

Personal Data Privacy and Records Management Policy



Policy Number: GP-C-18

Owner: Patricia Begley

Responsible Office: Chief of Staff

Approved By: Adam Stedham, President GP Strategies

Reviewed By & Date: Data Privacy Records Management Committee April 13, 2018

Approved Date: May 14, 2018

Review Date: May 14, 2019

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 laws worldwide. Second, to provide for the ongoing administration of privacy practices and procedures. 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 employee access to the program and for ongoing initiatives that must be conducted to comply with the applicable laws.

Our respect for personal privacy motivates us to build capabilities to protect data subject harm from exposure of Personal Identity Information (PII), build the trust of our colleagues through our privacy practices and achieve legal and contractual compliance with our clients and vendors for PII management.

2. Scope and Applicability

This Policy applies to GP Strategies and GP Strategies Personnel worldwide. This policy applies to all PII received by GP Strategies, in any format, including biometric, electronic, genetic, paper, verbal, 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.

Personal Data Privacy and Records Management Policy



GP Strategies uses the General Data Protection Regulation (GDPR) and the EU-U.S. Privacy Shield Principles 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 other country laws applicable to GP Strategies which may be stricter than these requirements.

GP Strategies adheres to the Privacy Shield Principles agreed to by the U.S. and the European Union (EU) for data transfers between these two countries. GP Strategies has certified to the U.S. Department of Commerce that it adheres to the Privacy Shield Principles. To learn more about the Privacy Shield program, and to view the GP Strategies Corporation certification, please visit www.privacyshield.gov.

If any law or regulation relating to privacy or the use of PII and records management establishes a stricter standard 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 sets a stricter standard than the Privacy Shield Principles, it is GP Strategies' policy to comply with the GDPR.

Some types of Personal Identity Information (PII), and where some standards set forth a category of Sensitive Personal Identity Information (SPII), may be subject to additional privacy-related policy and procedural requirements. For example, information:

- regarding and/or received from clients may be subject to any specific agreement with, or notice to, the client, as well as additional applicable laws and professional standards;
- regarding GP Strategies' personnel is subject to internal human resource policies; and
- Received via GP Strategies' websites is subject to our web and social media privacy 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 SPII data for government reporting purposes but such data will not provide individual identifiers.

GP Strategies has adopted this Policy to implement the GDPR's principles of Lawfulness, Fairness and Transparency; Purpose limitation; Data 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:

Personal Data Privacy and Records Management Policy



Where GP Strategies collects PII 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 PII about them, and any other information required by the GDPR and Privacy Shield Principles. Notice will be provided in clear and conspicuous language when individuals are first asked to provide PII 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 PII from its subsidiaries, affiliates or other entities it will use and disclose such information in accordance with the notices provided by such entities and the choices made by the individuals to whom such information relates.

GP Strategies may receive PII from its clients or other third parties in connection with the conduct of GP Strategies' business. GP Strategies will use any such PII 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 PII, 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 PII may be transferred to GP Strategies, including providing individuals with certain choices with respect to the use or disclosure of their PII, and obtaining any requisite consent. GP Strategies will administer such PII in accordance with its clients' instructions.

Personal Identity Information from GP Strategies Web and Social Media Sites Use: GP Strategies may collect PII when a person (data subject) chooses to access and use GP Strategies sites. Information about the application of this Policy for site use of PII 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 may be found at:

<http://www.gpstrategies.com>

Personal Identity Information Regarding GP Strategies Personnel: GP Strategies may exercise its rights under the GDPR and other laws to transfer 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, 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 or other applicable law or regulation.

Personal Data Privacy and Records Management Policy



CHOICE:

In accordance with the GDPR (or other applicable data protection law or regulation), when not already authorized by the lawful 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 PII to its agents for limited and specified purposes consistent with the GDPR and Privacy Shield Principles and will not transfer PII to its agents unless the agent has entered into an agreement (contract) with GP Strategies requiring the agent to protect the PII to at least the level required by the GDPR. 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 GDPR and the Privacy Shield Principles if its agent processes PII in a manner inconsistent with the GDPR 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 PII 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 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 and Privacy Shield Framework.

SECURITY:

GP Strategies will take reasonable appropriate technical and organizational measures to protect PII in its possession from loss, misuse and unauthorized access, disclosure, alteration and destruction.

DATA INTEGRITY/PURPOSE LIMITATION:

GP Strategies will use PII 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 PII 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 PII identifying or making identifiable the individual data subject only for as long as it serves a purpose consistent with the foregoing

Personal Data Privacy and Records Management Policy



purpose limitation. If GP Strategies terminates its voluntary certification in Privacy Shield we will continue complying with the GDPR and Privacy Shield Principles with respect to any PII collected under the Privacy Shield.

RECOURSE, ENFORCEMENT AND LIABILITY:

Verification. GP Strategies will conduct program periodic compliance audits 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.

Dispute Resolution and Remedies:

GP Strategies encourages employees and other parties affected by GP Strategies' data privacy practices to first contact the GP Strategies Privacy Program Office or their respective GP Strategies Data Privacy Officer (DPO) for Program information about practices. GP Strategies will investigate and attempt to resolve complaints and disputes regarding use and disclosure of PII by reference to the GDPR and Privacy Shield Principles.

GP Strategies will cooperate with the data protection authorities (DPA) of any EEA country and to 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 a complaint concerning GP Strategies processing of their PII with GP Strategies' Human Resources (HR) Department who will communicate and coordinate with the Program administrative structure established to implement this Policy. GP Strategies will take steps to remedy any Program administration issues arising out of a failure to comply with the GDPR and Privacy Shield Principles or this Policy. If a GP Strategies Personnel complaint cannot be resolved through this internal process, GP Strategies will cooperate with the relevant EEA data protection authority, as appropriate, and comply with their advice.

Alternatively: For non-EAA complaints, with no specific in-country governance procedures, that cannot be resolved between GP Strategies and the 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 allows for the collection and use of PII for the protection of the data subject and others who may be harmed. GP will collect and use PII in accordance with the GDPR and other applicable laws for preparing for and during emergency situations.

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

Personal Data Privacy and Records Management Policy



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 and Privacy Shield Principles may in some cases be limited (a) to the extent required in connection with its corporate 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. Requests for exceptions to this Policy must be submitted in writing to the Program administrators.

4. Related Policies, Standards, Procedures and Program Documents

GP Strategies Corporate Data Privacy and Records Management Program Documents - 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. All documents are available to employees.

5. Violations

Violation of this Policy may result in disciplinary action, up to and including termination for GP Strategies Personnel. 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 GP Strategies' Data Privacy Officer or such other persons identified in Program informational materials in an exception process prescribed by GP Strategies.

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).

"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 and available at www.privacyshield.gov.

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

Personal Data Privacy and Records Management Policy



“Business Contact Information” means 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. “Data Subject” 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” 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 means 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 information received from a third-party where that third-party treats and identifies the information 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