

DEUS X PAY INTERNATIONAL LTD

PRIVACY POLICY

Last Update: August 2026

1. INTRODUCTION

- 1.1. This Privacy Policy is issued by and applies to Deus X Pay International Ltd, a company registered with FINTRAC Canada as a Money Services Business under registration number: C100000383 and corporate access number: 2026416814, and registered as a Payment Service Provider (PSP) with the Bank of Canada (BOC), with its registered address at 5224C-7005, Fairmount DR SE Calgary, Alberta, Canada, T2H0K4, and trading under the name "Deus X Pay", as well as all of its affiliates, holding companies, and subsidiaries ("**DXP**", "**we**", "**us**" or "**our**").
- 1.2. Any reference in this Privacy Policy to DXP, we, us, or our shall include our employees, consultants, officers, directors, representatives, agents, shareholders, affiliates, subsidiaries, holding companies, related entities, advisors, sub-contractors, service providers and suppliers.
- 1.3. DXP is committed to protecting the privacy and personal data of visitors to our website, as well as our users and clients ("**you**" or "**your**") who make use of our platform and services.
- 1.4. We recognise and respect the importance of data protection and are committed to complying with applicable data privacy laws and regulations, including, but not limited to, the Canadian Personal Information Protection and Electronic Documents Act ("**PIPEDA**"), and any applicable provincial private-sector privacy legislation.
- 1.5. This Privacy Policy describes our data handling practices when you:
 - 1.5.1. register, login, access or use our platform or content we own or operate on the website located at www.deusxpay.com (our "**Website**") or any other associated websites;
 - 1.5.2. represent one of our clients;
 - 1.5.3. work with us as a service provider or introducing broker;
 - 1.5.4. visit a DXP office or register to attend a DXP event; or
 - 1.5.5. otherwise interact with us in circumstances that require the collection, use and disclosure of your personal data.
- 1.6. By accessing, browsing and using our Website, platform, or any of our services (collectively, the "**Services**"), you acknowledge that you have read, understood, and agreed to be bound

by the terms of this Privacy Policy. Your continued use of the Services will constitute your acceptance of this Privacy Policy and any amendments made to it from time to time.

- 1.7. This Privacy Policy applies to all users, including individuals, entities, and any other parties using our Services and interacting with our Website and/or platform.

2. PURPOSE OF THIS PRIVACY POLICY

- 2.1. The purpose of this Privacy Policy is to inform you about how DXP collects data from you when you interact with our Services. This includes your use of our Website, platform, digital wallets, and any other services we provide in connection with the custody, exchange or management of crypto assets.
- 2.2. To ensure transparency, our aim is to outline the nature and scope of the information we process and collect from you, the legal basis for such processing, how we use your information, the circumstances under which we may share it, and the measures we take to safeguard it, in compliance with the relevant data protection laws. These include, but are not limited to, PIPEDA, any applicable provincial private-sector privacy legislation, and, where relevant, other applicable data protection laws in jurisdictions where we operate (each a "**Data Protection Law**" and collectively, the "**Data Protection Laws**").
- 2.3. This Privacy Policy is also intended to outline your rights in relation to your personal information in order to help you make informed decisions when using our Services, and to demonstrate our commitment to responsible data management and regulatory compliance.
- 2.4. Additionally, this Privacy Policy serves to fulfil our obligations under the Data Protection Laws by clarifying our privacy practices and showing how we seek to ensure that your information is handled lawfully, fairly, transparently and that your trust in our Services is justified.

3. PRIVACY STATEMENT

3.1. Legal Justification for Processing Personal Data

- 3.1.1. Unless otherwise indicated, the processing of Personal Data refers to the collection, use, and disclosure of personal data under relevant Data Protection Laws.
- 3.1.2. Where there is any inconsistency or conflict between applicable Data Protection Laws, PIPEDA shall prevail.
- 3.1.3. For the purposes of this Privacy Policy, the meaning of processing personal data will be understood in accordance with PIPEDA:
 - 3.1.3.1. "**Personal Data**" is defined as any information relating to an identified or identifiable natural person ("**data subject**"); an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, voice,

image, identification number, geographic location, or to one or more factors specific to their physical, physiological, economic, cultural, or social identity.

3.1.3.2. **"Processing"** is defined as any operation or set of operations performed on personal data or on sets of personal data, whether or not by automated means. This includes, but is not limited to, collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination, alignment or combination, restriction, erasure, or destruction.

3.1.4. In accordance with PIPEDA, DXP shall only process your personal data depending on the nature of your interaction with our Services, and if at least one of the following legal bases applies:

3.1.4.1. **Consent**

In certain cases, we may ask for your explicit consent to the Processing of your Personal Data. We ensure that consent is, where required, given freely, specific and informed, and established by a clear affirmative act. Where consent is used as the legal basis, you have the right to withdraw it at any time without affecting the lawfulness of any Processing carried out before the withdrawal.

3.1.4.2. **Performance of a Contract**

Processing is necessary for the performance of a contract to which you are a party, or in order to take steps at your request before entering into such contract. This includes providing access to your crypto assets account, executing transactions, and delivering client support.

3.1.4.3. **Compliance with a Legal Obligation**

We are required to process certain data to comply with applicable laws and regulatory requirements, such as anti-money laundering ("**AML**"), counter-terrorism financing ("**CTF**"), tax obligations, know-your-customer ("**KYC**") regulations, the Retail Payment Activities Act ("**RPAA**"), as well as any requirements administered by FINTRAC or other relevant authorities from time to time.

3.1.4.4. **Protection of Vital Interests**

Although rare in the context of crypto asset services, we may process data to protect your vital interests, such as your life, health or physical integrity, or those of another natural person in urgent situations.

3.1.4.5. **Public Interest or Official Authority**

Processing is lawful when necessary for the performance of a task carried out in the public interest or in the exercise of official authority legally vested in DXP. This applies to activities required to ensure the integrity, security and transparency of the virtual asset sector.

3.1.4.6. **Legitimate Interests**

Where applicable, and subject to further guidance from the Office of the Privacy Commissioner of Canada ("OPC") or relevant authorities, processing may also be based on DXP's legitimate interests, provided such interests do not override your fundamental rights and freedoms. These interests may include fraud prevention, network and information security, and improving and securing our Services. In such cases, DXP will ensure that appropriate safeguards are in place and will maintain records of any balancing tests conducted.

3.2. **Categories and Types of Personal Data We Collect**

3.2.1. To provide our Services securely and in compliance with legal and regulatory obligations, we collect and process Personal Data primarily through electronic means, in accordance with PIPEDA. This includes data you provide directly through our Website, platform and written communications, particularly during the onboarding process and throughout your client relationship with us, as well as data we gather automatically as you interact with our Services.

3.2.2. The categories and types of Personal Data we collect include but are not limited to:

Category of Personal Data collected	Type of Personal Data collected
Identifiers	• Full name; • Date of birth; • Nationality; • Gender; • Signature; • Government-issued identification (passport number, ID number, driver's license); and • Photographs or biometric data (e.g., facial recognition, fingerprints) for identity verification.

Contact Data	• Email address; • Phone number; • Residential or mailing address; • Billing address; and • Social media handles or usernames (if applicable).
Professional or Employment-Related information	• Job title; • Company name; • Company registration number; and • Education background.
Financial and Transaction Data	• Account details; • Wallet details; • Source of funds; • Credit information; • Account Authentication details; • Transaction history; and • Payment method details.
Technical and Usage Data	• IP address; • Device information (e.g., device ID, operating system, browser type); • Log-in data (usernames and passwords) and session activity; • Two-factor authentication information; • Security questions and answers; • Location, time zone and geological data (where permitted); • Details of services accessed and platform usages; • Virtual asset transaction data, including wallet addresses and transaction amounts; and • Logs of user activity on the platform.
KYC and Compliance Data	• Background check information (e.g., sanctions screening, PEP status); • Responses to KYC/AML questionnaires; • Proof of identity and proof of address; and

	• Risk profiling and due diligence reports.
Communication Data	• Information provided in email correspondence, recorded calls, chat logs, or face-to-face meetings (including Zoom/Microsoft Teams online meetings); • Customers support interactions; • Notes or records from onboarding interviews or compliance meetings; and • Feedback or survey responses.
Marketing and Preferences Data	• Your preferences in receiving marketing communications; and • Data on how you interact with our communications and website content.
Legal	• Legal documents and Agreements entered into between you and us.

3.3. **Collection Methods**

3.3.1. We collect Personal Data through a range of methods to support the provision of our Services, maintain regulatory compliance, and enhance your experience when interacting with us.

3.3.2. These methods include information you provide directly, information we gather automatically, and information obtained from third parties or publicly available sources.

3.3.3. Specifically, we collect your Personal Data in the following ways:

3.3.3.1. **Direct Collection:** Personal Data is collected directly from you when you register an account, complete onboarding forms, communicate with us by email, participate in online meetings (such as via Zoom or Microsoft Teams), communicate with us via social messaging platforms or engage with us during in-person meetings;

3.3.3.2. **Third Parties:** We may receive Personal Data from third parties acting on our behalf or providing services to us, such as identity verification providers, sanctions screening services, and other compliance partners;

3.3.3.3. **Publicly Available Sources:** Where permitted by law, we collect information from publicly available resources, such as public records and information about you that is openly available on the internet; and

- 3.3.3.4. **Cookies and Online Tracking:** We use cookies and similar tracking technologies on our website and platform to enhance user experience, analyse traffic, and support security functions. These technologies may collect technical and usage data, including your IP address, browser type, session duration, and interactions with our Services. Where legally required, we obtain your consent before placing non-essential cookies on your device. You can manage your cookie preferences at any time through our cookie settings interface.

3.4. **How We Handle and Use Your Personal Data**

- 3.4.1. In accordance with the Data Protection Laws, we will process your Personal Data in a lawful, fair, transparent and secure manner. We will only collect and use your Personal Data for legitimate, specific and clearly defined purposes. The specific purposes for which the information is collected will be apparent from the context in which it is requested, and includes the following:

3.4.1.1. **To Verify Your Identity**

We use your Personal Data to confirm your identity and complete onboarding procedures.

3.4.1.2. **To Provide and Manage your Account**

We process your Personal Data to set up and maintain your user account, provide secure access to our platform and Services, deliver features and functionality, and improve the performance of our website and systems. This Processing is based on our legitimate interests and/or the performance of a contractual or pre-contractual relationship between you and us.

3.4.1.3. **To Comply with Legal and Regulatory Obligations**

As a regulated service provider, we are required to collect and process certain Personal Data to comply with legal and regulatory obligations, including AML, CTF, KYC, tax, and other applicable regulations. This includes identity verification, transaction monitoring, and screening against watchlists.

3.4.1.4. **To Facilitate Transactions and Process Billing**

We process your Personal Data to execute your instructions, process payments, transfer crypto assets, collect fees, and provide Services such as wallet management and trade execution. This is necessary to perform our contractual relationship with you.

3.4.1.5. **To Communicate with You**

Your contact and communication data is used to send you important service updates, respond to your inquiries, send you important updates about our Services or policies, and provide client support.

3.4.1.6. **To Detect and Prevent Fraud and Security Threats**

We use technical, behavioural, and transactional data to monitor for suspicious activity, enforce our terms of service, prevent fraud, and maintain the security and integrity of our systems.

3.4.1.7. **To Improve Our Services and User Experience**

We may analyse how users interact with our platform, using aggregated or pseudonymised data, to improve functionality, develop new features, troubleshoot issues, and enhance overall performance.

3.4.1.8. **For Marketing and Promotions (with Consent)**

If you have given your consent, or where permitted under applicable law, we may use your data to provide you with information about updates, promotions, and new Services. You can withdraw your consent or update your preferences at any time.

3.4.1.9. **For Record Keeping and Risk Management**

We retain Personal Data as part of our internal record-keeping obligations, audit trails, and risk assessment frameworks for a retention period of 8 years. This supports operational transparency and compliance with existing standards and the Retail Payment Activities Act ("RPAA").

3.4.1.10. **To Enrich and Maintain Data Accuracy (with Consent)**

With your explicit consent, we may use the Personal Data you provide (for example, through a "Contact Us" form or similar interaction) to enrich, supplement, and verify our records.

We use Apollo.io, a third-party data enrichment service provider, who acts as a data sub-processor on our behalf and processes Personal Data strictly in accordance with our instructions. This process enables us to maintain accurate, complete, and up-to-date information about clients and potential clients in our system, supporting improved communication and service delivery.

Consent is obtained through a tick-box at the point of data submission and is recorded in our system as part of our audit trail. You have the right to withdraw your consent to

data enrichment at any time, without affecting the lawfulness of any Processing carried out prior to withdrawal.

Any data obtained through enrichment is treated in the same way as Personal Data you provide directly, and remains subject to your rights of access, rectification, erasure, restriction, and portability under applicable Canadian privacy laws, including PIPEDA.

We take care to engage only reputable service providers, such as Apollo, and require that they comply with Data Protection laws. However, Deus X Pay is not responsible or liable for any unlawful actions, misconduct negligence or data breaches committed by Apollo or any third-party provider outside of our control, including, but not limited to, the theft, misuse, or unauthorised disclosure of Personal Data.

3.4.1.11. **For Internal Administrative Purposes**

We process data for internal non-marketing purposes, such as audits, record-keeping, troubleshooting, and risk management, based on our legitimate interests.

3.4.1.12. **For Legal Claims and Dispute Resolution**

We may process your Personal Data as necessary to establish, exercise, or defend legal claims or to protect our rights and interests.

3.4.2. We do not use your Personal Data for automated decision-making or profiling that produces legal or similarly significant effects without your explicit consent or a lawful basis under applicable Canadian privacy laws.

3.4.3. We do not retain your data indefinitely. We undertake periodic reviews to ensure that any Personal Data no longer required for the purposes for which it was collected is securely destroyed or deleted.

3.4.4. However, we may be required to retain certain Personal Data for specified periods to comply with applicable laws and regulations, such as record-keeping obligations for income tax, audit purposes, or other legal requirements.

3.4.5. The duration for which we retain different types of data may also be governed by specific business-sector requirements, contractual obligations, or agreed practices.

3.5. **Data Sharing with Third Parties**

3.5.1. We do not sell or rent your Personal Data to third parties. We may, however, share your information with carefully selected third parties, but only when such sharing is necessary, lawful, and proportionate to the purpose for which the data was collected.

3.5.2. We ensure all third-party recipients are bound by appropriate confidentiality and data protection obligations, in compliance with the Data Protection Laws. Instances where we may share your Personal Data include, but are not limited to, the following:

3.5.2.1. **Regulatory and Legal Obligations**

We may share your Personal Data with regulatory authorities, law enforcement agencies, tax authorities, courts, or other governmental bodies when required to do so by applicable Canadian law, regulation, court order, or legal process. This includes compliance with AML, CTF, and KYC regulations.

3.5.2.2. **Service Providers and Sub-Processors**

We engage trusted third-party service providers/processors to support our operations and deliver our Services. These third parties may process Personal Data on our behalf and are contractually bound to comply with strict confidentiality and data protection obligations, in accordance with applicable Canadian privacy laws. Service providers may include:

- Identity verification and KYC/AML compliance platforms;
- Cloud hosting and data storage providers;
- Payment processors and banking partners;
- Security and fraud prevention services;
- IT and technical support vendors; and
- Email, communication, and analytics platforms.

3.5.2.3. **Business Transfers**

In the event of a merger, acquisition, reorganisation, or sale of all or part of our business, your Personal Data may be transferred to third parties as part of the transaction. In such cases, we will ensure the confidentiality of your Personal Data is maintained and provide notice before any change in ownership or control.

3.5.2.4. **Group Companies and Affiliates**

If applicable, we may share your Personal Data with affiliated companies within our corporate group where necessary for legitimate internal business and administrative purposes, consolidated reporting, regulatory compliance, or delivery of joint services. All intra-group transfers are governed by the appropriate safeguards.

In the case of cross-border transfers, such sharing will be carried out consistent with PIPEDA's accountability principle, and any applicable safeguards required for international data transfers.

3.5.2.5. **With Your Consent**

Where required by law, we will obtain your explicit consent before sharing your Personal Data with third parties for purposes not covered by this Privacy Policy, such as for direct marketing by a third party.

3.5.2.6. **Links to other Websites**

Our Website may connect to various social media sites or apps, including Facebook, LinkedIn, and Instagram. If you want to use our Website for social media integration, including creating user-profiles and login functionality, we will share your information with the relevant social media sites or apps.

This Website may include links to other affiliated and unaffiliated sites such as Twitter, Instagram, and LinkedIn. Those websites will have their own privacy policies that you may wish to review. We have no responsibility for unaffiliated linked websites or any use of those sites and their privacy practices. This Website may also contain links to our presence on various social media platforms. As we do not operate or control such platforms, this clause does not apply to your use of such platforms.

3.6. **Data Storage and Protection**

3.6.1. We take the security and privacy of your Personal Data seriously. In compliance with the Data Protection Laws, we implement appropriate technical and organisational measures to ensure the confidentiality, integrity and availability of your data throughout its lifecycle.

3.6.2. The Personal Data we collect from you may be transferred to, stored and processed outside of the jurisdiction in which you live. The laws of those countries may vary from the laws applicable in your own country. Data gathered in Canada may be transferred to, stored and processed at a destination(s) outside of Canada. Unless otherwise indicated, where your Personal Data is transferred out of the jurisdiction of which it is collected, including jurisdictions that may not provide the same level of data protection as Canada, DXP will ensure that such Personal Data will continue to be protected by a standard of protection that is comparable to the protection the personal data would have had been under in the jurisdiction that it was originally collected.

3.6.3. We will not collect, use or disclose sensitive information (such as information about racial or ethnic origins or political or religious beliefs, where relevant) except with your specific consent or in exceptional circumstances permitted by law.

3.6.4. Accordingly, we will take all reasonable steps to prevent unauthorised access to, or disclosure of your Personal Data. Although absolute security cannot be guaranteed on the internet, we have in place up-to-date, reasonable technical and organisational security

measures to protect your Personal Data against accidental or intentional manipulation, loss, misuse, destruction or against unauthorised disclosure or access to the information we process online.

3.6.5. **Data Storage**

Personal Data is stored securely on encrypted servers, located either within Canada or in other jurisdictions, in which case we ensure a comparable level of protection consistent with PIPEDA's accountability principle.

3.6.6. **Technical and Organisational Measures**

To protect your data against unauthorised access, loss, misuse, or alteration, we employ a comprehensive range of appropriate technical and organisational measures, including:

- End-to-end encryption of data in transit and at rest;
- Multi-factor authentication and access controls;
- Secure software development lifecycle practices;
- Regular system monitoring, intrusion detection, and vulnerability assessments; and
- Staff training on data privacy and cybersecurity.

3.6.7. **Internal Access Controls**

Access to Personal Data is strictly limited to authorised employees, contractors, and service providers who need such access to perform their job functions. All personnel with access to Personal Data are bound by confidentiality obligations.

3.6.8. **Incident Response**

We maintain an internal incident response plan to address any potential data breaches. In the event of a security incident involving your Personal Data, we will notify you and report the incident to the OPC where required under PIPEDA, without undue delay, where the breach creates a real risk of significant harm to affected individuals.

3.6.9. **Data Minimisation and Retention**

We only collect and retain Personal Data that is necessary for the purposes identified in this Privacy Policy. Data is kept only for as long as required to fulfil these purposes or to meet legal, regulatory, and operational obligations. Once data is no longer needed, it is securely deleted or anonymised.

3.6.10. While we cannot ensure or warrant the absolute security of any Personal Data you provide us with, we will continue to maintain and improve these security measures over time in line with legal and technological developments. We have put in place procedures to deal

with any suspected Personal Data breaches and will notify you of a breach where we are legally required to do so.

3.7. Your Data Protection Rights

3.7.1. As a data subject under PIPEDA, you have a range of rights concerning how your Personal Data is collected, used, and stored. We are committed to upholding these rights and facilitating the exercise of them. You may contact us at any time to make a request regarding your Personal Data, and we will respond in accordance with applicable legal requirements. As a data subject and a user of our Services, you have the following rights in terms of PIPEDA:

3.7.1.1. **Right of Access**

You have the right to request confirmation of whether we process your Personal Data and, if so, to receive a copy of the data along with information about how and why it is processed.

3.7.1.2. **Right to Rectification**

If your Personal Data is inaccurate or incomplete, you have the right to request that we correct or update it without undue delay.

3.7.1.3. **Right to Erasure**

You may request the deletion of your Personal Data in certain circumstances, such as when the data is no longer necessary for the purposes for which it was collected, or when you withdraw consent and no other legal basis for processing exists. Take note that we may retain data where required for legal or regulatory reasons.

3.7.1.4. **Right to Restriction of Processing**

You have the right to request that we restrict the Processing of your Personal Data in specific situations. For example, if you contest the accuracy of the data or object to Processing while we verify legitimate grounds.

3.7.1.5. **Right to Object**

You have the right to object to the Processing of your Personal Data where Processing is based on our legitimate interests or is carried out for direct marketing purposes. We will respect your objection unless we have compelling legitimate grounds to continue Processing.

3.7.1.6. **Right to Withdraw Consent**

Where we rely on your consent to process your Personal Data, you may withdraw that consent at any time. Withdrawal does not affect the lawfulness of any Processing carried out before consent was withdrawn.

3.7.1.7. **Right to Lodge a Complaint**

If you believe we have violated your rights or mishandled your data, you have the right to file a complaint with the OPC, or any applicable provincial privacy commissioner.

3.7.2. We only process your Personal Data in compliance with this Privacy Policy and in accordance with the Data Protection Laws.

3.7.3. If you wish to raise a complaint regarding the Processing of your Personal Data or are unsatisfied with how we have handled your Personal Data, you have the right to lodge a complaint with the supervisory authority in your country.

4. **REVISIONS TO THIS POLICY**

4.1. We reserve the right to revise, update, or amend this Privacy Policy at any time to reflect changes in our practices, legal obligations, or the functionality of our Services. Any modifications will take effect upon publication of the updated Privacy Policy on our Website, unless otherwise required by applicable law.

4.2. Where required by applicable law or where the changes are material, we will notify you in advance through appropriate means, such as by email or via a prominent notice on our platform. We encourage you to review this Privacy Policy periodically to stay informed about how we protect your Personal Data.

4.3. Your continued use of our Services after any changes to this Privacy Policy constitutes your acceptance of the revised terms.

5. **CONTACTING US**

5.1. We have appointed a data protection officer ("**DPO**").

5.2. All enquires relating to the processing of Personal Data and this Privacy Policy can be addressed to our DPO at security@deusxpay.com.

5.3. When contacting our DPO, please state that your enquiry relates to DXP, and please refrain from enclosing any sensitive information along with your request.