Data Gumbo Anti-Bribery and Corruption ("ABC") & Sanction Review

Compliance Policy

Data Gumbo and its subsidiaries and affiliates are committed to conducting business fairly, honourably, with integrity, and in compliance with the law in all jurisdictions where it operates. Bribery is illegal and can expose the company to fines and other penalties, including imprisonment. All company directors, officers and employees must be familiar with and follow each of the requirements described in this Anti-Bribery and Anti-Corruption Compliance Policy (the "Policy"). Ambassadors, agents, consultants, business partners and any other individuals or entities doing business on behalf of Data Gumbo must also comply with this Policy.

In many countries, including in the U.S., laws and regulations prohibit the bribery or attempted bribery of any individual or entity. Consistent with these laws, Data Gumbo's policy prohibits bribes, kickbacks, and all other corrupt payments to any individual or entity. For purposes of this policy, whether the recipient of the act of bribery works in the public or private sector is irrelevant. This means that no Data Gumbo officer, director, or employee will authorize, pay, promise, or offer to give anything to any individual or entity to improperly influence that individual or entity to act favourably towards Data Gumbo. Individuals covered by this policy shall not request or authorize any third party to make any such payment, promise or offer. Such behaviour is unacceptable everywhere that Data Gumbo conducts business.

Many laws around the world prohibit bribery of Government Officials, including the U.S. Foreign Corrupt Practices Act (the "FCPA") and the U.K. Bribery Act 2010 (the "UKBA"), both of which are discussed in this policy. These laws impose fines, penalties, and imprisonment for violations. This Policy is designed to comply with the requirements of the FCPA, the UKBA, as well as the anti-bribery laws of other jurisdictions in which Data Gumbo conducts business.

Data Gumbo is also required to adhere to various sanctions imposed on countries by the US Government and other governments where Data Gumbo conducts business. Sanctions are commercial and financial penalties applied by one or more countries against a targeted self-governing state, group, or individual, and may include various forms of trade barriers, tariffs, and restrictions on financial transactions. These sanctions include penalties for companies that conduct business with these governments, entities or individuals including possible serious punishment, such as corporal or capital punishment, incarceration, or severe fines.

To ensure compliance with this policy, and consistent with the intent of Data Gumbo's Accounting Practices, Data Gumbo prohibits any "off-the books" accounts or payments and any knowing falsification of Data Gumbo's books and records. This prohibition applies regardless of the amount and includes the falsification of books and records to conceal bribes and other corrupt or improper payments.

1. **GENERAL.** Data Gumbo's Compliance Policy applies to all employees, officers, and directors of Data Gumbo and all of Data Gumbo's affiliates worldwide, as well as any third-party intermediaries or representatives such as resellers, contractors, or agents.

   Importantly, this Policy cannot cover every situation or provide information on every law that may be applicable where Data Gumbo conducts business. If you are uncertain about any situation or request, you should seek further guidance from the Company's Head of Compliance.

2. DEFINITIONS

Bribery is the offer, promise, giving, demanding or acceptance of an advantage as an inducement for an action which is illegal, corrupt, unethical or a breach of trust.

Corruption consists of an offer, payment, or promise that is intended to induce the recipient to misuse his or her official position, whether as a government official or as the representative or employee of a private business.

Acts of bribery and corruption are designed to influence the individual in the performance of their duty and incline them to act dishonestly. The person being bribed is generally someone who will be able to obtain, retain, or direct business.

3. WHO IS COVERED?

This policy prohibits bribery and corrupt behavior by:

- Any employee, officer, or director of the company, and
- Any person acting on behalf of the company, including third parties acting on behalf of the company as distributors, agents, representatives, consultants, and partners

Acts of bribery and corruption will commonly involve public or government officials. This policy prohibits the payment of bribes to the following Government Officials:

- Officers or employees of any local, provincial, or national government (for example, members of Parliament, police officers, firefighters, members of the military, tax authorities, customs inspectors, etc.)
- Directors, officers, representatives, agents, or employees of any government-owned or controlled business or company
- Officers or employees of a public international organization (for example, the United Nations, International Olympic Committee, International Red Cross, World Bank, etc.)
- Individuals acting in any official capacity or on behalf of any government or public international organization (for example, an official advisor to a government, government agency, or government official)
- Officers or employees of a political party
- Candidates for political office

Bribery can also involve corrupt payments to agents or employees of business partners to secure an advantage over competitors. This Policy therefore prohibits the payment of bribes and kickbacks to the following private persons:

- Employees of companies who are in a position to direct business to Data Gumbo
- Purchasing agents or procurement officers of customers and potential customers
- Third parties who are in a position to recommend or refer business to Data Gumbo

Any payment that cannot be made directly to an individual under this Policy also may not be made indirectly, such as to a close relative, through a friend, or via the individual's business.

4. WHAT MAY CONSTITUTE A BRIBE?

Bribes can take many different shapes and forms, but typically they involve corrupt intent. There will usually be a "quid pro quo" – that is, the bribe will be offered or paid in exchange for some benefit. Bribes can be made by using anything of value, including:

- Cash, cash equivalents (e.g., gift checks) or loans
- Payments for travel or entertainment
- Favors, including offers of employment or internships
- Gifts (e.g., perfume, jewelry, use of club memberships)
- Donations to a charity affiliated with or sponsored by a government official
- Political contributions

Some examples of improperly influencing a Government Official, include:

- The Government Official would not act if you did not make the gift, and you give a gift to increase the chances that the Government official will take such action
- The Government Official has a choice to act or not and decides based on the gift.

Some examples of improper business advantage include when a Government Official:

- Overlooks a violation or tolerates non-compliance with applicable laws
- Does not perform a task that should otherwise be performed (e.g., does not conduct a required inspection prior to issuing a permit)
- Reduces customs duties
- Grants a favorable tax treatment
- Directs business to Data Gumbo

Examples of commercial bribery would include:

- Paying a kickback to a purchasing agent in order to cause that agent to choose to buy the briber's products rather than those of a competitor
- Providing anything of value to an executive or officer of a business partner in order to cause that partner to conduct business with the briber
- Paying a third party in order to unlawfully obtain a recommendation or referral for Data Gumbo

5. WHAT IS NOT ACCEPTABLE?

This section discusses 5 areas:

- Gifts and hospitality
- Business Courtesies

- Facilitation Payments
- Political Contributions
- Charitable Contributions

5.1. GIFTS AND HOSPITALITY

Data Gumbo accepts normal and appropriate gestures of hospitality and goodwill (whether given to or received from third parties) so long as the giving or receiving of gifts meets the following requirements:

- It is not made with the intention of influencing the receiving party, to obtain or reward the retention of a business or business advantage, or as an explicit or implicit exchange for favors or benefits.
- It is not made with the suggestion that a return favor is expected.
- It is in compliance with local law.
- It is given in the name of the company, not in an individual's name.
- It does not include cash or a cash equivalent (e.g. a voucher or gift certificate).
- It is given or received openly, not secretly.
- It is not offered to, or accepted from a government official, representative, politician or political party without the prior approval of the company's Director of Compliance.

Data Gumbo recognizes that the practice of giving and receiving business gifts varies between countries, regions, cultures, and religions, so definitions of what is acceptable and not acceptable will inevitably differ for each.

If there is any uncertainty, seek further advice from the company's Head of Compliance.

5.2. BUSINESS COURTESIES

"Business Courtesy" refers to something of value that is provided to customers and potential customers as a means of developing a legitimate relationship with that customer. This includes meals, entertainment, discounts on products and services not readily available to the general public, payment of travel expenses, personal favors and token gifts.

Data Gumbo prohibits its employees from corruptly providing Business Courtesies of any value to any individual, including Government Officials, in exchange for that individual taking some action that benefits Data Gumbo.

Because some of Data Gumbo's customers and potential customers are state-owned or state-controlled companies, Business Courtesies to these customers may implicate both U.S. laws (including the FCPA) and local laws. The Company must take care to ensure that Business Courtesies do not constitute a corrupt payment to individuals, including Government Officials. Only legitimate and reasonable Business Courtesies, consistent with the Gift & Entertainment Policy, may be provided by Data Gumbo employees to certain customers. In addition, reimbursement of reasonable and bona fide travel, food, lodging and other comparable expenses for government officials, party officials or candidates may be permissible provided that:

- The payment is not contrary to United States, local or other applicable laws, and

- The payment is for legitimate expenses that relate directly to the demonstration or explanation of Data Gumbo services, or to the execution or performance of a contract with the foreign government or agency

Before any travel, food, lodging or other comparable expenses for government officials, party officials or candidates are provided, they must first be submitted to the Director of Compliance for approval.

Any questions regarding the propriety of Business Courtesies should be directed to Data Gumbo's Compliance Department.

5.3. FACILITATING PAYMENTS

While in some countries where Data Gumbo conducts business, it may be local practice for businesses to make payments of nominal value to low-level Government Officials in order to expedite or "facilitate" routine government action, such payments, whether legal or not, are prohibited by this policy. Examples of such routine, non-discretionary actions may include:

- providing police protection
- granting visas or utility services
- clearing customs

Such payments are called "facilitating payments." Facilitating payments, whether legal or not, are prohibited by this Policy.

5.4. POLITICAL CONTRIBUTIONS

Many Company employees participate in the political life of their respective communities. Data Gumbo fully supports active involvement in political processes by its Employees, such as voting according to their own beliefs and making political contributions with their own funds. However, employees are prohibited from making any direct or indirect contribution of cash, merchandise, services, or other property on behalf of the Company to any candidate for public office, or to any political party, political advocacy group or other political organization. Employees may not use Company resources and assets for personal activities in supports of their choice of political party, candidate, or cause. Corporate expenditures of a nonpartisan nature may be made in support of legislative issues of concern to the Company, but only with prior written approval from the CEO.

5.5. CHARITABLE CONTRIBUTIONS

Data Gumbo accepts (and indeed encourages) the act of donating to charities – whether through services, knowledge, time, or direct financial contributions (cash or otherwise) – and agrees to disclose all charitable contributions it makes.

Employees must be careful to ensure that charitable contributions are not used to facilitate and conceal acts of bribery.

For questions concerning whether charitable donations made are legal and ethical under local laws and practices, contact the company's Head Compliance.

6. THE UNITED STATES FOREIGN CORRUPT PRACTICES ACT.

The Foreign Corrupt Practices Act (FCPA) is a United States law passed in 1977 that prohibits U.S. firms and individuals, and any company doing business in and/or based in the US from paying bribes to foreign officials in furtherance of a business deal. U.S. companies are liable for failing to prevent such acts by those acting on its behalf, no matter where the act takes place. The FCPA places no minimum amount for a punishment of a bribery payment. Specifically, the FCPA prohibits:

- Offering or promising to pay, paying, or authorizing the payment of money (or anything of value) to a foreign official
- In order to influence any act or decision of the foreign official in his or her official capacity
- To secure any other improper advantage in order to obtain or retain business.

All Data Gumbo directors, officers, employees, worldwide offices, their associates, and all third parties acting on behalf of Data Gumbo as distributors, agents, representatives, consultants, and partners will comply with the letter and the spirit of the FCPA at all times.

The FCPA also requires Data Gumbo, including its employees and subsidiaries (U.S. and international), to keep books records, and accounts in reasonable detail so that they accurately reflect transactions undertaken and to devise and maintain a system of internal accounting controls sufficient to provide reasonable assurance that transactions are executed as authorized by management and recorded properly. There are no exceptions to these requirements. Employees may not take any step to undermine the accounting controls implemented by Data Gumbo to provide reasonable assurances against accounting errors and fraud.

Link to the official FCPA guide:

https://www.justice.gov/sites/default/files/criminal-fraud/legacy/2015/01/16/guide.pdf

7. THE UNITED KINGDOM BRIBERY ACT 2010.

The Act has a wide jurisdictional reach and underscores importance of “adequate procedures”. The UK Bribery Act is broader in scope than the US FCPA.

The Bribery Acts creates four distinct criminal offences:

- Corporate offence to fail to prevent bribery
- Offence of giving and receiving bribes
- Offence of bribing a foreign public official
- Offence targeted at senior officers of a corporation who consent to, or connive at, bribery

The Act generally extends jurisdiction to offenses committed in the UK and those committed elsewhere while retaining a “close connection” to the UK. British citizens, citizens of British Overseas Territories and bodies incorporated under the law of any part of the UK, among others, are deemed to have a “close connection” to the UK and may as a result be prosecuted also where the offense takes place outside the UK. For the corporate offense of failing to prevent bribery (section 7) the jurisdictional reach of the Act has been extended even further. Once it has been established that a commercial organization carries on parts of its business in the UK (regardless of its place of incorporation), jurisdiction exists even where the act of bribery itself takes place outside the UK. This means that, theoretically, also a Norwegian company, partly doing business in the UK, who’s North-

American agent bribes a Central-American official in Central-America, could be prosecuted in the UK for failure to prevent bribery.

Link to the official UK Bribery Act guide:
https://www.justice.gov.uk/downloads/legislation/bribery-act-2010-guidance.pdf

8. ADDITIONAL LAWS AND REGULATIONS.

Data Gumbo is required to abide by many international laws and regulations in addition to FCPA and UKBA, which includes but is not limited to, Brazilian Clean Company Act 2014, Italian Anti-mafia Legislation, UK MSA Supply Chain Provisions, and other applicable regulations. The requirements correspond with FCPA and UKBA regulations and will be executed in an identical manner and addressed on a case-by-case basis as needed.

9. SANCTIONS.

This section provides an overview of the current Office of Foreign Assets Control (OFAC) Laws. It is NOT intended to provide guidance on whether any specific activity or transaction is permitted under applicable laws and regulations. All services provided and all transactions conducted by or through the Data Gumbo must comply with all OFAC Laws. If there is a question concerning these requirements or if you have been asked to do something which conflicts with these requirements, you should promptly contact the Company's Head of Compliance.

9.1. OFAC administers economic sanctions against targeted non-U.S. countries, organizations, and individuals. OFAC Laws related to its sanctions programs can be found in a series of Presidential executive orders, statutes, and regulations. Sanctions, or restrictions, are imposed based on U.S. foreign policy and national security concerns. Many of the sanctions are based on United Nations and other international mandates. The OFAC Laws can involve prohibiting unlicensed trade, blocking assets, prohibiting certain types of unlicensed commercial and financial transactions, or a combination of these measures. The OFAC Laws discussed below have significant civil and criminal penalties and are vigorously enforced.

The United Nations Consolidated Sanctions List can be found at:
https://www.un.org/securitycouncil/content/un-sc-consolidated-list

9.2. The laws and regulations administered and enforced by OFAC prohibit or restrict "U.S. Persons" (as defined below) from engaging in or facilitating transactions involving specified countries, organizations, and individuals, which are listed on OFAC's List of Specially Designated Nationals ("SDN") and Blocked Persons ("SDN List"), the Executive Order 13599 List ("EO 13599 List") or which are otherwise the target of the OFAC Laws.

The OFAC Consolidated Sanctions List can be viewed at
https://sanctionssearch.ofac.treas.gov/

9.3. Countries and regions subject to broad comprehensive sanctions include but are not limited to the Ukraine, Cuba, Iran, North Korea, Sudan, and Syria and are subject to change. While there are differences among the regulations applicable to each country, as a general matter, OFAC Laws prohibit U.S. Persons, wherever located, from providing goods or services, including financial services, to persons where the benefit of such services is received in any of these countries. Each

of these sanctions includes licenses that permit certain types of transactions that are determined to be consistent with U.S. policy toward the applicable country. Any potential or existing business, trade or transaction with any of these countries (including any local citizens, institutions, organizations or groups) or involving goods or services received from or delivered to any of these countries, should be brought to the immediate attention of the Company's Head of Compliance.

9.3.1. The United States has recently eased sanctions related to Cuba and Iran. However, most elements of the U.S. embargo against these countries remain in place and most transactions involving these countries remain prohibited, unless licensed by OFAC.

9.3.2. OFAC also administers more targeted sanctions against specified narcotics traffickers, terrorists, transnational criminal organizations, malicious cyber-related activities and weapons proliferators, as well as individuals and entities associated with a broad range of countries and regimes—including but not limited to Iraq, the Democratic Republic of the Congo, Belarus, the Balkans, Burundi, Central African Republic, Lebanon, Liberia, Libya, Venezuela, Yemen, South Sudan, Sudan/Darfur, Somalia, and Zimbabwe—who are included on the SDN List. Entities that are owned or controlled by an SDN are also subject to OFAC sanctions, whether or not those entities appear on the SDN List. OFAC also maintains the EO 13599 List, which is a list of persons identified by OFAC as meeting the definition of the term Government of Iran or the term Iranian financial institution.

9.3.3. Some transactions may be permitted under a particular sanctions program, but generally, all transactions with SDNs or persons on the EO 13599 List are prohibited and any property in which the SDN or person on the EO 13599 List has an interest must be blocked. If any Data Gumbo director, officer, employee or agent encounters a transaction involving an SDN or person on the EO 1399 List, the Company's Head of Compliance should be contacted.

9.3.4. The United States maintains limited sanctions against persons in Russia's financial, energy and defense and related materials sectors that appear on OFAC's Sectoral Sanctions Identification List ("SSI List"). The sanctions against these companies are much more limited than the sanctions against persons on the SDN List and focus on dealings involving the debt and equity of these companies and the provision of goods and services to certain oil projects in Russia. Many transactions with SSI entities are still permitted, although the Company's Head of Compliance shall be consulted regarding transactions with companies on the SSI List.

Implementing regulations for many of the OFAC sanctions programs are Codified in Title 31 of the Code of Federal Regulations are available on the OFAC website at:
http://www.treasury.gov/ofac/

9.3.5. Specific organizations and individuals who have been targeted under the various sanctions programs are listed on the SDN List and the EO 13599 List and the Consolidated Screening List, which are supplemental but not exclusive lists of persons and entities with which the U.S. Persons who are directors, officers, employees or agents of Data Gumbo may not deal.

The SDN List and the EO 13599 List are accessible at the OFAC website. The Consolidated Screening List, which includes the SDN List and other U.S. government lists of sanctioned and prohibited individuals and entities, is available at:
http://apps.export.gov/cslsearch#/csl-search

9.3.6. In some instances, the OFAC Laws and regulations may require the rejection of a transaction, or the blocking of assets involved in a transaction. The summary provided above is current as of the latest revision date of this Compliance Policy. It is the responsibility of all directors, officers, employees, and agents to keep up to date on changes and additions made to the OFAC Laws.

9.4. Application of OFAC Prohibitions to U.S. Persons at Data Gumbo

9.4.1. OFAC's prohibitions apply to transactions involving the United States or conducted by any U.S. Person, wherever located. U.S. Person means any United States citizen, wherever in the world the person is located (including dual citizens), any permanent resident alien of the U.S. (wherever located), any person (natural or non-natural) located in the U.S., and any entity organized under the laws of a U.S. jurisdiction including its overseas branches/divisions. OFAC prohibitions thus apply to any director, officer, employee or agent of Data Gumbo who is a U.S. Person. The regulations generally prohibit a U.S. Person from "approving," "facilitating," participating in, financing or guaranteeing a transaction involving a person or entity on the SDN List, the EO 13599 List or who is otherwise the target of the OFAC Laws and regulations and from taking any action to evade or avoid OFAC Laws.

9.4.2. With respect to U.S. sanctions involving Cuba and in certain cases, Iran, the term "U.S. Person" also means any foreign subsidiary or affiliate owned or controlled by a U.S. Person. The Cuba and in certain cases, Iran sanctions programs apply not only to Data Gumbo as an entity, but also to any foreign subsidiaries of or entities controlled by Data Gumbo, wherever in the world they are located. Thus, under the *Cuba and (in certain cases) Iran* sanctions programs, Data Gumbo's non-U.S. subsidiaries and other non-U.S. entities controlled by Data Gumbo, and not just its U.S. directors, officers, employees and agents, would be considered U.S. Persons.

9.4.3. Data Gumbo's OFAC Policy prohibits U.S. Persons at Data Gumbo from entering into business relationships on behalf of Data Gumbo with any OFAC-sanctioned party, or any party owned or controlled by or acting on behalf of any OFAC-sanctioned party, and requires directors, officers, employees and agents to report the attempted transaction to a Compliance Officer and/or the General Counsel.

9.4.4. Data Gumbo shall ensure that customer screening and customer due diligence procedures are in place to promote the identification of potential sanctions violations or other potentially impermissible transactions. Such procedures shall also provide for appropriate distributor screening and distributor due diligence to ensure Data Gumbo's distributors comply with Sanctions laws applicable to the Company.

9.5. Recusal by an Employee Who is a U.S. Person

9.5.1. If a director, officer, employee or agent of Data Gumbo who is a U.S. Person, including any Data Gumbo director, officer, employee or agent who is in the United States temporarily, finds that he or she has been assigned to work on a transaction or business matter that has been identified as potentially involving OFAC sanctions, that director, officer, employee or agent must immediately recuse himself/herself from dealing with the transaction or business

matter. The U.S. Person must also immediately inform his or her supervisor, as well as the company's Head of Compliance of such recusal.

9.6. Background on EU Sanctions

9.6.1. This section provides an overview of current EU sanctions regulations. It is NOT intended to provide guidance on whether any specific activity or transaction is permitted under applicable laws and regulations. All services provided and all transactions conducted by or through the Data Gumbo must comply with applicable EU sanctions regulations. If there is a question concerning these requirements or if you have been asked to do something which conflicts with these requirements, you should promptly contact the company's Head of Compliance. Although the jurisdictional reach of EU sanctions regulations can vary depending on the targets, there are several common themes:

- EU organized entities must comply with EU sanctions.
- Other countries outside of the EU also often follow EU sanctions such as Switzerland, Norway or UK protectorates or dependencies.
- EU citizens are subject to EU laws, even if they are living or working outside of the EU.
- Activities in, or partially in, the EU are covered. Any non-EU entity or person is subject to EU Sanctions Laws while they are acting within the territory of the EU.
- The EU devolves enforcement of sanctions to competent authorities of each EU Member State, such as HM Treasury and the Office of Financial Sanctions Implementation in the United Kingdom.

The UK HMRC/OFSI Sanctions list can be located at
https://www.gov.uk/government/publications/financial-sanctions-consolidated-list-of-targets/consolidated-list-of-targets

9.6.2. EU sanctions can take different forms, but the most common measures are asset freezes ("EU Financial Sanctions"), and arms embargoes, general or specific sectoral trade or export embargoes ("EU Economic Sanctions", collectively with EU Financial Sanctions, "EU Sanctions"). EU sanctions apply to: (i) any person within the territory of the EU; (ii) any person inside or outside the territory of the EU who is a national of an EU Member State; (iii) any legal person, entity or body, inside or outside the territory of the EU, which is incorporated or constituted under the law of an EU Member State; (iv) any legal person, entity or body in respect of any business done in whole or in part within the EU; and (v) any person on board any aircraft or any vessel under the jurisdiction of an EU Member State (collectively, "EU Persons").

9.6.3. EU Financial Sanctions are imposed on persons or entities (so called "designated persons") listed on the EU's Consolidated List of Persons, Groups and Entities ("EU Consolidated List of Persons").

9.6.4. EU Financial Sanctions include measures against government or ex-government officials and others suspected of human rights abuses, violations of public international law, internal repression or political instability, theft of state assets or funds, war crimes or assassination, terrorism and terrorist financing, being a member of Al Qaida, and assisting in nuclear

proliferation. EU Financial Sanctions also target persons profiting from any such violations, crimes or abuses.

9.6.5. EU Financial Sanctions apply to conduct in and from the EU and generally also apply to EU citizens and companies outside EU territory. It is a criminal offense to breach an EU Financial Sanction, without an appropriate license or authorization.

9.6.6. Although each sanctions regime is implemented by each EU Member State individually, it can constitute a criminal offense for an EU national or company anywhere in the world to: (i) deal with the funds or economic resources belonging to or owned, held or controlled by a designated person; (ii) make funds or economic resources available, directly or indirectly, to, or for the benefit of a designated person; (iii) intentionally circumvent financial sanctions; or (iv) fail to notify the regulator of possession of funds owned or controlled by a designated person. The definition of "funds" is broadly construed to include cash, all kinds of payment instruments, deposits, shares, derivatives, interest, guarantees, letters of credit and rights of set-off.

The EU Consolidated List of Persons is accessible on the EU website at: https://eeas.europa.eu/headquarters/headquarters-homepage_en/8442/Consolidated%20list%20of%20sanctions.

9.6.7. EU Economic Sanctions include embargoes with respect to certain products and services exported to a particular country. Where it is not prohibited to import or export goods, the particular good or destination or use may be restricted and subject to licensing. It can constitute a criminal offense to import or export goods without the required license.

9.6.8. EU Economic Sanctions are imposed on a country and typically involve prohibiting or restricting trade, prohibiting, or restricting certain types of commercial and financial transactions with natural or legal persons in the respective country or other appropriate measures. Prohibitions or restrictions will apply in relation to goods and services which can be used for military purposes, internal repression or nuclear proliferation, for example, exporting or supplying arms or dual use products and associated technical assistance, training and financing or technologies. Sectoral EU Economic Sanctions include restrictions or prohibitions in various sectors including oil and gas, financial services, access to capital markets, luxury goods, certain computer software and technologies.

9.6.9. The summary provided above is current as of the latest revision date of this Compliance Policy. It is the responsibility of all directors, officers, employees, and agents to keep up to date on changes and additions made to the EU Sanctions.

9.7. Penalties

9.7.1. Violations of the Sanctions Laws carry significant civil and criminal penalties. For violations of the OFAC Laws, criminal penalties can include fines of up to $1,000,000 per violation and imprisonment for up to 20 years. Civil penalties for violations of the OFAC Laws can include fines of $250,000 per violation or twice the amount of the transaction that is the basis of the violation, whichever is greater. The consequences of a failure to abide by EU Sanctions can be similarly severe. Although, each Member State's penalties vary, violations of EU

Sanctions may lead to prosecution by EU Member States and result in serious criminal and administrative penalties for the Company and associated individuals.

10. RECORD KEEPING.

Data Gumbo will keep detailed and accurate financial records and will have appropriate internal controls in place to act as evidence for all payments made. We will declare and keep a written record of the amount and reason for hospitality or gifts accepted and given and understand that gifts and acts of hospitality are subject to managerial and Compliance department review.

11. EMPLOYEE RESPONSIBILITIES.

As an employee of Data Gumbo, you must ensure that you read, understand, and comply with the information contained within this policy, and with any training or other anti-bribery and corruption information you are given.

All employees and those under our control are equally responsible for the prevention, detection, and reporting of bribery and other forms of corruption. They are required to avoid any activities that could lead to, or imply, a breach of this anti-bribery policy.

Under the FCPA, guilty knowledge can be proven by evidence of unwarranted obliviousness or "willful blindness" to any action, inaction, language, or other evidence that should reasonably alert you to the high probability of an FCPA violation. Data Gumbo employees may not ignore circumstances suggesting that an otherwise legitimate payment is being used for corrupt purposes or bribery.

If you have reason to believe or suspect that an instance of bribery or corruption has occurred or will occur in the future that breaches this policy, you must notify the company's Head of Compliance.

Data Gumbo will not retaliate against support anyone who raises concerns in good faith under this policy in accordance with Data Gumbo's anti-retaliation policy, even the allegations are not substantiated following an investigation.

Data Gumbo will ensure that no one suffers any detrimental treatment as a result of refusing to accept or offer a bribe or other corrupt activities, or because they reported a concern relating to potential act(s) of bribery or corruption.

If you have reason to believe you've been subjected to unjust treatment as a result of a concern or refusal to accept a bribe, you should inform your direct supervisor and the company's Head of Compliance.

If any employee breaches this policy, they will face disciplinary action up to and including termination.

12. REVISION HISTORY

Date of Change	Responsible	Summary of Change
July 2021	Human Resource	Initiated
October 2021	J. Hertel, Head of Compliance	Updated