Date:

Memorandum of Understanding

between:

The Information Commissioner

for

The United Kingdom of Great Britain & Northern Ireland

- and -

Canadian Radio-television and Telecommunications Commission

for Cooperation in the Enforcement of Laws Protecting Personal Data

1. Introduction

1.1 This Memorandum of Understanding ("**MoU**") establishes a framework for cooperation between

(I) The Information Commissioner (the "**Commissioner**") and

(II) Canadian Radio-television and Telecommunications Commission (the "CRTC")

together referred to as the "**Participants**".

1.2 The Participants recognise the nature of the modern global economy, including the increased reliance on electronic means to carry out commercial activities, the increase in circulation and exchange of personal data across borders, the increasing complexity of information technologies, and the resulting need for increased cross-border enforcement cooperation.

1.3 The Participants acknowledge that they have similar obligations and duties for the protection and treatment of personal information in their respective countries.

1.4 This MoU recognizes that the Act known generally as the Canadian Anti-Spam Law (CASL) authorizes the CRTC to disclose information to an institution of the government of a foreign state in specified circumstances and under certain conditions and affirms the intent of the Participants to deepen their existing relations and to promote exchanges to assist each other in the enforcement of their respective laws.

1.5 This MoU sets out the broad principles of collaboration between the Participants and the legal framework governing the sharing of relevant information and intelligence between them.

1.6 The Participants confirm that nothing in this MoU should be interpreted as imposing a requirement on the participants to co-operate with each other. In particular, there is no requirement to co-operate in circumstances which would breach their legal responsibilities, including:

(a) in the case of the Commissioner: the General Data Protection Regulation (the "**GDPR**"); and

(b) in the case of the CRTC: CASL, the *Telecommunications Act*, and the Unsolicited Telecommunications Rules.

1.7 The MoU sets out the legal framework for information sharing, but it is for each Participant to determine for themselves that any proposed disclosure is compliant with the law applicable to them.

2. The role and function of the Information Commissioner

2.1 The Commissioner is a corporation sole appointed by Her Majesty the Queen under the Data Protection Act 2018 (the "**DPA**") to act as the UK's independent regulator to uphold information rights in the public interest, promote openness by public bodies and data privacy for individuals.

2.2 The Commissioner is empowered to take a range of regulatory action for breaches of the following legislation (as amended from time to time):

(a) Data Protection Act 2018 ("DPA");

(b) The General Data Protection Regulation ("GDPR");

(c) Privacy and Electronic Communications (EC Directive) Regulations 2003 ("PECR");

(d) Freedom of Information Act 2000 ("FOIA");

(e) Environmental Information Regulations 2004 ("EIR");

(f) Environmental Protection Public Sector Information Regulations 2009 ("INSPIRE Regulations");

(g) Investigatory Powers Act 2016;

(h) Re-use of Public Sector Information Regulations 2015;

(i) Enterprise Act 2002;

(j) Security of Network and Information Systems Directive ("NIS Directive"); and

(k) Electronic Identification, Authentication and Trust Services Regulation ("eIDAS").

2.3 The Commissioner has a broad range of statutory duties, including monitoring and enforcement of data protection laws, and promotion of good practice and adherence to the data protection obligations by those who process personal data. These duties sit alongside those relating to the other enforcement regimes.

2.4 The Commissioner's regulatory and enforcement powers include:

(a) conducting assessments of compliance with the DPA, GDPR, PECR, eIDAS, the NIS Directive, FOIA and EIR;

(b) issuing information notices requiring individuals, controllers or processors to provide information in relation to an investigation;

(c) issuing enforcement notices, warnings, reprimands, practice recommendations and other orders requiring specific actions by an individual or organisation to resolve breaches (including potential breaches) of data protection legislation and other information rights obligations;

(d) administering fines by way of penalty notices in the circumstances set out in section 152 of the DPA;

(e) administering fixed penalties for failing to meet specific obligations (such as failing to pay the relevant fee to the Commissioner);

(f) issuing decision notices detailing the outcome of an investigation under FOIA or EIR;

(g) certifying contempt of court should an authority fail to comply with an information notice, decision notice or enforcement notice under FOIA or EIR; and

(h) prosecuting criminal offences before Courts.

2.5 Regulation 31 of PECR, as amended by the Privacy and Electronic Communications (EC Directive) (Amendment) Regulations 2011, also provides the Commissioner with the power to serve enforcement notices and issue monetary penalty notices as above to organisations who breach PECR. This includes, but is not limited to, breaches in the form of unsolicited marketing which falls within the ambit of PECR, including automated telephone calls made without consent, live

telephone calls which have not been screened against the Telephone Preference Service, and unsolicited electronic messages (Regulations 19, 21 and 22 of PECR respectively).

3. ROLE AND FUNCTIONS OF CRTC

3.1 The CRTC is an independent Canadian government agency serving as the national telecommunications and broadcasting regulatory authority for Canada.

3.2 As part of its mandate, the CRTC is responsible for promoting and enforcing compliance with the provisions of CASL, including provisions that deal with the regulation of unsolicited commercial electronic messages (i.e. spam), the alteration of transmission data and the installation of computer programs without consent.

3.3 The CRTC is also responsible for regulating unsolicited telecommunications pursuant to section 41 of the *Telecommunications Act* and enforcing compliance with the Unsolicited Telecommunications Rules and National Do Not Call List. The CRTC may designate members of its staff to exercise a range of statutory powers of investigation, inspection, and enforcement, including:

(a) Issuing a notice to produce requiring the production of data, information or documents in a person's possession or control pursuant to sections 17 of CASL and 71(9) of the *Telecommunications Act*;
(b) Issuing preservation demands requiring a telecommunications service provider to preserve transmission data that is in or comes into its possession or control pursuant to section 15 of CASL;
(c) Execute inspections for the purpose of verifying compliance or preventing non-compliance pursuant to sections 71(1) and 71(4) of the *Telecommunications Act*;
(d) Executing a search of a place (business or dwelling-house) to examine, copy or remove documents or things pursuant to sections 19 of CASL and 71(6) of the *Telecommunications Act*;
(e) Issuing warning letters and entering into undertakings;

(f) Issuing a notice of violation, which may include the imposition of an administrative monetary penalty pursuant to sections 22 of CASL and 72.01 and 72.04 of the *Telecommunications Act*.

4. SCOPE OF CO-OPERATION

4.1 The Participants acknowledge that it is in their common interest to collaborate in accordance with this MoU, in order to:

(a) Ensure that the Participants are able to deliver the regulatory cooperation necessary to underpin their data-based economies and protect the fundamental rights of citizens of the United Kingdom and Canada respectively, in accordance with the applicable laws of the Participants' respective jurisdictions;

(b) Cooperate with respect to the enforcement of their respective applicable commercial electronic messaging, telemarketing, data protection and privacy laws;

(c) Keep each other informed of developments in their respective countries having a bearing on this MoU; and

(d) Recognise parallel or joint investigations or enforcement actions by the Participants as priority issues for co-operation.

4.2 For this purpose, the Participants may jointly identify one or more areas or initiatives for cooperation. Such cooperation may include:

(a) sharing of experiences and exchange of best practices on data protection policies, education and training programmes;

(b) implementation of joint research projects;

(c) exchange of information (excluding personal data) involving potential or on-going investigations or proceedings of the organisations in the respective jurisdictions;

(d) joint investigations into cross border personal data incidents involving organisations in both jurisdictions (excluding sharing of personal data);

(e) convening bilateral meetings annually or as mutually decided between the Participants; and

(f) any other areas of cooperation as mutually decided by the Participants.

4.3 This MoU does not impose on either the Commissioner or the CRTC any obligation to co-operate with each other or to share any information. Where a Participant chooses to exercise its discretion to co-operate or to share information, it may limit or impose conditions on that request. This includes where (i) it is outside the scope of this MoU, or (ii) compliance with the request would breach the Participant's legal responsibilities.

5. NO SHARING OF PERSONAL DATA

5.1 The Participants do not intend that this MoU shall cover any sharing of personal data or confidential information that includes personally identifiable information by the Participants.

5.2 If the Participants wish to share personal data or other confidential information that includes personally identifiable information, for example in relation to any cross border investigation or personal data incident, then each Participant shall consider compliance with its own applicable privacy and data protection laws, which may require the Participants to enter into a written agreement or arrangement regarding the sharing of such personal data or personally identifiable information. This may include the taking of additional appropriate measures to safely transmit and safeguard the materials containing personal data or personally identifiable information. Protective measures may include, but are not limited to, the following examples and their reasonable equivalents, which may be used separately or combined as appropriate in the particular circumstances:

(a) transmitting the material in an encrypted format;
(b) transmitting the material directly by a courier with package tracking capabilities;
(c) maintaining the materials in secure, limited access locations (e.g., password-protected files for electronic information and locked storage for hard-copy information); and
(d) if used in a proceeding that may lead to public disclosure, redacting personally identifiable information or filing under seal, if appropriate to proceedings.

6. INFORMATION SHARED BY THE COMMISSIONER

6.1 Section 132(1) of the DPA 2018 states that the Commissioner can only share certain information if she has lawful authority to do so, where that information has been obtained, or provided to, the Commissioner in the course of, or for the purposes of, discharging the Commissioner's functions, relates to an identifiable individual or business, and is not otherwise available to the public from other sources.

6.2 Section 132(2) of the DPA 2018 sets out the circumstances in which the Commissioner will have the lawful authority to share that information. Of particular relevance when the Commissioner is sharing information with the CRTC are the following circumstances, where:

(a) The sharing is necessary for the purpose of discharging the Commissioner's functions (section 132(2)(c));and

(b) The sharing is necessary in the public interest, taking into account the rights, freedoms and legitimate interests of any person (section 132(2)(f)).

6.3 Before the Commissioner shares such information with the CRTC, the Commissioner may identify the function of the CRTC with which that information may assist, and assess whether that function of the CRTC could reasonably be achieved without access to the particular information in question.

6.4 The Commissioner may choose to share certain information with the CRTC only if the CRTC agrees to certain limitations on how it may use that information.

7. INFORMATION SHARED BY THE CRTC

7.1 Section 60 of CASL sets out the circumstances in which the CRTC will have the lawful authority to share information with the Commissioner. Specifically, information may be disclosed:

(a) where it is believed that the information may be relevant to an investigation or proceeding in respect of a contravention of a law that is substantially similar to CASL or the *Telecommunications Act*; or

(b) where the disclosure is necessary to obtain information that may be relevant to a CRTC investigation or proceeding.

7.2 Information may only be disclosed for the purpose of investigations or proceedings regarding contraventions of the laws that do not have consequences that would be considered penal under Canadian law.

7.3 Subject to other laws which apply to the Participants (including in the case of the Commissioner, FOIA and in the case of the CRTC, the *Access to Information Act*) the Participants acknowledge that each request for information, the existence of any investigation related to the request, all materials related to each request, and all information and material provided in response to each request, may contain the other Participant's confidential information (unless the Participants reach a different understanding) and will treat such information accordingly.

8. SECURITY AND DATA BREACH REPORTING

8.1 Appropriate security measures shall be agreed to protect information transfers in accordance with the sensitivity of the information and any classification that is applied by the sender.

8.2 Where confidential material is shared between the Participants it will be marked with the appropriate security classification.

8.3 Where one Participant has received information from the other, it will advise the other Participant before passing the information to a third party or using the information in an enforcement proceeding or court case.

8.4 Where confidential material obtained from, or shared by, the originating Participant is wrongfully disclosed or used by the receiving Participant, the receiving Participant will bring this to the attention of the originating Participant without delay.

9. REVIEW OF THE MoU

9.1 The Commissioner and the CRTC will monitor the operation of this MoU and review it biennially, or sooner if either Participant so requests.

9.2 Any issues arising in relation to this MoU will be notified to the designated point of contact for each Participant.

9.3 This MoU may only be amended by the Participants in writing and signed by each Participant.

10. NON-BINDING EFFECT OF THIS MoU AND DISPUTE SETTLEMENT

10.1 This MoU is a statement of intent that does not give rise to legally binding obligations on the part of either the Commissioner or the CRTC.

10.2 The Participants will settle any disputes or disagreement relating to or arising from this MoU amicably through consultations and negotiations in good faith without reference to any international court, tribunal or other forum.

11. DESIGNATED CONTACT POINTS

11.1 The following persons shall be the designated contact points for the Participants for matters under this MoU:

Information Commissioner's Office	**CRTC**
Name: [redacted] Designation: Head of Intelligence	Name: Steven Harroun Designation: Chief Compliance and Enforcement Officer

11.2 The above individuals will maintain an open dialogue between each other in order to ensure that the MoU remains effective and fit for purpose. They will also seek to identify any difficulties in the working relationship, and proactively seek to minimise the same.

11.3 Each Participant may change its designated contact point for the purposes of this MoU upon notice in writing to the other Participant.

Signatories:

Stephen Eckersley **Director of Investigations**	**Steven Harroun** **Chief Compliance and Enforcement Officer**

[redacted] Date: 2.12.2019	[redacted] Date: 19/11/19