



+1 (613) 701-1502



[nmbolutions.ca](http://nmbolutions.ca)



1000 Innovation Dr Suite  
500, Ottawa, ON K2K 3E7

## DATA PROCESSING EXHIBIT

### FOR NMB SOLUTIONS CUSTOMERS

NMB Solutions Inc., NMB Solutions Ltd. or one of its affiliated companies ("**NMB Solutions**") and Customer have entered into a **Software License and Services Agreement** or other master agreement (as may be amended by the parties, the "**Agreement**") pursuant to which NMB Solutions and its affiliates may Process (defined below) or store certain Customer information on behalf of Customer in connection with NMB Solutions' supply chain software and services. This Data Processing Exhibit ("**DPA**") forms part of such Agreement and describes additional specific data transfer and processing requirements (including, without limitation, data protection, security and privacy compliance requirements). Capitalized terms not otherwise defined herein shall have the meaning set forth in the Agreement. Except as modified below, the terms of the Agreement shall remain in full force and effect.

**NMB Solutions Data Protection Contact:** NMB Solutions, ATTN: Nada Mahfouz  
1000 Innovation Dr Suite 500  
Ottawa, ON CANADA K2K 3E7  
[support@nmbolutions.ca](mailto:support@nmbolutions.ca)

**STANDARD CONTRACTUAL CLAUSES:** If this box is checked, the contractual clauses set out in **Schedule 1** ("**Standard Contractual Clauses**"), which are pursuant to the European Commission's decision (C(2010)593) of 5 February 2010, are incorporated herein and apply to the Processing of Personal Data of residents of the European Union or Switzerland by NMB Solutions in the course of providing services to Customer under the Agreement. The parties hereby agree that if a new version of the Standard Contractual Clauses is officially and formally adopted by the EU Commission pursuant to Article 28(7) of the GDPR, such new version shall automatically, and without further action of the parties, replace the current version of the Standard Contractual Clauses in Schedule 1, unless either party objects to such amendment by written notice to the other party, within ninety (90) days after the official public announcement of such adoption by the EU Commission.

#### 1. Definitions

1.1 In this DPA, the following terms shall have the meanings set out below:

1.1.1 "**Personal Data**" means any Personal Data relating to an identified or identifiable



- 1.1.2 natural person (also referred to herein as a “data subject”) that is Processed by NMB Solutions and/or its affiliates for Customer or on behalf of Customer pursuant to the terms of the Agreement. **[Quoted from Art. 4(1)]** Unless otherwise specified by applicable law, hashed, anonymized, encrypted or otherwise obfuscated or de-identified IP addresses and email addresses, device IDs, or machine IDs, or other similarly obfuscated data, and city, regional or country level geo-location information, shall not be deemed to be Personal Data under these Data Processing Exhibit.
- 1.1.3 **“Data Protection Laws and Regulations”** means laws and regulations applicable to the Processing of Personal Data under the Agreement, including laws and regulations of the European Union, the European Economic Area and their member states, Switzerland and the United Kingdom, including without limitation European Union (“EU”) Directive 95/46/EC (**“Directive”**), EU Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**“General Data Protection Regulation”** or **“GDPR”**) and EU Directive 2002/58/EC on Privacy and Electronic Communications (**“e-Privacy Directive”**) or, the superseding e-Privacy Regulation, once effective.
- 1.1.4 **“Processing”** means any operation or set of operations performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction. **[Quoted from Art. 4(2) definition of “processing”]**
- 1.1.5 **“Subprocessor”** means any Processor engaged by NMB Solutions in the provision of the NMB Solutions’ services to Company.

## 2. Protection of Personal Data

- 2.1 Processing by NMB Solutions: NMB Solutions shall Process Personal Data in accordance with Customer’s instructions: (i) solely for the purpose of performing NMB Solutions’ obligations, or as otherwise permitted, under the Agreement and this DPA, and (ii) in compliance with all applicable Data Protection Laws and Regulations. **[Art. 5(1)(b) requires that personal data be collected for “specified, explicit and legitimate purposes and not further processed” in an incompatible manner.]**



- 2.2 Notices and Consents: In connection with use of the NMB Solutions Software and Services (as such terms are defined in the Agreement), Customer shall comply with all applicable Data Protection Laws and Regulations, including: (i) providing all required notices and appropriate disclosures to all data subjects regarding Customer's (and any third parties acting on Customer's behalf, such as NMB Solutions) use, processing and transfer of Personal Data, and (ii) obtaining all necessary rights and valid consents from the data subjects to permit Processing by NMB Solutions of Personal Data for the purposes of fulfilling NMB Solutions' obligations, or as otherwise permitted, under the Agreement and this DPA. NMB Solutions' legal bases for the processing of Personal Data include: (i) consent and/or (ii) any other applicable legal bases, such as a legitimate interest in engaging in commerce, supporting internal business functions, offering products and services of value to customers, preventing fraud, ensuring information and network security, direct marketing and advertising, and complying with industry practices.
- 2.3 International Data Transfers:
- 2.3.1 NMB Solutions may use resources and servers located in various countries around the world, including the United States and other countries. Therefore, Personal Data about individuals or customers may be transferred, processed and stored outside the country where the NMB Solutions products and services are used, including to countries outside the European Union ("EU"), European Economic Area ("EEA") or Switzerland, where the level of data protection may not be deemed adequate by the European Commission.
- 2.3.2 If Personal Data is transferred from the European Economic Area or Switzerland to or by Customer as controller, or by NMB Solutions, as processor and/or subprocessor, to a jurisdiction which the European Commission or, where relevant, the Swiss Federal Data Protection and Information Commissioner, have not determined ensures an adequate level of protection of Personal Data, then either: (a) Customer or NMB Solutions, as applicable, shall subscribe to the appropriate legal instruments for the international transfer of data (such as the EU-U.S. Privacy Shield Framework); (b) NMB Solutions and Customer, or NMB Solutions and NMB Solutions' subprocessor, as applicable, shall execute mutually agreeable contractual instruments, such as the Standard Contractual Clauses (e.g., via the check box above) or (c) NMB Solutions or NMB Solutions' subprocessor, as applicable, shall execute Binding Corporate Rules (BCR) as such BCR are approved by the relevant supervisory authority. **[Arts. 44-49 set forth a regime for export of personal data from the EU.]**
- 2.4 Children; Sensitive Data: Customer will not use the NMB Solutions Software or Services to direct



any products or services to children (as defined under applicable law; for example, under 13 years old in the United States or under 16 years old in certain European countries). **[Art. 9 provides that, where consent is required for online collection of personal data, for a child under 16 (or as little as 13 if mandated by Member State law), consent must be given or authorized by the holder of parental responsibility. In the US, “verifiable parental consent” is required by the Children’s Online Privacy Protection Act. 15 USC §6502(b)(1)(A)(ii).]** Customer will not use the NMB Solutions Software or Services in connection with the collection of sensitive data concerning an identifiable individual, such as racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or an individual’s genetic data, biometric data, health data, or data regarding sex life or sexual orientation. **[Art. 9 prohibits processing such personal data (“special categories”) absent one of 10 enumerated exceptions.]**

- 2.5 Data Subjects & Subject Matter of Processing: The personal data transferred concern the following categories of data subjects: individual customers, employees, contractors, partners and vendors of Customer or Customer’s affiliates, and any other individuals interacting with NMB Solutions’ Software and Services in connection with Customer’s use of such Software and Services, or as otherwise agreed by the parties in the Agreement or otherwise. The subject matter of the Processing of Personal Data is the performance of the services pursuant to the Agreement. Details of the Processing, including information about the duration of the Processing, the nature and purpose of the Processing, the types of personal data and categories of data subjects and data Processed under this DPA are as set forth in the Agreement and any Orders or Statements of Work or similar documents issued by NMB Solutions under the Agreement, this DPA, or as otherwise agreed in writing by Customer and NMB Solutions.
- 2.6 Appointment of Subprocessors. Customer acknowledges and agrees that (a) NMB Solutions affiliates may be retained as Subprocessors; and (b) NMB Solutions and NMB Solutions affiliates respectively may engage third-party Subprocessors in connection with the provision of the NMB Solutions Software and Services. NMB Solutions or a NMB Solutions affiliate has entered into, or will enter into, a written agreement with each Subprocessor containing data protection obligations not less protective than those in the Agreement and this DPA with respect to the protection of Confidential Data (defined below) of Customer to the extent applicable to the nature of the services provided by such Subprocessor. **[Art. 28(4) requires that any processor- subprocessor agreement include the same data protection obligations as are in the controller-processor agreement.]** However, personnel of NMB Solutions, whether employees or contractors, shall not be deemed to be “Subprocessors” for purposes of the following subsections in this Agreement (2.6 and subsequent sections).
- 2.6.1** Upon Company’s request or as otherwise required by applicable Data Protection Laws and Regulations, NMB Solutions shall make available information about



Subprocessors who, to NMB Solutions' actual knowledge, will Process Personal Data of Company, including their functions relevant to the performance of NMB Solutions Services and locations. **[Art. 28(2) prohibits a processor from engaging a subprocessor absent prior specific or general written authorization of the controller.]**

**2.6.2** For the avoidance of doubt, NMB Solutions may continue to use those Subprocessors already engaged by NMB Solutions as at the date of this Agreement. **[Art. 28(4) provides that if a subprocessor fails in its data protection obligations, the processor is fully liable to the controller for performance of the subprocessor's obligations.]**

**2.6.3** NMB Solutions will inform Company of any new Subprocessor who, to NMB Solutions' actual knowledge, will be Processing Personal Data of Company and who is engaged during the term of the Agreement by updating the URL or Customer portal or account information or by email before the new Subprocessor processes Company Personal Data. If Company can reasonably show that the appointment of a new Subprocessor will have a material adverse effect on NMB Solutions' ability to comply with applicable Data Protection Laws and Regulations, then Company must promptly notify NMB Solutions in writing within fifteen (15) business days thereafter of its reasonable basis for objection to the use of a new Subprocessor. Upon receipt of Company's written objection, Company and NMB Solutions will work together without unreasonable delay to recommend an alternative arrangement. If the following conditions apply: a) a mutually acceptable and reasonable alternative arrangement is not found; b) Company has a termination right under applicable Data Protection Laws and Regulations, and c) Company has provided prompt written notice under this Section, then Company may terminate the Service Agreement only with respect to those services that cannot be provided by NMB Solutions without the use of the new Subprocessor. Unless prohibited by applicable Data Protection Laws and Regulations, in the event of such early termination by Company, NMB Solutions can retain or require payment for Services through the end of Company's current contract term for the terminated services.

**2.7** Additional GDPR Requirements: To the extent applicable and required under GDPR, the parties agree to be bound by and comply with the requirements of GDPR Article 28 and any additional GDPR requirements.

### **3. Confidentiality**

Per any confidentiality provisions in the Agreement and any Nondisclosure Agreement



between the parties, NMB Solutions and Customer shall take all appropriate legal, organizational and technical measures to ensure the confidentiality of Personal Data and Confidential Information (as defined in the Agreement or any Nondisclosure Agreement between the parties) of Customer (“Confidential Data”), and protect Confidential Data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, and against all other unlawful forms of Processing, keeping in mind the nature of such Confidential Data. **[Art. 28(3)(b) requires the controller-processor contract to ensure that persons authorized to process the personal data are under a confidentiality obligation.]** Unless otherwise permitted under the Agreement and any Nondisclosure Agreement between the parties, NMB Solutions may only disclose Confidential Data to third parties (including NMB Solutions employees, consultants, contractors, professional advisors or third party service providers) in connection with the provision of the NMB Solutions Software and Services or who otherwise have a legitimate basis for access and have signed agreements that require them to protect confidential information in a manner no less restrictive than the terms hereof, or to third parties as required by law or regulation. NMB Solutions shall hold such third parties with access to Confidential Data accountable for violations of this DPA, including imposing sanctions, and where appropriate and permitted under applicable law, terminating contracts and employment.

#### 4. **Data Integrity**

Promptly upon Customer’s request, or as otherwise may be necessary to comply with the Agreement or this DPA, NMB Solutions shall correct, delete and/or block Personal Data from unauthorized Processing. NMB Solutions shall promptly notify Customer if NMB Solutions receives any requests from an individual with respect to Personal Data, including but not limited to “opt-out” instructions, information access requests, information rectification or erasure requests, data portability requests, and all like requests, and shall cooperate with Customer in responding to any such requests. Customer shall promptly notify NMB Solutions if Customer receives any requests from an individual with respect to Personal Data Processed by NMB Solutions, including but not limited to “opt-out” specifications, information access requests, information rectification requests and all like requests. **[Art. 28(3)(e) requires controller-processor contract to obligate the processor to assist the controller, insofar as possible, to meet the controller’s obligations to respond to requests for exercising the data subject’s rights in Arts. 12-20 (rights to notice, access, rectification, erasure, restriction of processing, and portability).]**

#### 5. **Investigations**

NMB Solutions and Customer shall cooperate and provide each other with reasonable assistance and support in the event of an investigation by a data protection regulator or similar



authority, if and to the extent that such investigation relates to the collection, maintenance, use, processing or transfer of Personal Data under this DPA. **[Art. 28(3)(h) requires the controller-processor contract to obligate the processor to make available to the controller all information necessary to show compliance with the obligations of the processor set forth in in Art. 28 “and allow for and contribute to audits, including inspections....”]** Upon reasonable notice and during normal business hours no more than once per year, and to the extent that such access does not interfere with NMB Solutions’ security measures to protect the confidential information of other NMB Solutions customers or otherwise subject NMB Solutions systems or the NMB Solutions Software and Services to unwarranted security or operational risk, NMB Solutions shall provide to Customer, its authorized representatives and independent inspection body designated by Customer (i) access to NMB Solutions’ information processing premises and records and (ii) reasonable assistance and cooperation of NMB Solutions’ relevant staff for the purpose of auditing NMB Solutions’ compliance with its obligations under this DPA. The cost of any such assistance by NMB in an investigation and/or audit shall be borne by Customer. **[Art. 28(3)(h) requires the controller-processor contract to obligate the processor to make available to the controller all information necessary to show compliance with the obligations of the processor set forth in in Art. 28 “and allow for and contribute to audits, including inspections....”]**

## **6. Notice of Non-Compliance; Duties Upon Termination; Remedies**

In the event that NMB Solutions becomes aware it is unable to comply with the obligations stated in this DPA, NMB Solutions shall promptly notify Customer, and Customer may take any one or more of the following actions: (i) suspend the transfer of Personal Data to NMB Solutions; (ii) require NMB Solutions to cease Processing Personal Data for Customer; (iii) demand the return or destruction of Personal Data of Customer; or (iv) immediately terminate this DPA. Upon termination of this DPA for any reason, NMB Solutions shall promptly contact Customer for instructions regarding the return, destruction or other appropriate action with regard to Personal Data of Customer. **[Art. 28(3)(g) requires the controller-processor contract to state that, at controller’s option, processor must delete or return to controller all the personal data at the end of the provision of services.]**

**NOTWITHSTANDING ANYTHING CONTAINED HEREIN OR IN THE AGREEMENT TO THE CONTRARY, YOUR REMEDIES, AND NMB SOLUTIONS’ OBLIGATIONS, WITH RESPECT TO NMB SOLUTIONS’ BREACH OF THIS DPA, AND THE OVERALL AGGREGATE LIABILITY OF NMB ARISING OUT OF, OR IN CONNECTION WITH, SUCH BREACH WILL BE SUBJECT TO THE AGGREGATE LIMITATION OF LIABILITY THAT HAS BEEN AGREED TO BETWEEN THE PARTIES UNDER SECTION 12 OF THE AGREEMENT (THE “LIABILITY CAP”). FOR THE AVOIDANCE OF DOUBT, THE PARTIES INTEND AND AGREE THAT THE OVERALL AGGREGATE LIABILITY OF NMB SOLUTIONS ARISING OUT OF, OR IN CONNECTION WITH,**



**NMB SOLUTIONS' BREACH OF THIS DPA SHALL IN NO EVENT EXCEED THE LIABILITY CAP. NOTWITHSTANDING THE FOREGOING LIMITATION OF LIABILITY, IN THE EVENT THAT ANY UNAUTHORIZED ACCESS TO, OR ACQUISITION OF, PERSONAL DATA IS DIRECTLY CAUSED BY NMB SOLUTIONS' BREACH OF THIS DPA (A "DATA BREACH"), NMB SHALL PAY THE REASONABLE AND DOCUMENTED COSTS INCURRED BY YOU COMPRISED OF: (A) COSTS OF ANY REQUIRED FORENSIC INVESTIGATION TO DETERMINE THE CAUSE OF THE DATA BREACH, (B) PROVIDING NOTIFICATION OF THE DATA BREACH TO APPLICABLE GOVERNMENT AGENCIES, AND TO INDIVIDUALS WHOSE PERSONAL DATA MAY HAVE BEEN SO ACCESSED OR ACQUIRED, (C) IF APPLICABLE, PROVIDING CREDIT MONITORING SERVICE TO INDIVIDUALS WHOSE PERSONAL DATA MAY HAVE BEEN SO ACCESSED OR ACQUIRED FOR A PERIOD OF ONE (1) YEAR AFTER THE DATE ON WHICH SUCH INDIVIDUALS WERE NOTIFIED OF THE DATA BREACH FOR SUCH INDIVIDUALS WHO ELECTED SUCH CREDIT MONITORING SERVICE, AND (D) OPERATING A CALL CENTER TO RESPOND TO QUESTIONS FROM INDIVIDUALS WHOSE PERSONAL DATA MAY HAVE BEEN SO ACCESSED OR ACQUIRED FOR A PERIOD OF ONE (1) YEAR AFTER THE DATE ON WHICH SUCH INDIVIDUALS WERE NOTIFIED OF THE DATA BREACH. NOTWITHSTANDING THE FOREGOING, OR ANYTHING IN THE AGREEMENT TO THE CONTRARY, NMB SHALL HAVE NO RESPONSIBILITY TO PAY SUCH COSTS THAT ARE DUE TO CUSTOMER'S GROSS NEGLIGENCE, WILLFUL OR RECKLESS MISCONDUCT, OR FRAUD OF CUSTOMER OR ITS EMPLOYEES, AGENTS AND CONTRACTORS.**

## **7. Data Security Procedures**

7.1 NMB Solutions shall maintain reasonable operating standards and security procedures, and shall use commercially reasonable efforts to secure Confidential Data through the use of appropriate administrative, physical, and technical safeguards including, but not limited to, appropriate network security and encryption technologies, including but not limited to the following technologies or any technologies that provide comparable or enhanced protections:

7.1.1 Global Security. NMB Solutions shall require that all NMB Solutions personnel follow the security procedures set forth in NMB Solutions Information Security Exhibit, as referenced in the Agreement and as may be updated from time to time by NMB Solutions. The Information Security Exhibit sets forth NMB Solutions' security protocols.

7.1.2 Network Security. NMB Solutions, and any subcontractors engaged by NMB Solutions (such as any data centers or third party cloud providers such as Microsoft Azure) shall maintain appropriate security protocols, including:



- a) network segmentation, including but not limited to, firewalls, to segregate internal networks from the internet,
- b) intrusion detection and monitoring systems to detect and respond to attacks,
- c) data transfer via secure protocols, such as https, sftp, etc., and
- d) only authorized personnel have access to the credentials that use the data process system.

Customer shall be solely responsible for acquiring and maintaining technology and procedures for maintaining the security of its link to the Internet and Customer connections to the NMB Solutions Software and Services.

7.1.3 Vulnerability and Patch Management. NMB Solutions shall, within a reasonable period, such period depending on the nature and severity of the risk, after any update release, apply manufacturer-recommended security updates to NMB Solutions Software that is presently being marketed and/or supported by NMB Solutions and Processing Confidential Data for Customer or on behalf of Customer. NMB Solutions shall install, within a reasonable period of time after release, any software patches reasonably designated by NMB Solutions as “critical” for the NMB Solutions Software. NMB Solutions shall also conduct periodic vulnerability scans and penetration tests of any network storing or processing Confidential Data, and promptly remediate any identified critical vulnerability NMB Solutions deems commercially feasible to do so.

7.1.4 Access Controls.

- 7.1.4.1 Only personnel that reasonably need to access Confidential Data to operate and perform the NMB Solutions Software and Services shall be granted access thereto. Standard access security protocols shall be implemented, including:
- a) no admittance for unauthorized persons to data processing equipment,
  - b) check of identity cards for admittance to sensitive areas,
  - c) admittance to offices during office hours controlled by personnel,



- d) visitors who have access to physical areas containing Confidential Data shall be appropriately supervised by NMB Solutions personnel,
- e) recording of visitor access,
- f) network segmentation, including firewalls, to segregate internal networks from the internet,
- g) intrusion detection, monitoring, and logging systems to detect and respond to attacks, and
- h) access to the systems containing Confidential Data solely via individual user name and password.

7.1.4.2 If any NMB Solutions personnel no longer need access to Confidential Data, whether because of termination or re-assignment, NMB Solutions shall promptly disable such personnel's privileges to access Confidential Data.

7.1.5 Training. NMB Solutions shall require all NMB Solutions personnel that may have access to Confidential Data to undergo periodic training on commercial best practices for data security.

7.1.6 End-of-Agreement Data Handling. Upon termination or expiration of the Agreement or this DPA, or at any time at Customer's written request, NMB Solutions shall: (i) return to Customer all Confidential Data, including but not limited to, all paper and electronic files, materials, documentation, notes, plans, drawings, and all copies thereof, and ensure that all electronic copies of such Confidential Data are deleted from NMB Solutions' (and where applicable, its subcontractors') systems, except that NMB Solutions may retain a copy of any Confidential Data needed for, billing, invoicing, collections, audits (including any certifications and assessments), or otherwise required for compliance with applicable laws; or kept in accordance with its normal document retention and computer backup policies, provided that the Recipient shall continue to protect the confidential nature of such information; or (ii) if requested by Customer in writing, destroy or delete (if possible) and render unrecoverable in un-anonymized form when possible from NMB Solutions' systems (and where applicable, its subcontractors') all Confidential Data, and certify in writing within thirty (30) days of Customer's request for destruction the actions have been completed.



7.1.7 Security Breach Notification. NMB Solutions shall promptly notify Customer if NMB Solutions knows there has been misuse, loss, unauthorized disclosure or acquisition of, or unauthorized access to, Confidential Data ("Information Security Breach"), and NMB Solutions shall (i) promptly notify Customer of such Information

Security Breach, (ii) use diligent efforts to investigate, remediate, and mitigate the effects of the Information Security Breach, (iii) cooperate with Customer's investigation of the Information Security Breach, and (iv) provide Customer with adequate evidence of such investigation, remediation, and mitigation. NMB Solutions shall provide, at Customer's request, non-privileged information related to any such Information Security Breach, including but not limited to, vulnerabilities or flaws, start or end date, date of discovery, and specific actions taken to contain and/or mitigate the Information Security Breach, to the extent that the provision of such information does not put any NMB Solutions Software or data, or any other NMB Solutions customer's data, at risk. **[Art. 33(2) requires a processor to notify its controller "without undue delay after becoming aware of a personal data breach."]**

7.1.8 Security Standard. NMB Solutions shall implement reasonable security procedures consistent with prevailing industry standards to protect Customer data from unauthorized access (the "Security Standard"). Provided that NMB Solutions is in compliance with the Security Standard, the parties agree that NMB Solutions shall not, under any circumstances, be held responsible or liable for situations (i) where data or transmissions are accessed by third parties through illegal or illicit means, or (ii) where the data or transmissions are accessed through the exploitation of security gaps, weaknesses, or flaws unknown to NMB Solutions at the time.

## 8. General

This DPA is effective as of the effective date of the Agreement and, unless earlier terminated by either party, and will terminate when the Agreement terminates or expires, without further action required by either party. The representations, warranties, and liability of the parties hereto are, in all respects, as set forth in the Agreement and subject to any limitations set forth in the Agreement.



## SCHEDULE 1

### STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

(pursuant to Article 26(2) of Directive 95/46/EC)

NMB Solutions Inc., NMB Solutions Ltd. or one of its affiliated companies ("**NMB Solutions**") (also referred to herein as "**data importer**") and **Customer** (also referred to herein as "**data exporter**") have entered into an agreement (the "**Agreement**") pursuant to the terms of which NMB Solutions and its affiliates may Process or store certain Customer information on behalf of Customer and Customer's customers, together with a Data Processing Exhibit ("**DPA**") which incorporates the following Standard Contractual Clauses (also referred to herein as the "**Clauses**") in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of Personal Data of residents of the European Union or Switzerland for Processing under the Agreement.

#### *Clause 1*

#### **Definitions**

For the purposes of the Clauses:

- (a) '*personal data*', '*special categories of data*', '*process/processing*', '*controller*', '*processor*', '*data subject*' and '*supervisory authority*' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data;
- (b) '*the data exporter*' means the controller who transfers the personal data;
- (c) '*the data importer*' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;
- (d) '*the subprocessor*' means any processor engaged by the data importer or by any other subprocessor of the data importer who agrees to receive from the data importer or from any other subprocessor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;
- (e) '*the applicable data protection law*' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a data controller in the Member State in which the data exporter is established;



- (f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

## Clause 2

### **Details of the transfer**

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

## Clause 3

### **Third-party beneficiary clause**

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.
2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.
3. The data subject can enforce against the subprocessor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.



#### Clause 4

##### **Obligations of the data exporter**

The data exporter agrees and warrants:

- (a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;
- (b) that it has instructed and throughout the duration of the personal data processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;
- (c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 1;
- (d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;
- (e) that it will ensure compliance with the security measures;
- (f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;
- (g) to forward any notification received from the data importer or any subprocessor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;
- (h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for subprocessing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;
- (i) that, in the event of subprocessing, the processing activity is carried out in accordance with Clause 11 by a subprocessor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and
- (j) that it will ensure compliance with Clause 4(a) to (i).



## Clause 5

### ***Obligations of the data importer***

The data importer agrees and warrants:

- (a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;
- (c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;
- (d) that it will promptly notify the data exporter about:
  - (i) any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation,
  - (ii) any accidental or unauthorised access, and
  - (iii) any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;
- (e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;
- (f) at the request of the data exporter to submit its data processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;
- (g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for subprocessing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases



where the data subject is unable to obtain a copy from the data exporter;

- (h) that, in the event of subprocessing, it has previously informed the data exporter and obtained its prior written consent;
- (i) that the processing services by the subprocessor will be carried out in accordance with Clause 11;
- (j) to send promptly a copy of any subprocessor agreement it concludes under the Clauses to the data exporter.

#### *Clause 6*

##### ***Liability***

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or subprocessor is entitled to receive compensation from the data exporter for the damage suffered.
2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his subprocessor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, in which case the data subject can enforce its rights against such entity.  

The data importer may not rely on a breach by a subprocessor of its obligations in order to avoid its own liabilities.
3. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the subprocessor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the subprocessor agrees that the data subject may issue a claim against the data subprocessor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the subprocessor shall be limited to its own processing operations under the Clauses.

#### *Clause 7*

##### ***Mediation and jurisdiction***



1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:
  - (a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;
  - (b) to refer the dispute to the courts in the Member State in which the data exporter is established.
2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

#### *Clause 8*

#### **Cooperation with supervisory authorities**

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.
2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any subprocessor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.
3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any subprocessor preventing the conduct of an audit of the data importer, or any subprocessor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5 (b).

#### *Clause 9*

#### **Governing Law**

The Clauses shall be governed by the law of the Member State in which the data exporter is established.

#### *Clause 10*

#### **Variation of the contract**

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.



## *Clause 11*

### ***Subprocessing***

1. The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the subprocessor which imposes the same obligations on the subprocessor as are imposed on the data importer under the Clauses. Where the subprocessor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the subprocessor's obligations under such agreement.
2. The prior written contract between the data importer and the subprocessor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the subprocessor shall be limited to its own processing operations under the Clauses.
3. The provisions relating to data protection aspects for subprocessing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established.
4. The data exporter shall keep a list of subprocessing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5 (j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

## *Clause 12*

### ***Obligation after the termination of personal data processing services***

1. The parties agree that on the termination of the provision of data processing services, the data importer and the subprocessor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.
2. The data importer and the subprocessor warrant that upon request of the data exporter



and/or of the supervisory authority, it will submit its data processing facilities for an audit of the measures referred to in paragraph 1.



## **APPENDIX 1 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses

**Data exporter: Customer**

**Data importer: NMB Solutions Inc. and affiliates**

### **Data subjects**

The personal data transferred concern the following categories of data subjects: customers of Customer and any other individuals interacting with NMB Solutions' supply chain software and services, or as otherwise set forth or referenced in the Agreement and DPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

### **Categories of data**

The personal data transferred concern the following categories of data: as set forth or referenced in the Agreement and DPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

### **Special categories of data (if appropriate)**

The personal data transferred concern the following special categories of data: None, unless otherwise specified in the Agreement and DPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

### **Processing operations**

The personal data transferred will be subject to the following basic processing activities: as set forth or referenced in the Agreement and DPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.

## **APPENDIX 2 TO THE STANDARD CONTRACTUAL CLAUSES**

This Appendix forms part of the Clauses

### **Description of the technical and organizational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c):**

As set forth or referenced in the Agreement and DPA, or in any Orders or Statements of Work issued pursuant to the Agreement, or as otherwise agreed by the parties.