GeoComply Data Processing Addendum

Posted August 1, 2024

This GeoComply Data Processing Addendum, including its Annexes (collectively, this "**DPA**"), supplements and forms part of the commercial agreement between GeoComply and its customer ("**Customer**") pursuant to which GeoComply provides certain services to Customer (the "**Services**") if and only if the Order Form, Term Sheet, Customer Agreement, Master Agreement, and/or other similar written agreement between GeoComply and Customer (the "**Agreement**") explicitly states that this DPA is applicable. This DPA will apply to the Agreement to the extent that GeoComply processes Personal Information (as defined below) in the provision of the Services to Customer and reflects the Parties' agreement regarding the processing of Personal Information. In the event of a conflict or inconsistency between the terms of this DPA and other provisions of the Agreement, the terms of this DPA will control to the extent of such conflict. The Parties' respective liability and any indemnification obligations under this DPA will be in accordance with the liability limitation, indemnification, and related liability provisions of the Agreement.

Customer is subject to this DPA on behalf of itself and, to the extent required under Applicable Data Protection Laws, in the name and on behalf of its Approved Sublicensees, if and to the extent GeoComply processes Personal Information for which such Approved Sublicensees qualify as the "controller." For the purposes of this DPA only, and except where indicated otherwise, the term "Customer" will include Customer and Approved Sublicensees.

1. **DEFINITIONS.** Capitalized terms used but not defined in this DPA will have the meanings set forth in the Agreement.

    1.1. "**Applicable Data Protection Laws**" means any data protection laws, rules, regulations, self-regulatory guidelines or implementing legislation applicable to GeoComply's provision and/or Customer's use of an Offering, including data protection and privacy laws, rules, and regulations to which Personal Information is subject.

    1.2. "**Aggregated Data**" means data that relates to a group or category of natural Persons from which individual identities have been removed and that is not linked or reasonably linkable to any consumer or household, including via a device.

    1.3. "**Anonymous Data**" means data that does not relate to an identified or identifiable natural Person or to Personal Information that has been rendered anonymous in such a manner that such natural Person or Personal Information is no longer identifiable.

    1.4. "**CCPA**" means the California Consumer Privacy Act, Cal. Civ. Code § 1798.100 et seq., as amended, and its implementing regulations, including, but not limited to, the California Privacy Rights Act (CPRA).

    1.5. "**Data Breach**" means any breach of security leading to the accidental or unlawful destruction, loss, alteration or unauthorized disclosure of or access to Personal Information.

    1.6. "**DSAR**" means a data subject access request submitted to GeoComply on behalf of an End User or other Person whose Personal Information GeoComply may, currently or in the past, store or handle on behalf of Customer.

    1.7. "**De-identified Data**" means data that cannot reasonably identify, relate to, describe, be capable of being associated with or be linked, directly or indirectly, to a particular natural Person.

    1.8. "**EEA**" means the European Economic Area.

    1.9. "**GDPR**" means the EU General Data Protection Regulation ((EU) 2016/679).

1.10. "**Personal Information**" means any data regarding Customer's End Users that is processed by GeoComply pursuant to the Agreement and that is defined as "personally identifiable information," "personal information," "personal data" or similar terms under Applicable Data Protection Laws.

1.11. "**Sub-Processor**" means a third-party processor engaged by GeoComply who may, has or will have access to or process Personal Information from Customer.

2. DATA PROTECTION.

2.1. **Limitation on Use; Scope.** Under the Agreement, GeoComply acts as a "service provider" or "processor", as those terms are defined by Applicable Data Protection Laws. GeoComply will process Personal Information only (i) in accordance with the Customer's instructions in accordance with the Agreement and Applicable Law; (ii) when initiated by Customer in its use of the Services; and (iii) as needed to comply with Applicable Law, including Applicable Data Protection Laws, provided that GeoComply will not be required to act on an instruction given by the Customer which could (in the reasonable opinion of GeoComply) give rise to a breach of Applicable Law. GeoComply will inform the Customer if it believes that any Customer instructions regarding Personal Information processing would violate Applicable Laws. The scope of processing of Personal Information is as described below:

2.1.1. **Subject matter, nature, and purpose**: See Annex I-B

2.1.2. **Categories of individuals**: See Annex I-B

2.1.3. **Types of Personal Information**: See Annex I-B

2.2. **Security.** GeoComply will take reasonable steps to implement technical and organizational measures designed to protect Personal Information against anticipated threats or hazards to its security, confidentiality or integrity. See Annex II for more detail.

2.3. **Data Breach.** GeoComply will notify Customer without undue delay (and in accordance with any relevant incident response, support, and/or service level commitments in the Agreement) after becoming aware of a Data Breach involving Personal Information transmitted, stored, or otherwise processed by GeoComply or a Sub-Processor, unless such notification is prohibited by Applicable Law or GeoComply is otherwise instructed not to provide such notification by law enforcement or a regulatory authority. GeoComply will provide Customer with a description of the Data Breach as such information becomes available to GeoComply, including the date and/or time period during which the Data Breach is believed to have occurred, a description of the Personal Information affected, details about the affected End Users or other data subjects, and such other information as Customer may reasonably require to enable Customer to meet Customer's obligations under Applicable Laws. Customer, as the "business" or "controller" with respect to its End Users' Personal Information, will be responsible for notifying affected End Users of the Data Breach.

2.4. **Data Subject Access Requests.** If GeoComply receives a DSAR, as between Customer and GeoComply: (i) if such DSAR identifies Customer as the controller, then GeoComply will promptly notify Customer in writing of such data subject request and will direct the individual making the data subject request to Customer; and (ii) if such data subject request does not identify Customer as the controller, then GeoComply will promptly advise the individual making the DSAR to identify and contact Customer. At Customer's reasonable request and taking into account the nature of the processing, GeoComply will take reasonable steps to assist Customer with Customer's obligation to respond to individuals' requests to exercise their rights under Applicable Laws.

2.5. **Return or Disposal.** Upon the expiration or termination of the Agreement, or at such other times as instructed by Customer in writing, GeoComply will de-identify, anonymize, destroy, and/or return (at GeoComply's reasonable discretion) all Personal Information to Customer after the end of the provision of Services, unless Applicable Laws require GeoComply to retain the Personal Information. In the event Applicable Laws do not permit GeoComply to complete the de-identification, anonymization, destruction, and/or return of the Personal Information, GeoComply will ensure the strict confidentiality of the Personal Information retained and will not process any Personal Information by or on behalf of Customer after

expiration or termination of the Agreement. GeoComply will delete any back up copies of Personal Information as the backup media is recycled in the ordinary course of business.

2.6. **Assistance.** GeoComply will provide relevant information and assistance reasonably requested by Customer (to be exercised by Customer no more than once per 12-month period, upon at least 30 days' written request, unless required more frequently by a regulatory authority) to demonstrate compliance with this DPA and allow for and contribute to reasonable Customer audits. Upon request, GeoComply will supply a copy of its most recent third-party assessment (such as a SOC 2 audit). Customer agrees that such assessments will be used to satisfy any audit or inspection requests by or on behalf of Customer. The third-party assessment or other audit results will be GeoComply's Confidential Information and may not be disclosed without GeoComply's prior written consent, except as required by Applicable Laws. Taking into account the nature of the processing and the Personal Information available to GeoComply, GeoComply also will assist Customer at Customer's reasonable request in meeting its compliance obligations regarding carrying out privacy and data protection impact assessments and related consultations of supervisory authorities. GeoComply reserves the right to charge a reasonable fee to Customer for such requested assistance.

2.7. **Sub-Processors.** Customer authorizes GeoComply to transfer Personal Information to Sub-Processors for purposes of developing the Services and providing the Services to Customer, provided GeoComply has entered into a written agreement with each Sub-Processor containing data protection obligations generally not less protective than those in the Agreement and this DPA with respect to the protection of Customer's Personal Information, to the extent applicable considering the nature of the services provided by such Sub-Processor. GeoComply will maintain and regularly update a list of its Sub-Processors at https://www.geocomply.com/geocomply-subprocessors/. GeoComply will endeavor to update this list at least 10 days prior to a new Sub-Processor becoming active to allow Customer to submit any objections.

2.8. **CCPA.**

2.8.1. **Restriction on Processing.** Except as otherwise expressly permitted by the Agreement or this DPA or permitted by the CCPA, in no event may GeoComply: (i) sell or share Personal Information, as the CCPA defines those terms; (ii) disclose Personal Information to any third party for the commercial benefit of GeoComply or any third party; (iii) retain, use, disclose, or otherwise process Personal Information outside of its direct business relationship with Customer or for a commercial purpose other than the business purposes specified in the Agreement; or (iv) combine Personal Information with Personal Information that GeoComply receives from, or on behalf of, other Persons, or collects from its own interaction with an individual in violation of the CCPA.

2.8.2. **Legal Compliance.** GeoComply will provide California residents with the same data protection rights under CCPA as provided by Customer. GeoComply will notify Customer in writing if GeoComply makes a determination that it can no longer meet its obligations under the CCPA and Customer has the right, upon providing notice to GeoComply, to take reasonable and appropriate steps to stop and remediate unauthorized use of Personal Information, including where GeoComply has notified Customer that it can no longer meet its CCPA obligations.

3. DATA TRANSFERS; GDPR.

3.1. **Scope.** This Section 3 is applicable only to the transfer of data originating from or otherwise associated with the EEA and its qualifying residents as prescribed by the GDPR, the UK EU General Data Protection Regulation, and/or Switzerland's Federal Act on Data Protection, as applicable.

3.2. **Data Transfers Generally**. GeoComply may transfer Personal Information to countries outside the EEA. Such transfers will be completed in compliance with the GDPR and other Applicable Data Protection Laws.

3.3. **Restricted Transfers of Personal Information Subject to GDPR or Similar Countries' Data Protection Laws.**

3.3.1. Module 2 of the EU Standard Contractual Clauses, available at https://eur-lex.europa.eu/eli/dec_impl/2021/914/oj?uri=CELEX%3A32021D0914&locale=en and incorporated into this DPA by reference (the "**EU SCCs**") will apply to:

3.3.1.1. any transfer of Personal Information that is subject to the GDPR (or was subject to the GDPR prior to its transfer to data exporter) to an organization located outside of the EEA; and

3.3.1.2. any transfer of Personal Information that is subject to the data protection laws of a country outside the EEA in which the competent authority either has approved the use of the EU SCCs or a previous version of the EU Standard Contractual Clauses, including, but not limited to, Switzerland (each, a "**Similar Jurisdiction**") (or was subject to the data protection laws of the Similar Jurisdiction prior to its transfer to data exporter) to a data importer located outside of the Similar Jurisdiction.

3.3.2. Notwithstanding the foregoing, the EU SCCs will not apply to the extent the transfer is covered by (i) a decision adopted by a competent authority with jurisdiction over the data exporter declaring that a jurisdiction meets an adequate level of protection of Personal Information (an "**Adequacy Decision**").

3.3.3. For the purpose of Clause 9 of the EU SCCs, Option 2 will apply and the time period for GeoComply notifying Customer of changes to the list of Sub-Processors will be the time period specified in Section 2.7 above.

3.3.4. The optional language in Clause 11 of the EU SCCs is excluded.

3.3.5. Where the data transfer relates to Personal Information that is subject to the GDPR:

3.3.5.1. For the purpose of Clause 17 of the EU SCCs, the EU SCCs will be governed by the laws of the country in the EU where the Customer is established.

3.3.5.2. For the purpose of Clause 18 of the EU SCCs, any dispute arising from the EU SCCs will be resolved by the courts of the country in the EU where the Customer is established

3.3.5.3. For the purpose of Annex I.C of the EU SCCs, the data protection authority of the country in the EU where the Customer is established is the competent supervisory authority.

3.3.6. Where the transfer relates to Personal Information governed by the data protection laws of a Similar Jurisdiction:

3.3.6.1. All references in the EU SCCs to "EU," "Union" or "Member State" will be interpreted as references to the Similar Jurisdiction;

3.3.6.2. All references in the EU SCCs to provisions in EU law will be interpreted as references to the relevant provisions of the laws of the Similar Jurisdiction;

3.3.6.3. For the purpose of Clause 17 of the EU SCCs, the EU SCCs will be governed by the law of the Similar Jurisdiction;

3.3.6.4. For the purpose of Clause 18 of the EU SCCs, any dispute arising from the EU SCCs will be resolved by the courts of the Similar Jurisdiction; and

3.3.6.5. For the purpose of Annex I.C of the EU SCCs, the competent supervisory authority is the data protection authority of the Similar Jurisdiction.

3.4. **Restricted Transfers from the United Kingdom.** Where the transfer of Personal Information is subject to the laws of the United Kingdom (including the UK General Data Protection Regulation), the parties agree:

3.4.1. The provisions of the UK International Data Transfer Addendum to the EU Commission Standard Contractual Clauses, Version B1.0, in force from March 21, 2022, ("**UK SCCs Addendum**"), including Part 2 'Mandatory Clauses', will apply in full;

3.4.2. For the purposes of Table 1 of the UK SCCs Addendum, the names of the parties, their roles and their details will be set out in the attached Annex I;

3.4.3. For the purposes of Tables 2 and 3 of the UK SCCs Addendum, Module 2 of the EU SCCs incorporated into this DPA by reference will apply; and

3.4.4. For the purposes of Table 4 of the UK SCCs Addendum, either Party may end the UK SCCs Addendum.

4. **SEVERABILITY; ENFORCEABILITY.** If any provision of this DPA is held to be invalid or unenforceable by any court of competent jurisdiction, such holding will not invalidate or render unenforceable any other provision of this DPA or the Agreement or any other contract between Customer and GeoComply. If this DPA, or any actions to be taken or contemplated to be taken in the performance of this DPA, do not or would not satisfy either party's obligations under Applicable Laws, the parties will negotiate in good faith upon an appropriate supplement or amendment to this DPA or the Agreement.

5. **MODIFICATIONS.** GeoComply may, from time to time, unilaterally make reasonable updates and modifications to this DPA (i) to comply with changes in Applicable Laws, regulations, and/or best practices; or (ii) to reflect changes in GeoComply's products, solutions, processes, contracts, or systems.

ANNEX I

A. LIST OF PARTIES

Data Exporter(s):

- Name: Customer as identified in the Agreement
- Address: As per the Agreement
- Contact person's name, position and contact details: As per the Agreement
- Activities relevant to the data transferred under the Agreement and this DPA: As per the Agreement and this DPA
- Role (controller/processor): controller

Data Importer(s):

- Name: GeoComply Solutions Inc.
- Address: 545 Robson Street, Suite #2, Vancouver, British Columbia, Canada V6B 1A6
- Contact person's name, position and contact details: Maninder Malli, General Counsel & Corporate Secretary; privacy@geocomply.com
- Activities relevant to the data transferred under the Agreement and this DPA: As per the Agreement and this DPA
- Role (controller/processor): processor

B. DESCRIPTION OF TRANSFER(S)

Categories of data subjects whose Personal Information is transferred:

- Customer employees, contractors, and third-party administrators (such as administrative users, employees who manage the Services on behalf of Customer)
- Customer End Users and others utilizing or attempting to utilize Customer Applications and other Customer-offered products and services (such as players, members, subscribers to Customer Applications and services)

Categories of Personal Information transferred:

<u>GeoComply Core Offering:</u>

- De-Personalized ID that represents the End User.
- Device geolocation data derived from GPS, cellular network carrier, WiFi access points, network address (e.g. IP address), and other data available on the End User's device/browser to determine their physical location. Such data may consist of the End User's time zone, country, region, city, latitude, and longitude coordinates.
- Event data for geolocation requests from the Customer Application.
- Geolocation circumvention technologies that prevent or attempt to prevent Customer from fulfilling its obligations to determine where an End User is accessing their platform such as: VPNs, proxies, Tor nodes, or other software, applications, and services.
- Device fingerprints for fraud detection. Type of device, operating system, IP address, memory usage, applications installed, CPU, browser, browser plug-ins, screen size/resolution, and related data points.
- Event data used by GeoComply to secure the Services consisting of event data from Customer's employees, and End Users. Such data may include End Users' browser, operating system, IP addresses login times, data accessed, and configuration changes.

Authentication Services:

- Personal Information collected for GeoComply Core Offering
- First name, last name
- Contact information (phone number, e-mail address, address)
- Date of birth
- Last 4 digits of SSN/SIN

IDComply and Other Know Your Customer ("KYC") Services:

- Contact information of the individual (e.g. full name, address, phone number, email address)
- Date of birth
- IP Addresses
- Government identification numbers (e.g. SIN, SSN)
- Government ID expiry date
- Email address
- Photographs of government identification
- Photos of End Users for comparison with government identification
- Pass/failure status of Personal Information checks conducted by KYC vendors

Anti-Fraud Charge-Back Services:

- End User's contact information (e.g. full name, email address, physical address)
- Date and times of disputed charges
- Last 4 digits of credit, bank, payment card associated with the activity
- GeoComply username associated with the activity
- Transaction values of the disputed charges

GeoGuard Services:

- Network Address (e.g. IP address)

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved:

- Customers using the Services to meet their KYC obligations may choose to implement photo comparison / facial recognition. This may be considered biometric processing that may need to be disclosed by Customer to their End Users before its collection; please consult with your legal teams for specific advice surrounding notice, disclosure and consent requirements. GeoComply relies on specialized Sub-Processors for the creation and management of biometric data - this data is not transferred or stored by GeoComply. See also GeoComply's Biometric Data Privacy Policy here: https://www.geocomply.com/biometric-data-privacy-policy/

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis):

- Continuous basis as determined by Customer.

Nature of the processing:

- Processing of Personal Information to comply with the terms of the Agreement. GeoComply assists with reducing geolocation and financial fraud affecting Customer's products and services. Specifically, as documented in the Agreement, GeoComply may assist with:
    - Meeting contractual, legal, and regulatory obligations for ensuring that Customer Applications and other services and activities being offered by Customer to End Users are accessed from within a specific geography or location.
    - Verifying an individual's identity where Customer determines it is required to access their Customer Applications or other services.
    - Assisting prevention or investigation of fraudulent activity.
    - Disputing chargeback requests of Customer from payment processors where a Person disputes that a financial transaction took place.
    - Processing to comply with other documented reasonable instructions provided by Customer (e.g. via email) where such instructions are consistent with the terms of the Agreement.

Purpose(s) of the data transfer and further processing:

- As documented in the Agreement and instructed by Customer, GeoComply may assist with verifying the geolocation of Customer's End Users, preventing and investigating fraudulent activity such as financial fraud and identity theft, and preventing unauthorized account takeovers.
- In addition, GeoComply may use data provided by Customer for managing and improving the Services. Such processing may include:
    - Improving and introducing new features
    - Information security
    - Performance management
    - Providing technical and implementation support for Customer
    - Meeting gaming industry licensing and regulatory requirements where applicable
- GeoComply may create Aggregate Data, Anonymous Data, and De-identified Data from Personal Information to generate industry insights, analytics, and reports and to develop new features, products, and services.

The period for which the Personal Information will be retained, or, if that is not possible, the criteria used to determine that period:

- Personal Information will be retained for the term of the Agreement unless otherwise required by Applicable Law or agreed by the Parties.

For transfers to (Sub-) processors, also specify subject matter, nature and duration of the processing:

- GeoComply uses Sub-Processors to assist in developing and delivering the Services. See Section 2.7 above.

ANNEX II

SECURITY MEASURES

This Annex outlines the information security measures that will be taken by GeoComply.

1. Information Security Policies and Standards.

GeoComply will implement security requirements for its personnel who have access to Customer's Personal Information that are designed to ensure a level of security appropriate to the risk and address the requirements detailed in this Annex. GeoComply will conduct periodic risk assessments and review and, as appropriate, revise its information security practices whenever there is a material change in GeoComply's business practices that may reasonably affect the security, confidentiality, or integrity of Personal Information, provided that GeoComply will not modify its information security practices in a manner that will weaken or compromise the security, confidentiality, or integrity of Personal Information.

2. Physical Security.

GeoComply will maintain commercially reasonable physical security systems at all GeoComply sites at which an information system that uses or houses Personal Information are located. GeoComply reasonably restricts access to such Personal Information appropriately and has in place practices to prevent unauthorized individuals from gaining access to Personal Information.

3. Data Security.

GeoComply will implement procedures to prevent any subsequent retrieval of any Personal Information stored on media before disposed of or reused. GeoComply will implement security policies and procedures to classify sensitive information assets, clarify security responsibilities and promote awareness for employees. GeoComply will encrypt, using industry-standard encryption tools, Personal Information that GeoComply: (i) transmits or sends wirelessly or across public networks; and (ii) stores on portable devices or at rest, where technically feasible.

4. Network Security.

GeoComply will maintain network security using commercially available equipment and industry-standard techniques, including firewalls, intrusion detection and prevention systems, access control lists and routing protocols.

5. Access Control.

GeoComply will maintain appropriate access controls, including, but not limited to, restricting access to Personal Information to the minimum number of GeoComply personnel who require such access. GeoComply will maintain a list of the persons who have accessed Personal Information and a list of those who are permitted to access the Personal Information (including their identification numbers, access codes and the types of information to which they are permitted to access).

6. Endpoint Security.

GeoComply will install and maintain appropriate antivirus and malware protection software on its systems and will maintain scheduled malware monitoring and system scanning to protect Personal Information from anticipated threats or hazards and to protect against unauthorized access to or use of Personal Information.

7. Personnel.

GeoComply will require GeoComply personnel to comply with its information security program. GeoComply will implement a security awareness program to regularly train personnel about their security obligations.

8. Third Party Assessments

GeoComply regularly has third-party assessments (such as SOC 2 audits) conducted on its security program. Upon Customer's request, GeoComply will supply a copy of its most recent third-party assessment.

9. Business Continuity.

GeoComply will implement appropriate back-up and disaster recovery and business resumption plans. These plans will include processes to ensure recovery of Personal Information that was modified or destroyed due to unauthorized access. GeoComply will regularly review, test and update its business continuity systems and plans to ensure that they are up to date and effective.