Corporate Personal Data Privacy and Records Management Policy

Policy Number: GP-C-18
Owner: Candice Hester, Chief of Staff
Responsible Office: Chief of Staff
Approved By: Adam Stedham, President GP Strategies
Reviewed By & Date: Data Privacy Records Management Committee December 16, 2019
Original Approved Date: May 14, 2018
Currency Date: January 1, 2020
Review Date: January 1, 2021

1. Purpose

The purpose of this Policy is four-fold. First, to set the commitment, approach and framework for GP Strategies Corporation and its subsidiaries and controlled affiliates (GP Strategies) for complying with data subject privacy and records management laws worldwide. Second, to provide for the ongoing direction and administration of privacy data handling practices and procedures through the establishment of the Corporate Data Privacy and Records Management Program. Third, to provide management and administration assignment for oversight of company records, some of which may contain Personal Identity Information of employees, customers, business partners and others. Fourth, to provide an organizational focal point for rights administration on behalf of employees, access to the Program and for ongoing initiatives that must be conducted to comply with the applicable laws.

GP Strategies is motivated by our respect for personal privacy to build capabilities to protect data subjects from harm due to identity exposure, build the trust of our colleagues through our privacy practices and achieve legal and contractual compliance with our clients and vendors for personal data management.

2. Scope and Applicability

This Policy applies to GP Strategies and GP Strategies Personnel worldwide. This policy applies to all statutorily defined privacy data received by GP Strategies, in any format, including biometric, electronic, genetic, paper, verbal, recorded or visual and for the management of records administration practices and procedures.

Definitions related to this Policy are set forth in Section 7 below.

3. Policy

GP Strategies' policy is to comply with all privacy laws applicable to GP Strategies, including but not limited to privacy laws of the U.S. Government, the individual U.S. states, the Asia Pacific

Economic Cooperation (APEC) forum and the General Data Protection Regulation of the European Economic Area.

GP Strategies is committed to collecting, using, storing and disclosing personal information in compliance with the data privacy laws and regulations of all countries where we conduct business.

GP Strategies uses the General Data Protection Regulation (GDPR), the EU-U.S. Privacy Shield Framework, the Swiss-U.S. Privacy Shield Framework(s) (Privacy Shield) and U.S. state laws such as the California Consumer Privacy Act (CCPA) among others to guide its worldwide policy and compliance framework for data privacy and records management. A Data Privacy and Records Management Program shall be established to implement and oversee compliance consistent with this Policy and any country laws applicable to GP Strategies which may be stricter than the requirements stated herein.

GP Strategies complies with the EU-U.S. Privacy Shield Framework and the Swiss-U.S. Privacy Shield Framework(s) (Privacy Shield) as set forth by the U.S. Department of Commerce regarding the collection, use, and retention of personal information transferred from the European Union, the United Kingdom and Switzerland to the United States in reliance on Privacy Shield. GP Strategies has certified to the Department of Commerce that it adheres to the Privacy Shield Principles with respect such information. If there is any conflict between the terms in this privacy Policy and the Privacy Shield Principles, the Privacy Shield Principles shall govern. To learn more about the Privacy Shield program, and to view evidence of certification, please visit https://www.privacyshield.gov/.

If any law or regulation relating to privacy data use and records management establishes a stricter threshold than those set forth in this Policy becomes applicable to GP Strategies, it is GP Strategies' policy to comply with such requirement in connection with any information subject to such law or regulation. Where the GDPR and/or for example the CCPA sets a stricter standard than the Privacy Shield Principles, it is GP Strategies' policy to comply with the GDPR and /or CCPA among others.

It is the Policy of GP Strategies that we Do Not Sell or Buy Personal Information.

It is the responsibility of the Officers of GP Strategies to provide implementation of this Policy.

A committee, with Officer level executive sponsorship, of GP Strategies employees representing the organizational of GP strategies will be appointed to work with the committee staff to support corporate awareness outreach, training, lawful administration, employee feedback and Program implementation. The Committee shall set standards and procedures as needed to meet the spirit and intent of the various privacy laws.

To meet the requirements of the various laws the Program Committee shall establish, review and enforce records management and retention administration.

Privacy Data Handling Standards and Practices Adopted and Authorized by this Policy

In the laws of some countries, provinces and states, terms other than those in the GDPR and Privacy Shield are used to describe or structure privacy data handling practices. These handling practices are not a limitation but shall be recognized and used as appropriate. Some laws use the term Personal Identity Information (PII), and where some standards set forth a category of Sensitive Personal Identity Information (SPII), defined privacy data may be subject to additional privacy handling policy and /or procedural requirements. GP Strategies will recognize information:

- regarding and/or received from clients subject to any specific agreement with, or notice to, the client, as well as additional applicable laws and professional standards;
- where legal matters may be subject to data privacy handling laws;
- where risk management practices may be subject to data privacy handling laws;
- where information technology management and security practices may be subject to data privacy handling laws;
- where internal human resource policies regarding GP Strategies' personnel may be subject to data privacy handling laws; and
- received via GP Strategies' websites must adhere to this Policy and applicable country laws, may be subject to web and social media technological practices to administer data handling and that privacy information shall be provided on web site statements.

GP Strategies employees are permitted to internally and externally exchange Business Contact Information (BCI) credentials issued to them for the purposes for which they were hired and for conducting the business of the GP Strategies. (See definition section)

When required, GP Strategies may aggregate sensitive privacy data for government reporting purposes but such data will not provide individual identifiers.

GP Strategies has adopted this Policy to implement the GDPR, Privacy Shield, CCPA and others principles of Lawfulness, Fairness and Transparency; Purpose limitation; Data Collection and Retention Minimization; Accuracy; Rectification; Storage Limitation; Integrity and Confidentiality; and Accountability.

TYPES OF PERSONAL IDENTITY INFORMATION COLLECTED AND PURPOSES FOR WHICH PERSONAL IDENTITY INFORMATION IS COLLECTED AND USED:

Where GP Strategies collects privacy data directly from individuals it will make information available to them about the purposes for which it collects and uses such information, the types of third parties to which GP Strategies discloses that information, the choices and means, if any, GP

Strategies offers individuals for limiting the use and disclosure of data about them, and any other information required by the GDPR, CCPA and Privacy Shield Principles. Notice will be provided in clear and conspicuous language when individuals are first asked to provide privacy data to GP Strategies, or as soon as practicable thereafter, and in any event before GP Strategies uses or discloses the information for a purpose other than that for which it was originally collected.

Where GP Strategies receives or transfers privacy data from its subsidiaries, affiliates or other entities it will use and disclose such information in accordance with the applicable laws and the choices made by the individuals to whom such information relates.

GP Strategies may receive privacy data from its clients or other third parties in connection with the conduct of GP Strategies' business. GP Strategies will use any such data only as permitted by any agreement between GP Strategies and the other party and the other party's documented instructions. If a client engagement involves a transfer of privacy data, for example from the European Economic Area (EEA) to the United States, the relevant clients are responsible per the GDPR and Privacy Shield for providing appropriate notice, where required, to the individuals whose data may be transferred to GP Strategies, including providing individuals with certain choices with respect to the use or disclosure of their data, and obtaining any requisite consent. GP Strategies will administer such data in accordance with its clients' instructions.

Personal Identity Information from GP Strategies Web and Social Media Sites Use: GP Strategies may collect data defined as privacy data when a person ("data subject", "consumer") chooses to access and use GP Strategies sites. Information about the application of this Policy for site use of data collection shall be available on GP Strategies web and media sites.
Internet and Social Media Privacy: The application of this Policy to GP Strategies Web and Social Media Sites shall be made public and may be found at:

http://www.gpstrategies.com

Personal Identity Information Regarding GP Strategies Personnel: GP Strategies may exercise its rights under the GDPR, CCPA and other laws to transfer personally identifiable (privacy) information (PII) regarding GP Strategies personnel. This PII may include, without limitation, business contact information, employee ID, job role and reporting line, demographic information, work history, benefits information, travel activities, supervisor and colleague contacts, compensation and performance ratings. GP Strategies uses such information only as necessary to perform its contractual obligations to GP Strategies Personnel, to comply with legal obligations, and for the purposes of its legitimate interests in connection with its business, in each case only to the extent permitted by the GDPR, CCPA or other applicable law or regulation.

CHOICE:

Where applicable in accordance with the GDPR and CCPA (or other applicable data protection law or regulation), when not already authorized by the lawful statutory processing sections, GP Strategies will offer individuals the opportunity to choose (opt-in) whether their PII and SPII is (a) collected, (b) to be disclosed to a non-agent third-party, or (c) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

ACCOUNTABILITY FOR ONWARD TRANSFER (TRANSFERS TO AGENTS):

GP Strategies will only transfer designated privacy data to its agents for limited and specified purposes consistent with the GDPR, CCPA and Privacy Shield Principles and will not transfer privacy data to its agents unless the agent has entered into an agreement (contract) with GP Strategies requiring the agent to protect the data to at least the level required by the applicable law. Where GP Strategies has knowledge that an agent is using or disclosing information in a manner contrary to this Policy, GP Strategies will take reasonable steps to prevent or stop the use or disclosure. GP Strategies remains responsible under the applicable laws if its agent processes data in a manner inconsistent with the GDPR, CCPA and Privacy Shield Principles except where GP proves it is not responsible for the event giving rise to the damage.

ACCESS, CORRECTION AND DELETION:

Upon request, GP Strategies will grant individuals' access to privacy data that it holds, that is not already available in a self-service format, about them as required by applicable law or regulation. In addition, GP Strategies will permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete in accordance with the GDPR, CCPA and Privacy Shield Principles for records management. GP Strategies will also permit individuals to correct, amend, or delete accurate information that has been processed in violation of the GDPR, CCPA and Privacy Shield Framework.

SECURITY:

GP Strategies will take reasonable appropriate technical and organizational measures to protect privacy data in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction. GP Strategies will provide instruction and direction on using approved IT security frameworks for handling processing activities to all units of GP Strategies and third parties we contract with. Processing activities includes collecting, accessing, storing, transferring, analyzing and manipulating data.

DATA INTEGRITY/PURPOSE LIMITATION:

GP Strategies will use privacy information only in ways that are compatible with the purposes for which it was collected or subsequently authorized by the individual. GP Strategies will take reasonable steps to ensure that privacy data is collected under the principle of minimization,

securely stored, is stored for appropriately designated periods (records management), and is relevant to its intended use, accurate, complete, and current. GP Strategies will retain privacy data identifying or making identifiable the individual data subject only for as long as it serves a purpose consistent with the foregoing purpose limitation. If GP Strategies terminates its voluntary certification in Privacy Shield we will continue complying with the GDPR, CCPA, and Privacy Shield Principles with respect to any privacy data collected under the Privacy Shield certification regime.

RECOURSE, ENFORCEMENT AND LIABILITY:

Verification. GP Strategies will conduct periodic program compliance evaluations, audits, surveys or reports as appropriate of its relevant privacy practices to verify adherence to this Policy. As part of its verification, GP Strategies may engage third parties to conduct assessments of compliance with this Policy.

Intake and Processing of Inquiries, Dispute Resolution and Remedies:

GP Strategies encourages employees and other parties affected by GP Strategies' data privacy practices to first contact the GP Strategies Data Privacy and Records Management Program Office or their respective GP Strategies Data Privacy Officer (DPO) for information about data handling practices. The Program Office will support the employee and DPO by conducting research for inquiries and erasures, investigate breaches and attempt to resolve complaints and disputes regarding use and disclosure of privacy data by reference to the GDPR, CCPA and Privacy Shield Principles.

GP Strategies will cooperate with the data protection authorities (DPA) of any EEA country and participate in any dispute resolution procedures they establish. In non-EAA countries with data privacy laws where GP Strategies conducts business, GP will follow those laws.

Process for GP Strategies Personnel: GP Strategies Personnel may also file an inquiry or complaint concerning GP Strategies processing of their personal privacy data with GP Strategies' Human Resources (HR) Department who will communicate and coordinate with the Program Committee administrative structure established to implement this Policy. GP Strategies evaluate and take appropriate take steps to address Program administration issues arising out of a limitation or failure to recognize issues with the GDPR, CCPA and Privacy Shield Principles or others involved in this Policy. If a GP Strategies personnel complaint cannot be resolved through these internal processes, GP Strategies will consult and cooperate with the relevant EEA data protection authority (DPA), as appropriate, and comply with their advice.

Alternatively: For non-EAA inquiries/complaints, with no specific in-country governance procedures, that cannot be resolved between GP Strategies and the requestor/ complainant, both parties may voluntarily agree to use the dispute resolution procedures for investigation and resolution of complaints to resolve disputes pursuant to the Privacy Shield Principles.

Collection and Use of Information for Emergencies: The GDPR, CCPA and other laws allow for the collection and use of privacy data for the protection (warning, mitigating, responding, recovering) of the data subject/ consumer and others who may potentially be or have been harmed. GP Strategies will collect and use privacy data as needed in accordance with the GDPR and other applicable laws for preparing for and during emergency and public safety preparedness situations.

Federal Trade Commission Authority: GP Strategies Corporation is subject to the investigatory and enforcement powers of the U.S. Federal Trade Commission (FTC).

Binding Arbitration Possible: As further explained in the Privacy Shield Principles, a binding arbitration option will also be made available to address residual complaints not resolved by any other means.

LIMITATION ON APPLICATION OF PRINCIPLES:

Adherence by GP Strategies to the GDPR, CCPA and Privacy Shield Principles among other laws may in some cases be limited (a) to the extent required in connection with its c o r p o r a t e legal, contractual or ethical obligations; (b) to the extent necessary to meet national security, public interest or law enforcement obligations; and (c) to the extent expressly permitted by an applicable law, rule or regulation such as emergency contact information collection.

4. Related Policies, Standards, Procedures and Program Documents

GP Strategies Corporate Data Privacy and Records Management Program Documents shall be maintained for availability, this includes: Employee Frequently Asked Questions, Web and Social Media Site Frequently Asked Questions, Records Management Schedules, Web and Social Media Site Guidance, Fact Sheets, Program Administration Information. Privacy management Program documents are generally available to employees but may be subject to screening, redaction or denial of access after inspection for those containing fellow employee privacy data, company confidential information, patent information, financial information, or of a regulatory or statutory nature on a case by case basis.

5. Violations

Violation of this Policy may result in disciplinary action, up to and including termination from GP Strategies. Agents who violate this Policy are subject to contract termination.

6. Exceptions

Any request for an exception from this Policy must be submitted in writing to the GP Strategies Data Privacy and Records Management Committee, a country Data Protection Officer (DPO), Company Officers or such other persons identified in Program informational materials in an exception process prescribed by GP Strategies. Requests for exceptions to this Policy, recognizing GP Strategies may or may not have latitude to grant an exception, must be submitted in writing to the Program administrators for consideration.

7. Definitions

"General Data Protection Regulation" or "GDPR" means Regulation (EU) 2016/679 of The European Parliament and of The Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation) and as from time to time amended.

"Privacy Shield Principles" means the set of data protection principles issued per Treaty protocols by the United States Department of Commerce and the European Commission from time to time as amended and available at www.privacyshield.gov.

"California Consumer Privacy Act" or "CCPA" means the legislation enacted, and from time to time amended, to enhance privacy rights and consumer protection for residents of California, United States to amend Part 4 of Division 3 of the California Civil Code. The effective date is Jan 1st, 2020 and thereafter.

"Agent" means any third-party that collects, processes or uses privacy data under the instructions of, and solely for, GP Strategies or to which GP Strategies discloses privacy data for use on GP Strategies behalf.

"Business Contact Information" includes but may not be limited to: name, job title, job function, name of employer, information about the employer (such as business unit or group number), and work contact details of work telephone numbers, work email address, work mailing address and work office address.

"Consumer" from the California Consumer Privacy Act (CCPA) means a natural person who is a California resident, as defined in Section 17014 of Title 18 of the California Code of Regulations, as that section read on September 1, 2017, however identified, including by any unique identifier and as may be later amended.

"Data Subject" from the General Data Protection Regulation (GDPR) means an identified or identifiable natural person; an identifiable natural person is one who can be identified, directly

or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

"Encrypted Electronic Data" includes information that is encoded, pseudonymised or anonymized.

"GP Strategies Corporation" means GP Strategies Corporation, a Delaware corporation, its predecessors, successors, subsidiaries, divisions and groups in the United States.

"GP Strategies Personnel" in context means any current, former or prospective employee or independent contractor of GP Strategies.

"GP Strategies" means GP Strategies Corporation and its subsidiaries and controlled affiliates.

"Personal Identity Information" or "PII" means any information relating to an identified or identifiable natural person ("See Data Subject" definition).

"Sensitive Personal Identity Information" or "SPII" definitions may vary from country to country. In this Policy SPII usually means elements of PII that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, views or activities, that concerns health, sex or sex life, information about social security benefits, or information on criminal or administrative proceedings and sanctions other than in the context of pending proceedings. In addition, GP Strategies will treat as sensitive personal information any privacy information received from a third-party where that third-party treats and identifies the information specific to an applicable law or identifying it as sensitive (SPII).

8. Document Change Control

Date	Reason for Change	Author
February 9, 2018	Initial development. To include the GDPR and finalize approval.	J. Galante, J. LaFleur
May 14, 2018	Approval v1.0	A. Stedham
May 14, 2018	Formatting/numbering convention	T. Fobes
December 16, 2019	v2.0 Insert required updates for Privacy Shield for Brexit, the CCPA and change of Chief of Staff	A. Majeed, J. LaFleur