GPStrategies®
Your workforce transformation partner™

GP Strategies Information Security & Data Protection Fact Sheet

November 2023

Introduction

This Fact Sheet provides information on GP Strategies' information security and data protection practices and on the standards we use to achieve data privacy and to manage our records. More details about our data protection practices can be found in our Website Privacy Notice and our **Data Privacy and Records Management Policy**.

This Fact Sheet does not cover the practices or services of third parties, including (social networking) platforms of business clients who use GP Strategies' services to collect information from their customers. For information about third party security and privacy practices, please consult their privacy policies.

Standards for Information Technology Security

GP Strategies policies and procedures adhere to the ISO (International Standards Organization) security standard 27001&2. Where applicable we augment our ISO Information Security Management System framework with other standards, such as (but not limited to) the U.S. National Institute of Standards and Technology (NIST), UK Cyber Essentials Plus qualifications for certification and the Payment Card Industry, Data Security Standard (PCIDSS).

Security of Personal Information

The security of your and the personal information of all of us is important to GP Strategies. Below are examples of security measures GP has implemented. This list is in no way intended to provide a comprehensive overview, but touches upon important principles:

- We follow generally accepted industry standards to protect and encrypt the personal information submitted to us, both during transmission and once we receive it.
- When anyone enters sensitive information (such as log in credentials), we encrypt the transmission of that information using secure transport layer security (TLS).
- We maintain strict access controls.
- We have configurated firewalls and intrusion detection systems.
- We implement recommended hardening and patching procedures.
- We maintain malware protection.
- We maintain back-up and restoration policies.

No method of data transmission over the Internet, or method of electronic storage, is 100% secure, however. Therefore, we cannot guarantee its absolute security.

Data Protection and Security responsibilities within the organization

GP Strategies employs security professionals and takes technical and organizational measures designed to prevent unauthorized access, use, alteration, or disclosure of privacy data collected via GP sites. Further, GP has more than 30 years of experience in operating highly secured solutions with security controls that are continuously updated to meet industry standards and address emerging threats. This is described in detail in our information technology (IT) policies and procedures.

Employee Responsibility for data protection and security

Employees are required to complete training courses which include all or in part, a focus on data privacy rights and responsibilities regarding the personal data they provide to GP Strategies; the safeguarding of our colleagues' personal data; the requirements for protecting client privacy data; and GP Strategies' data privacy gathering practices.

GP web and social media site managers are required to post data privacy notices on our sites, along with supporting frequently asked questions (FAQ) information, policies, standards and practices.

GP Strategies Corporation
70 Corporate Center
11000 Broken Land Parkway, Suite 300
Columbia, MD 21044 USA

Phone: 443 367 9600
Email: info@gpstrategies.com
Website: gpstrategies.com

© 2023 GP Strategies Corporation. All rights reserved. GP Strategies and GP Strategies with logo design are registered trademarks of GP Strategies Corporation. All other trademarks are trademarks or registered trademarks of their respective owners.

As required by the GDPR, GP Strategies has appointed data protection officers (DPO) for compliance purposes to include ombudsman availability to employees for inquiries about data privacy practices.

Secure Data Storage

GP Strategies stores privacy data in cloud solutions with geolocations options in the United States, United Kingdom and other countries. These cloud solutions use certified centers which have one or more of the following: SOC 1 Type 2, SOC 2 Type 2, Lloyd's Register (LRQA) and ISO (International Standards Organization) 27001. (SOC = Service Organization Controls reports (1-3) of the AICPA (American Institute of Certified Public Accountants). ISO 27001 is one of the most recognized worldwide information technology security standards. SSAE 16 and ISAE 3402 – 22451 and PCI – Data 2334 Security Standard (SSAE = Statement on Standards for Attestation Engagements (#16 & 18), PCI = Payment Card Industry-Data Security Standard ((PCI-DSS)).

GP Strategies stores all data it collects in secure applications with access limited for employee services and to meet business operations needs. No personal data is shared with third parties other than services providers acting as GP Strategies contracted agents. Our processors of employee, vendor, client and site visitor data are contractually required to meet the same security standards that GP Strategies must meet for all of these same audiences and partners.

Control over Third Party Recipients of Personal Data

GP uses a number of third parties to process personal data on our behalf. These third parties have been carefully chosen and all are contractually required to comply with privacy legislation. Client managers and project managers are required to implement data privacy contract addendums with third parties that process our or our client's personal data. Such third parties are contractually bound by substantially similar or more stringent requirements as GP Strategies is required to adhere to in its client relationship, and requires the third party to protect the data to at least the level required by the applicable law.

Data Transfers to Third Countries

GP Strategies will only transfer privacy data when the limited and specified purposes consistent with the GDPR or other applicable laws and EU – U.S. or Swiss – U.S. Data Privacy Framework (DPF) Principles allow this. Where GP Strategies does not rely on the Data Privacy Framework (DPF) for transfer of data, it ensures that all contracts that result in a transfer of data rely on an adequacy decision or contain the Standard Contractual Clauses and meet the requirements thereof.

Data Breaches

Data breach reporting laws vary from country to country and state to state. GP Strategies will follow the applicable laws and definitions. We will report any confirmed unlawful material data breach of unencrypted personal information of our site's database or the database(s) of any of our third-party data processors to any and all relevant persons and authorities in the manner prescribed by applicable

GP Strategies Corporation
70 Corporate Center
11000 Broken Land Parkway, Suite 300
Columbia, MD 21044 USA

Phone: 443 367 9600
Email: info@gpstrategies.com
Website: gpstrategies.com

© 2023 GP Strategies Corporation. All rights reserved. GP Strategies and GP Strategies with logo design are registered trademarks of GP Strategies Corporation. All other trademarks are trademarks or registered trademarks of their respective owners.

law. Where GP Strategies is a processor, we will meet the contractual requirements with respect to data breach notifications.

Disclosures of Personal Data

In certain situations, GP Strategies may be required to disclose personal data:

- In response to lawful requests, such as to comply with a subpoena or other legal process, by public authorities including national security and law enforcement; GP Strategies will review any such request it receives, prior to responding to the request, to determine whether the request is valid, legally binding and lawful, and reject any request that is not valid, legally binding and lawful. GP Strategies will take all reasonable steps to ensure any data disclosure or access is limited to what is proportionate and strictly necessary for the purpose of complying with the request, and only furnish the minimum amount of Personal Data legally required to be disclosed.
- In the event that GP Strategies files for bankruptcy;
- To protect our rights;
- To protect your safety or that of others in case of an emergency;
- To investigate fraud;
- In the event of a merger or acquisition.

GP Strategies Corporation
70 Corporate Center
11000 Broken Land Parkway, Suite 300
Columbia, MD 21044 USA

Phone: 443 367 9600
Email: info@gpstrategies.com
Website: gpstrategies.com

© 2023 GP Strategies Corporation. All rights reserved. GP Strategies and GP Strategies with logo design are registered trademarks of GP Strategies Corporation. All other trademarks are trademarks or registered trademarks of their respective owners.