

## CANADIAN DATA PROCESSING ADDENDUM

**Last updated: March 28, 2023**

In addition to its obligations relating to confidentiality, data protection and privacy under the Agreement, Company shall comply with the provisions of this Canadian Data Processing Addendum ("Addendum") in connection with any Personal Information (defined below) that LG Electronics Canada Inc. or its representatives provide to Company, and any other Personal Information about individuals located in Canada that Company collects, receives, accesses, uses, stores, transmits, manipulates, discloses, or otherwise processes ("processes", and similar terms shall have corresponding meanings) on behalf of LG.

For clarity: (1) this Addendum is attached to and forms part of the Agreement between LG and Company; (2) to the extent that any terms or conditions in this Addendum contradict or conflict with any terms or conditions regarding the processing of Personal Information in the Agreement or any other agreement between the Parties, the provisions requiring the higher level of data privacy or security protection for individual persons shall prevail; and (3) capitalized terms that are not defined in this Addendum shall have the meanings ascribed to such terms in the Agreement.

The Parties agree as follows:

- 1) For the purposes of this Addendum, "**Personal Information**" means: (i) End User Data and LG Product Data; (ii) information about an identifiable individual, or information which in combination with other available information may reasonably be capable of identifying an individual, including (without limitation) the individual's name, mailing address, phone number, email address, financial and credit card information, customer or account number, biometric identifiers (including without limitation video or photographic images, fingerprints, and voice biometric data relating to individuals), health-related information or data, account password or answers to account security questions, or any other piece of information that allows the location of, identification of, or contact with a natural person; (iii) any data collected from an IP address, web beacon, pixel tag, ad tag, cookie, local storage object, software, or by any other means, or from a particular computer, web browser, mobile telephone, or other device or application, where such data (A) is collected from a particular computer or device regarding web viewing or other activities; or (B) is or may be used to identify, locate or contact an individual or device or application, to predict or infer the preferences, interests, or other characteristics of the device or application or of a user of such device or application, or to target advertisements or other content to a device or application, or to a user of such device or application; (iv) any other "personal information", as defined pursuant to applicable laws, including, without limitation, the Privacy Laws; and (v) any information that is associated, directly or indirectly (by, for example, records linked via unique keys), with any of the foregoing.
- 2) As between Company and LG, all Personal Information processed in connection with the Agreement is and will remain the exclusive property of LG, and LG retains all ownership, interest, and title in and to such Personal Information. Company shall not

divulge, sell, share or otherwise make available any such Personal Information to any third party, except as explicitly provided for in this Addendum.

- 3) To the extent that Company processes Personal Information on behalf of LG or in connection with the Agreement, Company shall:
  - a) collect, use, protect, disclose and otherwise process such Personal Information, at all times, in full compliance with applicable laws, including the Privacy Laws, and Company will at all times perform its obligations under the Agreement in a manner that will not cause LG to be in material violation of any applicable Privacy Laws;
  - b) collect, use, disclose and otherwise process Personal Information only to the extent and in such manner as is specified in the Agreement and this Addendum, as is reasonably necessary to exercise its rights or perform its obligations under the Agreement, and/or in accordance with LG's reasonable instructions from time to time;
  - c) keep a record of any processing of Personal Information it carries out on behalf of LG;
  - d) if collecting Personal Information on behalf of LG:
    - i) obtain consent or provide notice, as appropriate and in accordance with applicable laws, including the Privacy Laws; and
    - ii) collect only the minimum Personal Information required by Company to perform the Agreement;
  - e) ensure that all necessary and appropriate physical, organizational and technological safeguards are in place to protect Personal Information from loss, theft, or unauthorized access, use, disclosure, copying, alteration, destruction or other processing, including (without limitation) the Security Measures set out in Attachment 1 hereto. For the avoidance of doubt, such safeguards must include, without limitation:
    - i) implementation and maintenance of a comprehensive information security program that, at a minimum, (A) designates one or more employees to maintain such comprehensive information security program; (B) identifies and assesses reasonably foreseeable internal and external risks to the security, confidentiality, or integrity of any records containing Personal Information and which addresses evaluating and improving where appropriate the effectiveness of safeguards against such risks; (C) develops policies for the storage, access, and transportation of records containing Personal Information outside of Company's premises; (D) imposes disciplinary measures for violations of such comprehensive information security program; (E) provides for regular monitoring of the implementation of such comprehensive information security program, including reviews of the scope of Company's security measures at

least annually; and (F) requires documentation of responsive actions taken in connection with any incident involving a Security Breach (as defined below) and a mandatory post-incident review of events and actions taken in order to make changes in business practices;

- ii) encryption of Personal Information in transit and at rest;
  - iii) access controls and data integrity controls, including: (A) authentication credentials with an expiration period; (B) password complexity standards; (C) access on a “least privileges” basis; and (D) access logs that are maintained and audited and include any specific information required by applicable laws, including the Privacy Laws;
  - iv) appropriate patching policies/procedures, firewalls, network segmentation, anti-malware software, intrusion detection software, and vulnerability scanning tools;
  - v) a prudent disaster recovery plan, which meets or exceeds industry standards, and includes regular, secure backup of Personal Information;
  - vi) controls to physically secure hard copies of records containing Personal Information (e.g., storage in locked desks or cabinets), and adequate physical security for all premises where Personal Information is stored or processed;
  - vii) secure retention and disposal policies and procedures; and
  - viii) regular testing and auditing of safeguards and controls;
- f) maintain the confidentiality of Personal Information, with the same degree of care with which it protects its own confidential or proprietary information but, in any event, no less than a reasonable degree of care;
  - g) restrict access to Personal Information solely to it or its employees, agents, affiliates, representatives, and approved subcontractors who: (i) have a need to know the Personal Information for the purposes stated above; (ii) have been trained to handle the Personal Information in compliance with applicable laws, including the Privacy Laws; and (iii) have signed appropriate confidentiality agreements;
  - h) segregate Personal Information from other data or information held by Company;
  - i) promptly comply with any request from LG requiring Company to amend, transfer or delete Personal Information;
  - j) provide, at LG’s request, a copy of all Personal Information held by Company and provide reasonable cooperation in relation to any third-party complaint or request by an individual to have access to that person’s Personal Information;

- k) refer forthwith all requests by third parties for access to any Personal Information in its possession or custody to LG and cooperate with LG in responding to any request for access to Personal Information;
  - l) notify LG of any request by any government or government agency for access to Personal Information, to the extent permitted by applicable laws;
  - m) not disclose or permit disclosure of Personal Information to any third party unless in accordance with the Agreement and this Addendum or with the prior written agreement of LG; and
  - n) not transfer or store any Personal Information outside of Canada, except with LG's prior written consent and in accordance with Section 5).
- 4) Company shall not share or transfer Personal Information or delegate or assign any of its rights or obligations concerning Personal Information to any subcontractor or other outside entity without LG's prior specific written consent. Company shall contractually require that all approved subcontractors must comply with terms no less restrictive than the terms of this Addendum, and Company shall take reasonable steps to monitor and confirm its subcontractors' compliance with such obligations. Company shall be responsible for the acts and omissions of its subcontractors, as if they were its own.
- 5) Without limiting the generality of Section 3)a), Company shall not transfer, store or communicate any Personal Information outside the country or province where it was collected, unless Company first takes all required steps for compliance with applicable Privacy Laws. Without limiting the foregoing, prior to transferring or storing Personal Information regarding Quebec individuals outside Quebec, Company will: (i) take all reasonable steps to ensure that such Personal Information will not be used for any purpose other than the purposes for which it was collected, and to ensure that such information will not be disclosed to third parties without the consent of the relevant individual(s); and (ii) conduct any risk assessment that is required by applicable law (including the Privacy Laws), including, where required, an assessment of the sensitivity of the Personal Information, the purposes for which the information will be used, the protection measures (including contractual measures) that will apply to the information, and the legal framework in the jurisdiction to which the information will be communicated (including the data protection principles applicable in that jurisdiction). Company will refrain from communicating Personal Information outside Quebec, unless the above conditions are met, the results of any required assessment indicate that the Personal Information will receive adequate protection in compliance with generally accepted data protection principles, and Company otherwise complies with any other requirements of applicable Privacy Laws.
- 6) Audits.
- a) Company shall engage a third-party internationally recognized audit firm ("Auditor"), at Company's own cost, to perform periodic audits, scans, and tests as

follows at least once per year and after any Security Incident that occurs during the term and at the request of LG ("Audit Reports"):

- (1) ISO 27001, SSAE 18/SSAE 16/SOC-1, Type II audit and a SOC-2, Type II audit of Company's controls and practices relevant to security, availability, integrity, confidentiality and privacy of Personal Information (as defined in the Agreement);
  - (2) a network-level vulnerability assessment of all Company systems used to collect, receive, access, use, store, transmit, or otherwise process Personal Information under the Agreement; and,
  - (3) a risk assessment, which may include but is not limited to a formal penetration test of all systems used to collect, receive, access, use, store, transmit, or otherwise process Personal Information under the Agreement.
- b) In addition to Company's provision of Audit Reports to LG, LG, through its authorized representative, will have the right no more than once per year during the term during reasonable business hours and upon reasonable notice, to perform an operational audit of Company's compliance with its obligations under the Agreement.
- c) If LG has a good faith belief based on specific facts that Company's privacy practices and standards may not comply its obligations under this Policy, LG will have the right to conduct an audit through its authorized representative regardless of whether LG already conducted an audit during the year.
- d) In addition to the audit rights set forth in the Agreement, and for purposes of audits performed pursuant to this Policy, Company will grant LG representatives all relevant access to Company's books, facilities, procedures, and records as they may be reasonably required to ascertain facts directly relevant and necessary to verify that Company's privacy practices and standards comply with its obligations under this Addendum. In no event will this access include Company's financial books (such as ledgers, income statements, balance sheets, or cash flow statements), records that show Company cost information, return rates, product performance information, product engineering information, or information owned by a third party, unless the documents contain Personal Information. If the documents include Personal Information, information relating to Company's cost, profit and loss, or any third-party information protected by a nondisclosure agreement with Company will be redacted. Unless the privacy audit relates to an issue where LG has a good faith concern or obligation to urgently obtain information regarding Company's compliance with its obligations pursuant to this Addendum, LG will provide the specific scope of the scheduled audit with a list of specific information, if available, to be reviewed and a good faith summary of the types of information within the scope that may be requested during the audit within

ten (10) days of the scheduled audit. Company will provide authorized representatives of LG with this information and assistance as reasonably requested to perform the audits.

- e) If the Parties agree that any audit pursuant to this Addendum reveals an inadequacy or insufficiency of the Company's privacy practice and standards, then Company shall promptly develop and provide to LG a corrective action plan that must be reasonably satisfactory to LG and promptly implement the plan at Company's sole cost and expense. In this event, LG, through a third-party auditor as provided above, may perform one or more additional follow-up audits to verify performance under the corrective action plan (and to examine any areas potentially affected by the action plan) without regard to the time limitations set forth above.
- 7) In the event of any "confidentiality incident" or "breach of security safeguards" (each as defined under applicable Privacy Laws), or any other actual or alleged loss of, or unauthorized access to or disclosure of, Personal Information or any unauthorized intrusion, penetration, or security breach involving Company's systems or facilities (each, a "**Security Breach**"), Company will immediately (and in no event beyond 24 hours of the discovery of such Security Breach): (i) notify LG of such Security Breach; (ii) investigate, mitigate, minimize any damage from, and remediate the effects of, the Security Breach, consistent with any guidelines or requests reasonably made by LG; (iii) provide LG with detailed information about the Security Breach, with all details as may be requested by LG, at any frequency as may be requested by LG; (iv) permit LG and its designees, upon LG's request, to participate in the investigation and remediation of the Security Breach; (v) promptly provide LG with reasonable assistance in any efforts by LG and its designees to investigate, mitigate, or remediate the effects of the Security Breach, and in responding to any dispute, inquiry, or claim relating to the Security Breach; and (vi) provide LG with assurance satisfactory to LG that such Security Breach will not recur. To the extent any Security Breach is attributable to Company or to Company's personnel, including Company's failure to perform its obligations pursuant to the Agreement, Company will cure such Security Breach at its own cost and expense. In addition, Company shall review its safeguards on a regular basis and notify LG of security concerns of which Company becomes aware that may have an adverse effect on LG (including any LG affiliates), and Company will thereafter provide LG with a written action plan satisfactory to LG that addresses such security concerns. Without limiting any other rights or remedies of LG, if in connection with any Security Breach or any act or omission of Company or any of Company's personnel, notice to any individuals, legal authorities, or other third parties of any actual or suspected unauthorized access to or use of Personal Information, or of any other event or circumstance requiring such notice, is required under any law applicable to LG or Company, or LG otherwise determines in its sole discretion that notice of such event or circumstance is reasonably necessary (each, a "Notification Event"), Company will (i) assist LG in notifying such third parties of the Notification Event, and communicating with and assisting such third parties regarding the Notification Event; and (ii) if requested by LG, provide notice of the Notification Event to all persons and entities as may be requested by LG. The content of any statements,

communications, notices, filings or reports by or for Company related to any Notification Event, including those required by law, must be provided to LG within a reasonable time before any publication or release. All disclosures, filings, public statements, press releases, and notifications by or for Company that relate to any Notification Event that either (i) Company intends to be available to End Users or any LG customers, or employees, or (ii) reference LG in any manner, must be approved by LG prior to release. Company will be responsible for any costs of LG in connection with any notification to third parties or any other activities relating to any Security Breach or Notification Event, including costs of notifying consumers or other third parties, providing call center services, providing credit monitoring services, and taking other steps to mitigate or remediate the effects of any Security Breach or Notification Event.

- 8) In addition to any other indemnification obligation of Company set forth in the Agreement, Company shall indemnify, defend, and hold harmless LG, its successors, assigns, directors, officers, employees, agents, and affiliates from and against all actions, litigations, claims, suits, liabilities, losses, damages, expenses, or costs (including legal fees and expenses) which may arise out of, relate to, or be connected in any way with:

- (1) a Security Breach resulting from Company's negligence, fault, or breach of the Agreement, this Addendum, or any Privacy Laws;
- (2) Company's or any of its employees, agents, affiliates, representatives, and subcontractors' failure to comply with applicable Privacy Laws;
- (3) Company's or any of its employees, agents, affiliates, representatives, and subcontractors' negligence or willful misconduct in connection with its or their performance of the Agreement or this Addendum; and
- (4) Company's or any of its employees, agents, affiliates, representatives, and subcontractors' failure to comply with any term, condition, representation, warranty, obligation, or covenant of this Addendum.

LG will have no liability to Company for any failure or deficiency on the part of Company that results in Personal Information being disclosed, corrupted or otherwise compromised.

- 9) Company shall deliver to LG all Personal Information in its possession or control in whatever form (or at LG's request, destroy all such Personal Information where the foregoing is permitted by applicable laws), including all working papers, notes, memoranda, reports, data in machine readable form or otherwise, within five (5) business days of the completion or termination of the Agreement for any reason, or at such earlier time as LG may request and, upon delivery of the Personal Information to LG, Company shall ensure that no record of the Personal Information remains in Company's possession. For greater clarity, Company will not keep any Personal

Information after the expiry of the Agreement. Company will certify, in writing, its compliance with this Section 9), upon request by LG.

- 10) If Company does not comply with its obligations under this Addendum, and LG reasonably determines that such non-compliance creates a material risk to the security, privacy, or confidentiality of Personal Information (each, a "Material Personal Information Matter"), the Parties will take immediate steps to resolve the Material Personal Information Matter. Upon the discovery of a Material Personal Information Matter, notwithstanding any other provision of the Agreement, LG may, in its sole discretion, without penalty of any kind to LG, and without limiting any other rights or remedies of LG under the Agreement, (i) work with Company to implement alternative processes and controls that reasonably address or resolve the Material Personal Information Matter, (ii) suspend or terminate Company's access to Personal Information until the Material Personal Information Matter is resolved, and/or (iii) immediately terminate the Agreement.
- 11) LG and Company acknowledge that laws relating to privacy and data protection, including the Privacy Laws, are evolving and that amendment to the Agreement and/or this Addendum may be required in connection with future developments. The Parties agree to take such action as is necessary to implement the standards and requirements of the Privacy Laws or other privacy and data protection laws applicable to one or both Parties, including negotiating in good faith to amend the Agreement and this Addendum as necessary or prudent for compliance with such laws. Company shall also allow LG to conduct any other verification relating to the confidentiality requirements in the Agreement and this Addendum, as required for LG to comply with its obligations under applicable Privacy Laws.
- 12) If any term of this Addendum is determined by a court of competent jurisdiction to be, to any extent, illegal, otherwise invalid, or incapable of being enforced, such a term shall be excluded to the extent of such invalidity or unenforceability; all other terms herein shall remain in full force and effect; and, to the extent permitted and possible, the invalid or unenforceable term shall be deemed replaced by a term that is valid and enforceable and that comes closest to expressing the intention of such invalid or unenforceable term.



## **ATTACHMENT 1**

### **Security Measures**

Company shall implement the following safeguards and take any other measures reasonably necessary to provide for the security of Personal Information:

- 1) Workstation Configuration. Company shall ensure that Company's personnel only process or temporarily store Personal Information using secured workstations (including desktop and laptop PCs) provided by Company. All Company-provided workstations used to process or temporarily store Personal Information must be protected with the following precautions: (i) workstations must meet the requirements laid out in either the Federal Desktop Core Configuration (FDCC) security configuration [\(<http://nvd.nist.gov/fdcc/index.cfm>\)](http://nvd.nist.gov/fdcc/index.cfm) or [\(<http://csrc.nist.gov/publications/nistpubs/800-70-rev1/sp800-70r1.pdf>\)](http://csrc.nist.gov/publications/nistpubs/800-70-rev1/sp800-70r1.pdf) or USGCB Version 1.2 or higher; (ii) workstations must be located in a physically secure location, e.g., a location secured by the use of a badge reader, key, or appropriate security guard; (iii) workstations must lock automatically after 15 minutes of inactivity (i.e., require login); (iv) application and operating system patches and service packs must be kept up to date, either automatically or via a centrally controlled process, and must not, under any circumstances, be more than 30 days out of date; (v) a real-time virus scanner must be installed and running; signature files must be kept up to date; the virus scanner must run daily scan of the workstation; (vi) a host firewall must be enabled ('built-in' OS firewalls are acceptable, for example Windows XP/Vista or Mac OS X firewalls) and configured to be as restrictive as the environment allows; (vii) workstations must be configured to prevent other computers from accessing Personal Information remotely (i.e., workstations must not act as servers); (viii) an anti-spyware solution must be active; signature files must be kept up-to date; scans must be run at least weekly; (ix) documented controls must be in effect to prevent copying data to portable storage (e.g., CDs/DVDs, USB, disks, etc.); and (x) workstations must have full disk encryption (hardware or software) using the Advanced Encryption Standard (AES) with a minimum key length of 128 bits.
- 2) Customer-Provided Workstations. Company shall ensure that Company personnel do not tamper with, disable, modify, or otherwise yield inoperable any privacy, security, or access control on any laptops, workstations, or other equipment used to process or temporarily store Personal Information. Company shall maintain documented controls to prevent copying data to any portable storage device (e.g., CDs/DVDs, USB, floppy disks, etc.). All laptops, workstations, and other equipment must remain in a physically secure location.
- 3) Network Configuration. Company shall ensure that networks used to access Personal Information are configured as follows: (i) a firewall must be used to control access between the Internet and workstations used to process Personal Information; (ii) inbound Internet access must be protected from malicious code intrusion (e.g., scanning at email gateways, blocking links, stripping executables, intrusion

detection/prevention system); (iii) outbound Internet access must have controls to prevent leakage and misdirection of Personal Information (e.g., proxy server, content filtering, or other network control); and (iv) if wireless networking is used at any point along the data path, the wireless network must be secured using the WPA2 standard.

- 4) Data Usage. Company shall ensure that user accounts, passwords, and keys provided by LG remain confidential and are not shared between Company personnel. Personal Information may only be stored on workstations allocated to the processing of Personal Information. Personal Information must not be printed, except for temporary use to facilitate the processing of the data. At the end of any processing, all printed Personal Information must be destroyed using secure methods set forth below.
- 5) Data Transmission. Files containing Personal Information must be downloaded and uploaded using cryptographic means (e.g., SFTP, TLS).
- 6) Data Storage and Encryption. For Personal Information data stored in a data center or local network drive, access must be controlled and limited to authorized employees of Company specifically engaged for the Personal Information data project. Backups of Personal Information must be encrypted. Backup tapes must be stored in an access-controlled area. Transport of backup tapes to secure offsite storage must be in locked containers and tracked by chain-of-custody documentation. Upon termination of the Agreement or upon request by LG, after successful transfer of data as may be requested by LG, backups must be disposed in a secure manner. Company must encrypt, using an appropriate, industry-standard encryption algorithm, all Personal Information (A) during transfer across any network that is not owned and managed by Company solely as an internal network; (B) stored or transported outside of LG' or Company's facilities; or (C) stored on portable devices or portable electronic media (to the extent otherwise permitted under the Agreement).
- 7) Data Disposal. Personal Information must be securely deleted from all erasable media immediately after termination or expiry of the Agreement, or upon written request from LG. Tapes, printed output, optical disks, and other physical media must be physically destroyed by a secure method, such as shredding performed by a bonded Company.
- 8) Monitoring. Company environments that LG identifies at risk for data loss/data leakage are subject to monitoring by LG including agent- based or hosted data loss prevention systems.
- 9) Testing and Scans. Company will perform regular vulnerability scans of all Company and Company personnel infrastructure, applications, services, systems and devices that Company and Company's personnel use to access Personal Information, using an industry standard vulnerability scanner at reasonable intervals, but in no event less frequently than once per month. Company will have an accredited third party perform a security and privacy design review and penetration test of Company's and all of Company personnel's service(s), systems, and devices used to access Personal Information as circumstances reasonably require, but in no event less frequently than

once per year. Company hereby grants LG the limited right to perform logical assessments of the security of Company's workstation and network security via penetration, intrusion, and/or analysis services using intrusive or passive techniques and software tools ("Testing"). LG may conduct the Testing using a combination manual inspection (e.g., hidden fields examination, etc.) and commercial off-the-shelf tools. Company agrees to cooperate in good faith to identify mutually acceptable times for the Testing. During the Testing, Company will provide access to any devices and assistance to LG as LG may reasonably require.

- 10) Physical Security of Company Locations. Prior to beginning the performance of the Agreement and from time to time upon the written request of LG, Company shall provide LG with Company's written policy detailing physical security controls for each Company location. Company agrees to comply with such policy throughout the duration of the Agreement and agrees that LG has the right to audit such compliance pursuant to the terms of the Agreement.