TEREX CORPORATION

DATA PROTECTION POLICY

Index

1.0 Policy Statement, Purpose and Scope

Terex is committed to complying with data protection and security requirements in the countries in which it and its subsidiaries operate. Terex has adopted the policies and procedures in this Data Protection Policy in order to achieve worldwide compliance with applicable laws and regulations, with supplemental policies to be implemented as needed in those jurisdictions with unique requirements.

2.0 Requirements

2.1 Data Protection Principles

Terex will treat and process Personal Data lawfully. Such Data shall be obtained only for specified and legitimate purposes, and it shall not be further processed in any manner incompatible with those purposes. Personal Data shall be collected and processed to the degree necessary to meet the purposes of collection. It shall not be kept longer than necessary. Personal Data shall be collected and processed using technical and procedural measures taken to secure legal compliance.

Personal Data should be collected and processed only:

- with the consent of the Data Subject, or
- as permitted by contract with the Data Subject, or
- in order to comply with a legal obligation, or
- in the event of a Data Subject's vital interests, or
- in order to perform a task as requested or required by an official authority, or
- when there is a legitimate interest of Terex, or of a Third Party to whom the data is disclosed, to collect and process the Personal Data.

2.2 Communication and Transfer of Personal Data to Third Parties and within Terex

Personal Data shall not be transferred to another entity, country or territory unless reasonable and appropriate steps have been taken to maintain the required level of data protection and may only be communicated for reasons consistent with the purposes for which it was originally collected or for purposes authorized by law. All Sensitive Data transferred outside of Terex or across public communication networks shall be de-identified or protected by use of encryption. All data transfers to Third Parties, to the extent such transfers involve further Processing (as defined), shall be subject to Safe Harbor certifications (as applicable) or agreements that include appropriate data protection provisions. EU Personal Data shall only be transferred outside the EU and the European Economic Area if an adequate level of legal protection for the rights and freedoms of Data Subjects is guaranteed by standard contractual clauses, Safe Harbor or binding corporate rules.

2.3 Sources and Quality of Personal Data

Unless a legal exception exists, Personal Data should only be collected from the Data Subject. To protect Terex from the risk of incorrect collection, processing and storage of such Personal Data, each Terex legal entity is responsible for having its business units comply with applicable data protection laws from the moment of original collection of Personal Data.

2.4 Disclosure to the Data Subject

When Personal Data is collected from the Data Subject for the first time, the Data Subject should be informed as to how the Personal Data will be used, either orally, electronically via the Terex Intranet, or in writing unless the Data Subject already knows or should know how such Personal Data will be used. If there is a change in how the collected data will be used, the Data Subject should be informed of such change.

2.5 Sensitive Data

Sensitive Data shall only be processed if it is either authorized or required by law, or if the Data Subject consents, or in cases of urgent medical care. All contracts with employees and independent contractors who will have access to Sensitive Data must contain adequate confidentiality requirements or Terex may establish other means to assure that those handling Sensitive Data understand the appropriate confidentiality to be exercised with this kind of data. If Sensitive Data is processed under other circumstances, such processing must be pre-approved in writing by the Terex Chief Ethics & Compliance Officer or her designee.

2.6 Data Relating to Criminal Offenses

An investigation relating to criminal offenses will be conducted either (a) when initiated by Terex, in accordance with applicable Terex Corporation policies, or (b) under the control of an official authority in accordance with the local laws.

3.0 Notification to Data Protection Authorities Regarding Terex Processing Activities

If applicable law requires notifying the responsible Data Protection Authorities, Terex will not knowingly process such data until the notification is provided. Terex will comply with data notification requirements.

4.0 Data Security and Data Secrecy

Terex shall adopt technical and procedural measures to ensure the security of Personal Data at every Terex site, and shall also endeavor to prevent the alteration, loss, damage, unauthorized processing of or access to Personal Data, taking into consideration commercially acceptable practices, the nature of the data, and the risk of inadvertent disclosure of data. All management team members who deal with Personal Data as part of their work shall be required to maintain the secrecy of that data, both during and after their employment by Terex.

Adequate security measures shall be implemented at every Terex site to achieve:

- Entry Control: Preventing unauthorized persons from gaining access to data processing systems in which Personal Data are processed.
- Admission Control: Preventing data processing systems from being used by unauthorized persons.
- Access Control: Preventing persons entitled to use a data processing system from accessing data beyond their needs and authorizations. This includes preventing unauthorized reading, copying, modifying or removal during processing and use, or after storage.
- Disclosure Control: Ensuring that Personal Data in the course of electronic transmission during transport or during storage on a data carrier cannot be read, copied, modified or removed without authorization, and providing a mechanism for checking to establish who is authorized to receive, and who has received, the information.
- Input Control: Ensuring the ability to establish whether and by whom Personal Data have been accessed, modified or removed.
- Job Control: Ensuring that in the case of commissioned processing of Personal Data, the data can be processed only in accordance with the instructions of the Data Controller.
- Availability Control: Ensuring that Personal Data are protected against undesired destruction or loss.
- Use Control: Ensuring that data collected for different purposes can and will be processed separately.
- Longevity Control: Ensuring that data are not kept longer than necessary, including by requiring that data transferred to third persons be returned or destroyed.

5.0 Data Protection Trainings

Each Terex site will help protect Personal Data and comply with applicable law by providing training that includes:

- The contents of this Policy, especially each team member's duty to use and permit the use of Personal Data only by authorized persons and for authorized purposes, and the need for and proper use of the forms and procedures adopted to implement this Policy according to any principles set forth in section 2.1;
- The relationship of this Policy to other Terex policies, especially those identified in section 6.1;
- The security measures established according to section 4.0;
- A general prohibition of the transfer of Personal Data outside the internal network and physical office premises, except when compliant with this Policy;
- Securely storing manual files, print-outs and electronic storage media; and
- Proper disposal of confidential data by shredding, etc.

6.0 Specific Rules for Specific Countries

6.1 Integration with Other Terex Policies

This Policy applies to Terex operations globally and provides an overarching framework for the company's approach to data protection. Terex has also issued or will issue other data protection policies specifically applicable to particular countries or locations. In some instances, there may be a conflict between a local or different Terex policy (e.g., the Safe Harbor Privacy Policy) and this Policy. In those instances, always comply with the policy or

standard that requires the highest level of data protection and contact the Terex Chief Ethics & Compliance Officer or any attorney in the Terex Legal Department to assist you in resolving the conflict.

6.2 Limited Effect of Policy

This Policy shall not be interpreted as giving any individual rights greater than those to which such person would be entitled under applicable law.

7.0 Implementation

7.1 Publication: May 1, 2014.

7.2 Effective Date: May 1, 2014.

7.3 Revisions: This Policy may be revised at any time.

8.0 Sponsor / Custodian / Implementation

The sponsor of this Policy is the Terex Legal Department. The custodian of this Policy is the Terex Chief Ethics & Compliance Officer. The implementation of this Policy is the responsibility of each legal entity manager.

9.0 Severability

This Policy shall, whenever possible, be interpreted in a manner compatible with applicable law. Any provision held invalid shall be ineffective only to the extent necessary and the remainder of the Policy shall be construed in all respects as if such invalid or unenforceable provision were omitted.

10.0 Glossary

- "**Terex**" means Terex Corporation, and its affiliate operations, divisions and subsidiaries.
- "**Consent**" means "any freely given specific and informed indication of his wishes by which the Data Subject signifies agreement to Personal Data relating to him being processed."
- "**Data Controller**" means a person who (alone or with others) determines the purposes for which and the manner in which any Personal Data are, or are to be, processed. Generally, Terex itself will be the Data Controller, although there may be more than one Data Controller within a group of companies if local or overseas offices, subsidiaries or affiliates within the group enjoy a level of autonomy over the processing of the Personal Data they use.
- "**Data Processor**" means any person, other than an employee of the Data Controller, who processes the data on behalf of the Data Controller.

- "**Data Subject**" means the person to which data refers. Data Subjects include customers and web users, individuals on contact/e-mailing lists or marketing databases, team members, contractors and suppliers.

- "**EEA**" means the European Economic Area as constituted by the EU countries Austria, Belgium, Bulgaria, Cyprus, Czech Republic, Denmark, Estonia, France. Finland, Germany, Greece, Hungary, Ireland, Italy, Latvia, Lithuania, Luxembourg, Malta, The Netherlands, Poland, Portugal, Romania, Slovak Republic, Slovenia, Spain, Sweden, United Kingdom and the European Free Trade Association countries Iceland, Lichtenstein and Norway. Switzerland, a Free Trade European Association country, is neither a Member of the EU nor a member of the European Economic Area. Therefore, Switzerland and the U.S. signed a separate agreement upon identical Safe Harbor Principles that follows the known Safe Harbor Principles. Terex follows the latter as well as the former.

- "**Personal Data**" means any data relating to an identified or identifiable person; an identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. Personal Data does not include information that is anonymous.

- "**Processing**" includes obtaining, recording or holding the data or carrying out any operation or set of operations on the data, including:

  - Organization, adaptation, or alteration;

  - Disclosure by transmission, dissemination, or otherwise; and

  - Alignment, combination, blocking, erasure, or destruction.

- "**Sensitive Data**" means Personal Data that reveals race, ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or that concerns health matters or sexual orientation.