Appendix 1

AGCO GROUP BINDING CORPORATE RULES

SCOPE AND PURPOSE

1.1 AGCO Corporation and its global affiliated companies (the "**AGCO Group**") seek to operate on a seamless level and the ability of the AGCO Group to use Personal Data is fundamental to various aspects of AGCO Group's global operations which include manufacturing, distribution, sales and marketing, human resources, research and development, services and supply chain.

1.2 The purpose of these Binding Corporate Rules ("**Rules**") is to ensure that the AGCO Group provides an adequate level of protection for Processing of all Personal Data which was;

- subject to the EU Data Protection Laws and Regulations; and
- transferred from an AGCO Group affiliated company within the EEA to AGCO and/or an AGCO Group affiliated company outside the EEA and not in a country recognised by the EU Commission as ensuring an adequate level of protection

or

- subject to the Swiss Data Protection Laws and Regulations; and
- transferred from an AGCO Group affiliated company within Switzerland to AGCO and/or an AGCO Group affiliated company outside Switzerland and not in a country recognised by the EDÖB (Eidgenössischer Datenschutz- und Öffentlichkeitsbeauftragter) as ensuring an adequate level of protection.

These Rules shall be read and interpreted in accordance with the purpose set out in this section 1.2.

1.3 These Rules will apply globally to the extent set out in section 1.2 and in all cases where the AGCO Group transfers and/or processes Personal Data both by automated means and manually, and whether the Personal Data relates to AGCO Group employees, contractors, business contacts, customers or third parties. The AGCO Group and AGCO Group employees must comply with these Rules. To the extent that AGCO Group transfers personal data to which these Rules apply according to section 1.2, to third party service providers, suppliers and vendors, AGCO Group shall undertake to ensure the adequate level of protection of such transfers by adequate contractual means in accordance with section 10.

1.4 The AGCO Group will always comply with all applicable data protection laws and will ensure that the transfer and/or processing of Personal Data is carried out in accordance with such applicable data protection laws. Where there are no such data protection laws or the relevant data protection laws do not meet the standards set out in these Rules, AGCO Group will transfer and/or process Personal Data in compliance with these Rules.

1.5 AGCO Corporation has delegated data protection responsibilities in the EEA and Switzerland to AGCO SAS and AGCO SAS is responsible for ensuring compliance by the AGCO Group with these Rules.

1.6 A Data Subject can enforce these Rules against AGCO SAS as a third-party beneficiary as described in section 16.2.

DEFINITIONS

2. In these Rules:

"**AGCO**" means AGCO Corporation, a Delaware Corporation with its Global headquarters at 4205 River Green Parkway, Duluth, Georgia 30096, United States.

"**AGCO Group**" means AGCO and its wholly owned affiliated companies as set forth in Schedule 1.

"**AGCO SAS**" means an affiliated company of AGCO incorporated in France under registration number 317 358 380 RCS Beauvais with its registered office at 41 Avenue Blaise Pascal, B.P. 60307, 60026 Beauvais Cedex, France, and having delegated authority from AGCO to ensure compliance with these Rules by AGCO Group.

"**Chief Data Privacy Officer**" **/ "CDPO"** means the person in AGCO responsible for data governance system and data protection globally and holding the office of General Counsel & Corporate Secretary.

"**Consent**" of the Data Subject means any freely given specific and informed indication of the Data Subject´s wishes by which the Data Subject signifies agreement to the Processing of Personal Data relating to him or her.

"**Controller**" means the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the Processing of Personal Data. Controller must exercise control over the processing and carry data protection responsibility for it.

"**Processor**" means a natural or legal person, public authority, agency or any other body which processes Personal Data on behalf of the Controller. For clarity, an employee of a Processor is not considered itself to be a separate Processor.

"**Data Protection Authority**" means the relevant public authorities in each country in the European Union that are responsible for monitoring the application within such country of the EU Data Protection Laws and Regulations

"Data Protection Impact Assessment" means an assessment of the impact of the envisaged Processing operations on the protection of Personal Data that Controller shall carry out prior to commencing Processing activity that is likely to result in a high risk to the rights and freedoms of natural persons.

"**Data Subject**" means an identified or identifiable natural person whose Personal Data is transferred and/or processed within the scope of section 1.2. 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 the physical, physiological, mental, economic, cultural or social identity.

"**EEA"** means the member states of the European Union (EU) and the other signatories to the Treaty on the European Economic Area (EEA).

"**EU Data Protection Laws and Regulations**" means Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data, 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, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR") as well as the data protection laws in the EU country where the relevant Controller is located.

"**Exporter**" means a company based in the EEA or Switzerland that as Controller transfers Personal Data to another company based in a country that does not provide an adequate level of protection (Article 25(6) Directive 95/46/EC, Art. 6(1) DSG – Swiss Federal Data Protection Act - Bundesgesetz über den Datenschutz).

"**IA**" means Internal Audit Department.

"**Importer**" means a company based in a country that does not provide an adequate level of protection (Article 25(6) Directive 95/46/EC, Art. 6(1) DSG – Swiss Federal Data Protection Act - Bundesgesetz über den Datenschutz) and which receives Personal Data from the Exporter for processing in accordance with these Rules.

"**Personal Data**" means any information relating to a Data Subject who's Personal Data is transferred and/or processed within the scope of section 1.2;

"Processing" of Personal Data means any operation or set of operations which is performed upon Personal Data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission,

dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.

"Regional Data Privacy Officer / RDPO" means a person in AGCO regionally responsible for data governance system and data protection.

"**Special Categories of Personal Data**" means special categories of Personal Data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and data concerning health or sex life or sexual orientation as well as genetic data and biometric data for the purpose of uniquely identifying a natural person.

"Third Country" means any country that does not fall within the definition of EEA except Switzerland.

"Third-Party Controller" means any Controller which is not an AGCO Group affiliated company Controller.

"Third-Party Processor" means any Processor which is not an AGCO Group affiliated company Processor.

DATA TRANSFERS AND PROCESSING

3.1 The AGCO Group will transfer and/or process Personal Data fairly and lawfully and will collect Personal Data only for specified, explicit and legitimate purposes. The AGCO Group will provide fair information to make Data Subjects aware of such purposes at the time when Personal Data is obtained, except from cases of mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defense, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the Data Subject or the rights and freedoms of others.

3.1.1 When Personal Data is collected directly from the Data Subject, the fair information includes that before their Personal Data is Processed Data Subjects will be given the following information:

- the identity and the contact details of the Controller and, where applicable, of the Controller's EEA and Swiss representative AGCO SAS;
- the contact details of the Chief Data Privacy Officer, where applicable;
- the purposes of the Processing for which the Personal Data are intended as well as the legal basis for the Processing;

- where the Processing is based on point (f) of Article 6(1) of the GDPR, the legitimate interests pursued by the Controller or by a Third Party Controller;
- 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 and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in GDPR Article 46 or 47, or the second subparagraph of GDPR Article 49(1), reference to the appropriate or suitable safeguards and the means by which to obtain a copy of them or where they have been made available.

In addition to the information referred to above in section 3.1.1, 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 is based on Data Subject's explicit 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, referred to in GDPR Article 22(1) and (4) 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 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.

The above mentioned requirements shall not apply where and insofar as the Data Subject already has the information.

3.1.2 When Personal Data have not been obtained from the Data Subject, the fair information includes that before their Personal Data is Processed Data Subjects will be given the following information:

- the identity and the contact details of the Controller and, where applicable, of the Controller's EEA and Swiss representative AGCO SAS;
- the contact details of the Chief Data Privacy 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 recipients or categories of recipients of the Personal Data, if any;
- where applicable, that the Controller intends to transfer Personal Data to a recipient in a third country or international organisation and the existence or absence of an adequacy decision by the Commission, or in the case of transfers referred to in GDPR Article 46 or 47, or the second subparagraph of GDPR Article 49(1), reference to the appropriate or suitable safeguards and the means to obtain a copy of them or where they have been made available.

In addition to the information referred to above in section 3.1.2, the Controller shall provide the Data Subject with the following information necessary to ensure fair and transparent Processing in respect of the Data Subject:

- the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
- where the processing is based on point (f) of GDPR Article 6(1), the legitimate interests pursued by the Controller or by a Third Party Controller;
- 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 and to object to Processing as well as the right to data portability;
- where Processing is based on Data Subject’s explicit 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;
- from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;
- the existence of automated decision-making, including profiling, referred to in GDPR Article 22(1) and (4) 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.

The controller shall provide the information referred to in section 3.1.2 above:

- within a reasonable period after obtaining the Personal Data, but at the latest within one month, having regard to the specific circumstances in which the Personal Data are processed;
- if the Personal Data are to be used for communication with the Data Subject, at the latest at the time of the first communication to that Data Subject; or
- if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

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

Section 3.1.2 shall not apply where and insofar as:

- the Data Subject already has the information;
- the provision of such information proves impossible or would involve a disproportionate effort, in particular for Processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, subject to the conditions and safeguards referred to in GDPR Article 89(1) or in so far as the obligation referred to in paragraph 1 of this GDPR Article is likely to render impossible or seriously impair the achievement of the objectives of that Processing. In such cases the Controller shall take appropriate measures to protect the Data Subject's rights and freedoms and legitimate interests, including making the information publicly available;
- obtaining or disclosure is expressly laid down by Union or Member State law to which the Controller is subject and which provides appropriate measures to protect the Data Subject's legitimate interests; or
- where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Union or Member State law, including a statutory obligation of secrecy.

3.2 Personal Data will not be further processed in a way incompatible with those purposes, except from cases of mandatory requirements of the national legislation (as described in 3.1). The AGCO Group will obtain the Data Subjects Consent to any such new purposes, where necessary.

3.3 Personal Data will be processed based on the following grounds:

- Data Subject has unambiguously given his Consent or
- 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
  - compliance with a legal obligation to which the Controller is subject

- in order to protect the vital interests of the Data Subject
- 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 the Personal Data are disclosed or
- the purposes of the legitimate interests pursued by the Controller or by the third party or parties to whom the Personal Data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the Data Subject which require protection under Art. 1(1) of Directive 95/46/EC.

3.4 Special Categories of Personal Data will be provided with additional safeguards such as provided by the Directive 95/46/EC. Special Categories of Personal Data will only be processed if one or more of the following applies:

- Data Subject has given his explicit Consent to the Processing of those Special Categories of Personal Data, except where the applicable laws prohibit it; or

- Processing is necessary for the purposes of carrying out the obligations and specific rights of the Controller in the field of employment law in so far as it is authorized by national law providing for adequate safeguards; or

- Processing is necessary to protect the vital interests of the Data Subject or of another person where the Data Subject is physically or legally incapable of giving his Consent; or

- Processing is carried out in the course of its legitimate activities with appropriate guarantees by a foundation, association or any other non-profit-seeking body with a political, philosophical, religious or trade-union aim and on condition that the Processing relates solely to the members of the body or to persons who have regular contact with it in connection with its purposes and that the data are not disclosed to a third party without the Consent of the Data Subjects; or

- Processing relates to Special Categories of Personal Data which are manifestly made public by the Data Subject; or

- Processing of Special Categories of Personal Data is necessary for the establishment, exercise or defence of legal claims; or

- Processing of the Special Categories of Personal Data is required for the purposes of preventive medicine, medical diagnosis, the provision of care or treatment or the management of health-care services, and where those Special Categories of Personal Data are processed by a health professional subject under national law or rules established by national competent bodies to the obligation of professional secrecy or by another person also subject to an equivalent obligation of secrecy.

ACCURACY, QUALITY & RETENTION OF PERSONAL DATA, PRIVACY BY DESIGN & DEFAULT

The AGCO Group will ensure that Personal Data:

4.1 is kept accurate and up to date and will actively encourage Data Subjects to inform AGCO Group when their Personal Data changes;

4.2 is adequate, relevant and not excessive to properly fulfil the purpose for which that Personal Data was collected; and

4.3 is only kept for as long as is necessary for the purpose or purposes for which that Personal Data was collected.

4.4 AGCO Group shall 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.

AVAILABILITY AND TRANSPARENCY

5.1 These Rules will be made available on AGCO's intranet https://insideagco.agcocorp.com/company/departmentsfunctions/LegalCompliance/Pages/en/Global%20Compliance/Data-Privacy.aspx and made public in http://www.agcocorp.com/privacy.html.

DATA SUBJECTS RIGHTS

6.1 Data Subjects may make a written request to the AGCO Group affiliated company and/or AGCO (Controller) processing the Data Subjects Personal Data and be entitled to:

6.1.1 be informed of whether this AGCO Group affiliated company and/or AGCO holds and processes Personal Data of the Data Subject;

6.1.2 be provided without excessive delay or expense with a communication in an intelligible form of the Data Subjects' Personal Data held by the AGCO Group affiliated company and/or AGCO undergoing Processing and of any available information as to their source, the purposes for which any such Personal Data are being held and the recipients to whom the Personal Data is, or may be, disclosed.

6.2 The AGCO Group affiliated company and/or AGCO (Controller) may ask the Data Subject for any information that the Controller reasonably requires to confirm the Data Subjects identity and to locate the relevant Personal Data.

6.3 Data Subjects have the right to the rectification, deletion or to restriction of Processing of their Personal Data which is inaccurate or incomplete and to object, free of charge and at any time on legitimate grounds relating to his or her particular situation, in particular if the data are inaccurate or incomplete, to the Processing of their Personal Data (unless the Processing is required by law).

6.4 Data Subjects also have the right to opt in free of charge, to the use of their Personal Data for direct marketing purposes. The Controller will take all necessary steps to prevent marketing materials being sent to Data Subjects that have not opted in of receiving such marketing material.

6.5 Data Subjects have the right to object, at any time on compelling legitimate grounds relating to their particular situation, to the Processing of their Personal Data, unless that Processing is required by law. Where the objection is justified, the Processing must cease.

6.6 Data Subjects may address their request under this section 6 to the registered office address of the local AGCO Group affiliated company in their country or, to AGCO SAS (office address: 41 Avenue Blaise Pascal, B.P. 60307, 60026 Beauvais Cedex, France) for the attention of the Legal Department, The contact information can be also found here: http://www.agcocorp.com/contact/facilities-list.html. Data Subjects may also use this e-mail-address: DataPrivacy@agcocorp.com.

AUTOMATED INDIVIDUAL DECISIONS, INCLUDING PROFILING

7.1 The AGCO Group will not make an evaluation of or a decision about the Data Subject which significantly affects them based solely upon automated Processing of their Personal Data, including profiling, unless that decision:

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

- is authorized by a law which also lays down measures to safeguard the Data Subject's legitimate interests.

SECURITY OF PERSONAL DATA AND CONFIDENTIALITY

8.1 The AGCO Group will take appropriate technical and organisational measures to protect Personal Data. Taking into account the state of the art, the cost of implementation and the nature, scope, context and purposes of Processing as well as the risks of varying likelihood and severity for rights and freedoms of natural persons posed by the processing, AGCO Group 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 organisational measures, such as pseudonymisation, which are designed to implement data-protection principles, such as data minimisation, in an effective manner and to integrate the necessary safeguards into the Processing in order to meet the requirements of the GDPR and protect the rights of Data Subjects.

8.2 Each AGCO Group affiliated company and AGCO will take steps to ensure that its security measures include:

8.2.1 the physical and environmental protection of its computer data centre operations, admission controls, back-up and disaster recovery capabilities to ensure the continuity of Processing operations or to avoid the loss of data as a result of theft, or deterioration due to fire, water damage or other natural disasters;

8.2.2 the protection of its networks against intrusion and cyber-attacks by the use of firewalls and anti-malware software; and

8.2.3 the use of passwords including, software and hardware encryption of workplace computers and mobile devices and the administration of access rights to data and its Processing.

8.3 The AGCO Group will take steps to ensure the reliability of its employees who have access to Personal Data and that only authorised employees will process Personal Data and at all times subject to AGCO Group non-disclosure and confidentiality obligations applicable to employees and these Rules. Employees who breach these Rules may be subject to disciplinary action including, dismissal.

AGCO GROUP PROCESSORS

9.1 An AGCO Group affiliated company and/or AGCO that processes Personal Data as Processor on behalf of another AGCO Group affiliated company and/or AGCO will act only on the instructions of the AGCO Group affiliated company and/or AGCO on whose behalf the Personal Data is processed. These instruction shall be laid down by written contractual means, and set 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 and which includes stipulations regarding all requirements set out in Article 28(3) of the GDPR.

The AGCO Group affiliated company and/or AGCO on whose behalf the Personal Data is processed will choose the AGCO Group affiliated company and/or AGCO as Processor only if it provides sufficient guarantees in respect of the technical and organizational measures and governing the Processing to be carried out and if it ensures compliance with those measures to ensure a level of security appropriate to the risk of the Processing.

9.2 In the case of a Personal Data breach, the Controller or AGCO SAS shall without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the Personal Data breach to the Data Protection Authority in accordance with Article 33 of the GDPR. Where the notification to the Data Protection Authority is not made within 72 hours, it shall be accompanied by reasons for the delay. When the Personal Data breach is likely to result in a high risk to the rights and freedoms of natural persons, the Controller or AGCO SAS shall communicate the Personal Data breach to the impacted Data Subjects without undue delay in accordance with the Article 34 of the GDPR. Furthermore, any Personal Data breaches should be documented (comprising the facts relating to the Personal Data breach, its effects and the remedial action taken) and the documentation should be made available to the supervisory authority on request (Art. 33 and 34 of the GDPR).

THIRD-PARTY PROCESSORS AND INTERNATIONAL TRANSFERS

10.1 Any AGCO Group affiliated company and/or AGCO that engages a Third-Party Processor located in the EEA or Switzerland or in a country recognised by the EU Commission respectively the EDÖB as ensuring an adequate level of protection will ensure that the Third-Party Processor will be bound by a written contractual means stipulating that the Third-Party Processor will act only on instructions from the Controller and will be responsible for the implementation of the adequate security and confidentiality measures. These instruction set 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 and which includes stipulations regarding all requirements set out in Article 28(3) of the GDPR.

10.2 All transfers of Personal Data to Third-Party Processors located in a Third Country and not in a country recognised by the EU Commission respectively the EDÖB as ensuring an adequate level of protection will respect the rules relating to the processors (Articles 16-17 Directive 95/46/EC) in addition to the rules on transborder data flows (Articles 25-26 of Directive 95/46/EC and as of 25. May 2018 Articles 45, 46 or 49 of the GDPR) respectively the equivalent provisions of the Swiss Data Protection Laws and Regulations.

10.3 All transfers of Personal Data to Third-Party Controllers located in a Third Country and not in a country recognised by the EU Commission respectively the EDÖBas ensuring an adequate level of protection will respect the rules on transborder data flows (Articles 25-26 of Directive 95/46/EC and as of 25. May 2018 Articles 45, 46 or 49 of the GDPR) respectively the equivalent provisions of the Swiss Data Protection Laws and Regulations.

TRAINING

11.1 The AGCO Group will provide appropriate training to its employees who have been given access to Personal Data and/or who are involved in the collection of Personal Data and/or in the development of tools and applications used to process Personal Data to ensure that all such employees are aware of their obligations under these Rules. Employee training courses on these Rules will be provided at regular intervals and will be a mandatory requirement. The AGCO Group will keep records of employee training.

AUDIT

12.1 The AGCO Group independent **Internal Audit Department ("IA")** (or an external auditor appointed by AGCO Group) will conduct an audit on a rotational basis to evaluate and report to the Audit Committee on all aspects of AGCO Group compliance with these Rules as part of AGCO´s overall audit program. The audit shall be conducted every five years in AGCO entities acting as core centres of Personal Data Processing and the risk profile of the company so requires. In other AGCO entities, depending on the size of the operations, volume of transactions, the amount of Personal Data and relative risk profiles audits shall be conducted on rotational basis or as may be requested by the Chief Data Privacy Officer **("CDPO")** and/or AGCO's Director, Global Internal Audit).

12.2 The audit findings including recommendations of any corrective actions that need to be taken will be reported by the Global Internal Audit Director to the CDPO who shall report the findings to the Regional Data Privacy Officers **("RDPO")** and the management of the audited entity**.** The RDPO, typically the Director Legal Services for the regions and appointed by the CDPO, will ensure that any corrective action is implemented as soon as reasonably practicable. The results of all audits will also be reported at AGCO´s ultimate board and AGCO SAS. If requested by a relevant Data Protection Authority (DPA), the CDPO will provide a copy of the audit findings to a relevant DPA. The CDPO may redact parts of the audit data to the extent necessary to protect confidential and privileged information.

12.3 AGCO agrees that relevant DPA´s may conduct audits of the relevant AGCO Group affiliate for the purposes of demonstrating the AGCO Group affiliate's compliance with these Rules. Due regard shall be given to restrictions arising from confidentiality agreements or from business and trade secrets.

PRIVACY & DATA PROTECTION COMPLIANCE

13.1 The CDPO shall report annually at the **AGCO senior staff meeting** on all privacy compliance issues in the preceding twelve months. This report includes specifically the degree of implementation of the BCR in the AGCO Group.

13.2 The **CDPO** is responsible for overseeing all privacy and data protection issues, including ensuring compliance with all aspects of these Rules at a global level. The CDPO is also responsible for the definition of the data privacy strategy, internal structure and initiatives and creation respectively periodic amendments of data protection compliance related policies. Further responsibilities are incident management procedures as well as monitoring and reporting of data privacy activities and results. The CDPO is supported by a team of RDPO responsible for overseeing and ensuring compliance with these Rules on a day-to-day basis and at a regional level. The RDPO are also responsible for setting regional data protection compliance policies in line with the global policies set by the CDPO and address regional data privacy issues. The RDPO report any substantial or major privacy issues to the CDPO. The RDPO are supported by local legal team members appointed for local implementation of the BCR and management on a country by country basis. The local legal team members report privacy issues to the RDPO. The CDPO, RDPO and appointed local legal team members shall receive top management support.

13.3 From time to time, AGCO Group affiliated companies and AGCO each perform self-assessment of data protection compliance through a questionnaire to the competent RDPO. The self-assessment differentiates from audit as not being independent but is intended to serve the organization in being compliant with these Rules. The questionnaire will cover the specific points of the Rules` documented policies and processes and be developed by the RDPO in conjunction with the **IA**. The questionnaire will be issued sporadically to the heads of business units (e.g. distribution, sales and marketing, human resources, services and supply chain) that impact in particular;

- Processing of Personal Data
- Storage of Personal Data
- Security of Persona Data
- Disclosure of Personal Data to Third Parties
- Data Subject access to Personal Data
- Automated decision making
- Marketing activities
- Personal Data archiving & destruction
- Staff training
- Transmission of Personal Data to any Third Country
- Changes to Processing activity
- Whistleblower Policy
- Works Council & Union activities

13.4 RDPO will conduct ad hoc spot checks. Once the result of the questionnaires defined in section 13.3 above have been received RDPO will establish a program of ad hoc spot checks of specific areas and locations covering key data privacy policies and processes to

ensure compliance with the requirements in effect. Issues identified will be logged on an issue log and remediation actions will be implemented to correct any deviation from the data privacy processes & policies. If investigations or a deeper detailed analysis are required by the RDPO, the RDPO can call on the services of IA to assist if required.

CONFLICT OF LAWS

14.1 Any AGCO Group affiliated company or AGCO prevented by national laws in its country of operation from complying with these Rules is required to promptly notify the CDPO (unless otherwise prohibited by a law enforcement authority).

14.2 In the case of such conflict, the CDPO will make a responsible decision regarding what action to take and will consult with the competent DPAs. Furthermore, where any legal requirement an AGCO Group affiliated company or AGCO is subject to in a third country is likely to have a substantial adverse effect on the guarantees provided by these Rules, the CDPO must report to the competent DPA, unless there is a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. This includes legally binding requests for disclosure of the Personal Data by a law enforcement authority or other state authority of a third country. In such a case, the competent DPA should be clearly informed about the request, including information about the data requested, the requesting body, and the legal basis for the disclosure, unless there is a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation. If in specific cases the suspension and/or notification are prohibited, the requested AGCO Group affiliated company or requested AGCO will use its best efforts to obtain the right to waive this prohibition in order to communicate as much information as it can and as soon as possible, and be able to demonstrate that it did so.

If, in the above cases, despite having used its best efforts, the requested AGCO Group affiliated company or requested AGCO is not in a position to notify the competent DPAs, it commits to annually provide general information on the requests it received to the competent DPAs (e.g. number of applications for disclosure, type of data requested, requester if possible, etc.).

In any case, the transfers of Personal Data by AGCO Group affiliated company and/or AGCO to any public authority cannot be massive, disproportionate and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

COMPLAINT HANDLING PROCEDURE

15.1 A Data Subject may file a complaint with AGCO SAS or with a local AGCO Group affiliated company operating in the Data Subject's country of residence regarding any breach or failure by AGCO Group to comply with these Rules. Complaints should be addressed to the contact at the address for AGCO SAS (office address: 41 Avenue Blaise

Pascal, B.P. 60307, 60026 Beauvais Cedex, France, for the attention of the Legal Department) - the contact information can be also found here: http://www.agcocorp.com/contact/facilities-list.html or the relevant AGCO Group affiliated company to be found at http://www.agcocorp.com/contact.html . Data Subjects may also use this e-mail-address: DataPrivacy@agcocorp.com.

15.2 The Data Subject will be given prompt confirmation of receipt of the complaint by AGCO SAS respectively the AGCO Group affiliated company, depending on where the complaint is filed. The RDPO will investigate the complaint and provide an answer to the Data Subject within a reasonable period and at least within one month of receipt of the request. That period may be extended by two further months where necessary, taking into account the complexity and number of the requests. AGCO SAS respectively the AGCO Group affiliated company shall inform the Data Subject of any such extension within one month of receipt of the request, together with the reasons for the delay. If AGCO SAS respectively the AGCO Group affiliated company does not take action on the request of the Data Subject, AGCO SAS respectively the AGCO Group affiliated company shall inform the Data Subject without delay and at the latest within one month of receipt of the request of the reasons for not taking action and on the possibility of lodging a complaint with a supervisory authority and seeking a judicial remedy.

15.3 The Data Subject may dispute in writing the RDPO response to a complaint. In such event, the RDPO will refer the dispute to the CDPO who may review the dispute and respond to the Data Subject within three months after receipt of Data Subject´s dispute. The CDPO may accept the finding of the RDPO or, substitute it with a new finding. If the Data Subject's complaint is upheld, then the CDPO will take steps to ensure that any remedial action is promptly taken.

15.4 Data Subjects whose Personal Data originates in the EEA or Switzerland have the right to lodge a complaint to the competent DPA and/or to make a claim in a court of competent jurisdiction, in particular in the Member State of his or her habitual residence, place of work, place of the alleged infringement or in the courts of the EEA member state where the Controller or Processor has an establishment, if they are not satisfied with the way in which their complaint has been addressed or if they have suffered any loss or damage as a result of an alleged breach by the AGCO Group of these Rules. Data Subjects rights in relation to a claim and the competent DPA and the court of competent jurisdiction are more fully described below under section 16 of these Rules.

ACCOUNTABILITY, DATA PROTECTION IMPACT ASSESSMENT AND ENFORCEMENT

16.1 AGCO and AGCO Group affiliated companies are parties to an intra-company agreement under which AGCO and each AGCO Group affiliate is bound by and must comply with these Rules. Every AGCO Group affiliated company acting as a Controller shall be responsible for, and be able to demonstrate compliance with the BCR.

16.2 When a processing is likely to result in a high risk to the rights and freedoms of Data Subjects, a AGCO Group affiliated company and/or AGCO acting as Controller shall prior to the Processing carry out an assessment of the impact of the envisaged processing operations on the protection of Personal Data ("**Data Protection Impact Assessment**"). Where Data Protection Impact Assessment indicates that the Processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the competent DPA should be consulted prior to Processing.

16.3 Data Subjects whose Personal Data are processed in the EEA or Switzerland and transferred to AGCO and/or AGCO Group affiliated companies outside of the EEA or Switzerland and within the scope of section 1.2 shall have the right to enforce sections 3, 4, 5, 6, 7, 8, 10, 14, 15, 16 and 17 of these Rules as a third-party beneficiary and shall have the right to seek compensation for damage or loss suffered as a result of breach of sections 3, 4, 5, 6, 7, 8, 10, 14, 15, 16 or 17 of the Rules, including, but not limited to, a judicial award of compensation for damage suffered by the Data Subject as a result of breach of sections 3, 4, 5, 6, 7, 8, 10, 14, 15, 16 or 17 of these Rules. Any such claims may be brought by the Data Subject at Data Subject´s own option either in the competent courts of France or in the EEA country respectively Switzerland from which the relevant AGCO Group affiliated company exported the Personal Data outside of the EEA or Switzerland and within the scope of section 1.2 or where the Data Subject has his or her habitual residence, but in each case against AGCO SAS. For the avoidance of doubt, Data Subject´s third party beneficiary rights are limited to Personal Data transferred from the EEA or Switzerland and within the scope of section 1.2.

Data Subjects also have the right to file a complaint with (i) the competent DPA where the alleged breach occurred or (ii) the competent DPA in the EEA country where the data subject has his/her habitual residence or place of work or respectively Switzerland from which the relevant AGCO Group affiliated company exported the Personal Data outside of the EEA or Switzerland and within the scope of section 1.2 for a breach by any AGCO Group affiliated company and/or AGCO.

16.4 In the event that a Data Subject has established that it has suffered damage or loss as a result of a breach of sections 3, 4, 5, 6, 7, 8, 10, 14, 15, 16 or 17 of these Rules regarding Personal Data processed in the EEA or Switzerland and transferred to AGCO Group affiliated companies and/or AGCO outside of the EEA or Switzerland and within the scope of section 1.2, the burden of proof to show that the damage or loss are not attributable to the relevant AGCO Group affiliate and/or AGCO will rest with AGCO SAS. If AGCO SAS can prove that the other AGCO Group affiliated company or AGCO outside of the EEA or Switzerland is not liable for the violation, it may discharge itself from any responsibility.

16.5 In the event of a proven breach of sections 3, 4, 5, 6, 7, 8, 10, 14, 15, 16 or 17 of these Rules regarding Personal Data processed in the EEA or Switzerland and transferred to AGCO and/or AGCO Group affiliated companies outside of the EEA or Switzerland and

within the scope of section 1.2 AGCO SAS has sufficient assets and undertakes to pay compensation for any damages resulting from the breach of the mentioned sections of the Rules.

16.6 AGCO SAS accepts responsibility for and agrees to take the necessary action to remedy the acts of other AGCO Group affiliated companies or AGCO outside of the EEA or Switzerland.

16.7 Nothing in AGCO's BCR diminishes or reduces the data subject's rights afforded under Directive 95/46/EC or under 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, and repealing Directive 95/46/EC (General Data Protection Regulation or "GDPR") replacing the Directive as of 25. May 2018.

CO-OPERATION WITH DPAs

17.1 AGCO will and will cause AGCO Group affiliated companies to abide by the advice of the competent DPA on any issues related to the interpretation and application of these Rules.

17.2 Upon request AGCO and AGCO Group affiliated companies will provide copies of the results of any audit carried out in relation to these Rules to a DPA with competent jurisdiction and to the DPA of the EEA from which the transfer of Personal Data occurred. The CDPO may redact parts of the audit data to the extent necessary to protect confidential or privileged information.

17.3 AGCO SAS will and, if appropriate, will cause the relevant local AGCO Group affiliate or AGCO to respond to all requests for information from the relevant DPA provided that such requests relate to compliance with these Rules in the relevant jurisdiction or in relation to Personal Data transferred out of the EEA from the relevant jurisdiction by the local AGCO Group affiliate or AGCO. The CDPO may redact parts of the information to the extent necessary to protect confidential or privileged information.

UPDATES TO THESE RULES

18.1 AGCO SAS will notify all DPA´s in the EEA countries from which Personal Data on the grounds of these Rules were exported and Switzerland at least once a year if any material changes are made to these Rules and will provide a brief explanation of the reasons for any such change. Where a modification may affect the level of protection offered by the BCR, it must be promptly communicated to the DPAs in the EEA Countries from which Personal Data on the grounds of these Rules were exported and Switzerland.

18.2 AGCO SAS will communicate any substantive changes to these Rules to all AGCO Group affiliated companies and AGCO and to the Data Subjects who benefit from these Rules.

18.3 No transfer of Personal Data is made to a new AGCO Group affiliated company or AGCO until it is effectively bound by these Rules and can deliver compliance.

18.4 The CDPO (or another officer appointed by the CDPO with delegated responsibility) will maintain an up-to-date list of AGCO Group affiliates and AGCO bound by these Rules and maintain a record of any updates to these Rules.

18.5 AGCO SAS will report any changes to AGCO and the list of AGCO affiliates bound by these Rules to all DPA´s in the EEA countries from which Personal Data on the grounds of these Rules were exported and Switzerland.

The Effective Date of these Rules is 24 May 2018. These Rules were last updated on 23 April 2018.