Data Storage Policy

This Data Policy (hereinafter the Policy) is prepared by NEXT SOLUTIONS CORP., a company established under the laws of the Canada under a Company registration number 1001042225, Legal address: 155 East Beaver Creek Road, Suite 24-147, Richmond Hill, Ontario, L4B2N1, Canada., hereinafter referred to as " NEXT SOLUTIONS CORP." or "Company".

1. INTRODUCTION

1.1. When visiting the website through which provides services companies of NEXT SOLUTIONS CORP. (hereinafter when referring to the company, the terms “The Company”, “we” and “us” are used), when you write to us or establish a relationship with us as a client or a partner, we process your data as a data controller.

1.2. This Policy contains our current principles and obligations for data protection and storage. We strive to collect and process only such data that is strictly necessary in the context of our relationships with (potential) clients, (future) partners, users / visitors of our website(s) and online resources in order to provide services and / or information for specific and legal purposes.

The Company is committed to protecting the confidentiality of the information in its possession and to ensuring the proper use and protection of personal data in a transparent manner and in compliance with individuals’ rights under the applicable Canadian data protection laws, including the Personal Information Protection and Electronic Documents Act (PIPEDA) and relevant provincial privacy legislation.

We post this Policy in the most recent version on our website through which the Company provides services. Please read it carefully. It contains information about how we collect, use, transfer and protect the personal data we receive.

2. GENERAL CONDITIONS

2.1. This Policy should be read in the context of the terms of service/product (if applicable) provided by the Company, and should also apply to the use of our website and online systems in accordance with the relevant terms.

2.2 This Policy applies to the personal data stored by the Company as a data controller and as described in this document. It contains information about:

- The personal data we collect;

- The way we use the personal data;

- To whom the personal data may be transferred;

- What rights are granted to the Company.

2.3. This Policy is addressed to individuals ("data subjects") in the context of the relationship that arises between the Company and its clients, in which individuals are:

- Directors, signatories, representatives, shareholders, beneficial owners, secretaries, officers, employees of legal entities who are current or potential or former clients.

- Representatives of legal entities / clients, who have applied to the Company for a service / product offered by the Company, are users of the Company's service / product, website or online system (for example, Internet banking).

2.4. In this Notice, the "Personal Data "(also the "personal information", the "information", the "data") refers to the information that already identifies you or may identify you in the future (for example, your name, address,

identification number). "Processing" of the personal data means such actions as collection, processing, storage and protection of the personal data.

2.5. Some links on the Company's websites may contain links to websites not owned by the Company, or areas with their own data protection policies, which may differ from our Data Protection Policy. Before using other sites or areas, make sure that the relevant policies of other organizations are acceptable to you. The Company does not accept any responsibility for third-party websites. In addition, if you are not the data subject to whom this Policy is addressed, please read the privacy policy of the relevant person who controls your personal data to learn more about how this subject processes it.

3. REQUIRED PERSONAL DATA

3.1. Establishment and legality of a contractual relationship and provision of services between the Company and its Clients depend on provision of the information requested by the Company, which includes the personal data of the data subjects. We try to receive only the minimum necessary data from you. You must provide us with your personal data:

- In accordance with our legal obligations arising from the applicable Canadian anti-money laundering and counter-terrorist financing legislation, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA) and related regulations, which require us to identify you, verify your identity, and conduct a comprehensive or enhanced due diligence check where applicable, as well as to fulfill our other legal obligations under Canadian law.

- For contractual purposes. Establishment of a business relationship to provide services, performing transactions, and fulfillment of contractual obligations between both parties (the Company and its Clients) require provision of the certain personal data.

3.2. The personal data is requested before establishment and during validity of the contractual relationship. Failure to provide us with the requested data means that we will not be able to enter into a contract (establish a business relationship) or provide a service without the requested data, or that we will no longer be able to keep the existing relationship and provide the services and are forced to terminate a business relationship.

4. COLLECTION AND USE OF PERSONAL DATA

COLLECTION TOOLS - HOW WE COLLECT DATA

3.2. We collect the personal data from the following main sources:

PROVIDED DATA

This category includes:

a) Data provided by you (or a representative about you) during registration of an account and during a business relationship, via application forms, by email or via forms available on our website, or via other means of communication. In some cases, you may have previously provided your personal data to the Company (for example, in the context of the existing or former relationship). By submitting personal data to the Company, you also acknowledge that the Company may use this data in accordance with this Policy.

b) The data we collect when you use our services. This data may include:

- The payment and transaction data;

- The profile data (for example, data when connecting to Internet banking, SMS services, and data about how you use the services. We may collect data from devices that you use to connect to our services, such as computers and mobile phones, for example by using your IP address and cookies (see the Cookie Policy available on our website).

THIRD-PARTY DATA

Data that we legally receive from other organizations, such as service providers, information collection agencies, government agencies, individuals who refer you to us, companies in our Group, companies that process payments.

PUBLIC DATA

Databases and publicly available sources (for example, company registrars, commercial registries, mass media, the Internet).

4.2. As a rule, the provided data is the main source and tool of collecting data; this data is provided by you / about you during establishment of a business relationship and during it. Data generated from other sources is mostly based on / is a result of the data from the main source.

TYPES OF INFORMATION - WHAT WE COLLECT / PROCESS

4.3. Different types of the personal data are collected and processed in the context of the relationship that arises between you and the Company, depending on the services / products used and your capabilities. The following are approximate examples of categories and types of the personal data that may be processed:

Individual personal information. For example, name, surname, place of birth, language, information about whether you hold a prominent public position (PEP), residence permit.

Individual personal contact details. For example, work address, home address, email address, phone number.

Identification information. For example, passport or national identity card, citizenship, utility bill, tax residency and tax ID.

Financial information. For example, disclosing income, assets, financial position, source of origin of funds, personal bank details, professional status, employment, employer data, level of education, ownership of property, personal investments and income, loans, copies of settlement statements, tax returns and certificates of creditworthiness.

Authentication. For example, signatures samples, usernames and passwords. Personal data that we collect to identify the user (customer).

Connection. You can provide by filling out forms or contacting us (for example, sent to us in letters, emails, via our electronic channels).

Transaction and location information, as well as technical information. For example, the data required to perform payment transactions (including such data as date, time, amount, currencies, recipient data, location information, and merchant / ATM data associated with the transaction), additional / supporting documentary evidence related to the transactions, details arising from contractual obligations between the Company and Clients. Location data (for example, during a login or transaction); technical information about the devices and technologies you use, IP addresses and device information, visitor information and similar information collected automatically.

Publicly available data. For example, detailed information about you from public sources, the media, and information available on the Internet.

Documentary data. Detailed information about you stored in documents of different formats or copies of them.

Investigation data / results of due diligence and enhanced verification. For example, due diligence checks, AML checks, information for detecting and suppressing fraud. We may also collect data on criminal convictions and offenses (a special category of data) as part of regulatory compliance measures, as well as other supporting documents and personal data related to the

above categories.

Images. For example, from video surveillance systems (CCTV) in our offices (which can collect your photos or videos).

Approval. For example, any permissions or consents you provided to us.

PURPOSES FOR WHICH WE USE YOUR PERSONAL DATA

4.4 Your data is processed in accordance with the principle of data minimization. We strive to limit processing of your data and the type of the data processed strictly to the data that is legally necessary. The Company uses the data, in particular, for:

- Identity verification (for example, authentication, AML goals, and fraud prevention goals);

- Providing the requested services (for example, conducting business relationship procedures, opening an account);

- To provide communication channels (for example, online systems);

- To perform transactions;

- To fulfill obligations to act in accordance with legal instructions;

- To fulfill our contractual obligations;

- For conducting checks and assessments to control money laundering and financing of terrorism;

- In order to prevent crime and / or cooperate with the authorities;

- Analytics and statistics for internal purposes and improvement of the services and the website;

- To keep in touch with you and provide you with up-to-date information;

- To provide ongoing support, handle requests, complaints, and similar issues;

- To provide information about requested / provided products and services;

- To provide information about products / services (this may be advertising / marketing);

- To ensure compliance with internal procedures and measures for fraud, risks and financial crimes protection,

- For legitimate reporting;

- For internal operational support and administrative purposes (e.g. product development, audit, risk management);

- To receive reports on network problems (for example, with our website / online services);

- To perform general administrative functions (for example, maintaining our internal records necessary to update information in our systems, general accounting);

- To comply with our legal obligations and regulatory framework;

- To ensure or protect the rights of the Company or members of the group of companies;

- To ensure security and business continuity;

- To manage the quality of service and improve the product.

LEGAL BASIS FOR DATA PROCESSING

When processing your personal data, we will rely on one of the legal bases of processing specified below. We may process your personal data for several legitimate reasons, depending on the specific purpose for which we use your data.

4.5.1 PERFORMANCE OF CONTRACT

The processing of personal data is necessary to fulfill our obligations under the contract (for the provision of services) concluded with you, as well as during the application process, so that we can complete the client verification process in order to be able to enter into the contract.

4.5.2. FOR LEGAL OBLIGATIONS OR IN INTERESTS OF COMPANY

When we are required to process your personal data in accordance with a legal obligation. The Company is subject to various legal obligations, legal and regulatory requirements, including the Proceeds of Crime (Money Laundering) and Terrorist Financing Act (PCMLTFA), its associated regulations, and other applicable federal and provincial legislation in Canada. We are also obliged to comply with the regulations, guidance, and directives of supervisory authorities, including the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC) and other relevant Canadian financial regulatory authorities. The purposes of processing include identity verification, preventing money laundering, terrorist financing, and fraud, complying with our reporting obligations, tax obligations, risk control measures, and providing information to a competent authority, government agency, or law enforcement agency.

4.5.3. LEGITIMATE INTERESTS

If necessary, we may process personal data if we or a third party have a legitimate interest in pursuing commercial and business interests, unless such interests overlap with your interests, fundamental rights and freedoms.

4.5.4. YOUR CONSENT

In certain circumstances, we may ask you for specific permission to process your personal information for the certain purposes. Your data will be processed in this way if you agree to it. If the legal basis is your consent, you can withdraw your consent at any time. Revocation of your consent will not affect the legality of receiving data already processed before revocation.

5. DATA RETENTION PERIOD

5.1. Our retention period is primarily determined by our obligations under applicable law to store the data for the certain period. Destruction is not possible before this period expires. We are required to store the Client's data (including the personal data) during the existence of the contractual relationship and for at least 10 years after its termination (the last transaction) in accordance with AML legislation, unless legal or regulatory acts prohibit us from destroying the data.

5.2. The retention period may be extended in the case of other legitimate reasons justifying longer retention (for example, for complaints, court proceedings, investigations of tax crimes, violations/crimes in the field of money laundering and terrorist financing, and the prevention of crime and fraud).

5.3. For potential clients, the personal data will be stored for up to one year from the date of notification of rejection of an application for services and establishing a business relationship or data on the withdrawal of the application, unless legal or regulatory reasons prohibit us from destroying the data or there is another legitimate reason justifying longer storage (for example, for handling complaints, legal proceedings, investigations of tax crimes, violations/crimes in the field of money laundering and financing of terrorism, and prevention of crime and fraud).

6. WHO GETS ACCESS TO YOUR PERSONAL DATA

6.1. The Company receives your personal data in the context of the Company's own activities. This is required to fulfill requests and provide services, as well as to fulfill our contractual and legal obligations.

6.2. We will not transfer the personal data to third parties, except when it is necessary for our legitimate business needs, to fulfill requests, provide services and / or in accordance with the requirements of the law. Third parties in these circumstances include:

6.2.1. SERVICE PROVIDERS. We will disclose personal data to third-party partners and service providers (processors) so that they can process it on our behalf if necessary (for example, in the process of verifying the validity of the document provided). These service providers must provide sufficient guarantees in accordance with the Data protection Act (for example, contractual obligations for confidentiality and data protection). We will only share the personal data that they need to provide their services.

6.2.2. AUDITORS, ADVISORS AND CONSULTANTS. We may disclose personal data for the purposes and in the context of an audit (for example, an external audit, a security audit), to legal and other consultants to investigate security issues, risks, complaints, etc.

In this way, the personal data may be transferred and disclosed to:

- Money Laundering, Financing of Terrorism and Fraud Prevention Agencies, compliance/verification services, and risk prevention services. This is necessary to verify your identity, provide protection against fraud, and confirm your right to use our services/products.

- for Banks (other credit and financial institutions) and similar institutions. They allow us to provide our services and include correspondent banks and intermediary banks.

- for Payment systems (SWIFT, SEPA, Visa, MasterCard, JCB, Unionpay and other), payment service providers, processing companies. This allows us to provide our services.

- for Cloud storage, archiving, and data management service Providers.

- for Companies that assist us in providing our services (for example, providing technology services, solutions, support, such as support/maintenance/development of IT applications, technologies, website management, telephony/SMS services).

- for Customer support service Providers and marketing service providers.

- for Companies that are affiliated/related to us, acting as processors or supervisors for the purpose of providing services, optimized services, ensuring quality and efficiency throughout the group.

- for administrative service Providers.

- for obtaining audit and accounting services.

- for legal consultants.

6.2.3. **REGULATORY AUTHORITIES, LEGISLATION, COURTS.**

We may disclose personal data in accordance with applicable Canadian laws and regulatory obligations, and to respond to requests from regulatory authorities, government and law enforcement agencies, and courts in Canada and internationally, for example:

- Supervisory authorities, including the Financial Transactions and Reports Analysis Centre of Canada (FINTRAC), the Office of the Superintendent of Financial Institutions (OSFI), and provincial financial regulatory authorities;
- The police and other law enforcement agencies;
- Tax authorities, including the Canada Revenue Agency (CRA);

Other regulatory bodies, authorities, and public authorities where there is a statutory obligation to do so.

6.2.4. Other recipients may be any individual / legal entity / organization for which you request your data or give your consent to the transfer of personal data.

6.2.5. We may also disclose your data in the following cases:

If we are required to disclose or share your personal data in order to comply with any legal or

regulatory obligations or requests;

- To enforce or enforce the terms or any other agreement in force in the context of our relationship, and to investigate potential violations;

- To protect the rights, security or property of the Company, our customers or third parties / society. This includes sharing information with other companies and organizations in order to prevent money laundering, fraud prevention, and equivalent risks;

- If the Company or almost all of its assets are acquired by a third party, in this case, the personal data about its Clients stored by it will be one of the transferred assets.

TRANSFER OF DATA OUTSIDE EEA OR TO INTERNATIONAL ORGANIZATIONS

6.3. Your personal data may be transferred to third countries (outside the EEA) or to international organizations if you have given your consent to the processing of your data and the transfer is necessary and has a legal basis, as described in this document. Such a transfer takes place, for example:

- If necessary, and in the context of transactions (for example, card transactions, payment orders to third countries, via a correspondent bank in a third country);

- In accordance with current legislation (for example, tax legislation);

- Based on your instructions or consent;

- In the context of data processing carried out by third parties on our behalf (for example, data may also be processed by employees working outside the EEA who work for the Company, one of our third-party service providers. Such personnel may perform technical and support duties, duties related to processing your orders, providing support services, etc.).

6.4. Controllers in third countries in this case must be approved by the European Commission, which must provide an adequate level of data protection or must have appropriate guarantees with the level of data protection in the EU.

We strive to take all reasonably necessary steps to ensure the safe handling of your data in accordance with this Policy (for example, the requirement to comply with privacy standards equivalent to ours, compliance with security standards and procedures to prevent unauthorized access to data, the use of technologies such as encryption and firewalls to protect data during transmission and storage).

7. DECISION-MAKING AUTOMATION AND PROFILING

7.1. Automated decision-making means the process of making decisions using automated tools of processing the personal data without personal intervention. When establishing and maintaining business relationships, we usually do not use automated decision-making.

7.2. We may process the certain specific data automatically, using systems to automatically make suggestions or solutions, including profiling, based on information we have or collect from other authorized sources. This helps us to ensure that we can respond quickly and effectively to protect our clients.

Automated decisions that we can make include:

Fraud detection: we are obliged to take measures to combat money laundering and fraud. We may use your personal data to determine whether an account / payment instrument is being used for fraud or money laundering / terrorist financing purposes or sanctions violations. Such assessments are conducted to help us determine whether the account / payment instrument is being used for fraudulent activities or in a way that is unusual for you or our Client's business. If we determine that there is a risk of fraud, unauthorized use, or unusual activity, we may terminate the account and / or deny access to it.

8. WEBSITE AND AUTOMATIC COLLECTION-COOKIES AND IP ADDRESSES

8.1. The Company's website contains forms that can be used by visitors of the website. When visitors of the site send us information online via the forms on the website, in the context of providing the services, the information will be used for the purposes and in the ways set out in this Policy.

8.2. In some cases, the Company and other entities (for example, service providers) may use cookies and other technologies to automatically collect certain types of data when you visit the Company's websites and online platforms. The collection of this data allows the Company to improve the security and usability of websites and online resources, as well as to measure the effectiveness of marketing activities. We may collect information about your computer or mobile device (including, for example, the type of operating system and browser) for system administration.

For more information about cookies and the purposes for which we use them, see our Cookie Notice available on our website.

8.3. An IP address is a number assigned to your computer when accessing the Internet, which allows computers and servers to recognize and communicate with each other. The IP addresses of website visitors can be recorded for IT security and diagnostic purposes. This information can also be used in aggregated form to analyze trends and website performance. In the context of providing services, IP addresses may also be used for fraud prevention purposes.

9. DATA SECURITY INFORMATION

9.1. The Company has established internal security policies and procedures for the secure processing of personal data in order to protect the data from unauthorized access, loss, misuse, alteration or destruction. We try to ensure that access to personal data is restricted to persons other than those authorized to do so, and that those who have access are required to maintain their confidentiality. We use a number of technologies and security solutions to protect your data (for example, pseudonymization, storing the information you provide to us on secure servers in the EEA, using perimeter security mechanisms such as encryption, etc.). However, despite our best efforts, we cannot fully guarantee security against all threats.

9.2. The transfer of information by the Internet is not completely secure. We cannot fully guarantee the security of the data transmitted to us by email, to our website or online resources.

9.3. If you have access to our resources through means of user authentication (for example, user credentials), you are responsible for ensuring the security and confidentiality of your credentials and should not disclose them to third parties.

10. YOUR RIGHTS

RIGHTS OF DATA SUBJECT

10.1. Since most of processing of the personal data performed by us is the result of legal obligations, some of the rights may be limited by our legal and regulatory requirements or legitimate interests. You have the right to:

10.1.1. Obtain a copy of your stored personal data (the" Right of Access") provided to us.

10.1.2. Request the correction of incorrect or incomplete data about you stored by us. In this case, we may need to verify the accuracy of the data available and provided, and take steps to correct our records.

10.1.3. Right to object. You may object to our processing of personal data and require us to stop using the data in certain circumstances, such as:

- The processing is performed legally under legitimate interests or in the public interest, but

you object for reasons related to your specific situation. In such a case, we may continue processing if we demonstrate that we have a valid legal basis for processing that restricts your rights, or that the processing is necessary to establish, exercise, or defend a legal claim.

Please note that, despite your objection, we may continue to use your personal data. This happens in cases where the processing is required in accordance with the legal obligations imposed on us (the requirements of the legal obligations for processing and storing data cancel any right to object).

- The processing is performed for marketing purposes.

In the certain circumstances, if you object to the processing of certain personal data, we will not be able to provide you with the services and may need to stop providing the services.

10.1.4. Right to delete. You can request the deletion of your personal data (depending on the circumstances where:

- Processing is no longer required for the reasons why the data was collected or processed;

- We rely on consent as a legal basis, and you withdraw your consent;

- Did you object to the processing of the data;

- The data was processed without legal grounds;

- Data deletion is required by law.

We may continue to store your data if there is another legitimate reason to do so. Our compliance requirements with legal obligations (in particular record-keeping requirements) to process and store certain data will replace any right to request deletion, and we may also continue to store / use your data if there is another legitimate reason for doing so (to comply with legal requirements and / or act in the public interest).

10.1.5. Restriction of the processing of the personal data. You may request that we restrict / suspend the use of your personal data if:

- You have requested that we verify the accuracy of your personal data that we have;

- Processing is not required by law, but you do not request its removal;

- We no longer need to process and store the data, but you want us to keep it, because you need this data to establish, perform or defend a legal claim.

- You object to the processing of the data and expect confirmation of our primary legitimate interests.

In some cases, the restriction may prevent the Company from fulfilling its obligations under the contractual relationship with the Client. In this case, we will notify the Customer accordingly.

10.1.6. Withdrawal of consent. If we rely on the legal basis of your consent (i.e. we have requested and you have provided your consent), you can withdraw your consent at any time.

We may continue to process your data if there is another legitimate reason to do so. If we are unable to provide you with services due to withdrawal of consent, we will notify you.

10.1.7. Data portability. You can request that we provide your personal data directly to you in a format that is convenient for reuse, or to a third party, if technically possible.

This right applies only to personal information that you have provided to us in order to fulfill a contractual relationship with us or that we process based on your consent. This right may not be fully applicable in cases where the processing is performed in connection with a legal obligation of the Company.

EXERCISE OF YOUR RIGHTS

10.2. Please contact us directly using the contact details provided below to exercise your rights or if you have any questions about the use of your personal data.

10.3. You may be a subject to identification procedures and measures to ensure that no personal data is disclosed to third parties. We may also request additional information / clarification to process your request as quickly and efficiently as possible.

10.4. All requests must contain a clear description of the object of the request in the language provided on our website. We will not be able to handle incomprehensible requests.

10.5. We usually do not charge for access to your personal data (or for exercising other rights). We may charge you if your request is manifestly unreasonable, excessive, or repetitive. Alternatively, we may reject such a request as manifestly or unduly burdensome, unreasonable, and unfair.

10.6. Depending on the complexity of your request and the amount of data associated with it, we will strive to satisfy all legitimate requests within one month from the date of receipt or to inform you of the refusal, or to extend the period to three months to satisfy your request. We will notify you accordingly if it takes more than one month to complete your request.

RIGHT TO MAKE COMPLAINT

10.7. If you have any complaints about the use of your data, the exercise of your rights, please report and / or submit a complaint to us directly using the contact details provided below. We will review your complaint and inform you of the outcome of the review.

10.8. Complaints must be written in the language provided on our website exhaustively, contain sufficient details and a clear description of the complaint. We will not be able to process incomprehensible requests or complaints.

10.9. You may also make a complaint with the Data Protection Commissioner. Information about the submission is available on the Commissioner's website.

11. CONTACT DETAILS OF AUTHORIZED PERSON

Support service email indicated on the website through which the company provides the service.

12. YOUR RESPONSIBILITIES

12.1. You are responsible for ensuring that the set of information provided to the Company by you / about you or about the person you represent is accurate and up-to-date, and you must inform us if anything changes as soon as possible.

12.2. If you provide information about another person, you must inform them of this Policy and ensure that they also agree to the Company's use of their information as described in this Policy.

13. GENERAL TECHNICAL ISSUES OF DATA PROTECTION AND STORAGE

13.1. The main database (hereinafter DB) of the system is deployed on the PostgreSQL DBMS and is hosted on AWS RDS resources. The database for storing personal user information is deployed on the PostgreSQL DBMS and is hosted on AWS RDS resources that are separate from the main database of the system.

13.2. All web-interfaces of the system are scalable to provide load capacity and to protect against attacks. The servers for the web interfaces are separate from the rest of the system servers. The data transferred from the Web interface of the client is protected by SSL.

13.3. Data carriers containing the user data are encrypted. All data carriers containing the data about clients and their transactions have 2 independent backups. All backups are encrypted.

13.4. All backups are stored in different buildings and well-protected areas. Access to the premises with backup copies of authorized persons is strictly limited.

13.5. The computers providing access to the system servers are protected by external tools of

information protection, the servers are equipped with tools of information protection for unauthorized access. The computers providing access to the system servers are set in well-protected premises. Access of authorized persons to these premises is strictly restricted.

14. CHANGES TO OUR PRIVACY NOTICE

14.1. We may revise or update this Policy from time to time. In this case, we will post the most recent version of the Policy on our website, informing you of this by displaying the updated version and the relevant update date.

14.2. We recommend you to visit our website more often to review the latest version of our Data Protection and Storage Policy.

Effective as of August 5, 2025

NEXT SOLUTIONS CORP.
155 East Beaver Creek Road, Suite 24-147,
Richmond Hill, Ontario, L4B2N1, Canada

CEO

Vladimir Kochenov