Introduction

Yara has committed itself to the protection of Personal Data of Yara Customers, Suppliers, Business Partners and Employees by implementing the Yara Data Privacy Policy (the "**Policy**"). The Policy constitutes Yara's Binding Corporate Rules ("**BCRs**") for the Processing and transfer of Personal Data within Yara.

The purpose of these Binding Corporate Rules is to ensure an adequate level of protection for Processing of Personal Data within Yara. Binding Corporate Rules enable Yara to make intra-group transfers of Personal Data across borders, provided that the rules set out herein are complied with. The BCRs have been approved by the competent Data Protection Authorities and are binding on Yara International ASA and its Group Companies.

Under European data protection legislation, transfer of Personal Data to countries outside the EEA that do not provide an adequate level of protection require a legal basis. The objective of Yara's Binding Corporate Rules is to establish such legal basis for transfers of Personal Data from Group Companies established within the EEA to Group Companies established outside the EEA. The objective is also to establish an internal control system containing legally binding data protection principles for how Personal Data shall be processed within Yara, in accordance with the EU General Data Protection Regulation 2016/679 (GDPR).

This document is a public excerpt and summary of Yara's Binding Corporate Rules and contains the material provisions and the data protection principles set out in Yara's BCRs. It further explains Data Subjects' rights and how to exercise those rights. For a full version of the BCRs, please contact the Head of Data Privacy as set out in Article 23.

An overview of Group Companies bound by the BCR is available here.
Capitalized terms have the meaning set out in Annex 1 (Definitions).

1 Scope, Applicability and Implementation

1.1 Scope

These BCRs address the Processing of Personal Data of Customers, Suppliers, Business Partners and Employees by Yara or a Third Party on behalf of Yara. These BCRs do not apply to Processing of Personal Data listed in Annex 3.

1.2 Electronic and Paper-based Processing

The BCRs apply to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.

1.3 Applicability of Local Law and BCR

Nothing in the BCRs will be construed to take away any rights and remedies that Individuals may have under applicable local law. The BCRs provide supplemental rights and remedies

to Individuals only.

1.4 Procedures and Notices

Yara may supplement the BCRs through procedures or notices that are consistent with the BCRs.

1.5 Accountability

The BCRs are binding on Yara. The Country Legal Responsible is accountable for his or her Group Companies' compliance with the BCRs. Staff must comply with the BCRs.

Every Group Company acting as a Controller is responsible for and must be able to demonstrate compliance with the BCRs.

1.6 Third party Beneficiary Rights

All Individuals whose personal data is transferred from a Group Company within the EEA to a Group Company outside the EEA and processed there, shall be able to enforce the following elements of the BCRs as third-party beneficiaries:

(i) The right to have Personal Data Processed according to data protection principles (Articles 2, 4 and 5), legal basis (Article 3), security (Article 8) and transfers of Personal Data (Article 10);
(ii) The right to transparency and easy access to the BCRs (Article 1.7);
(iii) The right to information (Article 6), access, rectification, erasure, restriction, notification regarding rectification or erasure or restriction, objection to processing, right not to be subject to decisions based solely on automated processing, including profiling (Article 7);
(iv) The provisions on conflicts between the BCRs and applicable law (Article 19) and government access requests (Article 20);
(v) The procedure for filing complaints to Yara (Article 16);
(vi) Cooperation duties with the competent Data Protection Authorities and jurisdiction and liability provisions (Article 17);
(vii) The right to information about any update of the BCRs and of the list of Group Companies (Article 1.7);
(viii) This third-party beneficiary clause; and
(ix) The right to judicial remedies, redress and compensation (Article 17).

For the avoidance of doubt, the rights referred to in this Article 1.6 do not extend to those elements of the BCRs pertaining to internal mechanisms implemented in Yara, such as detail of training, audit programs and compliance network.

1.7 Effective Date and Availability of the BCRs

The BCRs were adopted for the first time by the Head of Legal of Yara International ASA on November 16th 2017 (Effective Date). A public version of the BCRs (this document) and a list of all Group Companies shall be published on the Yara company website.

1.8 BCRs Supersedes Prior Procedures

The BCRs supersedes all Yara privacy procedures and notices that exist on the Effective Date to the extent they are in contradiction with the BCRs.

1.9 Implementation

The BCRs shall be implemented in the Yara organization based on the timeframes specified in Article 21.

2 Purposes for Processing of Personal Data

2.1 Legitimate Business Purposes

Personal Data shall only be collected, used or otherwise Processed for specified, explicit and legitimate purposes objectively justified by the activities of Yara (**Business Purposes**).

A non-exhaustive description of Yara's Business Purposes is set out in Annex 2. The Business Purposes is related to Yara's business domains:

(i) **Management System**
(ii) **Mission, Vision and Strategy**
(iii) **Communication**
(iv) **Sales and Marketing**
(v) **Procurement**
(vi) **Supply Chain**
(vii) **Production and Site Execution**
(viii) **Product Management and Quality**
(ix) **Finance**
(x) **Health, Environment, Safety, Security and Quality (HESQ)**
(xi) **Information and Digital Technology**
(xii) **HR**
(xiii) **Plant Engineering and Maintenance**

2.2 Use of Data for Secondary Purposes

Generally, Personal Data shall be used only for the Business Purposes for which they were originally collected (**Original Purpose**). Personal Data may be Processed for a legitimate Business Purpose of Yara different from the Original Purpose (**Secondary Purpose**) only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Personal Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Individual, the secondary use may require additional measures such as:

(i) limiting access to the Data;
(ii) imposing additional confidentiality requirements;
(iii) taking additional security measures;
(iv) informing the Individual about the Secondary Purpose;
(v) providing an opt-out opportunity; or
(vi) obtaining an Individual's Consent in accordance with Article 3.4.

2.3 Generally Permitted Uses of Data for Secondary Purposes

It is generally permissible to use Personal Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 2.2:

(i) transfer of the Data to an Archive;
(ii) internal audits or investigations;
(iii) implementation of business controls;
(iv) IT systems and infrastructure related Processing such as for maintenance, support,

life-cycle management and security (including resilience and incident management);
(v) statistical, historical or scientific research;
(vi) preparing for or engaging in dispute resolution;
(vii) legal or business consulting; or
(viii) insurance purposes.

2.4 Consultation

Where there is a question whether a Processing of Personal Data can be based on a Business Purpose or a Secondary Purpose listed above, it is necessary to seek the advice of the appropriate Regional Data Privacy Coordinator before the Processing takes place.

3 Legal basis for Processing of Personal Data and Sensitive Data

3.1 Legal Basis for Processing of Personal Data

Yara shall make sure that all Processing of Personal Data only takes place for legitimate Business Purposes and has legal basis.

Personal Data may be processed by Yara for legitimate Business Purposes on the following legal basis:

(i) the Individual has given his or her Consent. In order to rely on Consent, Yara must follow the procedure set forth in Article 3.4 below;
(ii) the Processing is necessary for the performance of an agreement between the Individual and Yara, or in order to take steps at the request of the Individual prior to entering into such an agreement;
(iii) the Processing is necessary for compliance with a legal obligation under Applicable Law in an EEA country to which Yara is subject;
(iv) the Processing is necessary in order to protect the vital interests of the Individual or of another natural person;
(v) 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 Yara under Applicable Law in an EEA country; or
(vi) the Processing is necessary for legitimate Business Purposes pursued by Yara or by a Third Party to whom the Personal Data are disclosed, except where such interests are overridden by the interests or fundamental rights and freedoms of the Individual.

3.2 Legal Basis for Processing of Sensitive Data

As a starting point Processing of Sensitive Data is prohibited. Yara can, however, for legitimate Business Purposes, Process Sensitive Data on the following legal basis:

(i) the Individual has given his or her explicit Consent. In order to rely on Consent, Yara must follow the procedure set forth in Article 3.4 below;
(ii) the Processing is necessary for the purposes of carrying out the obligations and specific rights of Yara in the field of employment, social security and social protection law in so far as it is authorized by Applicable Law in an EEA country providing for adequate safeguards;
(iii) the Processing is necessary to protect the vital interests of the Individual or of another person;
(iv) the Processing relates to Sensitive Data which are manifestly made public by the

Individual;

(v) the Processing of Sensitive Data is necessary for the establishment, exercise or defense of legal claims (including for dispute resolution) or Processing is necessary for compliance with a legal obligation to which Yara is subject;

(vi) the Processing is necessary for the performance of a task for reasons of substantial public interest set out in Applicable Law in an EEA country;

(vii) the Processing of Sensitive Data is required for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the Individual, 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 Applicable Law in an EEA country, and the Personal Data are Processed by a health professional subject to Applicable 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;

(viii) the Processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health, on the basis of Applicable Law in an EEA country; or

(ix) the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes and the Processing is in accordance with Applicable Law in an EEA country.

3.3 Personal Data relating to criminal convictions and offences

Yara shall establish internal procedures for the Processing of Personal Data relating to criminal convictions and offences in compliance with Applicable Law. Such data shall not be Processed unless an exemption under Article 10 GDPR applies.

3.4 Consent

If Consent is allowed or required under Applicable Law for Processing of Personal Data or Sensitive Data, the following conditions apply:

(i) When seeking Consent, Yara must inform the Individual of:

a) the identity and contact details of the Group Company being the Controller for the Processing;

b) the Business Purposes for which his or her Data are Processed;

c) the categories of Third Parties to which the Data are disclosed (if any).

d) other relevant information provided in Article 6.1, if necessary to ensure that the Individual's Consent is informed.

(ii) Yara must be able to demonstrate that the Individual has consented to Processing of his or her Personal Data. This may be done by documenting the Consent via a written declaration. Where Processing is undertaken at the request of an Individual (e.g., he or she subscribes to a service or seeks a benefit), he or she is deemed to have provided Consent to the Processing.

(iii) If the Individual's Consent is given in the context of a written declaration which also concerns other matters, the request for Consent shall, if Applicable Law so requires, be presented in a manner which is clearly distinguishable from the other matters, in an intelligible and easily accessible form, using clear and plain language.

3.5 Denial or Withdrawal of Consent

The Individual may both deny Consent and withdraw Consent at any time. The withdrawal of Consent shall not affect the lawfulness of the Processing based on such Consent before its

withdrawal.

Prior to giving Consent, the Individual shall be informed of its right to withdraw his or her Consent. It shall be as easy to withdraw as to give Consent.

3.6 Consultation

If it is doubtful whether Processing has legal basis in accordance with this Article 3 the appropriate Regional Data Privacy Coordinator shall be consulted before any Processing starts.

4 Categories of Personal Data and Sensitive Data Processed

4.1 Categories of Personal Data

Yara's Processing includes but is not limited to the following categories of Personal Data:

(i) **General contact information:** this includes but is not limited to name, address, email address, phone number, picture and date of birth;

(ii) **IT-related information:** this includes but is not limited to user profile/account information, electronic logs regarding a person's use of IT resources and information from Yara websites (cookie information);

(iii) **Sub-contractor's information:** this includes but is not limited to name, address, email, address, phone number and picture;

(iv) **Information necessary to administer the Supplier/Customer/Business Partner relationship**: this includes but is not limited to information related to the use and purchase of Yara's products and services; and

(v) **Employee information**: this includes but is not limited to key information necessary for employment management (e.g., salary information, CV, education level, performance reviews, recruitment information, bank account number, insurance and details of next of kin), registration of hours worked, absences, holiday, overtime, information relating to travels (e.g., bookings, itineraries, invoices, crisis management-related information), records of compulsory training, e-learning and safety certificates, employment history within Yara (e.g., start date, company and corporate seniority, job grade, position, organizational unit (department), immediate superior, contract details, employee type, job location, leaving date) and other Personal Data for statistical purposes (e.g., gender, nationality, age).

4.2 Categories of Sensitive Data

Yara's Processing includes but is not limited to the following categories of Sensitive Data:

(i) **Racial or ethnic data:** this includes but is not limited to photos and video images of Individuals which qualify as racial or ethnic data in certain countries;

(ii) **Health data**: this includes but is not limited to data relating to health and safety issues relating to Yara's products and services. With regard to Employees, it includes but is not limited to emergency situations, crisis management, any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy;

(iii) **Sexual preference:** this includes but is not limited to data relating to partners of Employees;

(iv) **Trade-union membership:** this includes but is not limited to data necessary to accommodate and administer Employee membership rights;

(v) **Religious or philosophical beliefs:** this includes but is not limited to data necessary to accommodate specific products or services (such as dietary requirements or religious holidays);

(vi) **Biometric Personal Data (e.g., fingerprints):** this includes but is not limited to data necessary for e.g., access control etc.

4.3 Categories of Personal Data relating to criminal convictions and offences

Yara's Processing may include the following categories of Personal Data relating to criminal convictions and offences:

(i) **Criminal data:** this includes but is not limited to data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior, including but not limited to the Processing of such data in relation to ethics hotline/whistleblowing, integrity due diligence (IDD), capital value process (CVP) and required screening activities (e.g., for access to Yara's premises or systems), decisions about Employees and the protection of the interests of Yara with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against Yara or its Employees.

4.4 Records of Processing Activities

The Group Companies shall maintain written records of Processing activities under their responsibility in accordance with GDPR Article 30. These records shall be available to the Data Protection Authority on request.

4.5 Controller Records of Processing Activities

When a Group Company acts as a Controller, it shall maintain a record containing all the following information:

(i) the name and contact details of the Controller and, where applicable, the joint controller, the Controller's representative and the data protection officer;

(ii) the purposes of the processing;

(iii) a description of the categories of Individuals and of the categories of personal data;

(iv) the categories of recipients to whom the personal data have been or will be disclosed including recipients in third countries or international organizations;

(v) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;

(vi) where possible, the envisaged time limits for erasure of the different categories of data;

(vii) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR

4.6 Processor Records of Processing Activities

When a Group Company acts as a Processor, it shall maintain a record containing all the following information:

(i) the name and contact details of the Processor or Processors 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;

(ii) the categories of processing carried out on behalf of each Controller;

(iii) where applicable, transfers of personal data to a third country or an international organization, including the identification of that third country or international organization and, in the case of transfers referred to in the second subparagraph of Article 49(1) GDPR, the documentation of suitable safeguards;

(iv) where possible, a general description of the technical and organizational security measures referred to in Article 32(1) GDPR.

5 Data Protection Principles, including Quantity and Quality of Data

5.1 Lawfulness, Fairness and Transparency

Yara shall Process Personal Data in a lawful, fair and transparent manner in relation to the Individual, including by ensuring that all Processing has the necessary legal basis under Article 3.

5.2 No Excessive Data

Yara shall restrict the Processing of Personal Data to Data that are adequate, relevant and limited to what is necessary for the applicable Business Purpose. Yara shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.

5.3 Storage Period

Yara generally shall retain Personal Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations.

Yara may specify (e.g., in a procedure, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Data shall be:

(ii) securely deleted or destroyed;

(iii) anonymized; or

(iv) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

5.4 Quality of Data

Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.

5.5 Accurate, Complete and Up-to-date Data

It is the responsibility of Individuals to ensure that their Personal Data is accurate, complete and up-to-date. Individuals shall inform Yara regarding any changes to their Personal Data in accordance with Article 7. Where Yara requires an Employee to update his own Personal Data, Yara shall remind him or her at least once a year to do so.

6 Individual Information Requirements

6.1 Information Requirements where Personal Data are collected from the Individual

At the time when Personal Data are collected from the Individual, Yara shall inform Individuals e.g., through a published data privacy notice, or by other means about:

(i) the identity and the contact details of the Group Company being the Controller for the Processing;
(ii) contact information for sending enquiries or filing complaints, including, where appropriate, the contact details of the appropriate Regional Data Privacy Coordinator and /or online portal for data privacy requests;
(iii) the Business Purposes for which their Personal Data are Processed and the legal basis for the Processing;
(iv) which legitimate Business Purposes are pursued when the Processing is based on 3.1(vi);
(v) the recipients or categories of recipients to which the Personal Data are disclosed (if any);
(vi) whether the recipient is located in a country outside the EEA and about the existence or absence of an Adequacy Decision. In the absence of an Adequacy Decision, a reference to the applicable transfer mechanism shall be provided, cf. Article 10.6.

In addition, when required by applicable law and if necessary to ensure fair and transparent Processing, Yara shall provide the Individual with the following further information:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
(ii) how Individuals can exercise their rights pursuant to Articles 3.5 and 7;
(iii) where the Processing is based on Consent, the existence of the right to withdraw Consent at any time as described in 3.5;
(iv) the right to lodge a complaint with a DPA;
(v) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, and whether the Individual is obliged to provide the Personal Data and of the possible consequences of failure to provide such data;
(vi) the existence of automated decision-making, including profiling, referred to in Article 7.8 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 Individual.

This Article 6.1 shall not apply where and insofar as the Individual already has the information.

6.2 Personal Data not Obtained from the Individual

Where the Personal Data have not been collected from the Individual, Yara shall inform Individuals e.g., through a published data privacy notice, or by other means about:

(i) the identity and the contact details of the Group Company being the Controller for the Processing;
(ii) contact information for sending enquiries or filing complaints, including, where appropriate, the contact details of the appropriate Data Privacy Coordinator and/or online portal for data privacy requests;
(iii) the Business Purposes for which their Personal Data are Processed and the legal basis for the Processing;
(iv) the categories of Personal Data concerned;
(v) the recipients or categories of recipients of the Personal Data (if any);
(vi) whether the recipient is located in a country outside the EEA and about the

existence or absence of an Adequacy Decision. In the absence of an Adequacy Decision, a reference to the applicable transfer mechanism shall be provided, cf. Article 10.6.

In addition, when necessary to ensure fair and transparent Processing, Yara shall provide the Individual with the following further information:

(i) the period for which the Personal Data will be stored, or if that is not possible, the criteria used to determine that period;
(ii) which legitimate Business Purposes are pursued when the Processing is based on Article 3.1 (vi);
(iii) the existence of the right to request from Yara, access to and rectification or erasure of Personal Data or restriction of Processing concerning the Individual or to object to Processing as well as the right to data portability;
(iv) where Processing 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;
(v) the right to lodge a complaint with a DPA;
(vi) from which source the Personal Data originate, and if applicable, whether it came from publicly accessible sources;
(vii) 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 Individual.

Yara shall provide the Individual with the information set out in this Article 6.2:

(i) within a reasonable time after obtaining the Personal Data, at the latest within one month from obtaining the Personal Data;
(ii) if the Personal Data are used for communication with the Individual, at the latest at the time of the first communication to the Individual;
(iii) if a disclosure to another recipient is envisaged, at the latest when the Personal Data are first disclosed.

This Article 6.2 shall not apply where:

(i) the Individual already has the information;
(ii) providing such information proves impossible or would involve a disproportionate effort;
(iii) obtaining or disclosure is expressly laid down by Applicable Law in an EEA country and which provides appropriate measures to protect the Individual's legitimate interests; or
(iv) where the Personal Data must remain confidential subject to an obligation of professional secrecy regulated by Applicable Law, including a statutory obligation of secrecy.

6.3 Information related to use for Secondary Purposes

Where Yara intends to further Process the Personal Data for a Secondary Purpose, Yara shall, if Applicable Law so requires, provide the Individual prior to the further Processing with information on the Secondary Purpose and any relevant information as set out in Article 6.1.

7 Rights of Individuals

7.1 Right of Access

Every Individual has the right to know whether or not Personal Data concerning him or her are being Processed by Yara, and where that is the case, access to the Personal Data and the following information:

(i) for which purpose(s) the Personal Data are Processed;
(ii) the categories of the Personal Data concerned;
(iii) the recipients or categories of recipients to whom the Personal Data have been or will be disclosed, in particular recipients in third countries or international organizations;
(iv) where possible, the envisaged period for which the Personal Data will be stored, or, if not possible, the criteria used to determine that period;
(v) the existence of the right to request from Yara rectification or erasure of Personal Data, or restriction of Processing concerning the Individual or to object to such Processing;
(vi) the right to lodge a complaint with a supervisory authority;
(vii) where the Personal Data are not collected from the Individual, any available information as to their source;
(viii) 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 Individual;
(ix) where the Personal Data are transferred to a third country, information about the appropriate safeguards relating to the transfer.

The Individual shall upon a request for access be provided with a copy of the Personal Data Processed. For any further copies requested by the Individual, Yara may charge a reasonable fee based on administrative costs.

The right to obtain a copy shall not adversely affect the rights and freedoms of others, cf. the GDPR article 15(4). The right to obtain a copy may be restricted under Applicable Law pursuant to GDPR article 23.

7.2 Right to Rectification

An Individual shall have the right to obtain from Yara without undue delay the rectification of inaccurate Personal Data concerning him or her. Taking into account the purposes of the Processing, the Individual shall also have the right to have incomplete Personal Data completed, including by means of providing a supplementary statement.

7.3 Right to Erasure

The Individual may request from Yara the erasure of Personal Data concerning him or her. Yara shall erase Personal Data without undue delay where one of the following grounds applies:

(i) the Personal Data are no longer necessary in relation to the Business Purposes for which they were collected or otherwise Processed;
(ii) the Individual withdraws Consent on which the Processing is based and where there is no other legal ground for the Processing;
(iii) the Individual objects to the Processing in accordance with Article 7.5 and there

are no Overriding Interests for the Processing, cf. Article 11;

(iv) the Personal Data have been unlawfully Processed;

(v) the Personal Data have to be erased for compliance with a legal obligation in Applicable Law in an EEA country to which the Controller is subject;

(vi) the Personal Data have been collected in relation to the offer of information society services referred to in the GDPR article 8(1).

Where Yara has made the Personal Data public and is obliged to erase such Data, Yara, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform other Controllers which are Processing the Personal Data that the Individual has requested the erasure by such Controllers of any links to, or copy or replication of, those Personal Data.

This Article 7.3 shall not apply to the extent that Processing is necessary:

(i) for exercising the right of freedom of expression and information;

(ii) for compliance with a legal obligation set out in Applicable Law to which the Controller is subject, and which requires Processing for the performance of a task carried out in the public interest or in the exercise of official authority vested in the Controller;

(iii) for reasons of public interest in the area of public health in accordance with GDPR article 9(2) and (3);

(iv) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with the GDPR article 89(1) in so far as the right referred to in the first paragraph of this Article 7.3 is likely to render impossible or seriously impair the achievement of the objectives of that Processing; or for the establishment, exercise or defense of legal claims.

7.4 Right to Restrict Processing

The Individual has the right to obtain from Yara restriction of Processing where one of the following applies:

(i) the accuracy of the Personal Data is contested by the Individual, for a period enabling Yara to verify the accuracy of the Personal Data;

(ii) the Processing is unlawful and the Individual opposes the erasure of the Personal Data and requests the restriction of their use instead;

(iii) Yara no longer needs the Personal Data for the purposes of the Processing, but the Data are required by the Individual for the establishment, exercise or defense of legal claims;

(iv) the Individual has objected to Processing pursuant to the GDPR article 21(1), cf. Article 7.5 of these BCRs, pending the verification whether the legitimate grounds of the Controller override those of the Individual (cf. Article 11).

Where Processing has been restricted subject to the above, such Personal Data shall, with the exception of storage, only be Processed with the Individual's Consent or for the

establishment, exercise or defense of legal claims or for the protection of the rights of another natural or legal person or for reasons of important public interest.

Yara shall inform an Individual who has obtained restriction of Processing pursuant to the above before the restriction of Processing is lifted.

7.5 Notification regarding Rectification, Erasure and Restriction

The Controller shall communicate any rectification or erasure of Personal Data or restriction of Processing carried out in accordance with Articles 7.2, 7.3 or 7.4 to each recipient to whom the Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. The Controller shall inform the Individual about those recipients if the Individual requests it.

7.6 Right to Object

An Individual has the right to object, on grounds relating to his or her particular situation, at any time to Processing of Personal Data concerning him or her which is based on Article 3.1 (v) or (vi), including profiling based on those Articles.

Yara shall no longer Process the Personal Data unless it can demonstrate Overriding Interests in accordance with Article 11 or if it is necessary for the establishment, exercise or defense of legal claims.

Where Personal Data are Processed for direct marketing, the Individual shall have the right to object at any time to Processing as set out in Article 9 of these BCRs. If an Individual objects to Processing for direct marketing purposes, the Personal Data shall no longer be Processed for such purposes.

In the context of the use of information society services (as defined in the GDPR article 4(25)), the Individual may exercise his or her right to object by automated means using technical specifications.

Where Personal Data are Processed for scientific or historical research purposes or statistical purposes pursuant to the GDPR article 89(1), the Individual, on grounds relating to his or her particular situation, shall have the right to object to Processing of Personal Data concerning him or her, unless the Processing is necessary for the performance of a task carried out for reasons of public interest.

7.7 Right to Data Portability

An Individual may request from Yara to receive the Personal Data concerning him or her, which he or she has provided to Yara, in a structured, commonly used and machine-readable format and have the right to transmit those Data to another Controller without hindrance from Yara, where:

(i) the Processing is based on Consent or on a contract pursuant to point (ii) of Article 3.1; and
(ii) the Processing is carried out by automated means.

If technically feasible, Yara shall transmit the Personal Data directly to the other Controller.

The right referred to in this Article shall not adversely affect the rights and freedoms of other

Individuals.

7.8 Right Not to be Subject to Decisions Based Solely on Automated Processing

The Individual 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.

The previous paragraph shall not apply if the decision:

(i) is necessary for entering into, or performance of, a contract between the Individual and a Controller;
(ii) is authorised by European Union law or the national law in an EEA Member State law to which the Controller is subject and which also lays down suitable measures to safeguard the Individual's rights and freedoms and legitimate interests; or
(iii) is based on the Individual's explicit consent.

In the cases referred to in (i) and (iii) of the previous paragraph, the Controller shall implement suitable measures to safeguard the Individual's rights and freedoms and legitimate interests, at least the right to obtain human intervention on the part of the Controller, to express his or her point of view and to contest the decision.

Decisions referred to in the second paragraph of this Article shall not be based on Sensitive Data, unless point (i) or (vi) of Article 3.2 applies and suitable measures to safeguard the Individual's rights and freedoms and legitimate interests are in place.

7.9 Procedure

The Individual should send his or her request to the contact person or contact point indicated in the relevant privacy notice or online portal made available by Yara. If no contact person or contact point is indicated, the Individual may send his or her request through dataprivacy@yara.com.

Yara may fulfill the Individual's rights by providing self service solutions which, e.g. allows the Individual to access, update, correct, delete and otherwise manage his or her Personal Data.

Yara shall respond to the request in a concise, transparent, intelligible and easily accessible form, using clear and plain language, in particular for any information addressed specifically to a child. The information shall be provided in writing, or by other means, including, where appropriate, by electronic means. When requested by the Individual, the information may be provided orally, provided that the identity of the Individual is proven by other means.

Prior to fulfilling the request of the Individual, Yara may require the Individual to:

(i) specify the categories of Personal Data to which he or she is seeking access;
(ii) specify, to the extent reasonably possible, the data system in which the Data are likely to be stored;
(iii) specify the circumstances in which Yara obtained the Personal Data;
(iv) show proof of his or her identity; and
(v) in the case of a request for rectification, deletion or blockage, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with Applicable Law or the BCRs.

7.10 Response Period

Within four weeks of receiving the request, Yara shall inform the Individual in writing or electronically either (i) of Yara's position with regard to the request and any action Yara has taken or will take in response, or (ii) the ultimate date on which he or she will be informed of Yara's position. Provided that the requirements relating to requests in Article 7.9 have been fulfilled, such ultimate date shall be no later than eight weeks after the communication was sent to the Individual.

7.11 Complaint

An Individual may file a complaint in accordance with Article 16 if:

(i) the response to the request is unsatisfactory to the Individual (e.g., the request is denied);

(ii) the Individual has not received a response as required by Article 7.10; or

(iii) the time period provided to the Individual in accordance with Article 7.10 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period, in which he or she will receive a response.

7.12 Denial of Requests

Yara may deny an Individual's request if:

(i) the request does not meet the requirements of the above Articles 7.1-7.8;

(ii) the request is not sufficiently specific;

(iii) the identity of the relevant Individual cannot be established by reasonable means; or

(iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights. A time interval between requests of six months or less concerning the same matter shall generally be deemed to be an unreasonable time interval.

8 Security and Confidentiality Requirements

8.1 Personal Data Security

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 Individuals posed by the Processing, Yara shall take appropriate commercially reasonable technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access.

Yara has developed and implemented the Yara IT Operating Standards and other notices and procedures relating to the protection of Personal Data.

8.2 Staff Access

Yara shall provide Staff with access to Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

8.3 Confidentiality Obligations

Yara shall impose confidentiality obligations on Staff with access to Personal Data.

8.4 Personal Data Breach Notification to Data Protection Authorities

If a Personal Data Breach has occurred or is suspected to have occurred, the person who has become aware of or suspects the Personal Data Breach, shall immediately notify the Head of Data Privacy or the appropriate Regional Data Privacy Coordinator who shall forward the notification to the Head of Data Privacy. The Head of Data Privacy shall involve affected Group Companies to the extent necessary to investigate, handle and mitigate the Personal Data Breach.

The Head of Data Privacy shall notify a competent Data Protection Authority of a Personal Data Breach without undue delay and, where feasible, not later than 72 hours after having become aware of it, unless the Personal Data Breach is unlikely to result in a risk to Individuals' rights. If a notification is not made within 72 hours, it shall be accompanied by reasons for the delay. The notification shall at least:

(i) Describe the nature of the Personal Data Breach, including where possible:
  (a) the categories and approximate number of Individuals concerned; and
  (b) the categories and approximate number of Personal Data records concerned;
(ii) Contain the name and contact details of the Head of Data Privacy or appropriate Regional Data Privacy Coordinator where more information can be obtained;
(iii) Describe the likely consequences of the Personal Data Breach;
(iv) Describe the measures taken or proposed to be taken by Yara to address the Personal Data Breach, including measures to mitigate its possible adverse effects, where appropriate.

Yara shall document any Personal Data Breaches, comprising the facts relating to the Personal Data Breach, its effects and the remedial action taken. That documentation shall be available to the competent Data Protection Authority upon request.

8.5 Personal Data Breach Notification to Individuals

Yara shall notify the Individual of a Personal Data Breach without undue delay following discovery of such breach, if the Personal Data Breach is likely to result in a high risk to the rights and freedoms of the Individual. This applies unless one or more of the following conditions are met:

(i) Yara has implemented and applied appropriate technical and organizational protection measures (such as encryption) to the Personal Data affected by the Personal Data Breach;
(ii) Yara has taken subsequent measures which ensure that the high risk to the rights and freedoms of Individuals is no longer likely to materialize; or
(iii) Notifying the Individual would involve disproportionate effort. In such a case, there shall instead be a public communication or similar measure whereby Individuals are informed in an equally effective manner.

The Personal Data Breach notification to the Individuals shall describe in clear and plain language the nature of the Personal Data Breach and shall at least contain the information and measures referred to in Article 8.4 (ii), (iii) and (iv).

8.6 Data Protection by Design and by Default

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 Individuals posed by the Processing, Yara shall, both at the time of the

determination of the means and for Processing and the time of the Processing itself, implement appropriate technical and organizational measures which are designed to implement data protection principles and to facilitate compliance, in practice, with the requirements set up by the BCRs in accordance with Applicable Law.

8.7 Data Protection Impact Assessment

Where a type of Processing subject to the BCRs, in particular using new technologies, and taking into account the nature, scope, context and purposes of the Processing, is likely to result in a high risk to the rights and freedoms of Individuals, Yara shall, prior to the Processing, carry out an assessment of the impact of the envisaged Processing operations on the protection of personal data. A single assessment may address a set of similar Processing operations that present similar high risks. Yara shall seek advice from the Head of Data Privacy or Regional Data Privacy Coordinator when carrying out a Data Protection Impact Assessment.

8.8 Prior Consultation

Where an impact assessment under Article 8.7 indicates that the processing would result in a high risk in the absence of measures taken by the Controller to mitigate the risk, the Group Company acting as a Controller shall, prior to processing, consult the Competent Data Protection Authority in accordance with Article 36 GDPR.

9 Direct Marketing

9.1 Direct Marketing

This Article sets forth requirements concerning the Processing of Personal Data for direct marketing purposes (e.g., contacting the Individual by email, fax, phone, SMS or otherwise, with a view of solicitation for commercial or charitable purposes).

9.2 Consent for Direct Marketing (opt-in)

If Applicable Law so requires, Yara shall only send to Individuals unsolicited commercial communication by fax, email, SMS and MMS with the prior Consent of the Individual ("opt-in"). If Applicable Law does not require prior Consent of the Individual, Yara shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.

9.3 Exception

Prior Consent of the Individual for sending unsolicited commercial communication by fax, email, SMS and MMS is not required if:

(i) an Individual has provided his or her electronic contact details to a Group Company in the context of a sale of a product or service of such Group Company; and

(ii) such contact details are used for direct marketing of such Group Company's own similar products or services; and

(iii) the Individual clearly and distinctly has been given the opportunity to object free of charge, and in an easy manner, to such use of his or her electronic contact details when they are collected by the Group Company.

9.4 Information to be Provided in Each Communication

In every direct marketing communication that is made to the Individual, the Individual shall be offered the opportunity to opt-out of further direct marketing communications.

9.5 Objection to Direct Marketing

If an Individual objects to receiving marketing communications from Yara, or withdraws his or her Consent to receive such communications, Yara will take steps to refrain from sending further marketing communications as specifically requested by the Individual. Yara will do so within the time period required by Applicable Law.

9.6 Third Parties and Direct Marketing

No Personal Data shall be provided to, or used on behalf of, Third Parties for the Third Parties' own direct marketing purposes without the prior Consent of the Individual.

9.7 Personal Data of Children

Yara shall not use any Personal Data of Children for direct marketing, without the prior Consent of their parent or custodian.

9.8 Direct Marketing Records

Yara shall keep a record of Individuals that used their "opt-in" or "opt-out" right and will regularly check the public opt-out registers in accordance with Applicable Law.

10 Transfer of Personal Data to Third Parties

10.1 Transfer to Third Parties

This Article sets forth requirements concerning the transfer of Personal Data from Yara to a Third Party. Note that a transfer of Personal Data includes situations in which Yara discloses Personal Data to Third Parties (e.g., in the context of corporate due diligence) or where Yara provides remote access to Personal Data to a Third Party.

10.2 Third Party Controllers and Third Party Processors

There are two categories of Third Parties:

(i) **Third Party Processors:** these are Third Parties that Process Personal Data solely on behalf of Yara and at its direction (e.g., Third Parties that Process online registrations made by Customers);

(ii) **Third Party Controllers:** these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., Yara Business Partners that provide their own goods or services directly to Customers).

10.3 Transfer for Applicable Business Purposes Only

Yara shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 2 or purposes for which the Individual has provided Consent in accordance with Article 3.4).

10.4 Third Party Controller Contracts

Third Party Controllers (other than government agencies) may Process Personal Data transferred by Yara only if they have a written or electronic contract with Yara. In the contract, Yara shall seek to contractually safeguard the data protection interests of its Individuals when Personal Data is Processed by Third Party Controllers. Individual Business Contact Data may be transferred to a Third Party Controller without a contract if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate Business Purposes related to the Individual's job responsibilities.

10.5 Third Party Processor Contracts

Third Party Processors may Process Personal Data transferred by Yara only if they have a written or electronic contract with Yara (**Data Processing Agreement)**. The contract with a Third Party Processor must include the following provisions:

(i) the Third Party Processor shall Process Personal Data only in accordance with Yara's instructions and for the purposes authorized by Yara;

(ii) the Third Party Processor shall keep the Personal Data confidential;

(iii) the Third Party Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;

(iv) the Third Party Processor shall not permit subcontractors to Process Personal Data in connection with its obligations to Yara without the prior written Consent of Yara;

(v) Yara has the right to review the security measures taken by the Third Party Processor (a) by an obligation of the Third Party Processor to submit its relevant data Processing facilities to audits and inspections by Yara, a Third Party on behalf of Yara or any relevant government authority; or (b) by means of a statement issued by a qualified independent Third Party assessor on behalf of the Third Party Processor certifying that the data Processing facilities of the Third Party Processor used for the Processing of the Personal Data comply with the requirements of the Data Processing Agreement;

(vi) the Third Party Processor shall promptly inform Yara of any actual or suspected Personal Data Breach; and

(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide Yara with all relevant information and assistance as requested by Yara regarding the Personal Data Breach.

10.6 Transfer of Data to Third Parties Located Outside the EEA that are not Covered by Adequacy Decisions

This Article sets forth additional rules for Personal Data that is (a) collected originally in connection with activities of a Group Company located in the EEA; and (b) transferred to a Third Party located in a country, territory or sector outside the EEA that is not covered by an Adequacy Decision. Personal Data may be transferred to such Third Party if there is a legal basis for the transfer in accordance with the GDPR Chapter V, such as one of the following alternatives:

(i) the Third Party has implemented Binding Corporate Rules or a similar transfer mechanism that provides appropriate safeguards under Applicable Law;

(ii) Yara and the Third Party have provided appropriate safeguards by entering into EU Standard Contractual Clauses (model contract);

(iii) Yara and the Third Party have provided appropriate safeguards by entering into Standard Data Protection Clauses adopted by the EU Commission or a DPA;

(iv) the Third Party has been certified under the EU-US Data Privacy Framework or any other similar program that is covered by an Adequacy Decision; or

(v) an approved code of conduct or an approved certification mechanism pursuant to Article 46(1)(e) and (f) of the General Data Protection Regulation (**GDPR**) are provided for.

In specific situations where a transfer cannot be based on (i) to (v) above, transfer may take place on one or more of the following conditions:

(vi) the transfer is necessary for the performance of a contract between Yara and the

Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for Processing orders;

(vii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between Yara and a Third Party (e.g., in case of recalls);

(viii) the transfer is necessary for important reasons of public interest;

(ix) the transfer is necessary for the establishment, exercise or defense of a legal claim;

(x) the transfer is necessary to protect a vital interest of the Individual; or

(xi) the transfer is required by any law to which the relevant Group Company is subject.

10.7 Consent for Transfer

If none of the grounds listed in Article 10.6 exist or if applicable local law so requires Yara shall (also) seek the explicit Consent from the Individual for the transfer to a Third Party located in a country outside the EEA that is not covered by an Adequacy Decision.

Yara generally shall not seek Employee Consent for such transfers, in any case not if the transfer has foreseeable adverse consequences for the Employee. However, if none of the grounds for transfer listed in Article 10.6 exist or Consent is allowed or required under applicable local law, Yara shall (also) seek the explicit Employee Consent for the relevant transfer. The Consent must be requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Prior to requesting Consent, the Individual shall be informed of the possible risks of the transfer due to the absence of an Adequacy Decision and appropriate safeguards. When requesting Consent, the procedure set out in Article 3.4 shall be followed. The requirements set out in Article 3.5 apply to the granting, denial or withdrawal of Individual Consent.

10.8 Transfers where Both Group Companies and Third Party are Located in Countries not Covered by an Adequacy Decision

This Article sets forth additional rules for transfers of Personal Data that were collected in connection with the activities of a Group Company located in a country outside the EEA that is not covered by an Adequacy Decision to a Third Party also located in a country outside the EEA that is not covered by an Adequacy Decision. In addition to the grounds listed in Article10.6, these transfers are permitted if they are:

(i) necessary for compliance with a legal obligation to which the relevant Group Company is subject;

(ii) necessary to serve the public interest; or

(iii) necessary to satisfy a Business Purpose of Yara.

11 Overriding Interests

11.1 Overriding Interests

Some of the obligations of Yara or rights of Individuals as specified in Article 11.2 may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Individual (**Overriding Interest**). An Overriding Interest exists if there is a need to:

(i) Protect the legitimate business interests of Yara including
  (a) the health, security or safety of Employees or Individuals;
  (b) Yara's intellectual property rights, trade secrets or reputation;
  (c) the continuity of Yara's business operations;
  (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or
  (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes;
(ii) Prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law, breaches of the terms of employment, or non-compliance with the Yara Code of Conduct or other Yara notices or procedures applicable to Employees; or
(iii) Otherwise protect or defend the rights or freedoms of Yara, its Employees or other persons.

11.2 Exceptions in the Event of Overriding Interests

If an Overriding Interest exists, one or more of the following obligations of Yara or rights of the Individual may be set aside:

(i) Article 2.2 (the requirement to Process Personal Data for closely related purposes);
(ii) Article 6 (information provided to Individuals, Personal Data not obtained from the Individuals);
(iii) Article 7 (rights of Individuals);
(iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements);
(v) Articles 10.4, 10.5 and 10.6 (ii) (contracts with Third Parties); and
(vi) Article 3.2 (Sensitive Data) and 3.3, but only for the Overriding Interests listed in Article 11.1 (i) (a), (b), (c) and (e), (ii) and (iii).

11.3 Consultation with Head of Data Privacy

Setting aside obligations of Yara or rights of Individuals based on an Overriding Interest requires prior consultation of the Head of Data Privacy. The Head of Data Privacy shall document his or her advice.

11.4 Information to Individual

Upon request of the Individual, Yara shall inform the Individual of the Overriding Interest for which obligations of Yara or rights of the Individual have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 and 7.1, in which case the request shall be denied.

12 Supervision and Compliance

12.1 Head of Data Privacy

Yara International ASA shall appoint a Head of Data Privacy who shall, inter alia, inform and advise Yara of its obligations pursuant to the BCRs and monitor compliance with the BCRs in Yara, including the assignment of responsibilities, awareness-raising and training of Staff involved in Processing operations, complaint handling and audits.

12.2 Regional Data Privacy Coordinator

The Head of Data Privacy shall appoint Regional Data Privacy Coordinators who shall, inter alia, inform and advise the Group Companies within a defined region of their obligations

pursuant to the BCRs and monitor compliance with the BCRs in the defined region, including handling Individuals' requests and complaints as described in Article7.

13 Procedures and Guidelines

13.1 Procedures and Guidelines

Yara shall develop and implement procedures and notices to comply with the BCRs.

13.2 System information

Yara shall maintain information regarding the structure and functioning of systems and processes that Process Personal Data.

14 Training

14.1 Staff Training

Yara shall provide training on the obligations and principles laid down in the BCRs, related to confidentiality and other privacy and data security obligations to Staff members who have access to or responsibilities associated with managing Personal Data.

15 Monitoring and Auditing Compliance

15.1 Audits

Yara shall regularly carry out internal audits related to compliance with the BCRs. Upon specific request, a copy of the data privacy audit results will be provided by the Head of Data Privacy to the Norwegian Data Protection Authority and a Data Protection Authority competent to audit, according to Yara internal procedures.

15.2 Mitigation

Yara shall, if so indicated, ensure that adequate steps are taken to address breaches of the BCRs identified during the monitoring and auditing of compliance.

16 Procedure for Filing Complaints to Yara

16.1 Filing a Complaint

Individuals may file a complaint regarding compliance with these BCRs or violations of their rights under applicable local law in accordance with the complaints procedure set forth in the relevant privacy notice or contract, or by sending an email to dataprivacy@yara.com. Employees may use email or online portals made available by Yara. An Employee may always file a complaint to the line manager who shall deal with the complaint adequately. The complaint shall be forwarded to the appropriate Regional Data Privacy Coordinator and/or other relevant Yara Employee(s).

The appropriate Regional Data Privacy Coordinator, and/or other person dealing with the matter shall to the extent required:

(i) notify the Head of Data Privacy;
(ii) initiate an investigation; and
(iii) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

The appropriate Regional Data Privacy Coordinator, and/or other person dealing with the

matter may consult with any government authority having jurisdiction over a particular matter about the measures to be taken.

16.2 Reply to Individuals

Within four weeks of Yara receiving a complaint, the appropriate Regional Data Privacy Coordinator shall inform the Individual in writing or electronically either (i) of Yara's position with regard to the complaint and any action Yara has taken or will take in response or (ii) the ultimate date on which he or she will be informed of Yara's position. Provided that Yara has all relevant information to handle the complaint, cf. Article 7.9, such ultimate date shall be no later than eight weeks after the communication was sent to the Individual. The appropriate Regional Data Privacy Coordinator shall send a copy of the complaint and his or her written reply to the Head of Data Privacy.

16.3 Complaint to the Head of Data Privacy

An Individual may file a complaint with the Head of Data Privacy if:

(i) the resolution of the complaint by the appropriate Regional Data Privacy Coordinator is unsatisfactory to the Individual (e.g., the complaint is rejected);

(ii) the Individual has not received a response as required by Article 16.2;

(iii) the time period provided to the Individual pursuant to Article 16.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or

(iv) one of the events listed in Article 7.12 applies.

The procedure described in Articles 16.1 through 16.2 shall apply to complaints filed with the Head of Data Privacy.

17 Legal Issues and Cooperation

17.1 Complaints Procedure

Individuals are encouraged to first follow the complaints procedure set forth in Article 16 of the BCRs before filing any complaint or claim with the competent DPAs or the courts.

17.2 Local Law and Jurisdiction

The rights contained in this Article are in addition to, and shall not prejudice, any other rights or remedies that an Individual may otherwise have by law.

In case of a violation of these BCRs, the Individual may, at his or her choice, lodge a complaint

(i) with a Data Protection Authority, in particular in the EU/EEA member state of the Individual's habitual residence, place of work or place of the alleged infringement; and

(ii) before the competent court of the EU/EEA member states where the Yara controller or processor has an establishment, or where the Individual has its habitual residence.

The DPAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Individual will not prejudice the substantive or procedural rights he or she may have under Applicable Law.

Yara accepts that Individuals may be represented by a not-for-profit body, organization or association under the conditions set out in Article 80(1) GDPR.

17.3 Liability

Yara International ASA is responsible for and agrees to take the necessary action to remedy the acts of Group Companies established outside the EEA and to pay compensation in accordance with applicable EU/EEA law, for any material and non-material damages suffered by the Individual resulting from the violation of these BCRs by Group Companies established outside the EEA.

17.4 Right to Claim Damages and Burden of Proof

In case an Individual brings a claim for damages under Article 17.3, such Individual shall be entitled to compensation of damages to the extent provided by applicable EU/EEA law, provided that he or she has suffered actual damages and can establish facts which show that it is plausible that the damage has occurred because of a violation of these BCRs.

If a Group Company outside the EEA violates these BCRs, the courts or other judicial authorities in the EEA will have jurisdiction, and Individuals will have the rights and remedies against Yara International ASA as if the violation had been caused by Yara International ASA in Norway, instead of the Group Company outside the EEA.

To the extent permitted by Applicable Law, the compensation shall be limited to direct damages which exclude, without limitation, lost profits or revenue, lost turnover, cost of capital and downtime cost. It will subsequently be for Yara International ASA to prove that the damages suffered by the Individual due to a violation of these BCRs are not attributable to any Group Company established outside the EEA in order to avoid liability.

17.5 Mutual Assistance and Redress

All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:

(i) a request, complaint or claim made by an Individual; or
(ii) a lawful audit, investigation or inquiry by a competent government authority.

The Group Company which receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his or her request, complaint or claim except where circumstances dictate otherwise.

The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse Yara International ASA.

17.6 Advice of the Lead Data Protection Authority and Duty to Cooperate with the Competent Data Protection Authority

Yara shall abide by the advice of the Norwegian Data Protection Authority issued on the interpretation and application of these BCRs, and further abide by binding decisions of DPAs competent pursuant to Article 17.2. DPAs competent pursuant to Article 17.2 may conduct audits in order to ascertain Yara's compliance with these BCRs.

All Group Companies shall cooperate with, to accept to be audited and to be inspected,

including where necessary, on-site, by the competent DPA, including to take into account their advice, and to abide by decisions of these DPAs on any issue related to the BCRs.

All Group Companies shall upon request provide the competent DPA with any information about the Processing operations covered by the BCRs.

Any dispute related to the competent DPA's exercise of supervision of compliance with the BCRs will be resolved by the courts of the Member State of that DPA, in accordance with that Member State's procedural law. The Group Companies agree to submit themselves to the jurisdiction of these courts.

17.7 Mitigation

Yara International ASA shall ensure that adequate steps are taken to address violations of the BCRs by a Group Company.

17.8 Law Applicable to th BCRs

The BCRs shall be governed by and interpreted in accordance with Norwegian law.

18 Non-compliance

18.1 Staff Non-Compliance

Non-compliance of Staff with these BCRs may result in disciplinary action up to and including termination of employment.

18.2 Compliance Requirement

No transfer shall be made to a Group Company unless the Group Company is effectively bound by the BCRs and can deliver compliance.

18.3 Notification and Suspension

A data importing Group Company must promptly inform the data exporting Group Company if it is unable to comply with the BCRs, for whatever reason.

Where the data importing Group Company is in breach of the BCRs or unable to comply with it, the data exporting Group Company shall have the right to suspend the transfers.

18.4 Return or Deletion in case of Non-Compliance

The data importing Group Company shall, at the choice of the data exporting Group Company, immediately return or delete the personal data that has been transferred under the BCRs in its entirety, where:

(i) the data importing Group Company has suspended the transfer, and compliance with these BCRs is not restored within a reasonable time, and in any event within one month of suspension; or

(ii) the data importing Group Company is in substantial or persistent breach of the BCRs; or

(iii) the data importing Group Company fails to comply with a binding decision of a competent court or competent Data Protection Authority regarding its obligations under the BCRs.

The same commitments shall apply to any copies of the data. The data importing Group Company shall certify the deletion of the data to the data exporting Group Company.

Until the data is deleted or returned, the data importing Group Company shall continue to ensure compliance with the BCRs.

In case of Applicable Law prohibiting the return or deletion of the transferred personal data, the data importing Group Company shall warrant that it will continue to ensure compliance with the BCRs and will only process the data to the extent and for as long as required under that Applicable Law.

19 Conflicts between the BCRs and Applicable Local Law

19.1 Obligation to Assess Third Country Law and Practices

A Group Company can only use the BCRs as a tool for transfers where it has assessed that the law and practices in the third country of destination applicable to the processing of the personal data by the Group Company acting as data importer, including any requirements to disclose personal data or measures authorising access by public authorities, do not prevent it from fulfilling its obligations under the BCRs.

For the sake of clarity, 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 one of the objectives listed in Article 23(1) GDPR, are not in contradiction with the BCRs.

19.2 Non-Exhaustive List of Elements in the Assessment

In assessing the laws and practices of the third country which may affect the respect of the commitments contained in the BCRs, the Group Company must take due account, in particular, of the following elements:

(i) 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:

- (a) purposes for which the data are transferred and processed (e.g. marketing, HR, storage, IT support, clinical trials);
- (b) types of entities involved in the processing (the data importer and any further recipient of any onward transfer);
- (c) economic sector in which the transfer or set of transfers occur;
- (d) categories and format of the personal data transferred;
- (e) location of the processing, including storage; and
- (f) transmission channels used.

(ii) The laws and practices of the third country of destination relevant in light of the circumstances of the transfer, including those requiring to disclose data to public authorities or authorising access by such authorities and those providing for access to these data during the transit between the country of the data exporter and the country of the data importer, as well as the applicable limitations and safeguards.

(iii) Any relevant contractual, technical or organizational 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 country of destination.

19.3 Consultation with Head of Data Privacy

Where any safeguards in addition to those envisaged under the BCRs must be put in place in accordance with Articles 19.1 and 19.2, Head of Data Privacy must be informed and involved in the assessment.

19.4 Obligation to Document the Assessment

The Group Companies must document appropriately the assessment in accordance with Articles 19.1 and 19.2, as well as the supplementary measures selected and implemented, and must make such documentation available to the competent Data Protection Authority upon request.

19.5 Notification to the Data Exporter and Supplementary Measures

Any Group Company acting as data importer must promptly notify the data exporter if, when using the BCRs as a tool for transfers, and for the duration of the BCR 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 (such as a disclosure request). This information must also be provided to Yara International ASA.

Upon verification of such notification, the Group Company acting as data exporter, along with Yara International ASA, Head of Data Privacy and the relevant Regional Data Privacy Coordinator, must commit to promptly identify supplementary measures (e.g. technical or organizational measures to ensure security and confidentiality) to be adopted by the Group Company acting as data exporter and/or data importer, in order to enable them to fulfil their obligations under the BCRs. The same applies if a Group Company acting as data exporter has reasons to believe that a Group Company acting as its data importer can no longer fulfil its obligations under the BCRs.

19.6 Suspension of transfers

Where the Group Company acting as data exporter, along with Yara International ASA, Head of Data Privacy and the relevant Regional Data Privacy Coordinator, assesses that the BCRs – even if accompanied by supplementary measures – cannot be complied with for a transfer or set of transfers, or if instructed by the Competent Data Protection Authority, it commits to suspend the transfer or 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 Group Company acting as data exporter must end the transfer or set of transfers if the BCRs cannot be complied with and compliance with the BCRs is not restored within one month of suspension. In this case, personal data that have been transferred prior to the suspension, and any copies thereof, must, at the choice of the Group Company acting as data exporter, be returned to it or destroyed in their entirety.

19.7 Information to All Group Companies

Yara International ASA, Head of Data Privacy and the relevant Regional Data Privacy Coordinator must inform all other Group Companies of the assessment carried out under Articles 19.1 to 19.6 and of its results, so that the identified supplementary measures will be applied in case the same type of transfers is carried out by any other Group Company or, where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended.

19.8 Duty to Monitor Developments

Group Companies acting as data exporters must monitor, on an ongoing basis, and where appropriate in collaboration with Group Companies acting as data importers, developments in the third countries to which the data exporters have transferred personal data that could affect the initial assessment of the level of protection and the decisions taken accordingly on such transfers.

20 Government Access Requests

20.1 Notification of Government Request

A data importing Group Company will promptly notify the data exporting Group Company and Head of Data Privacy and, where possible, the Individuals (if necessary with the help of the data exporting Group Company) if it

(i) receives a legally binding request by a public authority under the laws of the country of destination, or of another third country, for disclosure of Personal Data transferred pursuant to the BCRs; such notification will include information about the Personal Data requested, the requesting authority, the legal basis for the request and the response provided;

(ii) becomes aware of any direct access by public authorities to Personal Data transferred pursuant to the BCRs in accordance with the laws of the country of destination; such notification will include all information available to the data importing Group Company

20.2 Demonstration of Best Effort to Waive Prohibition to Notify

If prohibited from notifying the data exporting Group Company and / or the Individuals, the data importing Group Company 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 exporting Group Company.

20.3 Information regarding the Request

The data importing Group Company will provide the data exporting Group Company, at regular intervals, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority or authorities, whether requests have been challenged and the outcome of such challenges, etc.). If the data importing Group Company is or becomes partially or completely prohibited from providing the data exporting Group Company with the aforementioned information, it will, without undue delay, inform the data exporting Group Company accordingly.

The data importing Group Company 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 Data Protection Authorities upon request.

20.4 Consideration of the Legality of and Challenging the Request

The data importing Group Company will review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public 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 laws of the country of destination, applicable obligations under international law, and principles of international comity.

The data importing Group Company will, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importing Group Company 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

20.5 Documentation of Assessment and Challenge of the Request

The data importing Group Company will document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporting Group Company. It will also make it available to the competent Data Protection Authorities upon request.

20.6 Limitation of Disclosure

The data importing Group Company will provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

20.7 Prohibition against Massive, Disproportionate, and Indiscriminate Transfers

Transfers of Personal Data by a Group Company to any public authority cannot be massive, disproportionate, and indiscriminate in a manner that would go beyond what is necessary in a democratic society.

21 Changes to the BCRs

21.1 Changes without Consent

The BCRs may be changed by Yara International ASA without an Individual's Consent even though an amendment may relate to a benefit conferred on Individuals.

21.2 Effective Date of Amendments

Any amendment shall enter into force and take immediate effect after it has been approved in accordance with Article 21.1 and is published on the Yara company website (public version of these BCRs) and Yara Intranet (Pulse), thereby informing all Group Companies of the amendment.

21.3 Governance of Inquiries

Any request, complaint or claim of an Individual involving the BCRs shall be judged against the version of the BCRs as it is in force at the time the request, complaint or claim is made.

22 Transition Periods and Termination

22.1 General Transition Period

Except as indicated below, there shall be a two-year transition period for compliance with the BCRs. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with the BCRs. During the transition period, any transfer of Personal Data to a Group Company under the BCRs as a transfer mechanism may only take place to the extent that the Group Company receiving such Personal Data is:

(i) compliant with the BCRs, or
(ii) there is a legal basis for the transfer in accordance with the GDPR Chapter V.

22.2 Transition Period for New Group Companies

Any entity that becomes a Group Company after the Effective Date shall comply with the BCRs within two years of becoming a Group Company.

22.3 Transition Period for Divested Entities

A Divested Entity may remain covered by the BCRs after its divestment for such period as may be required by Yara to disentangle the Processing of Personal Data relating to such Divested Entity.

22.4 Transition Period for IT Systems

Where implementation of the BCRs requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.

22.5 Transition Period for Existing Agreements

Where there are existing agreements with Third Parties that are affected by the BCRs, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

22.6 Transitional Period for Local-for-local Systems

Processing of Personal Data that were collected in connection with activities of a Group Company located in a country outside the EEA that is not covered by an Adequacy Decision shall be brought into compliance with the BCRs within five years of the Effective Date.

23 Contact Details

The Head of Data Privacy may be contacted through e-mail to dataprivacy@yara.com or by sending a mail to:

Head of Data Privacy
c/o Yara International ASA
Drammensveien 131
0277 Oslo
Norway
Tel: +47 2415 7000

Annex 1 Definitions

Adequacy Decision
ADEQUACY DECISION shall mean a decision issued by the European Commission under Article 45 of the EU General Data Protection Regulation that the third country, a territory or one or more specified sectors within that third country, or the international organization in question ensures an adequate level of data protection.

Applicable Law
APPLICABLE LAW shall mean the international, national or local law of the country applicable to the respective Group Companies. APPLICABLE LAW IN AN EEA COUNTRY refers only to EU, national or local law in the European Economic Area applicable to the Group Company

Archive
ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the Personal Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An Archive includes any data set that can no longer be accessed by any Staff other than the system administrator.

Article
ARTICLE shall mean an article in the BCRs.

Binding Corporate Rules
BINDING CORPORATE RULES shall mean Personal Data protection policies according to the General Data Protection Regulation Article 47 which are adhered to by a Controller or Processor established on the territory of an EEA 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.

Business Contact Data
BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Individual in his or her contact with Yara.

Business Partner
BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or has had a business relationship or strategic alliance with Yara (e.g., joint marketing partner, joint venture or joint development partner).

Business Purpose
BUSINESS PURPOSE shall mean a purpose for Processing Personal Data and Sensitive Data as specified in Article 2.

Children
CHILDREN shall mean Individuals under the age of thirteen (13) years.

Consent
CONSENT shall mean any freely given, specific, informed and unambiguous indication of the Individual's wishes by which he or she, by a statement or a clear affirmative action, signifies agreement to the Processing of Personal Data relating to him or her.

Controller

CONTROLLER shall mean the Group Company which alone or jointly with others determines the purposes and means of the Processing of Personal Data.

Country Legal Responsible
COUNTRY LEGAL RESPONSIBLE (CLR) shall mean the formal legal responsible for the Yara legal entities within a country, as described in the functional description in the Yara steering system: “Country Legal Responsible- Role responsibilities and mandate”.

Customer
CUSTOMER shall mean any Third Party that purchases, may purchase or has purchased a Yara product or service.

Customer Services
CUSTOMER SERVICES shall mean the services provided by Yara to Customers to support Yara products and services offered to or in use with their employees or customers. These services may include maintenance, upgrade, replacement, inspection and related support activities aimed at facilitating continued and sustained use of Yara products and services.

Data Privacy Coordinator
DATA PRIVACY COORDINATOR shall mean a Regional Data Privacy Coordinator referred to in Article 12.2.

Data Processing Agreement
DATA PROCESSING AGREEMENT shall mean the contract referred to in Article 10.5.

Data Protection Authority or DPA
DATA PROTECTION AUTHORITY or DPA shall mean any data protection authority of one of the countries of the EEA.

Dependent
DEPENDENT shall mean the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee

Divested Entity
DIVESTED ENTITY shall mean the divestment by Yara of a Group Company or business by means of:

(i) a sale of shares that result in the divested Group company no longer qualifying as a Group Company; and/or
(ii) a demerger, sale of assets, or any other manner or form.

EEA
EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.

Effective Date
EFFECTIVE DATE shall mean the date on which the BCRs originally became effective as set forth in Article 1.7.

Employee
EMPLOYEE shall mean the following persons:

(i) an employee, job applicant or former employee of Yara. This term does not include people working at Yara as consultants or employees of Third Parties providing

services to Yara; or

(ii) a (former) executive or non-executive director of Yara or (former) member of the supervisory board or similar body to Yara.

General Data Protection Regulation (GDPR)
GENERAL DATA PROTECTION REGULATION shall mean Regulation (EU) 2016/679 of the European Parliament and of the Council 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.

Group Company
GROUP COMPANY shall mean Yara International ASA and all subsidiaries bound by the BCR. This includes any directly or indirectly wholly owned subsidiary of Yara International ASA and other subsidiaries as listed in the document "Overview of Group Companies bound by BCR", which is available here.

Head of Data Privacy
HEAD OF DATA PRIVACY shall mean the Head of Data Privacy as referred to in Article 12.1.

Head of Legal
HEAD OF LEGAL shall mean the Head of Legal of Yara International ASA.

Individual
INDIVIDUAL shall mean Employee, Dependent and any (employee of or any person working for) Customer, Supplier or Business Partner.

Original Purpose
ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.

Overriding Interest
OVERRIDING INTEREST shall mean the pressing interests set forth in Article 11.1 based on which the obligations of Yara or rights of Individuals set forth in Articles 11.2, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.

Personal Data or Data
PERSONAL DATA shall mean any information relating to an identified or identifiable Individual.

Personal Data Breach
PERSONAL DATA BREACH shall mean a 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.

BCRs
BCRs shall mean the Yara Data Privacy Policy.

Processing
PROCESSING shall mean any operation or set of operations which is performed on Personal Data or on sets of Personal Data, whether or not by automatic 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.

Secondary Purpose
SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data is further Processed.

Sensitive Data
SENSITIVE DATA shall mean Personal Data revealing an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, genetic data, biometric data (for uniquely identifying an Individual), health, sex life or sexual orientation

Staff
STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities as Employees or individuals under the direct authority of Yara using Yara information technology systems or working primarily from Yara's premises.

Supplier
SUPPLIER shall mean any Third Party that provides goods or services to Yara (e.g., an agent, consultant or vendor).

Third Party
THIRD PARTY shall mean any person, private organization, entity or government body outside Yara.

Third Party Controller
THIRD PARTY CONTROLLER shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.

Third Party Processor
THIRD PARTY PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of Yara that is not under the direct authority of Yara.

Yara
YARA shall mean Yara International ASA and its Group Companies.

Yara International ASA
YARA INTERNATIONAL ASA shall mean Yara International ASA, having its registered seat in Norway.

Annex 2 Description of Processing and transfer of Personal Data

Yara business domains	Purposes for Processing Personal Data (Business Purposes)	Categories of data subjects	Categories of Personal Data	Transfer of Personal Data
Management System Key Processes and mechanisms by which Yara is governed, managed and controlled.	**Legal & Compliance** Processing of Personal Data to the extent necessary to protect legal interests, manage legal risk, provide legal governance and coordinate legal work, incl. mitigating risks related to corruption, fraud, integrity of business partners and human rights.	Customers, Suppliers, Business Partners, Employees.	General contact information and information relevant for legal proceedings. Information in IDDs (such as political exposure). Information about conflicts of interest (such as personal relations or ownership). Information related to investigations.	Due to Yara's organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA.
Communication Covers activities on corporate level related to branding, management of	**Corporate and Public Affairs:** Processing Personal Data to the extent necessary to facilitate the advocacy positioning of Yara's interest.	Third Parties.	General contact information including name and job title. Records of prior contact.	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA.

Yara's reputation and stakeholders such as media and the general public, as well as general internal and external communications, and advocacy positioning vis-à-vis stakeholders like governments, NGOs and ICOs.	**Corporate communication:** Processing Personal Data to the extent necessary to communicate externally and internally.	Employees, Third Parties (for both including social media followers and webpage visitors).	Names, job titles, phone number, pictures, IP address, browsing time, requests/comments on social media.	
	Brand and corporate positioning Processing Personal Data to the extent necessary to organize events and maintain Yara's brand center, which may include pictures of Employees and farmers.	Employees, Third Parties (consumers and farmers).	Name, contact details, image and food allergies (when relevant for events).	
Sales and Marketing Value creation activities to ensure Yara achieves the best possible long-term prices in the markets at an appropriate risk level.	**Case Handling** Processing of Personal Data to the extent necessary to register and handle Customers' complaints.	Customers.	General contact information including name.	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA.
	Lead Generation and Management Processing of Personal Data to the extent necessary to collect and manage leads about potential customers.	Customers.	Name, job title, crop & field data (for farmers).	

	Marketing Processing of Personal Data to the extent necessary to generate and distribute marketing material.	Employees, Third Parties (farmers).	Name, contact details, image, crop & field data (for farmers).	
	Account Management Processing of Personal Data to the extent necessary to maintain account details, so that Yara can execute on their obligation as agreed with the Customers.	Customers.	Name, contact details, financial information, information about agents/business partner (e.g. customs agent) of the Customer	
	In-field Demand Generation Processing Personal Data to the extent relevant to delivering farming solutions via various digital platforms/applications.	Customers.	Contact details, transaction data, farming activity, device and software data, relationship data (for example, support requests, ratings and feedback), fertilizer, field, soil and crop data. Other local and farming characteristics (for example, location and mapping, weather and farming conditions), machinery data, software and hardware data, information collected through cookies, pixel tags and other technologies. Financial data (for example, bank, card and account details, and other payment related information) Gender, date of birth and social media account data.	

	Sales order Processing Processing of Personal Data to the extent necessary to receive, register and deliver on the order received from the Customer	Customers, Third Parties (sales agents and supply chain partners).	Name, contact details, postal address and information about the order (may be considered Personal Data when the customer is a small holder farmer).	
Procurement Activities to facilitate procurement of goods and services.	**Source to contract:** Processing Personal Data to the extent necessary to establish and renew contracts.	Suppliers, Third Parties (vendors).	General contact information including name, email and phone numbers. Certificates and qualifications (if requested as part of procuring e.g. a consultancy service).	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA. However, Processing of Personal Data for procurement is limited and mainly conducted within the regions (Europe, Asia/Africa and Americas) and thus does not include any systematic transfer of Personal Data.
	Procure to pay: Processing of Personal Data to the extent necessary for the operational day-to-day Process from when requisition is made to payment is performed.	Employees, Suppliers, Third Parties (vendors).	General contact information.	
Supply Chain Activities that ensure having the right product at the right place at the right time (under consideration of constraints	**Transportation management:** Processing of Personal Data to book and administrate transportation of goods and ensure that the correct goods are picked up by the correct driver. This is	Third Parties (drivers).	Name and certificate (if necessary to ensure that dangerous goods are properly handled)	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA.

and profitability aspects).	necessary both for commercial reasons, to ensure that goods are not lost, and for safety reasons as the goods need to be properly handled.			
Production and Site Execution Activities to develop real-time visibility and transparency over plant operations, optimize production processes, materials and resources, and collaborate in global networks while lowering total production costs.	**Product handling & site logistics:** Processing of Personal Data from truck drivers to ensure they are certified to handle dangerous cargo.	Third Parties (drivers).	Certifications.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, Processing of Personal Data for Production and Site Execution is mainly conducted locally, and thus does not include any systematic transfer of Personal Data.
	Production execution: Processing of Personal Data may occur when monitoring the production, e.g. by camera surveillance of conveyer belts within a production facility to handle potential production incidents.	Employees, Third Parties (contractors and consultants).	Image.	
Finance All activities to ensure efficient financial management and financial	**Financial accounting:** Processing of Personal Data to the extent necessary to issue invoices and	Customers. Suppliers, Third Parties (vendors).	Name, address, phone number, bank Information. Name, address, phone number, bank information and time recording information.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, Processing of

control necessary to support all business activities.	conduct payment, such as contact details, and to estimate and check the correctness of payment.			Personal Data is mainly conducted locally or centrally, where the transfer of Personal Data (if any) would be mainly to the central teams located in Norway.
	Finance, Treasury & Insurance Processing of Personal Data to comply with financial institutions' "know your customer"-requirements and to the extent necessary to perform working capital analyses (to the extent customers are private persons).	Customers, Suppliers, Third Parties (vendors). Employees.	Name, contact details, credit terms, sales amount. Name, contact details, previous work history, utility bills, social security number, passport details, date and place of birth.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA.
	Investor Relations Processing of Personal Data to the extent necessary to manage shareholders rights and comply with legal obligations as a public share company, including amongst others to administer insider lists) and for relationship management and marketing (meetings	Employees. Third Parties. Other Third Parties (investors and shareholders).	Name, contact details, phone number, home address, personal email, social security number. Name, contact details (home address, email, phone), social security number. Name, contact details (phone, email), social security number, citizenship, share ownership, attendance and meeting details.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, Processing of Personal Data for this Process is mainly conducted centrally.

	and events with current and prospective shareholders), including to publish a list on Yara.com of banks/brokers' analysts that follow Yara International ASA.			
HESQ Activities to ensure that everyone goes home safe and healthy at the end of the day, we operate in an environmentally responsible and sustainable way, our work and products are of the highest quality, and we consider the wellbeing of our supply chain partners, Customers and neighbors.	**Security** Processing Personal Data to the extent necessary to protect Yara's assets (physical locations and employees) against incidents and threats. This includes camera surveillance, access control and information about threats from open external sources.	Third Parties (contractors and consultants). Third Parties (drivers.) Employees. Third Parties (visitors).	Criminal Records and Image. Image, Full Name and Signature. Image and Full Name. Image, Full Name and Signature.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, Processing of Personal Data is mainly conducted locally, or centrally where the transfer of Personal Data (if any) would be mainly to the central team located in Norway.
	Environment Processing Personal Data to the extent necessary to handle grievances (complaints and concerns) from Third Parties related to environmental impacts or potential	Third Parties.	Contact Details, home address, personal email, phone numbers, full name and negative impact caused by Yara.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA.

	impacts from Yara's operations or facilities.			
	Crisis & Emergency Management Processing Personal Data to the extent necessary to support Employees, contractors or consultants in case of accidents and health issues during business travel for Yara.	Third Parties (contractors and consultants), Employees.	Contact details, emergency contact details, phone numbers, geolocation information, health insurance policy information and health and safety related information and reporting.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, Processing of Personal Data is mainly conducted centrally where the transfer of Personal Data (if any) would be to the central team located in Norway.
	Occupational Health & Safety Process Processing Personal Data to the extent necessary to handle health, safety and welfare issues in the workplace.	Third Parties (contractors, consultants, visitors), Customers, Employees.	Description of injured parts of body, part of body injured and type of Injury.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA.
	Product stewardship Process Processing of Personal Data to comply with the explosive's precursors legislation in Europe.	Customers.	Copy of valid identification document.	Due to the organizational structure, with global teams, Personal Data may be transferred to all Group Companies outside the EEA. However, the Processing is mainly conducted within Europe.

Information and Digital Technology Activities to ensure the Yara strategy is fulfilled through building digital business capabilities delivering clear business outcomes according to the strategic objectives.	**Software Engineering and Digital Product Management:** Processing Personal Data to the extent necessary to conduct user acceptance testing of internally developed solutions before deployment.	Employees, Third Parties (contractors), Customers.	General contact information and IT-related information such as profile/account information, production data in internally developed systems.	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA. These activities are mainly happening in digital hubs in Singapore, Germany, Norway and Brazil.
	Cyber Security Processing Personal Data to secure Yara's digital systems and solutions and ensure we have adequate controls.	Employees, Third Parties (contractors).	General contact information and IT-related information such as profile/account information, security logs, login information, user credentials, device/software information.	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA. However, Yara has a Security Operation Center (SOC) that needs to be manned at all hours, and thus there are resources specifically located in Norway, Belgium, Singapore, India, Brazil, Colombia and the US.
	Digital Operations Management Processing Personal Data to run, operate and maintain digital systems and solutions.	Employees, Third Parties (contractors).	General contact information and IT-related information such as profile/account information, end date (relevant for a contractor) information about a request or incident (e.g. need for a new PC, new password, access to a specific system).	Due to the organizational structure, with global teams, Personal Data may potentially be transferred to all Group Companies outside the EEA. In particular, Personal Data will be transferred to a service desk operated mainly from India.
HR All activities	**Acquire:** Processing of	Employees (including prospective	Background and reference checks, emergency contact details, education	Due to the organizational structure, with global teams,

related to the hire to retire and termination end-to-end processes for all Yara employee classes.	Personal Data with the purpose of recruitment, hiring, onboarding, and employer branding.	employees).	records, languages, compensation data, hours of work, job title and role, office location, personnel number, previous work history, start date, national identify number, marital status, nationality, signature, image, profile assessment for senior positions (SHL). Home address, full name.	Personal Data may potentially be transferred to all Group Companies outside the EEA. Personal data is typically transferred when: • someone is applying for a job from another country than where the position is based • someone is reporting to a line manager in another country than where they are based themselves • HR support is provided to someone from another country than where they are based • The global HR system PeoplePath is used, as it is internally managed by a team located in Brazil
	Deliver: Processing Personal Data with the purpose of data management, compensation management, expense management and separation management.	Employees.	Annual leave, bonus payments, Yara legal company/entity, compensation data, contract type, hours of work, job title and role, life insurance information, pension information, salary or wage information, bank account details, personnel number (A number), full name, expenses information, image, trade union membership, business travel information.	
	Develop: Processing Personal Data with the purpose of talent and succession management, training, learning and competence management.	Employees.	Education, languages, skills, training history, company email, job title and role, line reporting manager, office location, performance rating, Yara legal company/entity, personnel number (A number), full name.	
	Empower Processing Personal Data with the purpose of performance management, employee	Employees.	Education, languages, training history, benefits and entitlements Data, Yara legal company/entity, company email, contract type, employee survey responses, job title and role, line reporting manager, office location, performance rating, previous work	

	engagement and relationship management.		history, personnel number (A number), date of birth, full name, nationality, performance evaluations.	
	Organize: Processing of Personal Data with the purpose of organizational design, position management, change management and communications, HR solutions, and compliance and governance.	Employees.	Company email, job title and role, line reporting manager, Yara legal company, personnel number (A number), full name.	
	Reward Processing of Personal Data with the purpose of compensation and benefits management, grading & benchmarking, salary reviews and incentive schemes.	Employees.	Annual leave, benefits and entitlements information, bonus payments, compensations data, contract type, hours of work, job title and role, line reporting manager, performance rating, salary or wage information, start date, Yara legal company, social security number, personnel number (A number), full name, gender.	
Asset management Activities related to safe, efficient, cost effective and high-quality care of assets (production sites,	**Plant Design & Engineering:** Processing Personal Data to the extent necessary to ensure that assets (such as plants) are planned by qualified personnel.	Third Parties.	Contact details, education records, previous work history, full name and certificates and qualifications.	Transfers may take place to all Group Companies outside the EEA. However, Processing of Personal Data for Asset management is mainly conducted locally, at the site, and thus does not include any systematic transfers of Personal Data.

warehouses, terminals, equipment etc.)	**Build:** Processing Personal Data to the extent necessary to ensure that assets (such as plants) are built by qualified personnel.	Third Parties.	Contact details, education records, previous work history, full name and certificates and qualifications.	
	Maintain: Processing Personal Data to the extent necessary to ensure that assets (such as plants and equipment) are maintained by qualified personnel.	Third Parties.	Contact details, education records, previous work history, full name and certificates and qualifications.	

Annex 3 Exceptions to the Scope of the Binding Corporate Rules

The Binding Corporate Rules does not apply to:

- Processing of Personal Data outside the EEA related to local security processes. This includes but is not limited to biometric and other access control, alcohol and drug testing and physical security measures at the site.
- Processing of Personal Data outside the EEA related to local background checks. This applies irrespective of which process or processes the background check relates to.
- Processing of Personal Data outside the EEA related to local DEI (Diversity, Equity and Inclusion) activities. This includes but is not limited to statistics, analyses and diversity audits, and applies irrespective of which process or processes the activity relates to.

Interpretations

INTERPRETATION OF THE BCRs:
(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;
(ii) headings are included for convenience only and are not to be used in construing any provision of the BCRs;
(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
(iv) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa;
(v) a reference to a document (including, without limitation, a reference to the BCRs) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by the BCRs or that other document; and
vi) a reference to law or a legal obligation includes any regulatory requirement, sectorial guidance and best practice issued by relevant national and international supervisory authorities or other bodies.