INNERWORKINGS, INC.
BINDING CORPORATE RULES

1. INTRODUCTION

These Binding Corporate Rules ("Rules") explain how the InnerWorkings group respects the privacy rights of its customers, employees, suppliers, vendors, and other individuals whose personal data InnerWorkings collects and uses. The Rules seek to ensure that personal data will be treated in a consistent, secure manner and with full respect for privacy rights and freedoms.

These Rules are binding on each member of the InnerWorkings group of entities; an up-to-date list of these entities is available from the office of the General Counsel. InnerWorkings group entities are based in the following countries: Argentina, Australia, Belgium, Brazil, Canada, Chile, China, Colombia, Costa Rica, Czech Republic, Denmark, Dominican Republic, Ecuador, El Salvador, France, Germany, Greece, Guatemala, Honduras, Hong Kong, Hungary, India, Ireland, Italy, Luxembourg, Mexico, Netherlands, Panama, Peru, Poland, Portugal, Puerto Rico, Russia, Singapore, South Africa, South Korea, Spain, Switzerland, Turkey, UAE, Ukraine, United Kingdom, United States and Venezuela. As binding, these Rules impose a duty on all InnerWorkings entities to respect and comply with the Rules.

These Rules are also binding on all employees of each InnerWorkings entity. InnerWorkings' Board of Directors has authorized the creation of these Rules and the Board and management team will work to ensure that the group is compliant with the Rules described herein. The Board has full authority to monitor compliance with the Rules for each member of the InnerWorkings group of entities and, where necessary, investigate complaints and enforce corrective action.

Specifically, the objective of the Rules is to be compliant with European data protection laws. Article 25 of the EU Data Protection Directive (95/46/EC) prohibits the transfer of personal data to a country or territory outside the European Economic Area ("EEA") unless that country or territory ensures an adequate level of protection for the rights and freedoms of data subjects in relation to the processing of personal data by companies. EU Privacy and Electronic Communications Directive (2002/58/EC), amended by Directive 2009/136/EC, mandates protection of personal data relating to the delivery of communication services, including that personal data is safeguarded. The Directive also provides that notice must be provided to the individual and the National Regulatory Authority in the event of a breach of personal data.

The Article 29 Working Party in June 2012 announced a new initiative on Binding Corporate Rules so that a multinational company's entities could transfer personal data outside of the EEA as an alternative to the Safe Harbor Principles or the Standard Contractual Clauses. In line with European data protection laws, InnerWorkings, its Board, and its management are dedicated to providing adequate protection for the processing and transfer of personal data through these Rules.

2. SCOPE

The purpose of these Rules is to set out a framework to ensure an adequate level of protection for all personal data that is transferred from InnerWorkings entities within the EEA to InnerWorkings entities outside the EEA.

These Rules apply to all transfers of personal data relating to InnerWorkings' employees, customers, suppliers and vendors whether by automatic means or manually, between:

(a) any EEA based InnerWorkings entity and any non-EEA based InnerWorkings entity;

(b) any non-EEA based InnerWorkings entity and any other non-EEA based InnerWorkings entity, to the extent that the first non-EEA based InnerWorkings entity received the relevant personal data as a result of a transfer from an EEA based InnerWorkings entity; and

(c) any EEA based InnerWorkings entity and any other EEA based InnerWorkings entity.

A description of the personal data to which these Rules apply is set out in Appendix 1 to these Rules (Description of Data) and a description of the purposes for which this personal data is processed and transferred is set out in Appendix 2 to these Rules (Purposes of Processing).

Each InnerWorkings entity will ensure that all processing of personal data is carried out in accordance with applicable data protection laws as provided by Article 4 of Directive 95/46/EC. Where there are no such data protection laws or the relevant data protection laws do not meet the standards set out in these Rules, the InnerWorkings entity will process personal data in compliance with these Rules.

In the event that any national law imposes a higher level of protection for personal data than that described in these Rules, then the relevant national law will take precedence over these Rules in respect of the point of conflict only.

InnerWorkings Europe Limited (UK) is the InnerWorkings entity which has been authorised by the Board, and by all other members of the InnerWorkings group of entities, to act on their behalf for the purpose of ensuring the group's compliance with data protection responsibilities in the EEA and with these Rules. Data subjects can enforce these Rules against InnerWorkings Europe Limited (UK) as a third-party beneficiary as described below.

In these Rules, the terms "personal data," "sensitive personal data," "processing," "data controller," "data processor," "third party," "Data Protection Authorities," and "data subject" have the meanings set out in EU Directive 95/46/EC. In these Rules,

"they" and "their" means any individual whose personal data InnerWorkings processes and "we," "us," and "our" means InnerWorkings. InnerWorkings interprets the terms of these Rules in accordance with EU Directives 95/46/EC and 2002/58/EC.

3. PURPOSE

InnerWorkings will process personal data fairly and lawfully, including in accordance with the conditions set out in applicable data protection laws (such as Recitals 28 and 30 and Articles 2-4, 6-8, 10-12, 14-17, 23-26 and 30 of Directive 95/46/EC). In particular, InnerWorkings will ensure it has a lawful basis for all processing activities.

InnerWorkings will only transfer and process personal data for specific and legitimate purposes, only if it is necessary, and only if there is a legitimate basis for doing so (for example, if it has the data subject's fully informed and freely given consent).If InnerWorkings wants to process a data subject's personal data for a purpose other than the purpose for which it was originally obtained, InnerWorkings will make the data subject aware of such a change unless there is a legitimate reason for not doing so (for example, where it is necessary to safeguard national security, the prevention or detection of crime, legal proceedings, tax purposes, or where otherwise permitted by law). In certain instances, national laws may require InnerWorkings to obtain a data subject's consent to any such new purposes.

Additionally, InnerWorkings will only process data subjects' sensitive personal data (personal data relating to their racial or ethnic origin, political opinions, religious or other beliefs, trade union membership, health, sex life, or criminal convictions) if it is necessary and where InnerWorkings has obtained a data subject's explicit consent, which must be genuine and freely given (unless there is another legitimate basis for processing without his or her explicit consent).

4. DATA QUALITY

InnerWorkings will keep personal data accurate and up to date. InnerWorkings encourages data subjects to inform InnerWorkings when their personal data changes by posting ways in which to update information in the InnerWorkings Privacy Policy.

InnerWorkings will ensure that personal data will be adequate, relevant and not excessive in relation to the purposes for which it is transferred and further processed.

InnerWorkings will ensure that personal data is not processed for longer than necessary for the purposes for which it is obtained and further processed and shall retain personal data in accordance with InnerWorkings' Document Retention and Destruction Policy and relevant schedule, as amended from time to time.

5. AVAILABILITY AND TRANSPARENCY

InnerWorkings shall ensure that these Rules (or the essence of them) are readily available to data subjects in their local language and the Rules shall be published on the InnerWorkings intranet site. An individual may request a hard copy of these Rules from InnerWorkings Europe Limited (UK) at the address set out below, or from the local InnerWorkings entity in his or her country.

InnerWorkings Europe Limited (UK) One Cranmore
Cranmore Drive
Solihull
B90 4RZ, Birmingham, U.K.

Before any InnerWorkings entity processes personal data, it will ensure that data subjects have been provided with the following information through its Privacy Policy:

(a) the identity of the InnerWorkings data controller(s) (and its (their) representative(s), if any);

(b) the types of personal data and sensitive personal data that the InnerWorkings entity will process;

(c) the purposes for which the personal data is intended to be processed;

(d) any further information such as:

(i) the recipients or categories of recipients of the personal data;

(ii) the existence of the data subject's right of access to and the right to rectify their data,

in so far as such further information is necessary, having regard to the specific circumstances in which the data is collected, to guarantee fair processing in respect of the data subject.

Where the personal data has not been obtained from the data subject, the obligation to inform the data subject as set out above, does not apply if the provision of such information proves impossible or would involve a disproportionate effort or if recording or disclosure is expressly laid down by applicable law.

6. DATA SUBJECTS' RIGHTS

Subject to exemptions provided by applicable law each InnerWorkings entity will ensure that all data subjects whose personal data is processed or transferred under these Rules have the right to:

(a) obtain the information which relates to them which is being processed by InnerWorkings. Provided that the data subject makes a request to InnerWorkings in writing, specifically he or she is entitled to:

(i) be informed of whether InnerWorkings holds and processes personal data about them;

(ii) be provided with a description of any personal data that InnerWorkings holds about the data subject, 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

(iii) a copy of the personal data held by InnerWorkings, in an intelligible form. InnerWorkings may ask a data subject for any information that InnerWorkings reasonably requires to confirm the identity of the person making the request and for InnerWorkings to locate the relevant information to which the subject access request relates.

(b) obtain the rectification, erasure or blocking of data in particular where the data is incomplete or inaccurate;

(c) object, at any time, to the processing of their personal data (unless the processing is required by applicable law). Where the objection is justified the relevant InnerWorkings entity will ensure that it ceases the processing that is of concern; and

(d) object, on request and free of charge, to the processing of personal data relating to him or her for the purposes of direct marketing by InnerWorkings, by contacting InnerWorkings at privacy@inwk.com.

Any requests under this section should be sent to: (a) the registered address of the data subject's local InnerWorkings entity, which can be found on InnerWorkings' website at www.inwk.com; or (b) InnerWorkings Europe Limited (UK), One Cranmore, Cranmore Drive, Solihull, B90 4RZ, Birmingham, U.K or (c) privacy@inwk.com.

7. AUTOMATED INDIVIDUAL DECISIONS

InnerWorkings will not make evaluations or decisions about a data subject that would significantly affect them based solely on processing by automated means, unless the evaluation or decision:

(a) is taken in the course of the entering into or performance of a contract, provided the request for the entering into or the performance of the contract, lodged by the data subject, has been satisfied or that there are suitable measures to safeguard his or her legitimate interests, such as arrangements allowing him to put across his or her point of view; or

(b) is authorized by applicable law which also lays down measures to safeguard the data subject's legitimate interests.

8. SECURITY AND CONFIDENTIALITY

InnerWorkings will take appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure, or access, in particular where the processing involves the transmission of data over a network, and against other unlawful forms of processing (including taking reasonable steps to ensure the reliability of employees who have access to personal data). InnerWorkings employees will process personal data in accordance with these Rules, and any employees who breach these Rules may be subject to disciplinary action, including dismissal. Sensitive personal data will be processed with enhanced security measures.

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

InnerWorkings will also adhere to its Global Information Security and Privacy Policy, which requires physical, technological, and administrative safeguards for the storage and transfer of personal data. In the event of a security incident, InnerWorkings will adhere to its Incident Response Plan which sets out how incidents will be assessed, contained, investigated and notified, as appropriate.

9. DATA PROCESSORS THAT ARE MEMBERS OF THE INNERWORKINGS FAMILY OF ENTITIES

If an InnerWorkings entity processes personal data on behalf of another InnerWorkings entity, the InnerWorkings entity which is the data controller will obtain contractual commitments from the InnerWorkings entity which is the data processor stipulating that the processor entity shall act only on the written instructions of the controller entity and requiring the processer entity to have in place appropriate technical and organizational security measures to safeguard the personal data.

10. THIRD-PARTY DATA PROCESSORS AND INTERNATIONAL TRANSFER

If an InnerWorkings entity acting as a data controller uses a third-party data processor to process personal data on its behalf, it will in compliance with the requirements of applicable law:

(a) ensure that such data processor provides sufficient guaranties to implement appropriate technical and organizational security measures governing the processing to be carried out and to protect the rights of data subjects,

including to ensure the ongoing confidentiality, integrity, availability and resilience of relevant systems and services and the ongoing availability and access to personal data;

(b) ensure and be able to demonstrate compliance with those measure;

(c) ensure by default only personal data are processed which are necessary for the specific purpose(s) of the processing;

(d) obtain binding contractual commitments in writing to safeguard the security of the personal data including (i) to require that the third party data processor shall act only on the documented instructions of the InnerWorkings entity in relation to the processing of that personal data; (ii) that the third party has in place appropriate technical and organizational security measures to protect the personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access, in particular where the processing involves the transmission of data over a network and against all other unlawful forms of processing at least equivalent to those required to be taken under applicable law, (iii) that persons authorized to process personal data are subject to binding obligations of confidentiality, (iv) that the processing will not be sub contracted or delegated to a third party without the consent of the InnerWorkings entity; (v) to assist the InnerWorkings entity to comply with its obligations under applicable law and make available all information necessary to demonstrate such compliance including by participation in and conduct of appropriate audits and assessments, evaluations and tests; (vi) to maintain all relevant records of processing activity required to be kept under applicable law; (vii) at the option of the InnerWorkings entity to delete or return all personal data; and (viii) to restore availability and access to personal data following an incident. Such contractual commitments shall specify the subject matter and duration of the processing, the nature and purpose of the processing, the type of personal data and categories of data subject and the obligations and rights of the controller.

An InnerWorkings entity will not transfer personal data to a third party (other than to another InnerWorkings entity subject to these Rules) outside of the EEA without ensuring an adequate level of protection for the personal data, as required under applicable law including where appropriate by requiring that contractual clauses (such as the EU standard contractual clauses) are in place with any third-party data processor and/or data controller to require an adequate level of protection of the personal data transferred.

11. TRAINING

InnerWorkings will provide appropriate training to InnerWorkings' employees who have permanent or regular access to personal data, who are involved in the collection of personal data, or who are involved in the development of tools used to process

personal data. The training shall be provided to ensure these employees are aware of their obligations under these Rules.

12. AUDIT

Under these Rules each member of the InnerWorkings group is under a duty to conduct - through its internal audit function (or using an external auditor appointed by InnerWorkings) - and to cooperate with, an audit at least annually (or within a shorter timescale as specifically requested by the Chief Compliance and Privacy Officer and/or InnerWorkings' internal audit function) to evaluate and report on all aspects of InnerWorkings' compliance with these Rules.

The results of the audit will be reported by the InnerWorkings internal audit function, or an external auditor (as appropriate), to the relevant Management Team, the Chief Compliance and Privacy Officer and InnerWorkings' Audit Committee (a committee of the Board of Directors), which will ensure that any corrective action takes place as soon as reasonably practicable. If requested, InnerWorkings' internal audit function will also provide a copy of the results of the audit to Data Protection Authorities (subject to applicable laws and respect for any confidential, privileged, or commercially sensitive information provided).

InnerWorkings agrees that Data Protection Authorities may conduct audits of relevant InnerWorkings entities for the purposes of demonstrating compliance with these Rules on giving reasonable prior notice and during business hours (unless this requirement is in conflict with local law), with full respect to the confidentiality of the information obtained and to the trade secrets of InnerWorkings. Each InnerWorkings entity shall comply with any directions issued by Data Protection Authorities issued following such audits.

13. COMPLIANCE

InnerWorkings has a Compliance Committee which is chaired by the General Counsel and is composed of senior management of InnerWorkings. The Chief Compliance and Privacy Officer is responsible for overseeing all privacy and data protection issues, including ensuring compliance with all aspects of these Rules. The Chief Compliance and Privacy Officer reports to the General Counsel. The Chief Compliance and Privacy Officer is supported by local teams responsible for overseeing and ensuring compliance with these Rules on a day-to-day basis at a local level. The local privacy teams report any substantial or major privacy issues to the Chief Compliance and Privacy Officer.

14. ACTIONS IN CASE OF NATIONAL LEGISLATION PREVENTING COMPLIANCE WITH THE RULES

Where InnerWorkings has reason to believe that legislation applicable to an InnerWorkings entity prevents InnerWorkings from fulfilling its obligations under these Rules and has a substantial effect on InnerWorkings' ability to comply with these Rules, InnerWorkings will promptly inform the Chief Compliance and Privacy Officer (unless otherwise prohibited by a law enforcement authority).

InnerWorkings will ensure that where there is a conflict between national law and these Rules, the Chief Compliance and Privacy Officer will make a responsible decision regarding what action to take and will consult with the relevant Data Protection Authority.

15. COMPLAINT HANDLING

InnerWorkings shall follow the Complaint Handling Procedure in relation to any complaints received from data subjects regarding InnerWorkings' compliance with these Rules and/or if the data subject claims to have suffered any loss as a result of an alleged breach of these Rules. All claims for compensation, and complaints - including compensation claims that relate to an alleged breach of these Rules - will be the responsibility of the InnerWorkings Europe Limited (UK). Such complaints may be submitted in the data subject's local language in any of the ways set out in the Complaints Handling Procedure - including by making contact with the local Group entity, by calling the Group's hotline, or by contacting InnerWorkings Europe Limited (UK) at:

One Cranmore
Cranmore Drive
Solihull
B90 4RZ, Birmingham, U.K.

16. THIRD-PARTY BENEFICIARY RIGHTS AND LIABILITY

All companies within the InnerWorkings group must comply with these Rules. Any data subjects whose personal data are used and/or collected in the EEA and transferred to InnerWorkings entities outside of the EEA shall have the right to enforce these Rules as a third-party beneficiary and shall have the right to seek compensation for damage where they establish facts which show that such damage is likely to be attributed to a breach of the Rules, including, but not limited to, a judicial award of compensation for damage suffered by the data subject as a result of breach of these Rules. Any such claims can be brought by the data subject in the EEA jurisdiction in which InnerWorkings exported the personal data outside of the EEA and the jurisdiction of InnerWorkings Europe Limited (UK). Data subjects also have

the right to lodge a complaint before applicable Data Protection Authorities. The claims which may be brought include claims to enforce the following rights:

- that the data subject has been informed or will be informed before any transfer of their personal data that their data could be transmitted to a third country not providing adequate protection;
- to obtain a copy of the binding corporate rules upon request;
- to be replied to in a reasonable time and to the extent reasonably possible about queries concerning the processing of this personal data outside the Community;
- to declare that a member of the corporation bound by the rules is not co-operating with the competent data protection authorities and/or is not abiding by the advice given by the data protection authority with regard to the processing of the data transferred;
- to declare that the legislation applicable to any of the members of the corporations outside the Community prevents him from fulfilling his obligations under the binding corporate rules;
- to declare that the processing of personal data of any member of the corporation bound by the rules is not in accordance with the binding corporate rules;
- to claim liability and, where appropriate, compensation in accordance with the terms set up in the binding corporate rules;
- to be able to use European jurisdiction in accordance with the terms set up in the binding corporate rules; and
- to declare that the rules have been varied contrary to the binding corporate rules or without respecting the procedural obligations set up thereof, or that any member of the corporation does not honour its obligations once he is no longer bound by the rules,

InnerWorkings Europe Limited (UK) takes responsibility for and agrees to take the necessary action to remedy the acts of other InnerWorkings entities outside of the EEA and to pay compensation for any damages resulting from the violation of these Rules by other InnerWorkings entities. Any claim arising out of or relating to a breach of these rules will be the responsibility of InnerWorkings Europe Limited (UK).

In the event of a claim by a data subject that he/she has suffered damage that could likely be attributed to a breach of these Rules, the burden of proof to show that the damages suffered by the data subject due to a breach of the Rules are not attributable to the relevant InnerWorkings entity will rest with InnerWorkings Europe Limited (UK). If InnerWorkings Europe Limited (UK) can prove that the InnerWorkings entity outside the EEA is not liable for the violation, it may discharge itself from any responsibility.

17. CO-OPERATION WITH DATA PROTECTION AUTHORITIES

Each InnerWorkings entity will cooperate with any competent Data Protection Authority and will comply with the advice of competent Data Protection Authorities on any issues related to the interpretation and application of these Rules.

InnerWorkings entities shall cooperate and assist each other to handle requests or complains from data subjects or investigations or inquiries by Data Protection Authorities.

18. UPDATES OF THE RULES

InnerWorkings will notify the relevant European Data Protection Authorities at least once a year of any changes made to these Rules or any changes to the list of InnerWorkings entities bound by these Rules and will provide a brief explanation of the reasons for any such changes. Where there is a major change to these Rules, InnerWorkings will notify the relevant European Data Protection Authorities either in advance of the change or promptly thereafter.

InnerWorkings will communicate any substantive changes to these Rules to the affected InnerWorkings entities. The Chief Compliance and Privacy Officer (or another party as appointed by the Chief Compliance and Privacy Officer with delegated responsibility) will maintain an up-to-date list of InnerWorkings entities bound by these Rules, maintain a record of any updates to these Rules, and provide any necessary information to data subjects or European Data Protection Authorities upon request.

No transfer of personal data will be made to a new InnerWorkings entity until the exporter of the data has made sure that the new member is effectively bound by these Rules and can deliver compliance.

Effective Date:

Appendix 1

Description of Data

These 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 to these Rules are 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.