Deere Group Binding Corporate Rules

Last Revised: 07 May 2024

Deere & Company, and its controlled affiliates and subsidiaries (collectively, John Deere), strive to comply with applicable laws, including data protection laws, in the countries in which John Deere operates. Certain John Deere group companies have adopted these Binding Corporate Rules to ensure an adequate level of protection for Personal Data and Special Categories of Personal Data that originate in the EEA and are subject to the GDPR or implementing Member State legislation, as set out below, in order to allow for the transfer of Personal Data from the EEA to Third Countries in accordance with the data protection rules governing international data transfers.

1. Definitions

For the purpose of these Binding Corporate Rules, the following definitions apply:

Binding Corporate Rules (BCRs) are Personal Data protection policies which are adhered to by a Controller or Processor established on the territory of a Member State for transfers or a set of transfers of Personal Data to a Controller or Processor in one or more Third Countries within a group of undertakings, or group of enterprises engaged in a joint economic activity; In the following, references to BCRs shall mean BCRs established within John Deere;

Bound Group Member means Deere & Company, and all affiliates and other entities that are directly or indirectly controlled by Deere & Company, which have committed to upholding these BCRs by signing an intra-group agreement;

Competent Supervisory Authority means Supervisory Authority competent for the Data Exporter;

Controller means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data; where the purposes and means of such processing are determined by EEA or Member State law, the Controller or the specific criteria for its nomination may be provided for by EEA or Member State law;

Data Exporter means a Bound Group Member in the EEA that transfers Personal Data to another Bound Group Member outside the EEA;

Data Importer means a Bound Group Member that receives from the Data Exporter Personal Data for further Processing in accordance with the terms of these BCRs;

EEA means the European Economic Area, currently comprising the EU Member States as well as Iceland, Liechtenstein and Norway;

Employees means permanent and temporary Employees as well as leasing Employees and contingents as well as retirees and former Employees;

General Data Protection Regulation (GDPR) means the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data;

Member State(s) means the member states which form the EEA;

Personal Data means any information relating to an identified or identifiable natural person ('Data Subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;

Personal Data Breach means breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, Personal Data transmitted, stored or otherwise processed;

Processor means a natural or legal person, public authority, agency or other body which processes Personal Data on behalf of the Controller;

Processing means any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction;

Recipient means a natural or legal person, public authority, agency or another body, to which the Personal Data are disclosed, whether a Third Party or not;

Special Categories of Personal Data means Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, as well as genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation;

Supervisory Authorities means the public authorities established by the EEA or a Member State that are responsible for monitoring the application of the GDPR, in order to protect the fundamental rights and freedoms of natural persons in relation to Processing and to facilitate the free flow of Personal Data within the EEA;

Third Country means a country located outside the EEA;

Third Party means a natural or legal person, public authority, agency or body other than the Data Subject, Controller, Processor and persons who, under the direct authority of the Controller or Processor, are authorised to process Personal Data.

Anything not defined in these BCRs shall have the meaning of the General Data Protection Regulation (GDPR).

2. Scope of these BCRs

These BCRs are intended to ensure an adequate level of protection for Personal Data (including Special Categories of Personal Data) that are transferred to Third Countries. They apply to Personal Data (including Special Categories of Personal Data) that originate in the EEA or that have otherwise become or are subject to the GDPR or implementing Member State legislation and which are transferred from a Data Exporter to a Data Importer outside the EEA (namely to Argentina, Australia, Brazil, Chile, China, Georgia, India, Japan, Malaysia, Mexico, Singapore, South Africa, Taiwan R.O.C., Thailand, Turkey, Ukraine, and the United States) including when onward transferred to other Bound Group Members outside the EEA.

Such Personal Data relate to Employees, dependents and job applicants (i.e., 'Employment-related' Personal Data); customers/users, prospects, borrowers, lessees and guarantors; dealers, suppliers, business partners, and their respective Employees; shareholders; visitors (i.e., 'Business-related' Personal Data); and other Data Subjects.

Bound Group Members Process Employment-related Personal Data in relation to: HR management (such as, succession planning, performance analysis, payroll and benefits management, disciplinary matters, recognition programs, attendance, coaching, terminations); recruitment/job application management; health and safety (such as to manage at-work health and safety incidents, maintain emergency/exposure programs, travel security); manage operations (such as Employment-related reporting, scheduling, global assets management, staffing, project management, audits, communications); and other Employment-related purposes.

Bound Group Members Process Business-related Personal Data in relation to: provide and deliver products and services (including related services such as maintenance and customer/user support, financing, leasing, operation of related online/account services); credit assessments; marketing activities (such as management of marketing communications, contests, loyalty programs, events); business communications; internal product/service evaluations and improvement activities; manage business operations (such as vendor/supplier/dealer/distributor management, service announcement, business maintenance activities).

Additionally, Bound Group Members Process both Employment and Business-related Personal Data in relation to: physical and network security, communications and IT (such as to manage access to/monitoring of facilities and company assets; protect intellectual property; administer its IT environment, systems and applications; prevent fraud and assert or defend against legal claims, security incident management); compliance with statutory requirements, laws and internal policies and procedures; acquisition, merger, demergers, and divestiture planning and process.

Bound Group Members Process the following Personal data categories which are Employment-related:

- Employee experience and qualifications;
- Documentation required under immigration/right to work laws;

- Job position;
- Work-place related information (such as emails, organizational and attendance data, systems usage information);
- Employee performance appraisals/career development;
- Travel data;
- Employee payroll and benefits data;
- To the extent strictly necessary, Special Categories of Personal Data related to employment.

Bound Group Members Process the following Personal data categories, which are Business-related:

- Transaction and financial account information;
- Preference and business relationship information.

Bound Group Members Process the following Personal data categories, which are both Employment and Business-related:

- Personal details and contact information;
- Compliance-related information;
- Computer, device, online service, social media and internet information;
- Other Personal Data collected in the course of regular business and employment organization.

For the sake of clarity, these BCRs also cover transfers of Personal Data covered by these BCRs to Data Importers who act as Processors for the Data Exporter.

These BCRs do not apply to Personal Data or Special Categories of Personal Data that do not originate in the EEA and are not otherwise subject to the GDPR or implementing Member State legislation. For example, if a US-based Bound Group Member transfers Personal Data originating in the US to an Australian-based Bound Group Member, such transfer and associated Processing is not subject to these BCRs. As another example, the Processing of Personal Data or Special Categories of Personal Data of a borrower resident in the US by a non-EEA based Bound Group Member related to a transaction where that resident seeks a loan from a non-EEA based Bound Group Member is not subject to these BCRs.

3. Binding Nature of these BCRs

These BCRs are legally binding on every Bound Group Member by virtue of an intra-group agreement. All Bound Group Members shall implement and comply with these BCRs. The executive management of each Bound Group Member is responsible for the implementation of, and compliance with, these BCRs by the respective Bound Group Member.

Every Bound Group Member shall strive to ensure that its Employees comply with the requirements set forth in these BCRs. Bound Group Members shall inform their

Employees that failure to comply with these BCRs may result in disciplinary action or employment law measures (for instance, formal warning or dismissal) being taken against the Employees in accordance with applicable employment, labor and works council laws, company rules and employment contracts.

4. Principles relating to the Processing of Personal Data

Bound Group Members commit to apply the following principles to the Personal Data Processed under these BCRs.

4.1. Lawfulness, fairness and transparency

Bound Group Members shall ensure that Personal Data are Processed lawfully, fairly and in a transparent manner in relation to the Data Subject

4.1.1. Lawfulness and fairness

Bound Group Members shall ensure that the Personal Data are Processed fairly and lawfully and in particular on the basis of at least one of the following legal grounds:

- The Data Subject has unambiguously given his/her consent;
- The Processing is necessary for the performance of a contract to which the Data Subject is party or in order to take steps at the request of the Data Subject prior to entering into a contract;
- The Processing is necessary for compliance with a legal obligation to which the Controller is subject;
- The Processing is necessary in order to protect the vital interests of the Data Subject;
- The Processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller or in a Third Party to whom Personal Data are disclosed;
- The Processing is necessary for the purposes of the legitimate interests pursued by the Controller or by the Third Party or Parties to whom Personal Data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject;
- The Processing is permitted under directly applicable EEA law or the national law of the respective Data Exporter which originally transferred the Personal Data to a Data Importer outside the EEA.

Bound Group Members will Process Personal Data relating to criminal convictions and offences or related security measures based on the above legal grounds only under the control of official authority or when authorised by EEA or Member State law providing for appropriate safeguards for the rights and freedoms of Data Subjects.

Additionally, Bound Group Members shall ensure that Special Categories of Personal Data are only Processed on the basis of at least one of the following grounds:

- The Data Subject has given explicit consent to the Processing of those Personal Data for one or more specified purposes, except where EEA or Member State law provide that the respective Processing is prohibited;
- The Processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the Controller or of the Data Subject in the field of employment and social security and social protection law in so far as it is authorised by EEA or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the Data Subject;
- The Processing is necessary to protect the vital interests of the Data Subject or of another natural person where the Data Subject is physically or legally incapable of giving consent;
- The Processing relates to Personal Data which are manifestly made public by the Data Subject;
- The Processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
- The Processing is necessary for reasons of substantial public interest, on the basis of EEA or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the Data Subject;
- The Processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of EEA or Member State law or pursuant to contract with a health professional and when those data are Processed by or under the responsibility of a professional subject to the obligations of professional secrecy under EEA or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under EEA or Member State law or rules established by national competent bodies.

4.1.2. Transparency

Bound Group Members shall further ensure to provide information in a transparent manner in relation to the Data Subject including:

- The identity and the contact details of the Controller;
- The contact details of the Data Protection Officer, where applicable;
- The purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

- The categories of Personal Data concerned;
- The legal basis for the processing (if the Processing is based on the legitimate interest pursued by the Controller or by a third Party, these interests need to be mentioned);
- The Recipients or categories of Recipients of the Personal Data, if any;
- Where applicable, the fact that the Controller intends to transfer Personal Data to a Third Country or international organisation outside the EEA and whether there is an adequacy decision by the Commission in place or if the transfer is based on appropriate safeguards. Such appropriate safeguards include binding corporate rules of the Recipient, standard data protection clauses adopted by the European Commission or adopted by a Supervisory Authority and approved by the European Commission, or an approved code of conduct or certification mechanism together with binding and enforceable commitments of the Recipient. The Controller shall reference the appropriate or suitable safeguards and the means by which a copy of them can be obtained or where they have been made available.

In addition to this information, the Controller shall, at the time when Personal Data are obtained, provide the Data Subject with the following further information necessary to ensure fair and transparent Processing:

- The period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- The existence of the right to request from the Controller access to and rectification or erasure of Personal Data or restriction of Processing concerning the Data Subject or to object to Processing as well as the right to data portability;
- Where the Processing of Personal Data and of Special Categories of Personal Data is based on consent, the existence of the right to withdraw consent at any time, without affecting the lawfulness of Processing based on consent before its withdrawal;
- The right to lodge a complaint with a Supervisory Authority;
- Whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Data Subject is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
- The existence of automated decision-making, including profiling and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such Processing for the Data Subject.

Where the Controller intends to further Process the Personal Data for a purpose other than that for which the Personal Data were initially collected, the Controller shall provide the Data Subject prior to that further Processing with information on that other purpose and with any relevant further information.

Where the Personal Data have not been obtained from the Data Subject directly, in addition to the above, the Controller shall provide the Data Subject with information from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources. In this case, the Controller shall inform the Data Subject within a reasonable time after obtaining the Personal Data, but at least within one month, having regard to the specific circumstances in which the Personal Data are Processed; or, if the Personal Data are used for communication with the Data Subject, at the latest at the time of the first communication to the Data Subject, or, if a disclosure to another Recipient is envisaged, at the latest, when the Personal Data are first disclosed.

The obligation to inform the Data Subject pursuant to this Section 4.1.2 does not apply where and insofar as the Data Subject already has the information or, in case the Personal Data has not been obtained from the Data Subject directly if:

- The provision of such information proves impossible or would involve a disproportionate effort;
- Obtaining or disclosure is expressly laid down by EEA or Member State law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests;
- Where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by EEA or Member State law, including a statutory obligation of secrecy.

4.2. Purpose limitation

Bound Group Members shall not further process Personal Data in a manner that is incompatible with the purposes it was collected for.

4.3. Data Minimization, Accuracy, Storage Limitation

Personal Data shall:

- Be accurate and, where necessary, kept up-to-date;
- Be adequate, relevant and not excessive in relation to the purposes for which they are transferred and further Processed;
- Not be Processed longer than necessary for the purposes for which they were initially obtained. Personal Data which are no longer necessary for the purposes for which they were initially Processed, shall be deleted or made anonymous, unless there is a legal ground for further Processing. Retention periods shall be specified in relevant policies.

4.4. Integrity and Confidentiality

Bound Group Members shall keep the Personal Data confidential and shall 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 all other unlawful forms of Processing by taking appropriate organizational and technical measures. For this purpose, the Bound Group Members have developed and implemented a number of security policies and practices, which include access control measures, measures to secure the integrity, availability and transmission of Personal Data and segregation controls.

Bound Group Members shall also ensure that their Employees keep the Personal Data confidential and secure, for instance, by means of confidentiality certifications and/or relevant contractual obligations. Employees and Processors shall only be authorized to Process Personal Data, which is subject to these BCRs, to the extent that this is necessary in order for them to perform their job and in accordance with these BCRs.

These measures are reviewed regularly and shall aim to provide a level of security appropriate to the risks represented by the Processing and the nature of the data to be protected. Where Special Categories of Personal Data are Processed, enhanced security measures shall apply.

4.5. Data Protection by Design and Data Privacy by Default

Bound Group Members shall:

- Take into account the state of the art , the cost of implementation and the nature, scope, context and purpose of Processing as well as the risk of varying likelihood and severity for rights and freedoms of natural persons posed by the Processing, the Controller shall, both at the time of the determination of the means for Processing and at the time of the Processing itself, implement appropriate technical and organization measures, such as pseudonymisation and data minimisation, which are designed to implement data protection principles, in an effective manner and to integrate the necessary safeguards into the Processing to meet the requirements of the GDPR and to protect the rights of Data Subjects;
- Implement appropriate technical and organisational measures for ensuring that, by default, only Personal Data which are necessary for each specific purpose of the Processing are Processed. That obligation applies to the amount of Personal Data collected, the extent of their Processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default Personal Data are not made accessible without the individual’s intervention to an indefinite number of natural persons.

4.6. Accountability

Bound Group Members shall be responsible for, and be able to demonstrate compliance with the above listed principles. In particular, they shall

- Maintain John Deere’s record of Processing activities that is accessible via internal online tools and make it available to the Competent Supervisory Authority upon request.

  Where Bound Group Members act as a Controller, the record shall contain the following information:

  - the name and contact details of the Controller and, where applicable, the joint Controller, the Controller's representative and the data protection officer;
  - the purposes of the Processing;
  - a description of the categories of Data Subjects and of the categories of Personal Data;
  - the categories of recipients to whom the Personal Data have been or will be disclosed including recipients in Third Countries or international organizations;
  - where applicable, transfers of Personal Data to a Third Country or an international organisation, including the identification of that Third Country or international organization and the documentation of suitable safeguards if transfer does not rely on appropriate safeguards (including BCRs) or derogations available under the GDPR;
  - where possible, the envisaged time limits for erasure of the different categories of Personal Data;
  - where possible, a general description of the technical and organizational security measures; and

  Where Bound Group Members act as a Processor, the record shall contain the following information:

  - the name and contact details of the Processor(s) and of each Controller on behalf of which the Processor is acting, and, where applicable, of the Controller's or the Processor's representative, and the data protection officer;
  - the categories of Processing carried out on behalf of each Controller;
  - where applicable, transfers of Personal Data to a Third Country or an international organisation, including the identification of that Third Country or international organization and the documentation of suitable safeguards if transfer does not rely on appropriate safeguards (including BCRs) or derogations available under the GDPR;
  - where possible, a general description of the technical and organizational security measures.

- Carry out data protection impact assessments prior to the Processing, which takes into account the nature, scope, context and purposes of the Processing, whenever the envisaged Processing, in particular using new technologies, is likely to result in a high risk to the rights and freedoms of natural persons;

- Where necessary, consult with the Supervisory Authority prior to the Processing where a data protection impact assessment indicates that the Processing would result in a high risk in the absence of measures to mitigate the risk;
- Cooperate, on request, with the Supervisory Authority in the performance of its tasks.

5. Privacy Governance Structure

Bound Group Members implement data protection processes and procedures, including the setting up of a global privacy network ("Privacy Network") which consists of senior leadership and councils within Deere providing privacy governance direction, key personnel from the law department and business, as well as key data protection and privacy functions ("Global Privacy Team"), designed to support its compliance with these BCRs and applicable data protection and privacy laws.

Further to the foregoing, John Deere's Senior Vice President and Chief Legal Officer and Worldwide Public Affairs, and Vice President, Digital Risk Officer and Assistant General Counsel provide internal governance leadership.

Also, further to the foregoing, the Director & Chief Privacy Officer ("Chief Privacy Officer") reports to the Vice President, Digital Risk Officer and Assistant General Counsel. The Chief Privacy Officer bears overall responsibility in Deere's Privacy Network and Global Privacy Team and is in charge of overseeing John Deere's compliance with applicable data protection and privacy laws and regulations, its policies related to the Processing of Personal Data and its commitments pursuant to these BCRs, and supervises the handling of local complaints from Data Subjects, and Personal Data Breach notifications. The Chief Privacy Officer makes regular reports directly to the Corporate Governance Committee of Deere & Company's Board of Directors and has the opportunity to communicate independently and directly with the Committee or Board, as needed.

Also, further to the foregoing, the Chief Privacy Officer is supported by a global network of full-time and part-time individuals. The Global Privacy Team consists of individuals who are responsible for monitoring compliance with applicable data protection laws and regulations, Bound Group Member's policies related to the Processing of Personal Data, and John Deere's commitments pursuant to these BCRs. The Global Privacy Team also consists of individuals in the Bound Group Members who are responsible for business functions that are Processing Personal Data.

6. Training

Bound Group Members maintain mandatory awareness and training programs for Employees that Process Personal Data and those Employees who are involved in the development of tools used in the Processing of Personal Data within the scope of these BCRs to make sure Employees are aware of the obligations thereunder and enable Employees to comply with these BCRs.

Depending on the department or job function handling Personal Data, an Employee may need varying levels of understanding of Personal Data-related compliance. Data protection and privacy-related training may be incorporated into other existing training programs or offered on a stand-alone basis. The Global Privacy Team provides general online training courses and awareness campaigns regarding core data protection, security and privacy requirements, including key data protection laws and regulations and Deere's commitments pursuant to the BCRs (including information on the consequences of breaching these BCRs) on a consistent basis (and in any case at least once a year).

In addition, Bound Group Members require Employees who on a permanent or regular basis Process Personal Data Subject to the BCRs, or who are involved in the development of tools used in the Processing of Personal Data (including for human resources, supply management, information technology, John Deere Financial, and marketing departments, to undertake more in-depth, focused training on the BCRs and data protection laws on a regular basis (and in any case at least every two years). In addition to the general training requirements, these Employees should be able to address and, if necessary, escalate Data Subject Right Requests or other complaints/issues involving Personal Data subject to these BCRs to the Global Privacy Team; and be able to manage/escalate Government Access Requests (as described in Section 13).

It is expected that individuals responsible for advising others on Deere's data protection-related policies, or Deere's BCRs, will remain current on applicable data protection law and must attend, on an annual basis, formal training programs, classes, and seminars.

Training courses and awareness campaigns are outlined in yearly training and awareness plans and will be repeated as deemed necessary. Aiming to consistently refresh and enhance knowledge of Bound Group Members Employees, the campaigns will be evaluated by the Global Privacy Team as deemed necessary.

7. Audits and Monitoring

Compliance with these BCRs is subject to review and Bound Group Members agree to be audited on a regular basis in connection with their implementation of, and compliance with, these BCRs as follows. The audits cover all elements of these BCRs. Primary responsibility for the performance of audits lies with the John Deere internal audit department, but, if needed, Bound Group Members may entrust appropriate, external third parties with this task. The results of such audits will be communicated to the Vice President, Digital Risk Officer and Assistant General Counsel, the Chief Privacy Officer and Competent Supervisory Authorities upon request. Significant findings are reported to the Audit Review Committee of Deere & Company's Board of Directors and John Deere GmbH & Co KG Board of Directors.

The audits will be carried out at least annually and may focus on selected parts of Bound Group Members' compliance with these BCRs, determined on the basis of the risk(s) posed by the processing activities covered by the BCRs to the rights and

freedoms of Data Subjects. The Vice President, Digital Risk Officer and Assistant General Counsel or Chief Privacy Officer may request additional audits or reviews outside the regular audit roadmap. In addition, the Global Privacy Team may also conduct audits in the form of a self-assessment by the Bound Group Members. The Chief Privacy Officer receives the results of the self-assessment and informs the Vice President, Digital Risk Officer and Assistant General Counsel and the John Deere internal audit department of significant findings.

If such audits determine that corrective action is needed, corrective actions will be implemented in the course of the audit process. Further details of the audits are outlined in an audit program.

8. Data Subject Rights - Access, Rectification, Erasure, Restriction, Objection, Portability and Automated Decision-Making

Bound Group Members shall use the implemented processes and procedures enabling every Data Subject whose Personal Data are subject to these BCRs to exercise their right, except where such rights may be restricted pursuant to directly applicable EEA law or the national law of the respective Data Exporter which originally transferred the Personal Data to a Data Importer outside the EEA:

- In addition to receiving **access** to information about Personal Data Processed (as outlined in Section 4.1.2), to obtain without constraint at reasonable intervals and without excessive delay or expense a copy of the same;
- To obtain **rectification** of inaccurate/complete the incomplete Personal Data;
- To obtain **erasure** of Personal Data if:
    - it is no longer necessary for the purposes for which it has been transferred;
    - Data Subject has withdrawn their consent and no other legal ground for Processing exists;
    - Data Subject has objected and no overriding legitimate grounds for the Processing exist;
    - the Processing is unlawful, or erasure is required to comply with a legal obligation; or
    - children's Personal Data have been collected in relation to the offer of information society services.

  The right will not apply if Processing is necessary for:
    - exercising the right of freedom of expression and information;
    - compliance with EEA/Member State law;
    - public interest in the area of public health;
    - archiving purposes in the public interest, scientific or historical research purposes or statistical purposes;

- the establishment, exercise or defense of legal claims.

- To obtain **restriction** of Processing if:
  - Data Subject contests - in good faith - the accuracy of Personal Data;
  - The Processing is unlawful and Data Subject opposes the erasure;
  - Personal Data is no longer necessary for Processing, but Data Subject requires it for the establishment, exercise or defense of legal claims;
  - Data Subject have objected to the Processing and Controller needs to verify the request.

  Bound Group Members may store restricted Personal Data/Process it for the establishment, exercise or defense of legal claims/protection of the rights of another person/important public interest.

- Additionally, to have the Controller communicate a rectification, erasure or restriction to recipients of Personal Data, unless this proves impossible or involves disproportionate effort and receive information about those recipients upon request;

- To **object**, on grounds relating to his or her particular situation, at any time to Processing of Personal Data (including profiling) concerning him or her which is based on the legitimate interests pursued by the Controller or by a third party. If Controller demonstrates compelling legitimate grounds, or Personal Data is needed for the establishment, exercise or defence of its legal claims, it may continue Processing. Data Subjects may at any time object to direct marketing, including related profiling;

- The Data Subject shall have the right **not to be subject to** a decision based solely on **automated Processing**, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her unless and in exceptional cases, the Processing is necessary for entering into, or performance of, a contract between the Data Subject and a data Controller or is authorised by EEA or Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests or is based on the Data Subject's explicit consent;

- The Data Subject shall have the right (so-called **data portability**) to receive the Personal Data concerning him or her, which he or she has provided to a Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Controller without hindrance from the Controller to which the Personal Data have been provided, where the Processing of Personal Data and Special Categories of Personal Data is based on the Data Subject's consent or on a contract; and the Processing is carried out by automated means.

Data Subjects can exercise their Data Subject Rights as laid out in Section 10.

9. Onward transfers

With respect to Personal Data that is subject to these BCRs, every Data Importer commits to apply the following additional measures including requirements set forth by Section 13 when sharing Personal Data with a Controller or a Processor.

9.1 Sharing Personal Data with a Controller

Every Data Importer shall only transfer Personal Data to another Controller if there is a legal ground for Processing in accordance with Section 4.1.1 and in accordance with the other Processing Principles listed in Section 4 of these BCRs. Where necessary and reasonably possible, the Data Importer shall obtain Contractual Assurances from the Controller to that effect. In case national law prevents the Bound Group member from complying with these BCRs Section 13 applies.

9.2. Joint Controlling

Every Data Exporter and Data Importer who jointly determine the purposes and means of Processing shall be bound by a written agreement that duly reflects the respective roles and relationships of the Joint Controllers vis-à-vis the Data Subjects. The essence of the arrangement shall be made available to the Data Subject. In particular, they shall in a transparent manner determine their respective responsibilities for compliance with the obligations under the GDPR, especially the exercising of the rights of the Data Subject and the duty to provide transparent information according to Section 4.1.2 of these BCRs.

9.3. Entrusting the Processing of Personal Data to a Processor

Every Data Importer that transfers to a Processor Personal Data covered by these BCRs shall only choose a Processor providing sufficient guarantees to implement appropriate technical and organizational measures in such a manner that the Processing will meet the requirements of the GDPR and these BCRs and ensures the protection of the Data Subject rights. For the avoidance of doubt, this clause shall apply to both external Processors which are not Bound Group Members as well as Bound Group Members that act as Processors for other Bound Group Members.

The Processor shall be bound by a written contract or other legal act under EEA or Member State law, that is binding on the Processor and that sets out the subject-matter and duration of the Processing, the nature and purpose of the Processing, the type of Personal Data and categories of Data Subjects and the obligations and rights of the Controller. The contract or other legal act shall stipulate in particular that the Processor:

- Processes the Personal Data only on documented instructions from the Controller, including with regard to transfers of Personal Data to a Third Country or an international organisation outside the EEA, unless required to do so by EEA or Member State law to which the Processor is subject; in such a case, the Processor shall inform the Controller of that legal requirement before Processing, unless that law prohibits such information on important grounds of public interest;

- Ensures that persons authorised to process the Personal Data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality;
- Takes appropriate technical and organizational measures to ensure a level of security appropriate to the risk;
- Respects the conditions referred to below for engaging another processor;
- Taking into account the nature of the Processing, assists the Controller by appropriate technical and organisational measures, insofar as this is possible, for the fulfilment of the Controller's obligation to respond to requests for exercising the Data Subject's Rights;
- Assists the Controller in ensuring compliance with the security of processing, notification requirements both to the Supervisory Authority and Data Subjects in case of a Personal Data Breach, data protection impact assessments and prior consultations of the Supervisory Authority, taking into account the nature of Processing and the information available to the Processor;
- At the choice of the Controller, deletes or returns all the Personal Data to the Controller after the end of the provision of services relating to Processing, and deletes existing copies unless EEA or Member State law requires storage of the Personal Data;
- Makes available to the Controller all information necessary to demonstrate compliance with these obligations and contribute to audits, including inspections, conducted by the Controller or another auditor mandated by the Controller. The Processor shall immediately inform the Controller if, in its option, an instruction infringes the GDPR or other EEA or Member State data protection provisions.

The Processor shall not engage another Processor without prior specific or general written authorisation of the Controller. In the case of general written authorisation, the Processor shall inform the Controller of any intended changes concerning the addition or replacement of other Processors, thereby giving the Controller the opportunity to object to such changes.

Where a Processor engages another Processor for carrying out specific Processing activities on behalf of the Controller, the same data protection obligations as set out in the contract or other legal act entered between the Controller and the Processor, which content is described above, shall be imposed on that other Processor by way of a contract or other legal act under EEA or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the Processing will meet the requirements of the GDPR. Where that other Processor fails to fulfil its data protection obligations, the initial Processor shall remain fully liable to the Controller for the performance of that other Processor's obligations.

9.4 International Transfers

If a Data Importer transfers Personal Data covered by these BCRs to a Controller or Processor which is not a Bound Group Member and which is located in a Third Country, it shall only transfer the Personal Data to a Recipient that is located in a country, territory, or sector for which the European Commission has decided that this particular Third Country, territory or specified sector ensures an adequate level of protection; or in the absence of such adequacy decision, the transfer is based on appropriate safeguards such as

- Binding corporate rules of the Recipient;
- Standard contractual clauses adopted by the European Commission or adopted by a Supervisory Authority and approved by the European Commission; or
- An approved code of conduct or certification mechanism, together with binding and enforceable commitments of the Recipient.

Data Importer shall assess whether Recipient located in a Third Country is subject to any legal requirement in that Third Country, which is likely to have a substantial adverse effect on the guarantees provided by the above safeguards. Where necessary, Data Importer shall identify and implement appropriate supplementary measures, to ensure its findings are addressed appropriately, in order to maintain sufficient level of Personal Data protection.

In exceptional cases (where the transfer cannot be based on an adequacy decision or appropriate safeguards), the transfer may take place on the basis of a statutory derogation, including:

- Explicit consent by the Data Subject to the transfer;
- The transfer is necessary for the performance of a contract between the Data Subject and the Controller or the implementation of pre-contractual measures taken at the Data Subject's request;
- The transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Data Subject between the Controller and another natural or legal person;
- The transfer is necessary for important reasons of public interest, as recognized in EEA or Member State law (to which the Controller is subject);
- The transfer is necessary for the establishment, exercise or defence of legal claims;
- The transfer is necessary in order to protect the vital interests of the Data Subject or of other persons, where the Data Subject is physically or legally incapable of giving consent.

In limited circumstances and only if none of the above is applicable, the transfer may take place, provided it is not repetitive, only concerns a limited number of Data Subjects and is necessary for the purposes of compelling legitimate interests pursued by the Controller which are not overridden by the interests or rights and freedoms of the Data Subject, and the Controller has assessed all the circumstances surrounding the data transfer and provided suitable safeguards to protect the Personal Data. The Competent Supervisory Authority shall be informed of such transfer.

Where required, the Data Exporter shall obtain authorization from a Competent Supervisory Authority.

10. Data Subject Rights and Complaint Mechanism

Data Subjects can at all times exercise their Data Subject Rights and file a complaint regarding a Bound Group Member's compliance with these BCRs. For Data Subject Right Requests a web form is provided under www.deere.com/privacy. Additionally, Data Subjects can use the complaint form available under www.deere.com/privacy to file a complaint. Data Subjects can also directly contact John Deere as laid out in Section 20.

In case of a Data Subject Right Request or a complaint submitted through the web form or the complaint form, the Data Subject will receive an automatic confirmation of receipt. Global Privacy Team will answer every Data Subject Right Request or complaint without undue delay and in any event within one month of receipt of the request or inform Data Subject why their Data Subject Right Request or complaint will not be satisfied, and of their right to lodge a complaint with a Competent Supervisory Authority and to seek a judicial remedy. In exceptional cases, that period may be extended by two further months where necessary, taking into account the complexity and number of the requests/complaints. The Data Subject shall be informed of any such extension within one month of receipt of the request, together with the reasons for the delay. Where Data Subject Right Requests are manifestly unfounded or excessive, Controller may charge a reasonable fee, or refuse to act on the request. Where a complaint is validated, the Controller will implement appropriate remediation towards the complainant and adjust its BCRs compliance program as necessary. The Bound Group Members will work with technical experts, legal advisors and translators, to resolve the complaint.

The Data Subjects can lodge a claim before a Competent Supervisory Authority or a court as described in Section 12. Whilst it is not required, Data Subjects are encouraged to first report their complaint through the Complaint Mechanism. This is to enable John Deere to provide an efficient and prompt response to the issue.

11. Personal Data Breaches

A Bound Group Member acting as a Controller which suffered a Personal Data Breach must report it to John Deere GmbH & Co KG and the Chief Privacy Officer without undue delay. When affected Bound Group Member acting as a Processor becomes aware of a Personal Data Breach, it must also notify the Bound Group Member acting as a Controller of the affected Personal Data.

Unless the Personal Data Breach is unlikely to result in a risk to the rights and freedoms of Data Subjects, the Bound Group Member acting as a Controller, must without undue delay, and, where feasible, not later than 72 hours after having become aware of the Personal Data Breach, report it to the Competent Supervisory Authority. If Personal Data Breach is likely to result in a high risk to the rights and

freedoms of Data Subjects, the Bound Group Member acting as a Controller must notify them without undue delay, unless:

- it implemented appropriate technical and organisational measures (e.g., encryption) to affected Personal Data;
- it implemented subsequent measures to ensure that such high risk to rights and freedoms of Data Subjects is no longer likely to materialize;
- it would involve disproportionate effort. In such a case, it should issue a public communication or similar measure to effectively inform Data Subjects.

The Global Privacy Team will document any Personal Data Breach. The documentation must include the facts relating to the Personal Data Breach, its effects and the remedial action taken and shall be made available to the Competent Supervisory Authorities on request.

12. Liability

John Deere GmbH & Co KG, John Deere Str. 70, 68163 Mannheim, Germany, accepts responsibility for any breaches of these BCRs by any Bound Group Member outside of the EEA and undertakes (i) to take the necessary action to remedy a breach committed by Bound Group Members outside of the EEA; and (ii) to pay appropriate compensation to any Data Subjects whose Personal Data are subject to these BCRs for any damages resulting from the breach of these BCRs by Bound Group Members outside the EEA in the same way and with the same scope from which the Data Subjects would benefit under either German law or the law of the EEA country of the respective Data Exporter in the EEA.

No provision of these BCRs shall allow any Data Subject to benefit from compensation for any damages beyond this, in particular any double recovery from or punitive damages for or compensation for damages relating to third parties for any breach of these BCRs or the intra-group agreement shall be excluded. Nothing in this clause excludes or limits liability for death or personal injury caused by either John Deere GmbH & Co KG or a Bound Group Member, for fraud or other liability caused by any intentional or gross negligence by John Deere GmbH & Co KG or a Bound Group Member.

13. Transparency when Compliance with BCRs is prevented by National Law, Practices and Government Access Requests

Bound Group Members commit to the below with regards to assessment and steps to be taken in response to Third Country national laws and practices affecting their BCRs compliance. They further commit to respond to a legally binding request by a public authority under Third Country national laws (“Requesting Authority”) for disclosure/access to Personal Data subject to the BCRs under Third Country national laws ("Request”), or a direct access by Third Country Requesting Authority to Personal Data (“Direct Access”), without prior interaction with Bound Group Members

(e.g., during the transit from the country of the Data Exporter and the country of the Data Importer) as follows.

13.1 Local laws and practices affecting compliance with BCRs

Bound Group Members will use BCRs as a tool for transfers only where they have assessed that the law and practices in the Third Country of destination applicable to the Processing of the Personal Data by the Data Importer, including any requirements to disclose such Personal Data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under these BCRs.

Bound Group Members will base such assessment on the understanding laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to safeguard national/public security, defence, and other important objectives of general public interest, are not in contradiction with the BCRs.

In assessing the laws and practices of the Third Country which may affect the respect of the commitments contained in the BCRs, the Bound Group Members will take due account, in particular, of the following elements:

- the specific circumstances of the transfers or set of transfers, and of any envisaged onward transfers within the same Third Country or to another Third Country, including (i) purposes for which the Personal Data are transferred and Processed; (ii) types of entities involved in the Processing (the data importer/recipients of any onward transfers); (iii) economic sector in which the transfer/set of transfers occur; (iv) categories and format of the transferred Personal Data; (v) location of the processing (including storage); and (vi) transmission channels used;
- laws and practices of the Third Country of destination relevant in light of the circumstances of the transfer, including those requiring disclosure of Personal Data to Requesting Authority/authorising their access and those providing for Direct Access, as well as the applicable limitations and safeguards; and
- any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under the BCRs, including measures applied during the transmission and to the Processing of the Personal Data in the Third Country of destination.

To the extent safeguards (in addition to those envisaged under the BCRs) should be put in place, John Deere GmbH & Co KG, and the Chief Privacy Officer, supported by Global Privacy Team, will be informed and involved in such assessment. Bound Group Members will appropriately document such assessment, as well as the supplementary measures selected and implemented and make such documentation available to the Competent Supervisory Authorities upon request.

The Data Importer will promptly notify the Data Exporter if, when using BCRs as a tool for transfers, and for the duration of its BCRs membership, it has reasons to believe that it is or has become subject to laws or practices that would prevent it from fulfilling its obligations under the BCRs, including following a change in the laws in

the Third Country or a measure (e.g., Request). It will also provide this information to John Deere GmbH & Co KG.

Upon verification of such notification, the Data Exporter, John Deere GmbH & Co KG, and the Chief Privacy Officer, supported by Global Privacy Team, will promptly identify supplementary measures to be adopted by the Data Exporter/Data Importer, in order to enable them to fulfil their obligations under the BCRs. The same applies if a Data Exporter has reasons to believe that a Data Importer can no longer fulfil its obligations under the BCRs.

Where the Data Exporter, John Deere GmbH & Co KG, and the Chief Privacy Officer, supported by Global Privacy Team, assess that the BCRs – even if accompanied by supplementary measures – cannot be complied with for a transfer/set of transfers, or if instructed by the Competent Supervisory Authority, it will suspend the transfer/set of transfers at stake, as well as all transfers for which the same assessment and reasoning would lead to a similar result, until compliance is again ensured or the transfer is ended.

Following such a suspension, the Data Exporter will end the transfer/set of transfers if the BCRs cannot be complied with and compliance with the BCRs is not restored within one month of the suspension. In such case, Personal Data that have been transferred prior to the suspension, and any copies thereof, should, at the choice of the Data Exporter, be returned to it or destroyed in their entirety.

John Deere GmbH & Co KG, and the Chief Privacy Officer, supported by Global Privacy Team will inform all other Bound Group Members of the assessment carried out and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by them or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

Data Exporters shall monitor, on an ongoing basis, and where appropriate in collaboration with Data Importers, developments in the Third Countries to which they have transferred Personal Data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

13.2 Obligations of Data Importer in case of Government Requests and Direct Access

Without prejudice to paragraph 13.1, the Data Importer will promptly notify the Data Exporter and where possible, the data subject with the help of the Data Exporter, as necessary if it:

- receives a Request, in which case such notification will include information about the Personal Data requested, the Requesting Authority, the legal basis for the Request and the response provided;
- becomes aware of any Direct Access, in which case, such notification will include all information available to the Data Importer.

If prohibited from notifying the Data Exporter/Data Subject, the Data Importer will use its best efforts to obtain a waiver of such prohibition, with a view to communicate as much information as possible and as soon as possible, and will document its best efforts in order to be able to demonstrate them upon request of the Data Exporter.

The Data Importer will provide the Data Exporter, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of Personal Data requested, Requesting Authority(s), whether Requests have been challenged and the outcome of such challenges, etc.). If the Data Importer is or becomes partially/completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly.

The Data Importer will preserve the abovementioned information for as long as the Personal Data are subject to the safeguards provided by the BCRs, and shall make it available to the Competent Supervisory Authority upon request.

The Data Importer will review the legality of the Request, in particular whether it remains within the powers granted to the Requesting Authority, and will challenge the Request if, after careful assessment, it concludes that there are reasonable grounds to consider that the Request is unlawful under the Third Country laws, applicable obligations under international law, and principles of international comity. The Data Importer will, under the same conditions, pursue possibilities of appeal. When challenging a Request, the Data Importer will seek interim measures with a view to suspending the effects of the Request until the competent judicial authority has decided on its merits. It will not disclose the Personal Data requested until required to do so under the applicable procedural rules.

The Data Importer will document its legal assessment and any challenge to the Request and, to the extent permissible under the Third Country laws, make the documentation available to the Data Exporter. It will also make it available to the Competent Supervisory Authority upon request. The Data Importer will provide the minimum amount of information permissible when responding to a Request, based on a reasonable interpretation of the Request.

In any case, the transfers of Personal Data by a Bound Group Member to any public authority shall not be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

14. Non-compliance with BCRs

The Data Importer should promptly inform the Data Exporter if it is unable to comply with the BCRs, for whatever reason, including as outlined in paragraph 13.1.

Where the Data Importer is in breach of the BCRs/unable to comply with them, the Data Exporter should suspend the relevant transfer.

The Data Importer should, at the choice of the Data Exporter, immediately return or delete the Personal Data that has been transferred under the BCRs in its entirety, where:

- the Data Exporter has suspended the transfer, and compliance with this BCRs is not restored within a reasonable time, and in any event within one month of suspension; or
- the Data Importer is in substantial or persistent breach of the BCRs; or
- the Data Importer fails to comply with a binding decision of a competent court or Competent Supervisory Authority regarding its obligations under the BCRs.

The same applies to any copies of such Personal Data. The Data Importer will certify such deletion of the Personal Data to the Data Exporter.

Until such Personal Data is deleted/returned, the Data Importer will continue to ensure compliance with the BCRs with regards to the Personal Data.

In case of local laws applicable to the Data Importer that prohibit the return/deletion of the Personal Data transferred under the BCRs, the Data Importer warrants that it will continue to ensure compliance with the BCRs, and will only Process the Personal Data to the extent and for as long as required under that local law.

The requirements of Section 4 may be set aside to the extent permitted by directly applicable EEA law or the Member State law of the respective Data Exporter which originally transferred the Personal Data to a Data Importer outside the EEA.

15. Relationship between BCRs and National Law

In case local legislation in the EEA applicable to a Bound Group Member's Processing of Personal Data requires a higher level of protection for Personal Data, it will take precedence over these BCRs.

In any event, Personal Data shall be Processed in accordance with the principles relating to Processing of Personal Data set forth by the GDPR and the relevant national law.

16. Mutual Assistance and Cooperation with Supervisory Authorities

Bound Group Members will reasonably cooperate and assist each other to handle requests or complaints from Data Subjects with regards to these BCRs.

Bound Group Members further undertake to cooperate with Competent Supervisory Authorities regarding investigations, audits or inquiries (including where necessary, on-site) regarding compliance with these BCRs, provide them with any requested information regarding Processing operations subject to these BCRs, and abide by decisions of the Competent Supervisory Authorities and take into account their advice with respect to the interpretation and application of these BCRs. Bound Group Members will agree to resolve disputes with Competent Supervisory Authorities related to their supervision of compliance with these BCRs, subject to procedural law and jurisdiction of the courts of the Competent Supervisory Authority's Member State.

17. Third-Party Beneficiary Rights

Data Subjects whose Personal Data are subject to these BCRs have the right to enforce Sections 4, 8, 9, 10, 11, 12, 14, 15, 17, 18, and 19 of these BCRs by virtue of third-party beneficiary rights, subject to the other provisions of these BCRs.

Data Subjects whose Personal Data are subject to these BCRs can seek to enforce compliance with the above-mentioned rules that are published according to Section 16 as well as the GDPR, including in particular but not limited to remedies, liabilities and penalties, and may claim compensation for damages by lodging a complaint before the Competent Supervisory Authorities (in particular in the Member State of Data Subject's habitual residence, place of work or place of the alleged infringement) and before the competent courts in the EEA (i.e., where Controller or Processor has establishment, or where the Data Subject has habitual residence), but not before any other supervisory authority, tribunal or court in any non-EEA jurisdiction. In case of a breach of these BCRs by Bound Group Members outside the EEA, they may also lodge a complaint before the Competent Supervisory Authorities and before the competent courts in the EEA, either of the jurisdiction of the Data Exporter as defined under these BCRs, or of the jurisdiction of John Deere GmbH & Co KG in which case the authorities or courts will have jurisdiction and the Data Subjects will have the rights and remedies against John Deere GmbH & Co KG as if the violation by the Bound Group Member outside the EEA had been committed by John Deere GmbH & Co KG. If a Data Subject brings such a claim, the burden of proof for demonstrating that the Bound Group Member outside the EEA is not responsible for the violation of these BCRs on which the Data Subject's claim is based lies with John Deere GmbH & Co KG. If the latter can prove that the Bound Group Member outside the EEA is not responsible for the act, it may discharge itself from any responsibility. Data subject may be represented in the above matters and related compensation claims by a not-for-profit body, organization or association which has been properly constituted in accordance with the law of a Member State, has statutory objectives which are in the public interest, and is active in the field of the protection of Data Subjects' rights and freedoms.

For the avoidance of doubt, these BCRs shall not affect the rights of Data Subjects under applicable local data protection legislation in the EEA or prejudice or otherwise limit the ability of Data Subjects to enforce their rights in accordance with any applicable local legislation in the EEA.

18. Updates of the Content of these BCRs and List of Bound Members

These BCRs may be updated and amended. John Deere GmbH & Co KG shall inform the Competent Supervisory Authorities by informing the lead Supervisory Authority once a year of any change to these BCRs or to the list of Bound Group Members (including a brief explanation for such changes) and also inform the Data Subjects of such changes in an appropriate manner. Competent Supervisory Authorities should also be notified once a year in instance where no changes have been made.
John Deere GmbH & Co KG shall report all changes to the BCRs or to the list of Bound Group Members to the Bound Group Members.

Where a modification would possibly affect the level of the protection offered by these BCRs or significantly affect these BCRs (i.e. changes to the binding character), it must be promptly communicated to the Bound Group Members and prior to such modifications to the relevant Competent Supervisory Authorities via the lead Supervisory Authority (including a brief explanation for such changes).

The Global Privacy Team shall keep a fully updated list of the Bound Group Members, which is provided as an Appendix to these BCRs, keep track of and record any updates to the BCRs, and provide necessary information to Data Subjects (by publishing the BCRs as explained in Section 19) and upon request to Competent Supervisory Authorities. No transfers of Personal Data under these BCRs will take place until the new member/unless Bound Group Member is effectively bound by these BCRs and can deliver compliance, including by onboarding its Employees into the training and awareness program (as described in Section 6).

19. Publication

These BCRs shall be published and a link shall be made available on the website of every Bound Group Member in the EEA and for Employees on the Intranet.

This public version of the BCRs will always contain at least the following information as it relates to the BCRs:

- scope of the BCRs;
- Bound Group Members' liability;
- data protection principles;
- lawfulness of the Processing;
- security and Personal Data Breach notifications;
- restrictions on onward transfers;
- Data Subjects rights;
- Data Subjects' third-party beneficiary rights and the means to exercise them;
- mechanism for complaints regarding compliance with these BCRs;
- list of definitions/abbreviations used.

Data Subjects may request a copy of these BCRs by contacting John Deere as explained in Section 20.

20. Contact Information

EEA contact:

EEA/UK Group Data Protection Officer
R2DataPrivacyManager2@JohnDeere.com
John Deere GmbH & Co KG
John Deere Str. 70 68163

Mannheim
Germany

Non- EEA contact:

Privacy Manager
PrivacyManager@JohnDeere.com
Center for Global Business Conduct
Deere & Company
One John Deere Place
Moline, Illinois 61265-8089
U.S.A.

Effective date: 07 May 2018

Appendix

List of Bound Group Members – status 07 May 2024

Country	Entity Name	Entity Address	Company Registration
Argentina	John Deere Credit Compañia Financiera, Sociedad Anonima	Juan Orsetti 481, Granadero Baigorria, Provincia De Santa Fe, Argentina, S2152CFA	30-70702485-9
Australia	John Deere Financial Limited	166 - 170 Magnesium Drive, Crestmead, Queensland, 4132 Australia	ACN 078 714 646
Australia	John Deere Limited	166 - 170 Magnesium Drive, Crestmead, Queensland, 4132, (P.O. Box 2022 Crestmead, Queensland) Australia	ACN 008 671 725
Australia	Waratah Forestry Equipment Pty. Ltd.	5 Collins Road, Melton Victoria, 3337, Australia	ACN 006 562 545
Australia	Wirtgen Australia Pty. Ltd.	Street address: Lot 2, Great Eastern Highway (off Apac Way), South Guildford WA 6055, Australia Postal address: PO Box 279, Guildford WA 6935, Australia	ACN 002 968 167
Austria	Kreisel Electric GmbH	Kreiselstraße 1 4261 Rainbach im Mühlkreis, Austria	FN 585301m
Austria	Wirtgen Österreich GmbH	Dr. Linsinger Str. 5, 4662 Steyrermühl, Austria	FN 218183h
Belgium	Wirtgen Belgium B.V.B.A.	Schoonmansveld 19a, 2870 Puurs, Belgium	413842778
Brazil	Banco John Deere S.A.	Rod. Eng. Ermenio de Oliveira Penteado (SP-075) s/n, km 57,5 Prédio 1, 1º Andar, Bairro Helvétia, Indaiatuba, Sao Paulo 13337-300 Brazil	NIRE 35300443462
Brazil	Ciber Equipamentos Rodoviários Ltda.	Rua Senhor Do Bom Fim, 177, Porto Alegre / RS CEP 91140-380, Brazil	NIRE 4320371161-6
Brazil	John Deere Brasil Ltda.	Engenheiro Jorge Antonio Dahne Logemann, 600, Distrito Industrial, Horizontina, Rio Grande do Sul, Brazil	NIRE 43205042584; IE 0620007826
Brazil	John Deere Equipamentos do Brasil Ltda.	Engenheiro Ermênio de Oliveira Penteado, s/nº - entre km 61+160 metros ao km 61+280 metros – Pista Norte, Helvétia, Indaiatuba, São Paulo, Brasil	NIRE 35213887915

Brazil	Pla Maquinas Pulverizadoras e Fertilizadoras LTDA	Av. Getúlio Vargas 10465, Canoas Rio Grande do Sul, Brazil 92426-000	NIRE 43.209.344.496
Bulgaria	Wirtgen Bulgaria EOOD	10, Rozova Gradina Str., 1588 Krivina, Bulgaria	UIC 121164324
Chile	John Deere Financial Chile SpA	Avenida Presidente Riesco No. 5561, Bldg. Arrau, 4th Fl, No. 401, Las Condes, Santiago, Chile	761708473
China	John Deere (China) Investment Co., Ltd.	12F, 10# Building, No.6 Jiuxianqiao Road, Chaoyang District, Beijing, China	91110000710938941J
China	John Deere (Jiamusi) Agricultural Machinery Co., Ltd.	No. 1 Lianmeng Road, Jiamusi 154002, Heilongjiang Province, China	91230800606542285D
China	John Deere (Tianjin) Company, Limited	No. 89, 13th Avenue, TEDA, Tianjin, China 300457, China	911201167736005852
China	John Deere (Tianjin) International Trading Co., Ltd.	No. 309\310, 3rd Floor, No.92 Haibin 5th Road, Tianjin Free Trade Zone (Bailment No.20170416, of Tianjin Shengxin Business Secretary Co., Ltd.), China	91120116718262384Q
China	John Deere Finance Lease Co., Ltd.	1st Floor, No. 89, 13th Avenue, TEDA, Tianjin, China 300457	91120116562683843D
China	Wirtgen (China) Machinery Co. Ltd.	No. 395, Chuang Ye Road, Langfang Economic and Technical Development Zone, Hebei, 065001, P.R. China	91131000755456671L
China	Wirtgen (Foshan) Machinery Co. Ltd.	No. 41 Xile Ave., Leping Town, Sanshui District Foshan 528137, China	91440607MA4UQ8GR8M
China	Wirtgen (Taicang) Machinery Co. Ltd.	12 Xinmiao Road, Taicang Economy Development Area, Taicang, China	913205853983398 12Q
China	Wirtgen Hong Kong Ltd.	Unit C, 20/F., Morrison Plaza, 9 Morrison Hill Road, Wan Chai, Hong Kong, China	273723
Denmark	Wirtgen Denmark A/S	Taulov, Taulov Kirkevej 28, 7000 Fredericia, Denmark	CVR-81667217
Estonia	OÜ Wirtgen Eesti	Saha-Loo tee 14, Iru küla 74206, Jõelähtme vald, Harju Maakond, Estonia	10622518
Finland	John Deere Forestry Oy	Lokomonkatu 21, PL 474 Tampere, FIN-33900, Finland	1592331-8
Finland	Waratah OM Oy	Rahtikatu 14, Joensuu, 80100, Finland	1865718-2

Finland	Wirtgen Finland Oy	Huurrekuja 11, 04360 Tuusula, Finland	1012387-2
France	John Deere S.A.S.	1 rue John Deere Cedex, Fleury Les Aubrais, France 45401	086 280 393
France	John Deere Solutions Réseau S.A.S.	23 Rue du Paradis, 45140 Ormes, France	818 865 149
France	Ribouleau Monosem S.A.S.	16 rue du Général de Gaulle Largeasse, France 79240	626 620 116
France	Wirtgen France S.A.S.	7, rue Marc Seguin - BP 31633, 95696 Goussainville Cedex, France	722 036 134
Georgia	Wirtgen Georgia LLC	Uznadse Str. 4, 0102 Tbilisi, Georgia	404491974
Germany	baukema Handel GmbH	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRB 14063
Germany	Benninghoven Zweigniederlassung der Wirtgen Mineral Technologies GmbH	Benninghovenstr. 1, 54516 Wittlich, Germany	HRB 23351
Germany	Deere & Company European Office	John Deere Strasse 70, Mannheim, Germany 68163	HRB 1653
Germany	Hamm AG	Hammstraße 1, 95643 Tirschenreuth, Germany	HRB 1851
Germany	John Deere GmbH & Co. KG	John-Deere-Str. 70, 68163 Mannheim, Germany	HRA 704371
Germany	John Deere Walldorf GmbH & Co. KG	John-Deere-Str.1, Walldorf Germany 69190	HRA 707944
Germany	John Deere Walldorf International GmbH	John-Deere-Str.1, Walldorf Germany 69190	HRB 743035
Germany	Joseph Vögele Aktiengesellschaft	Joseph Vögele Strasse 1, 67075 Ludwigshafen, Germany	HRB 62108
Germany	Kleemann GmbH	Manfred-Wörner-Str. 160, 73037 Göppingen, Germany	HRB 530810
Germany	Maschinenfabrik Kemper GmbH & Co. KG	Breul, 48703 Stadtlohn, Germany	HRA 2556
Germany	Wirtgen Deutschland Vertriebs- und Service GmbH	Ulstettstraße 6, 86167 Augsburg, Germany	HRB 20259
Germany	Wirtgen GmbH	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRB 14080
Germany	WIRTGEN GROUP Branch of John Deere GmbH & Co. KG	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRA 704371
Germany	Wirtgen International GmbH	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRB 12873
Germany	Wirtgen Mineral Technologies GmbH	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRB 23351
Germany	Wirtgen North Africa GmbH	Reinhard-Wirtgen-Str.2, 53578 Windhagen, Germany	HRB 21670

Germany	Wirtgen Road Technologies GmbH	Reinhard-Wirtgen-Str. 2, 53578 Windhagen, Germany	HRB 23312
Hungary	Wirtgen Budapest Kft.	Erdöalja u.1, 2363 Felsöpakony, Hungary	13-09-183587
India	John Deere Financial India Private Limited	Tower XIV, Cybercity, Magarpatta City, Hadapsar, Pune Maharashtra, 411 013, India	U65923PN2011PTC141149
India	John Deere India Private Limited	Tower XIV, Cybercity, Magarpatta City, Hadapsar, Pune Maharashtra, 411 013, India	U74220PN1997PTC112441
India	Wirtgen India Pvt. Ltd.	Gat No.301/302, Bhandgaon-Khor Road, Village-Bhandgaon, Tal.Daund, Dist.Pune - 412214, India	No. 08/18808 of 1995
Ireland	John Deere Forestry Limited	Ballyknocken, Glenealy, Co. Wicklow, Ireland	105782
Ireland	The Vapormatic Company (Ireland) Limited	Kestral Way, Sowton Industrial Estate, Exeter, United Kingdom Ireland	20235
Ireland	Wirtgen Ireland Ltd.	Enfield Industrial Estate, Trim Road, Enfield, Co. Meath, Ireland	354269
Israel	JDBH Works Ltd.	Kibbutz Beith Hashita, Tzvaim Industrial Zone, Israel 10801	514395136
Italy	John Deere Acceptances S.r.l.	Via Guiseppe di Vittorio 1, Vignate (Milano) 20060, Italy	MI-1656534
Italy	John Deere Italiana S.r.l.	Via Roma 108F, Cassina de' Pecchi,Milano, Italy 20051, Italy	MI-1869021
Italy	Mazzotti S.r.l.	Via Dismano, 138/A, 48124 Ravenna RA, Italy	RA – 165367
Italy	Wirtgen Macchine S.r.l.	Via delle Industrie 7, 20082 Noviglio (Milano), Italy	MI-1101267
Japan	Wirtgen Japan Co. Ltd.	Tsunekura Building 3F, 20-6, Jinbo-cho 2 chome, Kanda, Chiyoda-ku, Tokyo 100-0051, Japan	0100-01-011456
Latvia	SIA Wirtgen Latvia	Mežapurva iela 7, Riga, LV-1064	40003474522
Lithuania	UAB Wirtgen Lietuva	Liepkalnio g. 188, 13242 Vilnius, Lithuania	111642847
Luxembourg	John Deere Bank S.A.	43, avenue John F. Kennedy, Luxembourg 1855 Grand-duchy of Luxembourg	B 74106
Luxembourg	John Deere Cash Management	43, avenue John F. Kennedy, Luxembourg 1855 Grand-duchy of Luxembourg	B 101957
Luxembourg	John Deere Holding Brazil S.à r.l.	43, avenue John F. Kennedy, Luxembourg 1855 Grand-duchy of Luxembourg	B 164743

Luxembourg	John Deere Luxembourg Canada Holding S.à r.l.	43 avenue John F. Kennedy, Luxembourg, L-1855, Grand-duchy of Luxembourg	B278069
Luxembourg	John Deere Luxembourg Holding S.àr.l.	43 avenue John F. Kennedy, Luxembourg, L-1855, Grand-duchy of Luxembourg	B285065
Luxembourg	John Deere Luxembourg Investment S.à r.l.	43, avenue John F. Kennedy, Luxembourg 1855 Grand-duchy of Luxembourg	B 165923
Luxembourg	John Deere Mexico S.à r.l.	43 Avenue John F. Kennedy, Luxembourg, L-1855, Grand-duchy of Luxembourg	B 164760
Luxembourg	John Deere Technologies S.C.S.	17 Boulevard FW Raiffeisen, Luxembourg 2411	B218141
Malaysia	Wirtgen (M) SDN BHD	Business address: No.12A Jalan Mandolin 33/5, Shah Alam Premier Industrial Park, Seksyen 33, 40400 Shah Alam Selangor, Malaysia Registered office: 18A, Jalan Mutiara Raya, Taman Mutiara, 56000 Kuala Lumpur, Malaysia	531649-M
Mexico	John Deere Financial Mexico, S.A. de C.V. SOFOM, ENR	Boulevard Diaz Ordaz número 500, interior A, Colonia la Leona, San Pedro Garza Garcia, Nuevo Leon, 66210, Mexico	56623*9
Mexico	John Deere Shared Services Mexico S. de R.L. de C.V.	Boulevard Diaz Ordaz #500, Garza Garcia, Nuevo Leon, Mexico	N-2017096712
Mexico	Motores John Deere S.A. de C.V.	Carretera a Mieleras Km. 6.5 s/n, C.P. 27400, Torreon, Coahuila, Mexico	55257
Mexico	Servicios Administrativos John Deere S.A. de C.V.	Boulevard Diaz Ordaz número 500, interior A, Colonia la Leona, San Pedro Garza Garcia, Nuevo Leon, 66210, Mexico	69988*9
Mexico	Vapormatic de Mexico S.A. de C.V.	Acceso V #110-A Nave 5, Desarrollo Montana 2000 Section III 76150, Querteraro, Qro., Mexico	28742
Norway	John Deere Forestry AS	Industriveien 13, Kongsvinger, N-2212, Norway	957 269 222
Norway	Wirtgen Norway AS	Gallebergveien 18, Postboks 64, 3071 Sande i Vestfold, Norway	968 469 940
Poland	John Deere Polska Sp. z o.o.	ul. Poznańska 1B, 62-080 Tarnowo Podgórne, Poland	0000129369
Poland	Wirtgen Polska Sp.z o.o.	Ul. Ostrowska 344, 61-312 Poznan, Poland	KRS-0000010741

Romania	Wirtgen Romania S.R.L.	Str. Zborului nr 1-3, Otopeni, 075100 Bucuresti - Otopeni, Romania	J23/397/2003
Singapore	John Deere (Singapore) Service Co. Pte. Ltd.	438 Alexandra Road #12-01/04, Alexandra Point, Singapore, 119958, Singapore	202312098M
Singapore	John Deere Asia (Singapore) Private Limited	438 Alexandra Road #12-01/04, Alexandra Point, Singapore, 119958, Singapore	200610270R
Singapore	Wirtgen Singapore Pte. Ltd.	No. 5 Tuas Avenue 18A, Singapore 638854, Singapore	199602575N
South Africa	John Deere (Proprietary) Limited	Hughes Extension 47, 38 Oscar Street, Boksburg, Gauteng, 1459 South Africa	UC.37595
South Africa	Wirtgen South Africa (Pty) Ltd.	52 Maple Street, Pomona, Kempton Park 1619, South Africa	1999/010901/07
Spain	John Deere Iberica S.A.	Apartado de Correos 14412, 28080 Madrid, Spain	Hoja M-13643 Tomo 655 Folio 116
Spain	King Agro Europa, S.L.	C/Doce 10Polígono Industrial Canya dels Cond Picassent (Valencia), Spain, 46220	138255
Sweden	John Deere Forestry AB	Fyrgatan 8, Box 502, Maersta, S-195 25, Sweden	556584-6614
Sweden	Svenska John Deere A.B.	Box 503 195 91 Märsta, Sweden	556063-2431
Sweden	Wirtgen Sweden AB	Björnstorpsvägen 18, 342 30 Alvesta, Sweden	556465-2534
Taiwan, R.O.C.	Wirtgen Hong Kong Ltd. Taiwan Branch	No. 1190, Sec. 3, Fuguo Road, Luzhu Shiang, Taoyuan County 33849, Taiwan R.O.C.	16743485
Thailand	John Deere (Thailand) Limited	No. 90, CW Tower A, 32nd Floor, Unit No. A3202, Ratchadapisek Road, Huai Kwang Sub-District, Huai Kwang District Bangkok Metropolis, Bangkok, 10310, Thailand	105554098371
Thailand	Wirtgen (Thailand) Co. Ltd.	99/9 Moo 6, Bangna-Trad Km. 24 Rd., T.Bang Sao Thong, A. Bang Sao Thong, Samutprakarn 10540 Thailand	115540004433
The Netherlands	John Deere Enschede B.V.	Rigtersbleek-Aalten 4 – K1.11, 7521 RB Enschede, The Netherlands	6022728
The Netherlands	John Deere Fabriek Horst B.V.	Energiestraat 16, NL-5961 PT Horst, Postbus 6006, The Netherlands	12020529
The Netherlands	John Deere Nederland B.V.	Energiestraat 16, NL-5961 PT Horst, Postbus 6006, The Netherlands	12023490
The Netherlands	John Deere Real Estate B.V.	Energiestraat 16, NL-5961 PT Horst, Postbus 6006, The Netherlands	53870816

The Netherlands	Wirtgen Nederland B.V.	Velsenstraat 1, 4251 LJ Werkendam, Netherlands	RSIN 002982055
Turkey	Wirtgen Ankara Makine Sanayi Ve Ticaret Ltd. Sti.	Wirtgen Ankara Gölbasi Tesisleri, Konya - Ankara Kara Yolu 3.Km. Ankara Caddesi No:223, Pk. 06830 Gölbasi, Ankara, Turkey	233562
Ukraine	John Deere Ukraina TOV	Business center "Chayka Plaza", Soborna Street 1-B, 5th floor, Kiev-Svjatoshin district, Kiev region	35982633
Ukraine	PIK Wirtgen Ukraine	Pyrogivskyy shlyakh Str. 28, 03083 Kyiv, Ukraine	25638086
United Kingdom	John Deere Forestry Ltd.	Carlisle Airport Trading Estate, Carlisle, Cumbria, Carlisle, England CA6 4NW, United Kingdom	02218900
United Kingdom	John Deere Limited	Harby Road, Langar, Nottingham, NG13 9HT, UK	SC028492
United Kingdom	The Vapormatic Company Limited	Kestrel Way, Sowton Industrial Estate, Exeter, EX2 7LA, England	538655
United Kingdom	Vapormatic Europe Limited	Kestral Way, Sowton Industrial Estate, Exeter, United Kingdom	10701451
United Kingdom	Vapormatic U.K. Limited	Kestral Way, Sowton Industrial Estate, Exeter, United Kingdom	10698462
United Kingdom	Wirtgen Ltd.	Wirtgen Group House, Overfield Park, Godfrey Drive, Newark, England NG24 2UA, United Kingdom	3026300
United States	ATI Products, Inc.	5100-H W.T. Harris Blvd., Charlotte, NC 28269	0119690
United States	Blue River Technology LLC	C/O One John Deere Place, Moline, IL 61265	729204
United States	Deere Credit Services, Inc.	6400 N.W. 86th Street, P.O. Box 6600, Johnston, IA 50131-6600	2083737
United States	Deere Credit, Inc.	6400 N.W. 86th Street, P.O. Box 6600, Johnston, IA 50131-6600	0820863
United States	Deere Payroll Services, Inc.	C/O Deere & Company, One John Deere Place, Moline, IL 61265	782625
United States	John Deere Agricultural Holdings, Inc.	C/O Deere & Company, One John Deere Place, Moline, IL 61265	2602726
United States	John Deere Capital Corporation	PO Box 5328, Madison, Wisconsin 53705-0328	525920
United States	John Deere Construction & Forestry Company	C/O Deere & Company, One John Deere Place, Moline, IL 61265	716911
United States	John Deere E-Commerce LLC	400 East Court Avenue, Des Moines, IA 50309-2017	W01347996

United States	John Deere Electric Powertrain LLC	One John Deere Place, Moline, IL 61265	6407612
United States	John Deere Forestry Group LLC	C/O Deere & Company, One John Deere Place, Moline, IL 61265	386421
United States	John Deere Shared Services LLC	C/O Deere & Company, One John Deere Place, Moline, IL 61265	729218
United States	John Deere Thibodaux LLC	244 Highway 3266, Thibodaux, LA 70301-1602	729315
United States	NavCom Technology, Inc.	20780 Madrona Ave, Torrance, CA 90503, United States	C1997002
United States	Timberjack Corporation	3650 Brookside Parkway, Suite 400, Alpharetta, GA 30022-4426	2028187
United States	Waratah Forestry Attachments LLC	375 International Park, Suite 200, Newnan, GA 30265	K920710
United States	Wirtgen America, Inc.	6030 Dana Way, Antioch, TN 37013, USA	000162073