

# SAFE HARBOR PRIVACY POLICY

---

## INTRODUCTION

KnowledgePoint360 Group, LLC and its affiliated subsidiaries (collectively “KnowledgePoint360”, “the Company”, “we”, “us” or “our”) is a leading provider of healthcare information and communications. We respect your personal information and strive to use it in a manner consistent with the laws in the countries in which we do business, and in connection with the Company’s business operations only. Therefore, the Company made the decision to participate voluntarily in the Safe Harbor principles available to U.S. organizations under the European Commission’s (EC) directive on data protection.

This Safe Harbor privacy policy (the “Privacy Policy”) sets forth the Company’s policy and practices for protecting personal information and sensitive personal information transferred from the European Union/European Economic Area (EEA) to the U.S. The Company adheres to the Safe Harbor Principles as agreed between the U.S. Department of Commerce and the EC, governing the transfer of personal information from the EEA to the U.S., and as agreed between the U.S. Department of Commerce and the Federal Data Protection and Information Commissioner (FDPIIC) of Switzerland, governing the transfer of personal information from Switzerland to the U.S.

## SCOPE

This Privacy Policy applies to all personal information that the Company receives in the U.S. from the EEA and Switzerland, in any format, including electronic, paper and verbal. This Policy also applies to Agents (defined below) that handle and process EEA personal data on behalf of the Company or its affiliate U.S. companies.

## DEFINITIONS

For the purposes of this Privacy Policy, the following definitions shall apply:

**“Personal information”** is any information collected, used, received by, and transferred to the Company from the EEA or Switzerland that pertains to a specific individual and that identifies or could be used to identify that individual. It does not include information that has been anonymized, or publicly available information that has not been combined with non-publicly available information.

**“Sensitive personal information”** is personal information that reveals race, ethnic origin, political opinions, religious or philosophic beliefs, trade union membership or that concerns an individual’s physical or mental health, or sex life.

An **“Agent”** is any third party that collects, receives, processes or uses personal information on behalf of and under instruction from the Company.

## PROCESSING OF EEA PERSONAL DATA

We may from time to time process certain EEA personal information about customers, business partners, service providers, healthcare professionals, employees and candidates for employment, including information recorded on various media as well as electronic data.

We will use personal information concerning business partners and customers to provide customers and business partners with information and services and to help our personnel better understand the needs and interests of these business partners and/or customers. Specifically, we use information to help customers and business partners complete a transaction or order, to facilitate communication, to deliver products/services, to bill for purchased products/services, and to provide ongoing service and support. Occasionally our personnel may use personal information to contact customers and business partners to complete surveys that are used for marketing and quality assurance purposes.

We also collect personal information concerning service providers to help us select services and personnel appropriate to the needs of our business and specific customer accounts, to facilitate communication, and to pay for purchased products/services. We may occasionally contact service providers to complete surveys that are used for marketing and quality assurance purposes.

We collect personal information on healthcare professionals (HCPs) to allow HCPs to register for events and services; to allow us to deliver certain products/services to our customers; to work collaboratively with HCPs for performance of a contract or otherwise agreed services to a customer, to which the HCP is an independent party; or with a view to the HCP entering into such a contract/agreement with the customer. We use HCP personal information to facilitate communication, to pay for purchased services directly or on behalf of a customer, to book travel, accommodation and event registration, and to facilitate document submission to congresses or publishers. We may also use HCP personal information to directly engage the services of such HCPs, or to conduct occasional surveys to help us better understand a therapeutic or market area, or healthcare practices.

We may also share personal information between the subsidiary companies within KnowledgePoint360 and with our service providers and suppliers for the sole purpose and only to the extent needed to support the customers' business needs. Service providers and suppliers are required to keep confidential any personal information received from us and may not use it for any purpose other than originally intended. We may also share HCP personal information with our customers for the sole purpose and only to the extent needed to undertake a contract or otherwise agreed service to which the HCP is an independent party.

We also collect personal information concerning our employees (Human Resources Data) in connection with administration of our Human Resources programs and functions and for purpose of communicating with our employees. These programs and functions may include compensation and benefit programs, employee development planning and review, performance appraisals, absence records, disciplinary records, training, business travel and expense reimbursement, access to our facilities and computer networks, employee profiles, internal employee directories, Human Resource record keeping, and other employment related purposes. We also collect and use personal information to consider candidates for employment opportunities within the company.

Human Resources data may be shared with third party vendors for the exclusive purpose of enabling the vendor to provide service and/or support to us in connection with these Human Resource programs and functions. Human Resource data is not shared with third parties for non-employment related purposes. Third parties receiving personal information are required to apply the same level of privacy protection as contained in this Policy.

## **PRIVACY PRINCIPLES**

The Company abides by the following privacy principles, which are based on the Safe Harbor Privacy Principles.

### **Notice**

When the Company collects personal information directly from individuals in the EEA or Switzerland, or as soon thereafter as is reasonably practicable, and in any event before the Company uses or discloses the information for a purpose other than that for which it was originally collected, or discloses it for the first time to a (non-agent) third party, the Company will provide notice in clear and conspicuous language as to the following: the purposes for which the Company collects and uses the personal information; the choice and means by which an individual may limit the Company's use and/or disclosure of their personal information; and how to contact the Company with inquiries or to amend personal information maintained by the Company. All personal information received in the U.S. from the Company's European subsidiaries will be used and disclosed in accordance with the prior notices provided by such subsidiaries and the prior choices made by the individuals to whom the personal information relates.

### **Choice**

**Opt-out:** When the Company collects personal information directly from individuals in the EC/EEA or Switzerland, or as soon thereafter as is reasonably practicable, the Company will provide the individual with an opportunity to "opt-out" from having the Company disclose their personal information to non-agent third parties. An individual may at any subsequent time direct the Company not to disclose their personal information to third parties by submitting a request to the Company's Compliance Officer at the address set forth at the end of this Privacy Policy.

If the Company plans to use an individual's personal information for a purpose other than that for which it was originally collected or subsequently authorized by the individual, the Company will first provide the individual with the opportunity to "opt-out" of having their personal information used for this new purpose.

**Opt-in:** For sensitive personal information, the Company will give individuals the opportunity to affirmatively and explicitly consent (opt-in) to the disclosure of such information to non-agent third parties, or to use the information for a purpose other than that for which it was originally collected or subsequently authorized by the individual.

### **Onward Transfer**

We will only disclose personal information to non-agent third parties consistent with the terms of this Privacy Policy, including the Notice and Choice principles described above. The Company may transfer personal information without providing notice or choice when required to do so by law.

**Agents:** The Company will only transfer personal information to an agent if the agent either: (i) is subject to EU Directive 95/46/EC (the EU Data Protection Directive); (ii) is subject to the Swiss Federal Act on Data Protection; (iii) is Safe Harbor certified; (iv) is located in another country recognized by the EC as providing adequate protection (such as Canada, Argentina, Guernsey, Isle of Man); (v) agrees in writing to provide at least the same level of protection to transferred personal information as that afforded by this Privacy Policy and the Safe Harbor Principles.

### **Data Security**

The Company will take reasonable precautions to protect personal information from loss, misuse, and unauthorized or inadvertent access, disclosure, alteration and destruction.

### **Data Integrity**

The Company will use personal information only in ways that are compatible with and relevant to the purposes for which it was collected or subsequently authorized by the individual. The Company will take reasonable steps to ensure that personal information in its possession is accurate and reliable for its intended use.

### **Access**

Upon request, the Company will grant individuals reasonable access to their personal information, except where the burden or expense of providing access would be disproportionate to the risk to the privacy of the individual, or where such access would require disclosure of personal or confidential information pertaining to other individuals or to the Company. The Company will also take reasonable steps to allow individuals to correct, amend or delete their personal information if it is inaccurate or incomplete.

Further information on procedures for accessing or amending personal information may be obtained by contacting the Compliance Officer at the address set forth below.

### **Enforcement**

**Verification:** The Company has implemented a self-assessment audit process to verify ongoing adherence to the terms of this Privacy Policy. Any employee that the Company determines is in violation of the Privacy Policy will be subject to disciplinary action up to and including termination of employment.

**Dispute Resolution:** The Company has implemented mechanisms to address complaints or concerns regarding the Company's collection or use of personal information.

The Company will investigate and attempt to resolve complaints and disputes regarding use and/or disclosure of personal information by reference to the principles contained in the Privacy Policy. If the Company is unable to resolve the dispute with the complainant, the dispute will be referred to one of the following third-party dispute resolution services:

- (i) the Panel established by the EU Data Protection Authorities (DPA) for disputes received by the Company from the EU/EEA
- (ii) the Swiss FDPIC for disputes involving personal information received by the Company from Switzerland.

The Company has made itself subject to, and agrees to cooperate and comply with, the dispute resolution, enforcement and sanctioning powers of the DPA Panel and FDPIC to resolve disputes pursuant to the Safe Harbor principles.

Questions or concerns, or further information regarding dispute resolution procedures, should be directed to the Compliance Officer at the address set forth below.

### **LIMITATION ON PRIVACY POLICY**

If there is any conflict between this Privacy Policy on the one hand and the Safe Harbor Principles on the other hand, the Safe Harbor Principles shall govern.

Adherence by the Company to this Privacy Policy may be limited to the extent required to meet legal or ethical obligations or to meet national security or law enforcement obligations, and is subject to the provisions of any other applicable law or regulation in any of the jurisdictions in which we conduct our business.

#### **SALE OF COMPANY**

If the Company (or any part of it) is sold or transferred at any time, the information we hold may form part of the assets transferred, although it will still only be used in accordance with the terms of this Privacy Policy.

#### **CHANGES TO PRIVACY POLICY**

The Company reserves the right to amend its Privacy Policy consistent with the Safe Harbor Principles. Any such amendments will be reflected on the Safe Harbor Privacy Policy posted on the Company's website. Once posted on the website, the amended Privacy Policy will take immediate effect and will replace all prior versions.

#### **CONTACT INFORMATION**

For any questions or feedback relating to this Safe Harbor Privacy Policy, amendments to personal information, opt-out, personal information access requests, or complaints, contact:

**Angela Cairns**

Global Compliance Officer

KnowledgePoint360 Group

Victoria Mill, Windmill Street

Macclesfield, Cheshire

SK11 7HQ

United Kingdom

Tel: +44 (0)1625 664000

Fax: +44 (0)1625 664007

e-mail: [compliance@kp360group.com](mailto:compliance@kp360group.com)

**EFFECTIVE DATE:** 24 February 2011