Data Privacy Directive for Customer, Supplier and Business Partner Data
Public version

Introduction

Yara has committed itself to the protection of Personal Data of Yara Customers, Suppliers and Business

Partners by implementing the Yara Data Privacy Directive for Customer, Supplier and Business Partner Data (the "**Directive**"), which together with the Yara Data Privacy Directive for Employee Data, 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 Data Protection Directive 95/46/EC, and from 25 May 2018, the EU General Data Protection Regulation 2016/679 (GDPR).

This document is a public excerpt and summary of Yara's Data Privacy Directive for Customer, Supplier and Business Partner Data 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 Directive and a list of Group Companies bound by the BCR, please contact the Head of Data Privacy. Capitalized terms have the meaning set out in Annex 1 (Definitions).

1. Scope, Applicability and Implementation

1.1 Scope

The Directive addresses the Processing of Personal Data of Customers, Suppliers and Business Partners by Yara or a Third Party on behalf of Yara. The Directive does not address the Processing of personal data relating to Employees by Yara.

1.2 Electronic and Paper-based Processing

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

1.3 Applicability of Local Law and Directive

Nothing in the Directive will be construed to take away any rights and remedies that Individuals may have under applicable local law. The Directive provides supplemental rights and remedies to Individuals only. Individuals shall benefit from the rights set out in the Directive and have the right to enforce those rights as set out in Article 18.

1.4 Sub-policies and Notices

Yara may supplement the Directive through sub-policies or notices that are consistent with the Directive.

1.5 Accountability

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

1.6 Directive Supersedes Prior Policies

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

1.7 Implementation

This Directive shall be implemented in the Yara organization based on the timeframes specified in Article 22.

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**).

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

(i) **Development and improvement of products and/or services:** this purpose includes Processing of Personal Data that is necessary for the development and improvement of Yara products and/or services, research and development;

(ii) **Performance of Customer Services:** this purpose addresses the Processing of Personal Data necessary for the performance of Customer Services;

(iii) **Conclusion and execution of agreements with Customers, Suppliers and Business Partners:** this purpose addresses the Processing of Personal Data necessary to conclude and execute agreements with Customers, Suppliers and Business Partners, including required screening activities (e.g., for access to Yara's premises or systems) and to record and financially settle delivered services, products and materials to and from Yara;

(iv) **Relationship management and marketing:** this purpose addresses activities such as maintaining and promoting contact with Customers, Suppliers and Business Partners, account management, customer service, recalls, collection of Personal Data through Yara websites and the development, execution and analysis of market surveys and marketing strategies;

(v) **Business process execution, internal management and management reporting:** this purpose addresses activities such as managing company assets, ethics hotline/whistleblowing, conducting internal audits and investigations, integrity due diligence (IDD), capital value process (CVP), finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes, managing mergers, acquisitions and divestitures, and management reporting and analysis;

(vi) **Health, safety, security and integrity, including the safeguarding of the security and integrity of the business sector in which Yara operates:** this purpose addresses activities such as those involving health and safety, the protection of Yara and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights (such as required screening activities for access to Yara's premises or systems); and

(vii) **Compliance with legal obligations:** this purpose addresses the Processing of Personal Data necessary for the performance of a task carried out to comply with a legal obligation to which Yara is subject.

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.

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 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 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; 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 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;
(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, 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; or
(ix) the Processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes.

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.

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:
- the identity and contact details of the Group Company being the Controller for the Processing;
- the Business Purposes for which his or her Data are Processed;
- the categories of Third Parties to which the Data are disclosed (if any).
- 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.

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

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;
(iii) **Religion or beliefs Personal Data:** this includes but is not limited to data necessary to accommodate specific products or services (such as dietary requirements or religious holidays);
(iv) **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).

5. Quantity and Quality of Data

5.1 No Excessive Data

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

5.2 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 sub-policy, 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:

(i) securely deleted or destroyed;
(ii) anonymized; or
(iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).

5.3 Quality of Data

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

5.4 Accurate, Complete and Up-to-date Data

It is the responsibility of Individuals and Yara to ensure that Individuals' 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.

6. Individual Information Requirements

6.1 Information Requirements

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

(i) the identity and the contact details of the Group Company being the Controller for the Processing;
(ii) the contact details of the appropriate Data Privacy Coordinator;
(iii) the Business Purposes for which their Data are Processed and the legal basis for the Processing;
(iv) the categories of Personal Data obtained;
(v) which legitimate Business Purposes are pursued when the Processing is based on Article 3.1 vi);
(vi) the categories of Third Parties to which the Data are disclosed (if any);
(vii) whether the Third Party 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 11.6.

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 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 10 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.

6.2 Personal Data not Obtained from the Individual

If applicable local law so requires, where Personal Data have not been obtained directly from the Individual, Yara shall provide the Individual with the information set out in Article 6.1:
(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.

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.

6.4 Exceptions

The requirements of Article 6.1 may be set aside where and insofar as the Individual already has the information.

The requirements of Article 6.2 may be set aside if:
(i) the Individual already has the information;
(ii) it is impossible or would involve a disproportionate effort to provide the information to Individuals;
(iii) it results in disproportionate costs; or
(iv) obtaining or disclosing the Personal Data is expressly required by applicable law which provides appropriate measures to protect the Individual's legitimate interests.

7. Individual Rights of Access, Rectification and Deletion

7.1 Rights of Individuals

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 about 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.

If the Personal Data are incorrect, incomplete, unnecessary or not Processed in compliance with applicable law or the Directive, the Individual has the right to have his or her Data rectified, deleted or restricted (as appropriate).

In addition, the Individual has the right to object to:
(i) the Processing of his or her Data on the basis of compelling grounds related to his or her particular situation; and
(ii) receiving marketing communications on the basis of Article 9.5.

7.2 Procedure
The Individual should send his or her request to the contact person or contact point indicated in the relevant privacy policy. If no contact person or contact point is indicated, the Individual may send his or her request through the general contact section of the Yara website.

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 Directive.

7.3 Response Period
Within four weeks of Yara receiving the request, the Data Privacy Coordinator shall inform the Individual in writing or electronically either (i) of Yara 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, which shall be no later than eight weeks after the communication was sent to the Individual.

7.4 Complaint
An Individual may file a complaint in accordance with Article 17.3 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 7.3; or
(iii) the time period provided to the Individual in accordance with Article 7.3 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.

7.5 Denial of Requests
Yara may deny an Individual’s request if:
(i) the request does not meet the requirements of Articles 7.1 and 7.2;
(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 shall generally be deemed to be an unreasonable time interval.

8. Security and Confidentiality Requirements

8.1 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 policies 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 Data Security Breach Notification to Data Protection Authorities

If a Data Security Breach has occurred or is suspected to have occurred, the person who has become aware of or suspects the Data Security 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.

Yara shall follow internal procedures and applicable data protection law for handling such suspected or actual Data Security Breaches in an appropriate and timely manner and notify the competent Data Protection Authority when required.

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

8.5 Data Security Breach Notification to Individuals

If required under applicable law, Yara shall notify the Individual of a Data Security Breach without undue delay following discovery of such breach, if the Data Security 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 Data Security 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 Data Security Breach notification to the Individuals shall describe in clear and plan language the nature of the Data Security Breach and shall at least contain the information and measures referred to in 8.4 (b), (c) and (d).

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 (opt-out)

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 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. Automated Decision Making

10.1 Automated Decisions

Automated tools may be used to make decisions about Individuals but decisions with a negative outcome for the Individual may not be based solely on the results provided by the automated tool. This restriction does not apply if:

(i) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation to which Yara is subject;

(ii) the decision is made by Yara for purposes of (a) entering into or performing a contract or (b) managing the contract, provided the underlying request leading to a decision by Yara was made by the Individual (e.g., where automated tools are used to filter promotional game submissions); or

(iii) suitable measures are taken to safeguard the legitimate interests of the Individual (e.g., the Individual has been provided with an opportunity to express his or her point of view).

11. Transfer of Personal Data to Third Parties

11.1 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.

11.2 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).

11.3 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).

11.4 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 Data Security Breach involving Personal Data; 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 Data Security Breach.

11.5 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 or a country covered by an Adequacy Decision; 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:

(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 Privacy Shield or any other similar program that is covered by an Adequacy Decision;

(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.

Items (vii) and (x) above require the prior approval of the Head of Data Privacy.

11.6 Consent for Transfer

If none of the grounds listed in Article 11.6 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.

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.

11.7 Transfers Between Group Companies 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 Article 11.6, 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.

12. Overriding Interests

12.1 Overriding Interests

Some of the obligations of Yara or rights of Individuals as specified in Articles 12.2 and 12.3 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; or
(iii) Otherwise protect or defend the rights or freedoms of Yara, its Employees or other persons.

12.2 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 6.1 and 6.2 (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); and
(v) Articles 11.4 and 11.5 (ii) (contracts with Third Parties).

12.3 Sensitive Data

The requirements of Article 3.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (b), (c) and (e), (ii) and (iii).

12.4 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.

12.5 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 or 7.1, in which case the request shall be denied.

13. Supervision and Compliance

13.1 Head of Data Privacy

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

13.2 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 Directive and monitor compliance with the Directive in the defined region, including handling Individuals' requests and complaints as described in Article 7.

14. Policies and Procedures

14.1 Policies and Procedures

Yara shall develop and implement sub-policies and procedures to comply with the Directive.

14.2 System information

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

15. Training

15.1 Staff Training

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

16. Monitoring and Auditing Compliance

16.1 Audits

Yara shall regularly carry out internal audits related to compliance with the Directive as set forth in the corporate audit programme. A copy of the data privacy audit results will be provided to the Norwegian Data

Protection Authority and a Data Protection Authority competent to audit upon request, according to Yara internal procedures.

16.2 Mitigation

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

17. Complaints Procedure

17.1 Complaint to Data Privacy Coordinator

Individuals may file a complaint regarding compliance with the Directive or violations of their rights under applicable local law in accordance with the complaints procedure set forth in the relevant privacy policy or contract. The complaint shall be forwarded to the appropriate Data Privacy Coordinator.

The appropriate Data Privacy Coordinator shall:

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

17.2 Reply to Individual

Within four weeks of Yara receiving a complaint, the appropriate 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) when he or she will be informed of Yara's position, which shall be no later than eight weeks after the communication was sent to the Individual. The appropriate Data Privacy Coordinator shall send a copy of the complaint and his or her written reply to the Head of Data Privacy.

17.3 Complaint to 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 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 17.2;
(iii) the time period provided to the Individual pursuant to Article 17.2 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 7.4 applies.

The procedure described in Articles 17.1 through 17.2 shall apply to complaints filed with the Head of Data Privacy.

18. Legal Issues

18.1 Complaints Procedure

Individuals are encouraged to first follow the complaints procedure set forth in Article 17 of the Directive before filing any complaint or claim with the competent DPAs or the courts.

18.2 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 the Directive, the Individual may, at his or her choice, submit a complaint or a claim to the DPA or the courts:

(i) in the EEA country at the origin of the Personal Data transfer, against the Group Company in such country of origin responsible for the relevant data transfer;
(ii) in Norway, against Yara International ASA; or
(iii) in the EEA country where the Individual resides or has its place of work, against the Group company being the Controller of the relevant Personal Data.

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.

18.3 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 damages resulting from the violation of the Directive by Group Companies established outside the EEA.

18.4 Right to Claim Damages and Burden of Proof

In case an Individual brings a claim for damages under Article 18.2, 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 the Directive.

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 the Directive are not attributable to any Group Company established outside the EEA in order to avoid liability.

18.5 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 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.

18.6 Advice of the Lead DPA

Yara shall abide by the advice of the Norwegian Data Protection Authority issued on the interpretation and application of the Directive, and further abide by binding decisions of DPAs competent pursuant to Article 18.2. DPAs competent pursuant to Article 18.2 may conduct audits in order to ascertain Yara's compliance with the Directive.

18.7 Mitigation

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

18.8 Law Applicable to the Directive

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

19. Conflicts Between the Directive and Applicable Local Law

19.1 Conflict of Law when Transferring Data

Where a legal requirement to transfer Personal Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Head of Data Privacy. The Head of Data Privacy shall seek the advice of the Head of Legal. The Head of Data Privacy may seek the advice of the Norwegian Data Protection Authority or another competent government authority.

19.2 Conflict Between Directive and Law

In all other cases, where there is a conflict between applicable local law and the Directive, the relevant Country Legal Responsible and Regional Data Privacy Coordinator shall consult with the Head of Data Privacy to determine how to comply with the Directive and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

20. Changes to the Directive

20.1 Changes without Consent

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

20.2 Effective Date of Amendments

Any amendment shall enter into force and take immediate effect after it has been approved in accordance with the procedure for updating the BCRs and once it has been published on the Yara company website in this public version of the Directive and the Yara Intranet (Pulse).

20.3 Governance of Inquiries

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

21. Transition Periods

21.1 General Transition Period

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

(i) compliant with the Directive, or

(ii) the information transfer meets one of the grounds for transfer listed in Articles 11.6 to 11.8.

21.2 Transition Period for New Group Companies

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

21.3 Transition Period for Divested Entities

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

21.4 Transition Period for IT Systems

Where implementation of the Directive 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.

21.5 Transition Period for Existing Agreements

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

21.6 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 Directive within five years of the Effective Date.

21.7 Effective Date

The Directive was adopted by the Head of Legal of Yara International ASA on November 16th 2017 (**Effective Date)**. This public version of the Directive shall be published on the Yara company website and the full version of the BCR shall be published on the Yara Intranet (Pulse). In addition, the list of Group Companies bound by the BCR and the full version of the BCR shall be made available to Individuals upon request to the Head of Data Privacy.

22. 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

The Regional Data Privacy Coordinators may be contacted by sending an e-mail to dataprivacy@yara.com or by sending a mail to your local Yara office.

ANNEX 1 Definitions

Adequacy Decision
ADEQUACY DECISION shall mean a decision issued by the European Commission under Article 25 of the EU Data Protection Directive or the EU General Data Protection Regulation Article 45 that a country or region or a category of recipients in such country or region is deemed to provide an “adequate” level of data protection.

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 Employee other than the system administrator.

Article
ARTICLE shall mean an article in the Directive.

Binding Corporate Rules
BINDING CORPORATE RULES shall mean a privacy policy of a group of undertakings which under applicable local law (such as Article 25 of the EU Data Protection Directive) is considered to provide an adequate level of protection for the transfer of Personal Data within that group of undertakings.

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 13.2.

Data Privacy Network
DATA PRIVACY NETWORK shall mean the network referred to in Article 13.1.

Data Processing Agreement
DATA PROCESSING AGREEMENT shall mean the contract referred to in Article 11.5.

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

Data Security Breach
DATA SECURITY 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.

Directive
DIRECTIVE shall mean the full version of the Data Privacy Directive for Customer, Supplier and Business Partner Data.

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
(i) 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 Directive becomes effective as set forth in Article 1.6.

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

EU Data Protection Directive
EU DATA PROTECTION DIRECTIVE shall mean the Directive 95/46/EC of the European Parliament and of the Council on the protection of individuals with regard to the processing of and the free movement of such data or any successor or replacement thereof.

General Data Protection Regulation (GDPR)
GENERAL DATA PROTECTION REGULATION 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”.

Head of Data Privacy
HEAD OF DATA PRIVACY shall mean the Head of Data Privacy as referred to in Article 13.1.

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

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

Organizational Unit
ORGANIZATIONAL UNIT shall mean each business unit and staff function of Yara.

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 12.1 based on which the obligations of Yara or rights of Individuals set forth in Articles 12.2 and 12.3 may, 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.

Processing

PROCESSING shall mean any operation that is performed on Personal Data, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.

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.

Interpretations

INTERPRETATION OF THE DIRECTIVE:

(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 Directive;

(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 Directive) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by the Directive 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.