



Aptum's Privacy Policy

Introduction

Aptum group of companies, including Aptum Managed Services (Canada) Inc., Aptum Technologies (UK) Limited Aptum Technologies (USA) Inc. and CloudOps Inc. (collectively, "**Aptum**") provides its Customers with data infrastructure technology and services. Data is at the heart of everything we do, and we therefore understand the importance of protecting and securing that data and the privacy of any individuals that such data relates to. For this reason, we have business procedures and security safeguards in place to protect any data that we either collect or that our clients process using our services - and we constantly are looking at how we can further our efforts to protect this data.

Aptum is committed to providing transparency with respect to its practices in handling personal information and data. This Privacy Policy sets out the standards, responsibilities and obligations of Aptum in respect of any personal information provided to Aptum. It is intended to establish responsible and transparent practices for the management of personal information and to satisfy the requirements of rules established by applicable privacy laws and standards in the jurisdictions in which we operate.

Application and Scope

This Privacy Policy applies to any personal information (as defined below in the section entitled "**Definition of Personal Information**") collected or generated by Aptum. Individuals, about whom personal information is collected by Aptum, are protected by the rights and safeguards contained in this Privacy Policy.

To ensure our commitment to transparency is met, we will provide further information in notices and policies where relevant explaining how Personal Information is collected and used so that you can make an informed choice whether to provide your personal information to Aptum or do business with us.

Data Processed using Services provided by Aptum

Our customers may use services provided by Aptum to process or store personal information they are responsible for (i.e. for which they are the data controller) ("**Hosted Data**"). Aptum does not determine the personal information our customers hold or processes using our services; our customers are responsible for compliance with any relevant data protection laws in relation to the Hosted Data and are responsible for all decisions relating to the processing of the personal information. Aptum' scope of responsibility for Hosted Data, including under data protection laws as either a processor or sub-processor where applicable, is defined in its agreements with its customers and is outside the scope of this Privacy Policy. Any subject access requests or other privacy complaint or enquiries relating to Hosted Data will be directed to our Customer.

Definition of Personal Information

For the purposes of this policy, when we refer to personal information, we usually mean any information about an identifiable individual. Depending on the jurisdiction in which we operate, this may include, for example, email addresses you have provided, contact details you have given in connection with an account with us, or such other information you have given to us relating to our services. Personal information that is aggregated and cannot be associated with an identifiable individual is not considered to be personal information.

Collection and Use of Personal Information

Most of the personal information we hold we collect directly from you, with your consent, for the purposes outlined below and we will have referred you to this privacy policy and/or provided a privacy notice. We will never use personal information for any other or new purpose without obtaining further consent, unless required or authorized by law.

Occasionally we may also obtain personal information about you from third parties, where you have provided that third party with your consent for them to share it with us. For example, to evaluate your suitability for a role at Aptum, we may need to run a background check with an independent agency. We may also contact you using information in the public domain if we legitimately believe that the

information we provide will be of specific interest to you, for example because of an existing or recent business relationships or where you have recently made an enquiry. In such circumstances we will carefully consider the nature of the data we are using, what your reasonable expectations are in relation to how we use that data, and the potential impact that the use of the data will have.

Aptum collects personal information for the following purposes:

- **Contact information:** We collect personal information to establish, develop and preserve our business relationships with customers and other individuals with whom we deal with or have a legitimate interest in receiving details of our services. We will usually collect your name, address, phone number(s) and email address, as well as other account and payment information, including information pertaining to your use of our products and services when you register for our services in order to create, establish and administer your account, to provide services, and to respond to inquiries. We will also use personal information in respect of know-your-client (KYC) requirements and potentially to establish or verify the eligibility and credit of persons that use, or intend to use, one or more of the products or services offered by Aptum.
- **Security and accuracy:** We use personal information to authenticate the identity of our customers, to preserve the confidentiality and security of our customers contacting Aptum by telephone, electronic means or otherwise and to ensure our records are accurate in order to protect customers and Aptum from error and fraud.
- **Management and quality:** We collect personal information for internal training and quality assurance purposes, and to manage our businesses and ensure the efficiency, reliability and security of our systems and networks.
- **Customer Service:** From time to time we may also use personal information to conduct surveys on the quality of our products, services or customer service, to provide our customers with offers for additional products and services that we feel may be of interest to our customers or to provide personalized products and services as well as product recommendations and to understand and assess the interests, wants and changing needs of customers with a view to improving our products and services and developing new ones.
- **Human Resources:** If you have applied for employment with Aptum, the personal information submitted with your job application will be used for recruitment and other customary human resources purposes. For example, we may send you information about new job opportunities within Aptum as well as other career development resources.

Your Consent

Aptum obtains consent from the individuals concerned for the collection, use or disclosure of personal information through various means, this includes orally (e.g. over the phone), through written documents including agreements, forms or other printed or electronic communications. In general, by purchasing our services you are providing your consent to the collection, use and disclosure of personal information as set out in this Privacy Policy.

In certain circumstances, personal information may be collected, used or disclosed without consent. These exceptional circumstances may include:

- where it is clearly in the interest of the individual and consent cannot be obtained in a timely way, such as in emergencies, where the life, health or safety of the individual is threatened, or where legal, medical or security reasons make it impossible or impractical to obtain consent;
- when information is being collected, used or shared for the detection, prevention of or remediation to, the breach of an agreement, fraud or other illegal activity, and the collection of consent might defeat the purpose of collecting the information;
- to collect a debt; and

- to comply with a subpoena, warrant or other court order, or as may be otherwise required or authorized by law or by any regulatory bodies having jurisdiction.

Withdrawing your consent and data deletion

Your consent to us collecting and using your personal information may be withdrawn at any time on reasonable notice and subject to any legal or contractual restrictions. Without such consent, Aptum may limit the services or products it provides you. You may also withdraw your consent as follows:

- **Email.** You can always limit the communications that Aptum sends to you. We often use technologies that enable you to stop communications or tailor them such as providing links to “unsubscribe” or “opt-out”. Where that isn’t possible you may also request we delete your data by contacting privacy@aptum.com. Please note that even if you opt-out of promotional communications, we may still need to contact you with important information about your account. If you have any questions about your choices or if you need any assistance with opting-out, please refer to our Anti-Spam commitment below.
- **Postal marketing, Telephone marketing and Quality control communications.** You may decide that you prefer Aptum not to use your personal information to promote new and/or additional products and services which may be of interest to you and refuse that we contact you by mail or telephone for marketing or quality control purposes. If this is the case, you may advise us by contacting customer service or contacting us using the information detailed in the ‘How to Contact Us’ section below.

Sharing of Personal Information with Third Parties

Your personal information may be made available by Aptum to third-parties or service providers to fulfill the purposes set out in this Privacy Policy. Aptum will never sell, rent or trade your personal information to any third party. Only those employees of Aptum or trusted third party contractors, who need access for business reasons, or whose duties reasonably so require, will be granted access to personal information.

We may hire service providers, including affiliates, to perform services on our behalf, for example the collection of customer accounts, customer credit verification and installation of services. We provide them with the limited amount of information which is necessary in order for them to provide the services required and they are prohibited from using the information for purposes other than to facilitate and carry out the services they have been engaged to provide. Aptum will strive to protect personal information disclosed to third parties by contractual agreements requiring that those third parties adhere to confidentiality and security procedures and protections that are, at a minimum, equivalent to those employed by Aptum itself.

We may disclose personal information to a third party in connection with a sale or transfer of business or assets, an amalgamation, re-organization or financing of parts of our business. However, in the event the transaction is completed, your personal information will remain protected by applicable privacy laws. In the event the transaction is not completed, we will require the other party not to use or disclose your personal information in any manner whatsoever and to completely delete such information.

We may also disclose information to our accountants, auditors, agents and lawyers in connection with the enforcement or protection of our legal rights.

Cross-border Transfer of Personal Information

In some cases, personal information that we manage may be transferred, processed and stored outside the jurisdiction in which it was collected, and therefore may be available to government authorities under lawful orders and laws applicable there.

Aptum may receive personal information from its affiliate entities located in another jurisdiction in order to assist those affiliates in providing services and conducting their business operations. Where Aptum receives personal information in this manner, it acts as a processor under data protection laws, and the relevant affiliate is deemed to act as the data controller or equivalent under applicable privacy laws.

Disclosure of Personal Information as Permitted or Required by Law

From time to time, Aptum may be compelled to disclose personal information in response to a law, regulation, court order, subpoena, valid demand, search warrant, government investigation or other legally valid request or enquiry. In these circumstances, Aptum will protect the interests of its customers by making reasonable efforts to ensure that orders or demands comply with the laws under which they were issued, and that it discloses only the personal information that is legally required and nothing more. Aptum does not voluntarily comply with requests for personal information from government or law enforcement authorities that do not meet these standards.

We also reserve the right to report to law enforcement agencies any activities that we, in good faith, believe to be unlawful or to law enforcement and emergency services providers, in an emergency or where required or permitted by law. We may release certain personal information when we have reasonable grounds to believe that such release is reasonably necessary to protect the rights, property and safety of others and ourselves, in accordance with or as authorized by law.

Security of Personal Information

We will use reasonable security measures to protect your personal information against unauthorized access. Aptum has implemented security measures that contain administrative, technical and physical controls that are designed to safeguard your personal information. Personal information is stored in electronic format in our company databases.

Retention

Personal information will be retained only as long as necessary for the fulfilment of the purposes for which it was collected and for which consent was received, unless otherwise required by law. Personal information that is no longer required to fulfil the identified purposes will be destroyed, erased or made anonymous.

Access and Correction

Aptum respects your right to access and correct your personal information. Where it is required by law, on request we will:

- Provide a copy of your personal data that we hold (this may be subject to a small fee);
- Correct your personal data if you believe it is inaccurate;
- Erase your personal data, under certain conditions;
- Restrict the processing of your personal data; and/or
- Request your data be transferred to you or another organization (under certain restrictions).

If you need assistance updating your personal information, please contact us using the contact information detailed in the How to Contact Us section below.

How to Contact Us

If you have questions, concerns or complaints regarding this Privacy Policy or the personal information that Aptum has about you, please contact:

George Hill, Director, Security, Information Governance & Chief Privacy Officer

Postal Address: Aptum, Building 5000, Langstone Technology Park, Havant PO9 1SA

Phone number: +44 23 8212 2980



E-mail: privacy@aptum.com

In accordance with the European General Data Protection Regulations, we have appointed a European representative. If you are based in the EEA you can contact our representative through the following channels:

Postal Address: The DPO Centre Europe Ltd, 10 Place Vendome, 75001 Paris, France

Phone number: +33 1 53 45 54 72

Email: EURep@aptum.com

Change of Privacy Policy

Aptum will review and update its policies and procedures as required to keep current with rules and regulations, new technologies, standards and customer concerns. Our Privacy Policy may therefore change from time to time. We will post any privacy policy changes on our website and, if the changes are significant, we will provide a more prominent notice.

On the same or similar subject, you may want to review our other policies:

Canada's anti-spam legislation ("CASL") – Anti-Spam Commitment

This Anti-Spam Commitment generally applies to any commercial electronic messages ("**CEM**") sent by Aptum to external parties and is completed by a range of business procedures, processes and policies to ensure that such messages comply with CASL. Aptum, in its electronic communications with external parties, has to comply with the rules established by CASL and enforced by the Canadian Radio-television and Telecommunications Commission ("**CRTC**"), the Competition Bureau and the Privacy Commissioner of Canada. CASL regulates all CEMs, which are messages that include, among their purposes, the encouragement of participation in a commercial activity.

Aptum has modified its email footers to manage CASL's content requirements. Under CASL, all CEMs sent must include certain prescribed content including identifying Aptum as the sending party, contact details, and details of an unsubscribe mechanism.

Aptum sends CEM's in the following circumstances:

- To current or potential clients (both individuals and businesses) for marketing its Services and for customer experience purposes, as well as partner and prospective partner businesses; and
- To employees, prospective candidates and vendors in relation to service provision and potential recruitment opportunities.

Withdrawal from Privacy Shield

The Court of Justice of the European Union issued a judgment in July 2020 declaring the European Commission Decision 2016/1250 (on the adequacy of the protection provided by the EU-US Privacy Shield) as invalid. Aptum (USA) Inc has determined that it is no longer appropriate to participate in this program and instead has updated its legal terms to include the necessary legal mechanisms to continue to ensure the legal flow of data from the EU to the US. Please see our Data Processor Addendum for further details.