GP Strategies
Web and Social Media Sites
Data Privacy and Records Management Information
Frequently Asked Questions

Introduction to this Document

At GP Strategies our Data Privacy and Records Management Policy is a commitment to protecting the privacy of employee, client and web and social media site visitor personal data. GP Strategies (GP) makes every reasonable effort to protect the privacy of data collected when individuals visit our sites.

This statement ("Statement") of frequently asked questions (FAQ) explains how GP Strategies uses and protects the privacy information we collect. It applies to any personal information you provide to GP and, subject to deviations for local laws, any personal information we collect from other sources.

Privacy data is inconsistently defined by countries and states around the world in laws and regulations. GP is providing this privacy data handling information in compliance with the thresholds in the General Data Protection Regulation (GDPR) of the European Union (EU) and the EU-U.S. Privacy Shield agreement. We believe they are currently overall the most stringent law providing for your personal data security and for our requirements as a data controller for presenting you right-to-know information. GP has adopted the GDPR and Privacy Shield as the management framework for our Company Data Privacy and Records Management Program.

Throughout this Statement, "GP Strategies" refers to the GP Strategies Corporation and all affiliated companies and subsidiaries (also referred to as "we", "us", or "our"). The term “site” is intended to cover all GP web and social media sites – Facebook, twitter, Yammer, GP blogs, GP forums, et. al. For more assistance see the contact information at the conclusion of the Statement.

GP Strategies employs professional security personnel and takes technical and organizational measures designed to prevent unauthorized access, use, alteration, or disclosure of privacy data collected via GP sites. We try to be both selective and proactive in checking the security background for certain external social media sites and other sites that we come in contact with but do not control. GP has been in business for over 50 years and has more than 30 years of experience in operating highly secured data repositories with security controls that are continuously updated to meet industry standards and address protective measures for emerging threats. Security practices are described in detail in our internal information technology (IT) policies and procedures. Also see our IT fact sheet on information security practices for more information.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

Changes to this Statement

GP Strategies may update this Frequently Asked Questions (FAQ) Statement regarding web and social media site data privacy and data management from time to time. We encourage you to periodically review these Statements so that you will be aware of our privacy practices. Contact information for inquiries about this FAQ material on web and social media sites privacy data management is at the end of this FAQ.

Contents

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

As a GP Strategies site visitor does the "GDPR", Privacy Shield and other similar data privacy and records management requirements apply to my data?

- Companies within the EU, or who are externally located controllers and processors of the personal privacy data of EU residents in the context of collecting privacy data while soliciting and providing goods or services, will need to comply with the GDPR. GP Strategies (GP) has adopted the GDPR and Privacy Shield as our worldwide standard for data privacy. As a GP site visitor we do collect your business contact information. However, we may also collect or process privacy data for the purpose of providing additional services. We are very aware that combining multiple data elements, even if not considered personal data when taken alone, may result in them being considered personal privacy data when combined into a listing.

- We may move your data within or to locations outside of the European Economic Area (EAA). These data transfers are legal under the GDPR and Privacy Shield as long as we adhere to the requirements for legal processing. We encrypt all data in transit and in storage.

- GP has evaluated our obligations under the GDPR and Privacy Shield, in part, based on: (1) the type of visitor data that we collect via our sites, and (2) the legal basis on which you rely for the protection of your data. We will exercise data privacy stewardship on all of our sites.

How will my personal information be used and shared by GP Strategies for internal management of their sites?

The personal information we collect in our various sites allows us to:

- respond to your inquiries;
- provide the information, products and services you have ordered;
- verify your identity and details of your payment method or credit card amount;
- administer our sites and provide user services;
- meet legal, regulatory and compliance requirements;
- monitor and analyze the use of any account to prevent, investigate and/or report fraud, terrorism, misrepresentation, security incidents or crime;
- gather management information to form statistical and trend analysis;
- communicate with you;
- investigate any complaints about our sites;
- personalize your experience of the sites;
- contact you about our products and services which we think might be of interest to you (where we have the appropriate permissions to do so);
- when warranted, we share your personal information with our GP affiliate companies and their brands for the above purposes;
- employ the services of third party service providers to help us in certain areas, such as site hosting, maintenance and call center operation. In some cases the third party may receive your information. However, at all times we use third parties, we will control and be responsible for the use of your information and place contractual requirements on privacy data sent to our sub-processors.

- If you provide a credit or debit card, we may also use third parties to check the validity of the sort code, account number and card number you submit in order to prevent fraud as well as to process any transaction you attempt via the website.
- If false or inaccurate information is provided and fraud is identified, we will follow legal processes if details will be passed to fraud prevention agencies. Law enforcement agencies may access and use this information. We and other organizations may also access and use this information to prevent fraud and money laundering, for example when:
  - checking details in applications for credit and credit related or other facilities
  - managing credit and credit related accounts or facilities
  - recovering debt
  - checking details on proposals and claims for all types of insurance
  - checking details of job applicants and employees.

Where does GP Strategies store my privacy information?

- GP Strategies stores privacy data in data centers in the United Kingdom and the United States. These are certified centers: 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)).

How is GP Strategies as an organization affected by data privacy laws?

- GP Strategies sees the European Union General data Protection Regulation (GDPR) and Privacy Shield Principles as on opportunity to strengthen our already strong commitment to protecting personal data company-wide at a global level. This is the same framework we use for protecting the privacy data of our employees. GP has an internal Data Privacy and Records Management Program which outlines and provides oversight for managing the many ways in which GP supports the protection of personal data and ensures compliance with the GDPR law and any similar country specific legislation and guidelines like the Asia Pacific Economic Cooperation forum approach.

- Our goal is to make GP Strategies' data protection policies and efforts transparent throughout our organization so employees, customers, site browsers and partners may fully understand our commitment to data protection and the related practices needed to reinforce that commitment at all levels of engagement.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

What is GDPR and when does it come into effect?

- "GDPR" stands for the European Union (EU) General Data Protection Regulation affecting "processing" (which includes the collection, storage, transfer or use) of personal data related to European Union (EU) citizens, wherever they may be located physically. GP Strategies has adopted the GDPR and the EU-U.S. Privacy Shield as our internal data privacy management program thresholds.
- The GDPR is a 2018 EU regulatory framework designed to replace a patchwork of laws with a single law and set of recitals that is enforceable throughout the entire European Economic Area (EEA). Privacy Shield provides the U.S. and EU countries an approved data transfer mechanism.
- GDPR and Privacy Shield protect the privacy rights of EU citizens and empowers their control of the collection and use of their personal data by giving them expanded right to insight and control of their personal data.
- GDPR also places new obligations on organizations that market to, track or handle EU personal data on web and social media sites, no matter where an organization is located.

What constitutes personal privacy data?

- Any personal information related to a natural person (called a 'data subject' by the GDPR) that can be used to directly or indirectly identify the person when not encrypted and used individually or in combinations to create a profile.
- Personal privacy data is a very broad range of personal information and can be any information item that might be used to create a profile beyond what GP Strategies considers basic business contact information of name, business address, business phone and business title or business job. Personal privacy information would be: an identifiable photo; identifiable voice recordings; fingerprints; biometric data; a personal email address, home phone number, home address; numbered identifiers - bank account, credit information and credit card, passport, country identification and driver's license numbers and social security; family member information; medical information; political opinions; sex, sexual preferences; computer IP address; data on children; travel profiles; trade union membership; criminal records. Some countries consider some of these listed items as Sensitive Personal Identification Information (SPII).

What is the difference between a data processor and a data controller?

- A controller is the entity that determines the purposes, conditions and means of the processing of personal data. A controller can be a processor. A site owner is a controller.
- A data processor is an entity which processes personal data on behalf of the controller.
- GP Strategies is a controller and/ or a processor at varying times in our conduct of business.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

Is GP Strategies a data processor or data controller in regard to my personal data?

- GP Strategies acts as a data controller and in some cases is also a processor (or sub-processor) for personal data provided to GP through our customers, by individuals and other third parties such as partners.
- If you as a data subject provide your personal data directly to GP Strategies (such as a site visitor, a forum or conference attendee, a site browser, etc.) GP acts as the data controller for that personal data. Note, if GP also processes that personal data in some fashion, GP also qualifies as a data processor in regard to that personal data.

Is GP Strategies organized to manage the data processor obligations imposed by the GDPR, Privacy Shield and other similar laws and regulations?

- GP Strategies established a Data Protection and Records Management Committee and appointed Data Protection Officers (DPOs) to manage the program and comply with the GDPR. The Committee is tasked with instituting GP's internal data privacy compliance initiatives.
- For GP Strategies, keeping site visitor data secure is a high priority. Along with ensuring data security, it is important that a site visitor's confidence is always maintained and a high level of security around processes and protection is strongly administered.
- At GP Strategies, we strongly value and base our business on the trust that our site visitors, employees and customers have placed upon us. We will continue to earn and reinforce that trusted relationship by cooperating with requests related to our GDPR, Privacy Shield and other country data privacy obligations.
- GP Strategies is committed to taking advanced measures to support and continuously enhance the security of our systems, to ensure that we collect and process personal data in a manner compliant with GDPR, Privacy Shield or any similar legislation.
- GP Strategies management strongly believes that information technology security/compliance is a key business service. Information security objectives and strategy must be continually aligned with GP's business strategy and objectives.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

When does GP Strategies delete client data?

GP Strategies deletes client data, including backups based on our records management schedule. In some cases that can be shortly after you leave one of our sites. Web and social media privacy information is deleted after you finish browsing or have opted out of receiving our communications or you have been unresponsive to our inquiry messages for a period of time. If you acknowledge our site use rules to continue browsing or you agree when specifically requested to opt-in your information is transferred to our secure customer relations management data base. In some cases we are legally and/ contractually required to keep some data for more extended periods of time consistent with the lawful processing provisions of the GDPR. Data is held in various categories in our records management deletion schedules. These data retention categories range from nearly immediate up to seven (7) years unless there is a longer legal requirement. For more information about data retention times please contact us.

Does GP Strategies provide clients with the option to delete client data?

GP Strategies supports the deletion of client data; however, such a request needs to be in writing and needs to be done in conjunction with GP' Technical Support team in the event it is not a temporary storage item like non-persistent web and social media cookies.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

In GP Strategies' Commitment to data protection what steps have been taken to protect my data?

- ✓ GP Strategies initiated a data privacy data management compliance review and update effort beginning in October 2017 to ensure alignment with the May 2018 requirements of the European Union (EU) General Data Protection Regulation (GDPR) and other similar privacy data regulatory obligations coming into force around the world. GP was also certified into the Privacy Shield regime by the U.S. Department of Commerce in 2017. These efforts are Companywide, ongoing and driven by a chartered Committee sponsored by senior corporate leaders. We meet regulatory requirements, to include these examples:
- ✓ We have not identified any information technology shortfalls in data privacy transmission and storage encryption.
- ✓ The standing Data Privacy and Records Management Committee currently meets bi-monthly and has a web based administration site where it keeps its meeting records and products.
- ✓ An internal informational data portal about data privacy is available for employees.
- ✓ Privacy data owners' storage information submissions are being continuously catalogued and are annually updated.
- ✓ The annual review of the initial data privacy impact risk assessments of the catalogued submissions from data owners is an ongoing Committee activity.
- ✓ We have standard contract language amendments for subcontractors/processors in-place.
- ✓ We have available an employee frequently asked data privacy questions (FAQ) document to enhance transparency on our internal portal.
- ✓ We have inventoried all of our worldwide web and social media sites to evaluate our privacy policy statement status and have been taking enhancement actions as periodically required.
- ✓ In December 2017 GP obtained EU-U.S. Privacy Shield certification for the international transfer of EU privacy data. To learn more about the Privacy Shield Framework, and to view our certification, visit the Department of Commerce Privacy Shield web site.
- ✓ In December 2017 GP obtained authorized UK Government Cyber Essentials certification.
- ✓ A new Company master policy on data privacy and records management supporting our due diligence and transparency requirements for the new privacy protection laws is in effect.
- ✓ We have an approved charter for the permanent standing Committee to administer the ongoing post May 2018 data privacy records management program to meet the GDPR and Privacy Shield.
- ✓ We conduct employee data privacy awareness training annually.

If you need additional elaboration on Committee actions please contact us.

In addition to efforts by the Committee, 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 policies and procedures. Also see our IT fact sheet on information security practices.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

What are GP Strategies site cookie policies?

Use of Cookies – Practices and Procedures

- GP Strategies uses cookies for a variety of purposes such as remembering your preferences, measuring your activity on GP Strategies' websites, mobile sites and mobile applications ("sites") or optimizing your user experience. Disabling cookies on your internet browser will stop tracking of any part of your visit to pages within the site. All traffic (transferral of files) between the site and your browser is encrypted and delivered over HTTPS.

  Please also review our FAQs, Fact Sheets and Privacy Policy statements for more information about GP privacy practices.

Cookie Settings

The types of cookies GP Strategies and others may place on your device are described below.

- GP will read or set only the types of cookies that are strictly necessary for quality browsing or specifically allowed by your browser preference settings.
- GP only places cookies that set your preferred language, deliver specific content based on visit history, and give access to various sections of the sites.
- Cookies set by our sites will remain on your device but GP will not access or use those non-strictly-necessary cookies. You may remove them using functionality provided by your browser. Please note that cookies are specific to the browser or device you use, as well as to the domain, and you will therefore have to configure your preferences again if you change your browser or device, or visit a different domain.
- Any specific questions regarding these cookie settings may be sent to gpwebmaster@gpstrategies.com

How do you use Web Beacons?

- Some of our web pages may contain electronic images known as web beacons (sometimes known as clear gifs) that allow us to count users who have visited these pages. Web beacons collect only limited information which includes a cookie number, time and date of a page view, and a description of the page on which the web beacon resides. We may also carry web beacons placed by third party advertisers. These beacons do not carry any personally identifiable information and are only used to track the effectiveness of a particular campaign.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

How do you use Social Media Widgets?

- GP Strategies Corporate sites can include certain social media features, such as the Facebook button. These features may collect your IP address, may collect which page you are visiting on our sites, and may set a cookie to enable such feature to function properly. Social media features are either hosted by a third party or hosted directly on our sites. Your interactions with these features are governed by the privacy policy of the company providing it.

How do you use Blog Information?

- Should you choose to add a comment to any posts that we have published on our sites for example in a blog, the name and email address you enter with your comment will be saved to the site's database, along with your computer's IP address and the time and date that you submitted the comment. This information is only used to identify you as a contributor to the comment section of the respective blog post and is not passed on to any of the third party data processors. Only your name will be shown on a site that is public-facing.
- Your posted comment(s) and its associated personal data will remain on this site until we see fit to either 1) remove the comment, or 2) remove the blog post. Should you wish to have the comment and its associated personal data deleted, please email us listed with your contact information using the email address that you commented with.
- If you are under 18 years of age we request you obtain parental consent before posting a comment on our blog and sites.
- NOTE: You should avoid entering personally identifiable information to the actual comment field of any blog post comments that you submit on this site.

How do you use Contact Forms and Email Links?

- Should you choose to contact us using a contact form on our sites or an email link, the data you supply will be stored in our customer relationship management database or may be passed on to be processed by a third party data processor(s). We do retain information from data requests in our customer relationship management system. Collated and transferred data is encrypted before being sent across the internet. We do not sell personal information.

FREQUENTLY ASKED QUESTIONS - GP STRATEGIES
WEB AND SOCIAL MEDIA SITES DATA PRIVACY AND RECORDS MANAGEMENT INFORMATION
UPDATED APRIL 14, 2018

How do you use information we provide to you?

- As a compliance philosophy GP Strategies makes every effort to apply a data minimization approach in our privacy data gathering and storage activities. We do collect and hold some personal information you give us. These are the general types of information we may collect from you:

Registration and Profile Information

- We try to gather only the most necessary information for the involved inquiry or purpose. When you enter or register to use our site, our services, to receive information, to participate in our events, and create or update your forum profiles, we may collect various kinds of information about you. For example, we may collect: your name; postal address; phone number; fax numbers and email address; your log-in ID and password; your title; company; and other event specific profile information you provide; demographic information; and information linked with your profile such as comments you may post. We need this information to be able to respond to you, secure the site and provide services as applicable.

Information We Automatically Collect

- When you visit our site or use GP Strategies site services, as do many companies, some information is collected and recorded automatically such as your computer's operating system, Internet Protocol (IP) address, access times, browser type and language, and the website you visited before our corporate sites, so we are aware of transfers and linking for security due diligence (blocking and enhancing) of our site and to protect you the user. This is logged automatically and stored in log files. We also collect information about your usage and activity on our corporate sites. We may tie your IP address to information we automatically collect on our corporate sites. We may also tie information we automatically collect with personal information, such as your login ID and information you give us for a registration. We use our own products, and products of third parties acting on our behalf, to analyze, optimize, securely protect and improve our site.

- GP will also collect information on your usage to ensure the security of the data we collect on behalf of our clients. You cannot opt-out of this collection and processing as it is necessary to ensure the security of the service we provide for our sites and for our clients.

- We use cookies to collect information allowing for analytics, user experience and session tracking, as well as video use tracking. Users can control the use of cookies at the individual browser level. If you reject cookies, you may still use our site, but your ability to use some features or areas of our site may be limited.

- GP Strategies may also use device-recognition technologies combined with other identifiers to create cross-browsers and cross-devices identities to provide you with better services and security.

Does GP Strategies obtain information about me from other sources?

- GP Strategies may collect information about you from third party sources and services. We may buy or lease contact, marketing, and demographic data from brokers. GP Strategies may also access certain profile information such as friends, profile picture, etc. from social networking platforms and services that you use on or to interact with GP Strategies Corporate sites. We may combine that third party information with information we collect directly from you.

###

END