SAFE HARBOR POLICY

Safe Harbor Policy for Transmission to the U.S. of Human Resource Data from Businesses Located in the European Union

Policy Statement

iNRCORE acknowledges the EU's standard for personal data protection. iNRCORE has a need to extract and compile the Human Resource Data of employees in the EU. This Policy addresses the privacy concerns of European employees and the business concerns of iNRCORE.

To affect this Policy, iNRCORE adheres to the United States Department of Commerce Safe Harbor Principles and self-certifies on an annual basis to the United States Department of Commerce compliance with the Safe Harbor Principles. This Policy applies to all Human Resources Data transmissions from iNRCORE operations in EU countries to the United States. This includes transmission of data over phone lines, computer lines, and in hard copy, and includes such material as human resources and payroll records, and any material that identifies a particular individual employee.

The use of EU employee personnel data includes global enterprise headcount reporting, statistical analysis, compensation planning and related transactions, staffing, international personal security issues, law enforcement inquiries, U.S. Government agency inquiries and mergers, acquisitions and divestitures.

Guidelines

iNRCORE has adopted the seven Safe Harbor principles of notice, choice, onward transfer (transfer to third parties), access, security, data integrity and enforcement with respect to Human Resource Data to be transferred to the U.S. from iNRCORE operations in the EU.

1. **NOTICE**

   iNRCORE collects Personal Information for, among other reasons, human resource management such as payroll administration, filling employment positions, maintaining accurate benefits records, meeting governmental reporting requirements, security, company network access, authentication and Global Headcount. iNRCORE does not request or gather information regarding political opinions, religion, philosophy, or sexual preference. To the extent iNRCORE maintains information on an individual's medical health or ethnicity (only for countries where it is legally required) iNRCORE will protect, secure and use that information in a manner consistent with this Policy and law.

   If iNRCORE collects Personal Information directly from individuals, it will inform them about the purposes for which it collects and uses Personal Information about them, the types of Non-Agent Third Parties to which iNRCORE discloses that information, and the choices and means iNRCORE offers individuals for limiting the use and disclosure of their Personal Information. Notice will be provided in clear and conspicuous language when individuals are first asked to provide Personal Information to iNRCORE, or as soon as practicable thereafter, and in any event before iNRCORE uses the information for the purpose other than for which it was originally collected. iNRCORE may disclose Personal Information if required to do so by law or to protect and defend the rights of property of iNRCORE.

2. **CHOICE**

   iNRCORE will offer individuals the opportunity to choose (opt-out) whether their Personal Information is: (a) to be disclosed to a Third Party which is not an Agent; or (b) to be used for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual.

   For Sensitive Personal Information, iNRCORE will give individuals the opportunity to affirmatively and explicitly (opt-in) consent: (a) to the disclosure of information to a non-Agent Third Party; or (b) the use of the information for a purpose other than the purpose for which it was originally collected or subsequently authorized by the individual. iNRCORE will provide individuals with reasonable mechanisms to exercise their choices should requisite circumstances arise.

iNRCORE, LLC
311 Sinclair Road, Bristol, PA 19007-6812 USA
Tel: +1.215.781.6400 Fax: +1.215.781.6430
www.iNRCORE.com

3. ONWARD TRANSFER (Transfer to Third Parties)

Prior to disclosing Human Resource Data to a third party, iNRCORE applies the notice and choice principles, enumerated above.
iNRCORE will ensure that any third party keeper of Human Resources Data also subscribes to the Safe Harbor Principles or any other EU adequacy finding. iNRCORE will also enter into written agreements with such third parties requiring them to provide at least the same level of personal data protection as is maintained by iNRCORE.

4. ACCESS AND CORRECTION

Upon request, iNRCORE will grant individuals reasonable access to Personal Information that it holds about them. In addition, iNRCORE will take reasonable steps to permit individuals to correct, amend, or delete information that is demonstrated to be inaccurate or incomplete (except when the burden or expense of providing access would be disproportionate to the risks of the indivdual privacy in the case in question or if the rights of persons other than the individual woudl be violated). Any employee that desires to review or update his or her Personal Information can do so by contacting their local human resources representative. If the employee is not satisfied with the response of the local human resources representative, the employee should submit a written description of the matter the the Global Human Resources Manager.

5. SECURITY

iNRCORE will take reasonable precautions to protect Personal Information in its posession from loss, misuse and unauthorized access, disclosure, alteration and destruction. iNRCORE limits access to Personal Information and data to those persons in iNRCOREs' organization, or as Agents of iNRCORE, that have a specific business purpose for maintaining and prcoessing such Personal Information and data. Any individuals who are granted access to Personal Information will have been made aware of their responsibilities to protect the security, confidentiality, and integrity of that information and will have been provided training and instruction on how to do so.

6. DATA INTEGRITY

The Company will collect only Personal Informatoin which is relevant for the purposes for which it is to be used. The Company will take reasonable steps to ensure that Personal Information is relevant, accurate, complete, and current, to its inteded use.

7. ENFORCEMENT

To ensure compliance with these Safe Harbor Principles, iNRCORE will:

a. Cooperate with the Data Protection Authorities (DPAs) fo the EU countries in the investigation and resolution fo the complaints and comply with advice given by DPAs;

b. Periodically verify iNRCOREs' complaince with the Safe Harbor Principles;

c. Remedy issues arising out of any failure to comply with the Principles. iNRCORE acknowledges that its failure to provide an annual self-certification to the Department of Commerce will remove it from its list of participants and the transfers of information will not be allowed unless iNRCORE otherwise complies with the EU Data Protection Directive.
The iNRCORE Human Resources Director & IT Manager are the internal mechanisms for ensuring compliance with the Safe Harbor Principles and facilitating the independent recourse mechanisms referenced in item 7 above of this Policy.

8. EFFECTIVE DATE AND CHANGES TO THE SAFE HARBOR PRIVACY POLICY

The practices described in this Policy are the current Personal Information protection policies as of September 21, 2011. iNRCORE reserves the right to modify or amend this Policy at any time consistent with the requirements of the Safe Harbor Principles. Appropriate public notice will be given concerning such amendments.

iNRCORE, LLC
311 Sinclair Road, Bristol, PA 19007-6812 USA
Tel: +1.215.781.6400 Fax: +1.215.781.6430
www.iNRCORE.com

Definitions

European Union
The European Union (EU) consists of 15 member countries: Austria, Belgium, Denmark, Finland, France, Germany, Greece, Ireland, Italy, Luxembourg, The Netherlands, Portugal, Spain, Sweden, and the United Kingdom.

Human Resource Data (for the purpose of this policy)
Any Human Resource information related to an identified or identifiable natural person who is an iNRCORE employee and who can be identified, directly or indirectly, in particular by a reference to an identification number or to one or more factors specific to his or her physical, physiological, mental, economic, cultural or social identity.

Self-Certification to the Department of Commerce
iNRCORE must certify to the U.S. Department of Commerce that it abides by the Safe Harbor Principles. iNRCORE must also state annually in its published privacy policy statement that it adheres to the Safe Harbor.

Sensitive Data
Sensitive Data is data that pertains to racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, health, sexual orientation or alleged commission of any offense. This data may not be transferred unless an individual gives explicit consent.

Responsibilities
Questions regarding the transmission of Human Resources Data from the European Union (EU) to the United States or any other non-EU location, or any further transmission of the personnel data once received in the United States, should be referred to the iNRCORE Human Resources Manager, Karlynne Hathaway. iNRCORE must annually, in writing, certify to the Department of Commerce that it adheres to the Safe Harbor Principles.

iNRCORE, LLC
311 Sinclair Road, Bristol, PA 19007-6812 USA
Tel: +1.215.781.6400 Fax: +1.215.781.6430
www.iNRCORE.com