Corporate Personal Data Privacy and Records Management

Number	POL.XGB.018		
Geography	Global		
Scope	Corporate		
Owner	Sprenkeling, Kelly		
Reviewed By	Anderson, David; Brunson, Valderia; Majeed, Abu	**Date:**	November 13, 2024
Approved By	Maggio, Bill	**Date:**	November 13, 2024
Effective Date	MAY 14, 2018		

1. Purpose

At GP Strategies, we are committed to protecting the personal data and privacy of our employees, clients, marketing contacts and all other data subjects. Our goal is to build trust through our privacy practices, prevent identity exposure, and achieve legal and contractual compliance with our clients and vendors. To achieve these aims, GP Strategies operates according to this Corporate Personal Data Privacy and Records Management Policy ("**Policy**"). The Policy has four purposes:

1. Provide a regulatory framework for GP Strategies to ensure its global compliance with data privacy and records management laws (section 3.1).
2. Define the responsibilities of the Corporate Data Privacy and Records Management Program ("**Program**") with respect to managing the direction and administration of privacy data handling practices and procedures (section 3.2).
3. Assign responsibility for management, administration and oversight of company records that contain personal data of employees, customers, business partners and others (section 3.3).
4. Provide a central point responsible for rights administration on behalf of data subjects as well as answering questions related to the Program, as well as for ongoing initiatives that are conducted to comply with the applicable laws (section 3.4).

2. Scope and Applicability

This Policy applies globally to:

- All company business units. GP Strategies will establish a U.S. Government Subsidiary in 2025. This subsidiary will have its own policies and procedures but will comply with this Policy unless there is a conflicting legal or contractual requirement;
- All GP Strategies employees, including part-time, full-time, temporary and regular employees, its Board of Directors and business partners where applicable;
- All statutorily defined personal data processed and managed by GP Strategies, in any format, including biometric, electronic, genetic, paper, verbal, recorded or visual, as applicable under law;
- GP Strategies' Web and Social Media Sites and is therefore published on all public facing sites.

Personal data received from clients may be subject to specific requirements laid down in any specific agreement with the client, as well as additional applicable laws and professional standards. While GP Strategies may deviate from sections in this Policy to comply with client agreements, GP Strategies may not deviate from applicable laws in its agreements.

3. Policy

3.1 Regulatory framework

GP Strategies complies with all personal data protection laws applicable to GP Strategies, including but not limited to privacy laws of the U.S. Government, the individual U.S. states, the General Data Protection Regulation (GDPR) of the European Economic Area the General Data Protection Regulation of the UK (UK GDPR).

GP Strategies has implemented and will continue to strengthen the implementation of the (UK) GDPR, the Data Privacy Framework, California Consumer Privacy Act (CCPA) and other principles of Lawfulness, Fairness and Transparency; Purpose limitation; Data Collection and Retention Minimization; Accuracy; Rectification; Storage Limitation; Integrity and Confidentiality; and Accountability through laying the foundations in this Policy.

GP Strategies has committed to the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, and the Swiss-U.S. Data Privacy Framework(s) as set forth by the U.S. Department of Commerce and will continue to self-certify its compliance with its requirements. If there is any conflict between the terms in this Corporate Personal Data Privacy and Records Management Policy and the Data Privacy Framework Principles, the Data Privacy Framework Principles shall govern.

GP Strategies uses the (UK) GDPR, the EU-U.S. Data Privacy Framework, the UK Extension to the EU-U.S. DPF, the Swiss-U.S. Data Privacy Framework(s) (Data Privacy Framework) and U.S. State laws such as the CCPA to guide its worldwide policy and compliance framework for data privacy and records management. If any law or regulation relating to privacy data use and records management establishes a stricter threshold than those set forth in this Policy is applicable to GP Strategies, GP Strategies will comply with the requirements laid down in these laws or regulations where required.

GP Strategies Corporation is committed to cooperate with EU data protection authorities (DPAs), the Swiss Federal Data Protection and Information Commissioner (FDPIC), and the UK Information Commissioner's Office (ICO) and will comply with the advice given by such authorities with regard to human resources data transferred from the EU, UK and Switzerland in the context of employment relationship and/or a business services relationship. To learn more about the Data Privacy Framework program, and to view evidence of certification, please visit: https://www.dataprivacyframework.gov.

Adherence by GP Strategies to the GDPR, CCPA and Data Privacy Framework Principles among other laws may in certain scenarios be influenced a) corporate legal, contractual or ethical obligations; (b) national security, public interest or law enforcement requirements; and (c) specific provisions or limitations set by applicable laws, rules or regulations.

3.2 Data Privacy and Records Management Program

It is the responsibility of the GP Strategies Executive group to support the creation of credible services and programs to protect the personal data GP Strategies processes by implementing this Policy. For this purpose, GP Strategies has established a Data Privacy and Records Management Program consisting out of the following two facets:

3. A joint Data Protection Steering Committee with its parent company, Learning Technologies Group. On GP Strategies end, this Committee consists of the Chief Information Officer, Head of Legal, Head of IT Infrastructure & Operations and the Data Privacy Manager. This Steering Committee is responsible for establishing strategic priorities, monitoring the governance structure, determining key projects, and approving policies.
4. A GP Strategies Data Privacy & Records Management Committee ("**Committee**") to further day-to-day management of the Program and implement and oversee compliance with applicable laws and consistent with this Policy. This Committee is led by the Data Privacy Manager and consists of GP Strategies employees that represent the organizational structure of GP Strategies. The Committee is responsible for supporting corporate awareness outreach, training, lawful administration, employee feedback and Program implementation. The Committee sets standards and procedures as needed to meet the spirit and intent of the various privacy and records management laws. To meet the requirements of the various laws the Program has and continues to establish, review and enforce records management and retention administration.

GP Strategies Program Documents shall be maintained and made available on appropriate locations.

3.3 Management Principles

3.3.1 Transparency

Where GP Strategies collects personal 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, that individuals have for limiting the use and disclosure of data about them; and any other information required by the applicable laws. Notice will be provided in clear and conspicuous language when individuals are first asked to provide personal 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.

3.3.2 Limitations on purposes of collection, processing, and storage

GP Strategies will use privacy data 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 data minimization, is securely stored, is stored for appropriately designated periods (records management), is relevant to its intended use, and is accurate, complete, and current. GP Strategies will retain personal data only for as long as it serves a purpose consistent with the foregoing purpose limitation.

If GP Strategies terminates its voluntary certification in the Data Privacy Framework, it will continue to comply with the GDPR, and the Data Privacy Framework with respect to any privacy data collected under the Data Privacy Framework certification regime.

When required by law or contract, GP Strategies may aggregate sensitive privacy data for client and government reporting purposes. Unless required by law, such data will not provide individual identifiers.

3.3.2.1 Personal Data from GP Strategies web and social media sites use

GP Strategies may collect Personal Data from its web site visitors when a person ("data subject", "consumer") accesses and use GP Strategies sites. Information about the application of this Policy for site use of data collection is available on GP Strategies web and media sites.

3.3.2.2 Personal Data regarding and used by GP Strategies personnel

GP Strategies may transfer Personal Data of its personnel and contractors in accordance with the GDPR, CCPA and other applicable laws. This Personal Data 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, applications and performance ratings and other information GP Strategies is required by law to keep in an employee's personnel file. 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 activities.
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.

3.3.2.3 Personal Data from clients or third parties

GP Strategies may receive Personal 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 law and in accordance with the agreement between GP Strategies and the other party and, where applicable, the other party's documented instructions.

3.3.3 Integrity and confidentiality

GP Strategies will take reasonable steps to ensure that the personal data it processes is accurate and up to date. In order to do so, GP Strategies may regularly review the personal data.

GP Strategies will ensure that any person, including employees, suppliers or other third parties, that it authorizes to process personal data is subject to a strict duty of confidentiality (whether a contractual duty or a statutory duty).

3.3.4 Use of third parties and international transfers

GP Strategies will only share personal data with third parties where an agreement with GP Strategies is in place. This agreement will require the third party to protect the data to at least the level required by the applicable law. GP Strategies remains responsible under the applicable laws if its agent processes data in a manner inconsistent with the GDPR, CCPA and Data Privacy Framework Principles except where GP proves it is not responsible for the event giving rise to the damage.

GP Strategies will only transfer personal data to a third country in accordance with applicable law.

3.3.5 Data subject rights

As required by applicable law, upon request, GP Strategies will grant individuals' access to privacy data that it holds about them. GP Strategies will not provide any privacy data that is not already available in a self-service format. GP Strategies will permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete. GP Strategies will also permit individuals to correct, amend, or delete accurate information that has been processed in violation of applicable laws. GP Strategies will not discriminate against individuals exercising any of their rights including:

- by denying them goods or services;
- charging different prices or rates for goods or services, including through the use of discounts or other benefits or imposing penalties;
- providing different levels or quality of goods or services; or
- suggesting that individuals making a request may receive a different price or rate for goods or services or a different level or quality of goods and services.

GP Strategies will decide on a case-by-case basis if GP Strategies can make business communications and related documents available after receiving a request. Relevant factors to such a decision include that GP Strategies is required to protect the rights and freedoms of the employees involved in such business communications and is required to protect its internal confidential information. Any business communication that is requested, is therefore subject to an inspection for privacy data, company confidential information, patent information, financial information, information involved in a legal proceeding, or of a contractual, regulatory or statutory nature. Any information that is made available may be redacted.

The applicable laws may require GP Strategies to offer individuals the choice as to whether their personal data 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.

Where applicable, GP Strategies will offer individuals such opportunity to opt-in or opt-out.

3.3.6 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 include collecting, accessing, storing, transferring, analyzing and manipulating data.

3.3.7 Accountability

Where GP Strategies has knowledge that an employee or 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.

3.3.8 Verification

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

3.3.9. Exceptions

Subsidiaries, affiliates and other GP Strategies entities may not have policies and practices contrary to those laid out by the Committee. When approved by the Committee, these bodies may have addendums to this Policy to address specific country laws for privacy data handling and records management. Such addendums will not replace this Policy and its related documents.

Any request for an exception from this Policy must be submitted in writing to the GP Strategies Data Privacy and Records Management Committee, Company Officers or such other persons identified in Program informational materials. 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.

3.3.10. Violations

Violations must be submitted to the Program Administrators for consideration and may be presented to any of the Program Committee, GP Strategies Legal Office and/or a regional Data Protection Officer. Where a violations of the law or this Policy is established GP Strategies may has the authority to address a violation in accordance with the applicable law and/or applicable agreements.

3.4 Intake and processing of inquiries, dispute resolution and remedies

GP Strategies encourages employees and other parties affected by GP Strategies' data privacy practices to contact the Office of the GP Strategies Data Privacy and Records Management Program Committee or their respective GP Strategies regional 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 applicable laws.

In compliance with the Data Privacy Framework (DPF) Principles and other applicable laws, GP Strategies commits to responding to inquiries about our collection or use of personal information.

EU, UK, Switzerland, U.S. and individuals worldwide with inquiries regarding our privacy policy should contact us at:

GP Strategies Global Privacy Office, GP Strategies Corporation
70 Corporate Center, Suite 300, 11000 Broken Land Pkwy,
Colombia, MD 21044 USA
OR: dataprivacy@gpstrategies.com

GP Strategies will cooperate with the data protection authorities (DPA) of any EEA country or any other country with data privacy laws where GP Strategies conducts business and participate in any dispute resolution procedures they establish.

3.4.1 Process for GP Strategies personnel

GP Strategies Personnel may file an inquiry or complaint concerning GP Strategies processing of their personal data. They may file this inquiry or complaint with any member of the Data Privacy Program Committee, a regional Data Protection Officer or with GP Strategies' Human Resources (HR) Department, who will communicate and coordinate with the Office of the GP Strategies Data Privacy and Records Management Program Committee. GP Strategies will evaluate and take appropriate steps to address Program administration issues arising out of a limitation or failure to recognize issues with the applicable laws. If a GP Strategies personnel complaint cannot be resolved through this internal process, GP Strategies may consult and cooperate with the relevant EEA data protection authority (DPA), and apply their advice to the situation.

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 Data Privacy Framework Principles.

3.4.2 Federal Trade Commission Authority

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

4. Definitions

- Definitions used in this Policy that are defined by law, like "personal data", "processing" and "data subject" shall have the meanings given in the applicable law.
- "**General Data Protection Regulation**" or "**GDPR**": 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.
- "**The EU-U.S., the UK Extension to the EU-U.S. DPF, and Swiss-U.S. Data Privacy Frameworks**": the set of principles designed, and from time to time amended, by the U.S. Department of Commerce, and the European Commission, United Kingdom and Swiss Administration, respectively, to provide companies on both sides of the Atlantic with a mechanism to comply with data protection requirements when transferring personal data from the European Union, United Kingdom and Switzerland to the United States in support of transatlantic commerce.

- "**The United Kingdom General Data Protection Regulation of the UK**" or "**UK GDPR**": The United Kingdom General Data Protection Regulation, as it forms part of the law of England and Wales, Scotland and Northern Ireland by virtue of section 3 of the European Union (Withdrawal) Act 2018.
- "**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.
- "**Third Party**" means any third-party that collects, processes or uses personal data under the instructions of GP Strategies or to which GP Strategies discloses personal 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.

5. References (Related Documentation)

None

Document Change Control

Date	Version	Reason for Change	Author
February 9, 2018	1.0	Initial development. To include the GDPR and finalize approval.	J. Galante, J. LaFleur
May 14, 2018	1.0	Approval v1.0	A. Stedham
May 14, 2018	1.0	Formatting/numbering convention	T. Fobes
December 16, 2019	2.0	v2.0 Insert required updates for Privacy Shield for Brexit, the CCPA and change of Chief of Staff	A. Majeed, J. LaFleur
January 27, 2020	2.0	Adding additional information for Swiss Privacy Shield per U.S. Department of Commerce requirement.	A. Majeed, J. LaFleur
JAN 27, 2020	2.0	Approval 2.0	A. Stedham
JAN 27, 2020	2.0	Approval 2.0	A. Stedham
OCT 16, 2021	2.0	Approval 2.0	A. Stedham
OCT 22, 2022	2.0	Reviewed by Gov Committee (no changes)	A. Stedham
OCT 20, 2022	2.0	Reviewed by Gov Committee (no changes)	A. Stedham
DEC 22, 2022	3.0	Reviewed by Tim Fobes (Insert required updates for the Data Privacy Framework, name change from Shield)	Fobes, Tim
DEC 23, 2022	3.0	Reviewed by Gov Committee (See changes in box above)	A. Stedham
NOV 3, 2023	3.1.	Reviewed by Kelly Sprenkeling (removal of United Kingdom under Data Privacy Framework)	K. Sprenkeling
NOV 7, 2023	3.1.	Approved by W. Maggio (Executive Vice President)	W. Maggio
Nov 27, 2023	3.2.	Reviewed by Kelly Sprenkeling (Draft to include DPF UK certification for (re)certification purposes)	K. Sprenkeling
DEC 8, 2023	4.0	Approved by W. Maggio (Executive Vice President)	W. Maggio
Oct 29, 2024	5.0	Updated and revised by Kelly Sprenkeling	K. Sprenkeling

Nov 13, 2024	5.0	Reviewed by David Anderson (Vice President of IT), Valderia Brunson (Vice President of Legal) and Abu Majeed (Crisis & IT Security Compliance Manager) and, no changes	V. Brunson, D. Anderson
Nov 13, 2024	5.0	Approved by W. Maggio (Executive Vice President)	W. Maggio