InnerWorkings and International Data Privacy

Certain data protection laws prohibit the transfer of personal information to countries outside of the European Economic Area that are viewed as not ensuring an “adequate” level of data protection. Many of the countries in which InnerWorkings operates - including the United States - are not regarded by the EEA as providing such “adequate” protection. As such, InnerWorkings has put in place an agreement between it and its various affiliates on standard terms approved by the EEA in order to ensure such “adequate” protection and is working toward adopting a set of binding corporate rules and supporting procedures and principles (“Rules”) that seek to ensure that personal information of covered individuals in the EEA is treated in an appropriate manner in accordance with applicable law even where it is transferred to countries that are outside of the EEA.

These Rules will apply globally to all InnerWorkings entities where they process the personal data (described in Appendix 1) of employees, contractors, business contacts, customers or third parties in the EEA for the purposes described in Appendix 2 - whether by automatic means or manually. Each InnerWorkings entity must comply with these Rules.

Among other things, InnerWorkings’ Rules will provide for the following with respect to the processing of personal data of covered individuals (employees, contractors, business contacts, customers or third parties) in the EEA:

I. Fairness

InnerWorkings will process personal data fairly and lawfully and will respect the rights and freedoms of individuals in relation to privacy.

II. Purpose

InnerWorkings will limit its processing of personal data to the fulfilment of the specific and legitimate purposes for which it was collected and will only carry out processing of personal data that is compatible with such purposes or with appropriate consent.

III. Proportionality

InnerWorkings will limit its processing of personal data to that which is adequate, relevant and not excessive in relation to the purposes for which it processes such data.

IV. Transparency

InnerWorkings will adopt and publish policies which govern its processing of personal data and will make available to relevant individuals details of its identity and the purposes of its processing.

V. Data Quality

InnerWorkings will keep personal data collected in the EEA accurate and up to date and only for as long as necessary for its specific and legitimate purposes. InnerWorkings encourages individuals to inform InnerWorkings when their personal data changes by posting ways in which to update information in the InnerWorkings Privacy Policy.

VI. Security

InnerWorkings will take commercially reasonable technical and organizational measures to protect personal data against accidental or unlawful destruction or loss and against unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network, and against other unlawful forms of processing.

InnerWorkings will require that service providers also adopt commercially reasonable security measures and enter into contractual arrangements with InnerWorkings that provide that the service provider has in place such technical and organizational security measures to safeguard personal information.

VII. Individuals' Rights

Individuals whose personal information is collected and/or used in the EEA and transferred between InnerWorkings entities under the Rules have the right to obtain the information which relates to them and which is being processed by InnerWorkings. Provided that an individual whose personal information is collected and/or used in the EEA makes a request to InnerWorkings in writing, he or she is entitled to:

(a) be informed of whether InnerWorkings holds and processes personal data about themselves;

(b) be provided with a description of any personal data that InnerWorkings holds about an individual, the purposes for which any such personal data are being held, and the recipients or classes or recipients to whom the information is, or may be, disclosed; and

(c) a copy of the personal data held by InnerWorkings.

Relevant individuals also have the right to:

(a) ask InnerWorkings to correct or delete personal data about them that may be incomplete, inaccurate or excessive;

(b) object to the processing of personal data about them (unless the processing is required by applicable law); and

(c) opt out, without charge and on request, to the use of their personal data for direct marketing purposes by InnerWorkings.

Any such requests and objections may be sent to: (a) our online web form available by clicking here; (b) or the registered address of their local InnerWorkings entity, which can be found on InnerWorkings' website at www.inwk.com; or (c) InnerWorkings Europe Limited, 5 Cranbrook Way, Solihull, B90 4GT, Birmingham, U.K. or (d) privacy@inwk.com.

VIII. Further information or complaints

If you would like to request a copy of the Rules, or you have a complaint related to any potential misuse of your information or a potential breach of the Rules, you may contact your local InnerWorkings entity or InnerWorkings Europe Limited (UK) at:

InnerWorkings Europe Limited
5 Cranbrook Way
Solihull
B90 4GT, Birmingham, U.K.
privacy@inwk.com

InnerWorkings Europe Limited (UK) is responsible for investigating and resolving complaints under the Rules. Upon receiving a complaint, it is InnerWorkings Europe Limited (UK)'s policy to acknowledge receipt of the complaint within five business days. Individuals are then notified as appropriate regarding the outcome of the complaint. In the event that an individual submits a complaint that he/she has suffered damage that could likely be attributable to a breach of the Rules by a particular InnerWorkings entity, it is InnerWorkings Europe Limited (UK)'s burden to prove that the damages were not attributable to the relevant InnerWorkings entity. If InnerWorkings Europe Limited (UK) can prove that the relevant InnerWorkings entity was not liable for the violation, it may discharge itself from any responsibility.

In addition, the Rules will provide that, where an individual has suffered damage that could likely be attributed to a breach of the Rules, the individual whose personal information is collected and/or used in the EEA, or transferred out of the EEA, is able to enforce privacy rights using the Rules through a regulator or a court.

Last updated: March 2018

Appendix 1

Description of Personal Data

The Rules apply to the following three categories of personal data: employee (HR) data, customer data, and supplier/ vendor data.

Employee (HR) data includes:
Name/title, employee status, User ID, government ID, date of birth, gender, email/telephone/business and home address, department, hire date, job title, salary, employment application information, employee profile (work history, languages, education), performance/goals, development plan, rating/evaluation information, CV, health insurance information, background check information, race/ethnic/religion information (only if required for payroll purposes), photograph (optional).

Customer data includes:
Name, mailing address, e-mail address, social media identifiers/usernames, birthday, phone and fax number, corporate and/or business name and company data, job title, account name, order/purchase and order history, registration history, IP address, country/geographic location, payment and billing information, digital identifiers, information needed to conduct a credit check, behavioral information, data exporter/importer-webpage browsing data, language preferences, client lists and information included on such lists.

Supplier/vendor data includes:
Name, mailing address, e-mail address, social media identifiers/usernames, birthday, phone and fax number, corporate and/or business name and company data, job title, account name, contractual information, IP address, country/geographic location, payment and billing information, information needed to conduct a credit check, language preferences, supplier lists and information included on such lists.

Appendix 2

Purposes of Processing

The categories of personal data described in Appendix 1 will be processed for the purposes described below:

Employee (HR) data:
Employee (HR) data of employees of the EEA InnerWorkings Group companies may be stored on the local servers of those EEA Group companies to enable each EEA Group company to perform day to day HR management functions.

Employee (HR) data of employees of the EEA InnerWorkings Group companies is also transmitted to the United States and stored on network servers in the United States for the purpose of centralised decision making and ensuring consistent HR administration and management across the Group as a whole, in areas including: recruitment, remuneration, performance management, promotions, employee resource and workflow management, workforce mobility, benefits management, equal opportunities monitoring, management forecasting and compliance with legal and regulatory obligations.

Employee (HR) data of employees of the EEA InnerWorkings Group companies may also be transferred between InnerWorkings Group companies both within and outside of the EEA on an exceptional basis for purposes including the temporary working arrangements and re-location/secondment of individual employees.

Customer data and supplier/vendor data:
Customer data and supplier/Vendor Data of the EEA InnerWorkings Group companies may be stored on the local servers of those EEA Group companies for purposes including: providing products and services to clients, charging for such products and services and providing support and maintenance activities in relation to such products and services, contacting customers and suppliers and validating their identities, performing credit checks and debt collection, performing market research and behavior analysis, advertising, record keeping and to meet legal and regulatory obligations.

Customer data and supplier/vendor data of the EEA InnerWorkings Group companies is also transmitted to the United States and stored on network servers in the United States for the purposes of centralised decision making and global strategy, product and service fulfilment, record keeping and compliance with legal and regulatory obligations.

Customer Data and Supplier/Vendor Data may also be transferred between InnerWorkings Group companies both within and outside of the EEA on an exceptional basis, where the relevant customer relationship so requires.