such data in order to comply with a legal obligation or to establish, exercise or defend legal claims.

**Right to Restriction of Processing** (GDPR Article 18)

You have the right to restrict our processing of your personal data where you believe such data to be inaccurate; our processing is unlawful; or if we no longer need to process such data for a particular purpose unless we are not able to delete the data due to a legal or other obligation or because you do not wish us to delete it.

**Right to Portability** (GDPR Article 20)

You have the right to obtain personal data we hold about you, in a structured, electronic format, and to transmit such data to another data controller, where this is (a) personal data which you have provided to us, and (b) if we are processing that data on the basis of your consent or to perform a contract with you or the third party that subscribes to **Armour Cybersecurity** services.

**Right to Objection** (GDPR Article 21)

Where the legal justification for our processing of your personal data is our legitimate interest, you have the right to object to such processing on grounds relating to your particular situation. We will abide by your request unless we have compelling legitimate grounds for processing which override your interests and rights, or if we need to continue to process the data for the establishment, exercise or defense of a legal claim.

**Right Not to Be Discriminated** (CCPA). You have the right not to be denied service or have an altered experience based on having executed any of your CCPA rights.

## Withdrawing Consent

If you have consented to our processing of your personal data, you have the right to withdraw your consent at any time, free of charge, such as where you wish to opt out from marketing messages that you receive from us. If you wish to withdraw your consent, please contact us at [privacy@armourcyber.ca](mailto:privacy@armourcyber.ca).

## How to Exercise Your Rights

You can make a request to exercise any of these rights in relation to your personal data by sending the request by mail to

**Data Protection Officer**

**Armour Cybersecurity**

**77 Bloor St West, Suite 600**

**Toronto, Ontario**

**M5S 1M2**

or email to [privacy@armourcyber.ca](mailto:privacy@armourcyber.ca).

For your own privacy and security, at our discretion, we may require you to prove your identity before providing the requested information.

## Changes

We may modify this Policy at any time. If we make changes to this Policy then we will post an updated version of this Policy on our website at <https://PrivacyCompliance.Group>.

When using our services, you will be asked to review and accept our Privacy Policy. In this manner, we may record your acceptance and notify you of any future changes to this Policy.

## Contact Us

To contact us, please email [privacy@armourcyber.ca](mailto:privacy@armourcyber.ca) or write to us at:

**Data Protection Officer**

**Armour Cybersecurity**

**77 Bloor St West, Suite 600**

**Toronto, Ontario**

**M5S 1M2**

## Complaints

If you have a complaint about this Policy or any element of your personal information that we hold then please contact us at the above address. If you are not satisfied, then you have the right to lodge a complaint with the local data protection authority.

If you are based in the EEA, please visit this website (<http://ec.europa.eu/newsroom/article29/document.cfm?action=display&doc_id=50061>) for a list of local data protection authorities .

Last updated: April 2020, Version 1.0

Copyright © 2020 Armour Cybersecurity All rights reserved.