Koninklijke DSM N.V.

Privacy Code for Customer, Supplier and Business Partner Data

Introduction

DSM has committed itself to the protection of personal data of DSM Customers, Suppliers and Business Partners in the DSM Code of Business Conduct.

This Code indicates how this principle shall be implemented. For the privacy code applicable to Employee Data, refer to the *Privacy Code for Employee Data*. **[insert hyperlink to Code]**

Article 1 – Scope, Applicability and Implementation

Scope	1.1	This Code addresses the Processing of Personal Data of Customers, Suppliers and Business Partners by DSM or a Third Party on behalf of DSM. This Code does not address the Processing of Employee Data of DSM.
Electronic and paper-based Processing	1.2	This Code applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Code	1.3	Individuals keep any rights and remedies they may have under applicable local law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.
Sub-policies and notices	1.4	DSM may supplement this Code through sub-policies or notices that are consistent with this Code.
Responsibility	1.5	The Responsible Executive shall be accountable for compliance with this Code.
Effective Date	1.6	This Code has been adopted by the Managing Board of Koninklijke DSM N.V. and shall enter into force as of April 1, 2014 (**Effective Date**) and shall be published on the DSM website and DSM intranet and be made available to Individuals upon request.
Code supersedes prior policies	1.7	This Code supersedes all DSM privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	This Code shall be implemented in the DSM organization based on the timeframes specified in Article 22.

Role of Koninklijke DSM N.V.

1.9 Koninklijke DSM N.V. has undertaken the task of the coordination and implementation of this Code.

Article 2 – Purposes for Processing Personal Data

Legitimate Business Purposes

2.1 Personal Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (**Business Purposes**):

(i) **Development and improvement of products and/or services.** This purpose includes Processing that is necessary for the development and improvement of DSM products and/or services, research and development;

(ii) **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 and to record and financially settle delivered services, products and materials to and from DSM;

(iii) **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 and the development, execution and analysis of market surveys and marketing strategies;

(iv) **Business process execution, internal management and management reporting.** This purpose addresses activities such as managing company assets, conducting internal audits and investigations, finance and accounting, implementing business controls, provision of central processing facilities for efficiency purposes managing mergers, acquisitions and divestitures, and Processing Personal Data for management reporting and analysis;

(v) **Safety and security.** This purpose addresses activities such as those involving safety and security of Customers, Suppliers and Business Partners, the protection of DSM and Employee assets, and the authentication of Customer, Supplier or Business Partner status and access rights;

(vi) **Compliance with legal obligations.** This purpose addresses the Processing of Personal Data necessary for compliance with a legal obligation to which DSM is subject; or

(vii) **Protection vital interests of Individuals.** This is where Processing is necessary to protect the vital interests of an Individual.

Where there is a question whether a Processing of Personal Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Officer before the Processing takes place.

Consent

2.2 If a Business Purpose does not exist or if applicable local law so requires DSM shall (also) seek consent from the Individual for the Processing.

Where Processing is undertaken at the request of an Individual (e.g. he subscribes to a service or seeks a benefit), he is deemed to have provided consent to the Processing.

When seeking consent, DSM must inform the Individual:

(i) of the purposes of the Processing for which consent is required; and
(ii) other relevant information (e.g., the nature and categories of the Processed Data, the categories of Third Parties to which the Data are disclosed (if any) and how Individuals can exercise their rights).

Denial or withdrawal of consent

2.3 The Individual may both deny consent and withdraw consent at any time.

Article 3 – Use for Other Purposes

Use of Data for Secondary Purposes

3.1 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 DSM 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 Individual consent in accordance with Article 2.2 or Article 4.3 (if applicable).

Generally permitted uses of Data for Secondary Purposes

3.2 It is generally permissible to use Personal Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1:

(i) transfer of the Data to an Archive;
(ii) internal audits or investigations;
(iii) implementation of business controls;
(iv) statistical, historical or scientific research;
(v) preparing for or engaging in dispute resolution;
(vi) legal or business consulting; or
(vii) insurance purposes.

Article 4 – Purposes for Processing Sensitive Data

Specific purposes for Processing Sensitive Data

4.1 This Article sets forth specific rules for Processing Sensitive Data. DSM shall Process Sensitive Data only to the extent necessary to serve the applicable Business Purpose.

The following categories of Sensitive Data may be collected, used or otherwise Processed only for one (or more) of the purposes specified below:

(i) **Racial or ethnic data**: in some countries photos and video images of Individuals qualify as racial or ethnic data. DSM may process photos and video images for the protection of DSM and Employee assets, site access and security reasons, and the authentication of Customer, Supplier or Business Partner status and access rights;

(ii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior) for protecting the interests of DSM with respect to criminal offenses that have been or, given the relevant circumstances are suspected to have been, committed against DSM or its Employees.

(iii) **Health data**: for the protection of the safety and security of Customers, Suppliers and Business Partners visiting DSM sites, for instance if Customers, Suppliers and Business Partners are involved in industrial accidents.

General Purposes for Processing of Sensitive Data

4.2 In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed under (one or more of) the following circumstances:

(i) the Individual has given his explicit consent to the Processing thereof;

(ii) as required by or allowed under applicable local law;

(iii) for the establishment, exercise or defense of a legal claim;

(iv) to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first; or

(v) to the extent necessary to comply with an obligation of international public law (e.g. treaties).

Denial or withdrawal of consent

4.3 The information requirements of Article 2.2 and Article 2.3 apply to the granting, denial or withdrawal of consent.

Prior Authorization of Privacy Officer

4.4 Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, the Processing requires the prior authorization of the appropriate Privacy Officer.

Use of Sensitive Data for Secondary Purposes	4.5	Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3.

Article 5 – Quantity and Quality of Data

No Excessive Data	5.1	DSM shall restrict the Processing of Personal Data to Data that are reasonably adequate for and relevant to the applicable Business Purpose. DSM shall take reasonable steps to delete Personal Data that are not required for the applicable Business Purpose.
Storage period	5.2	DSM 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. DSM 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 Responsible Executive shall direct that the Data be: (i) securely deleted or destroyed; (ii) anonymized or de-identified; or (iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).
Quality of Data	5.3	Personal Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.
Accurate, complete and up-to-date Data	5.4	It is the responsibility of the Individuals to keep his Personal Data accurate, complete and up-to-date. Individuals shall inform DSM regarding any changes in accordance with Article 7.

Article 6 – Individual Information Requirements

Information requirements	6.1	DSM shall inform Individuals through a privacy policy or notice about: (i) the Business Purposes for which their Data are Processed; (ii) which Group Company is responsible for the Processing; (iii) the categories of Third Parties to which the Data are disclosed (if any); if the Third Party is located in a Non-Adequate Country, the Employee will be informed thereof as well; and (iv) other relevant information (e.g., the nature and categories of the Processed Data and how Individuals can exercise their rights).

Personal Data not obtained from the Individual

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

(i) at the time that the Personal Data are recorded in a DSM database; or

(ii) at the time that the Personal Data are used for a mailing, provided that this mailing is done within six months after the Personal Data are recorded in a DSM database.

Exceptions

6.3 The requirements of Article 6.2 may be set aside if:

(iii) it is impossible or would involve a disproportionate effort to provide the information to Individuals; or

(iv) it results in disproportionate costs.

These exceptions to the above requirements qualify as Overriding Interests.

Article 7 – Individual Rights of Access and Rectification

Rights of Individuals

7.1 Every Individual has the right to request an overview of his Personal Data Processed by or on behalf of DSM. Where reasonably possible, the overview shall contain information regarding the source, type, purpose and categories of recipients of the relevant Personal Data.

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

In addition, the Individual has the right to object to the Processing of his Data on the basis of compelling grounds related to his particular situation.

Procedure

7.2 The Individual should send his 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 request through the general contact section of the DSM website.

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

(i) specify the type of Personal Data to which he 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 DSM obtained the Personal Data;

(iv) show proof of his identity; and

(v) in the case of rectification, deletion, or blockage, the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with applicable law or the Code

Response

7.3 Within four weeks (4) of DSM receiving the request, the Privacy Officer shall

period inform the Individual in writing either (i) of DSM position with regard to the request and any action DSM has taken or will take in response or (ii) the ultimate date on which he will be informed of DSM's position, which date shall be no later than four (4) weeks thereafter.

Complaint 7.4 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 will receive a response.

Denial of requests 7.5 DSM may deny an Individual 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 6 months or less shall generally be deemed to be an unreasonable time interval.

Article 8 – Security and Confidentiality Requirements

Data security 8.1 DSM 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. To achieve this, DSM adheres ISO 27002 relating to the protection of Personal Data.

Staff access 8.2 Staff members shall be authorized to access Personal Data only to the extent necessary to serve the applicable Business Purpose and to perform their job.

Confidentiality obligations 8.3 Staff members who access Personal Data must meet their confidentiality obligations.

Article 9 – Direct Marketing

Direct marketing 9.1 This Article sets forth requirement 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).

Consent for direct marketing (opt-in) 9.2 If applicable law so requires, DSM shall only sent 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, DSM shall in any event offer the Individual the opportunity to opt-out of such unsolicited commercial communication.

Exception (opt-out) 9.3 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 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;

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

Information to be provided in each communication 9.4 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 communication.

Objection to direct marketing 9.5 If an Individual objects to receiving marketing communications from DSM, or withdraws his consent to receive such materials, DSM will take steps to refrain from sending further marketing materials as specifically requested by the individual. DSM will do so within the time period required by applicable law.

Third Parties and Direct marketing 9.6 No Data shall be provided to, or used on behalf of, Third Parties for purposes of direct marketing without the prior consent of the Individual.

Direct marketing records 9.8 DSM shall keep a record of Individuals that used their "opt-in" or "opt-out" right and will regularly check to public opt-out registers.

Article 10 – Automated Decision Making

Automated decisions 10.1 Automated tools may be used to make decisions about Individuals but decisions 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 required or authorized by law;

(ii) the decision is made by DSM for purposes of (a) entering into or performing a contract or (b) managing the contract, provided the underlying request leading to a decision by DSM 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 point of view.

Article 11 – Transfer of Personal Data to Third Parties

Transfer to Third Parties

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

Third Party Controllers and Third Party Processors

11.2 There are two categories of Third Parties:

(i) **Third Party Processors:** these are Third Parties that Process Personal Data solely on behalf of DSM 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., DSM Business Partners that provide their own goods or services directly to Customers).

Transfer for applicable Business Purposes only

11.3 DSM shall transfer Personal Data to a Third Party to the extent necessary to serve the applicable Business Purpose (including Secondary Purposes as per Article 3 or purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller contracts

11.4 Third Party Controllers (other than government agencies) may Process Personal Data only if they have a written contract with DSM. In the contract, DSM shall seek to contractually safeguard the data protection interests of its Individuals. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. 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 Individual's job responsibilities.

Third Party Processor contracts

11.5 Third Party Processors may Process Personal Data only if they have a written contract with DSM. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. 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 DSM's instructions and for the purposes authorized by DSM;

(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 DSM without the prior written consent of DSM;
(v) DSM has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by DSM or any relevant government authority;
(vi) the Third Party Processor shall promptly inform DSM of any actual or suspected security breach involving Personal Data; and
(vii) the Third Party Processor shall take adequate remedial measures as soon as possible and shall promptly provide DSM with all relevant information and assistance as requested by DSM regarding the security breach.

Transfer of Data to a Non-Adequate Country

11.6 This Article sets forth additional rules for the transfer of Personal Data to a Third Party located in a country that is not considered to provide an "adequate" level of protection for Personal Data (**Non-Adequate Country**). Personal Data may be transferred to a Third Party located in a Non-Adequate Country only if:

(i) the transfer is necessary for the performance of a contract with the Individual, for managing a contract with Individual or to take necessary steps at the request of the Individual prior to entering into a contract, e.g., for processing orders;
(ii) a contract has been concluded between DSM and the relevant Third Party that provides for safeguards at a similar level of protection as that provided by this Code; the contract shall conform to any model contract requirement under applicable local law (if any);
(iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Individual between DSM and a Third Party (e.g. in case of recalls);
(iv) the Third Party has been certified under the United States Safe Harbor Program or any other similar program that is recognized as providing an “adequate” level of data protection;
(v) the Third Party has implemented binding corporate rules or a similar transfer control mechanism which provide adequate safeguards under applicable law;
(vi) the transfer is necessary to protect a vital interest of the Individual;
(vii) the transfer is necessary for the establishment, exercise or defense of a legal claim;
(viii) the transfer is necessary to satisfy a pressing need to

protect the public interests of a democratic society; or

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

Items (vii), (viii) and (ix) above require the prior approval of the Chief Privacy Officer.

Consent for transfer

11.7 If none of the grounds listed in Article 11.6 exist or if applicable local law so requires DSM shall (also) seek consent from the Individual for the transfer to a Third Party located in a Non-Adequate Country.
Prior to requesting consent, the Individual shall be provided with the following information:

(i) the purpose of the transfer;
(ii) the identity of the transferring Group Company;
(iii) the identity or categories of Third Parties to which the Data will be transferred;
(iv) the categories of Data that will be transferred;
(v) the country to which the Data will be transferred; and
(vi) the fact that the Data will be transferred to a Non-Adequate Country.

Article 2.3 applies to denial or withdrawal of consent.

Transfers between Non-Adequate Countries

11.8 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 Non-Adequate Country to a Third Party also located in a Non-Adequate Country. 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 DSM.

Article 12 – Overriding Interests

Overriding Interests

12.1 Some of the obligations of DSM or rights of Individuals under this Code 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 DSM including:
  (a) the health, security or safety of Employees or Individuals;
  (b) DSM's intellectual property rights, trade secrets or reputation;
  (c) the continuity of DSM'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 DSM, its Employees or other persons.

Exceptions in the event of Overriding Interests

12.2 If an Overriding Interest exists, one or more of the following obligations of DSM or rights of the Individual may be set aside:
(i) Article 3.1 (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 7.1 (rights of Individuals);
(iv) Articles 8.2 and 8.3 (Staff access limitations and confidentiality requirements); and
(v) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).

Sensitive Data

12.3 The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (c) and (e), (ii) and (iii).

Consultation with Chief Privacy Officer

12.4 Setting aside obligations of DSM or rights of Individuals based on an Overriding Interest requires prior consultation of the Chief Privacy Officer.

Information to Individual

12.5 Upon request of the Individual, DSM shall inform the Individual of the Overriding Interest for which obligations of DSM 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.

Article 13 – Supervision and compliance

Chief Privacy Officer

13.1 Koninklijke DSM N.V. shall appoint a Chief Privacy Officer who is responsible for:
(i) supervising compliance with this Code;
(ii) providing periodic reports, as appropriate, to the Managing Board of Koninklijke DSM N.V. on data protection risks and compliance issues; and
(iii) coordinating, in conjunction with the appropriate Privacy Officer, official investigations or inquiries into the Processing of Data by a government authority.

Privacy Council

13.2 The Chief Privacy Officer shall establish an advisory Privacy Council. The Privacy Council shall create and maintain a framework for:
(i) the development, implementation and updating of local Individual data protection policies and procedures;
(ii) the development, implementation and updating of the policies,

procedures and system information (as required by Article 14);
(iii) the development, implementation and updating of the training and awareness programs;
(iv) the monitoring and reporting on compliance with this Code;
(v) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and
(vi) determining and updating appropriate sanctions for violations of this Code (e.g., disciplinary standards).

Privacy Officers 13.3 Each Business Group and Service Group and the Koninklijke DSM N.V. Headquarters shall designate a Privacy Officer. These Privacy Officers may, in turn, establish a network of Privacy Officers sufficient to direct compliance with this Code within their respective organizations.

The Privacy Officers shall:
(i) regularly advise their Responsible Executive and the Chief Privacy Officer on privacy risks and compliance issues;
(ii) maintain (or ensure access to) an inventory of the system information (as required by Article 14.2);
(iii) establish a framework for a privacy compliance program as required by the Chief Privacy Officer ;and
(iv) cooperate with the Chief Privacy Officer and the other Privacy Officers.

Default Privacy Officer 13.4 If at any moment in time there is no Privacy Officer designated for a function or business, the Marketing Director of a Business Group, Service Group or Corporate Staff for the relevant function or business is responsible for supervising compliance with this Code.

Privacy Officer with a statutory position 13.5 Where a Privacy Officer holds his position pursuant to law, he shall carry out his job responsibilities to the extent they do not conflict with his statutory position.

Article 14 – Policies and procedures

Policies and procedures 14.1 DSM shall develop and implement policies and procedures to comply with this Code.

System information 14.2 DSM shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Personal Data (e.g. inventory of systems and processes, privacy impact assessments).

Article 15 – Training

Staff training 15.1 DSM shall provide training on this Code and related confidentiality obligations to Staff members who have access to Personal Data.

Article 16 – Monitoring compliance

Audits

16.1 DSM Corporate Operational Audit shall audit business processes and procedures that involve the Processing of Personal Data for compliance with this Code. The audits shall be carried out in the course of the regular activities of DSM Corporate Operational Audit or at the request of the Chief Privacy Officer. The Chief Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Chief Privacy Officer and the appropriate Privacy Officers shall be informed of the results of the audits.

A copy of the audit results will be provided to the Dutch Data Protection Authority upon request.

DSM shall, if so indicated, ensure that adequate steps are taken to address breaches of this Code identified during the auditing of compliance pursuant to this Article 16.1.

Annual Privacy Report

16.2 The Chief Privacy Officer shall produce an annual Personal Data privacy report for the Managing Board on compliance with this Code and other relevant issues.

Each Privacy Officer shall provide information relevant to the report to the Chief Privacy Officer.

Article 17 – Complaints procedure

Complaint

17.1 Individuals may file a complaint regarding compliance with this Code 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 Privacy Officer.

The appropriate Privacy Officer shall:

(a) notify the Chief Privacy Officer;
(b) initiate an investigation; and
(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance.

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

Reply to Individual

17.2 Within four (4) weeks of DSM receiving a complaint, the appropriate Privacy Officer shall inform the Individual in writing either (i) of DSM's position with regard to the complaint and any action DSM has taken or will take in response or (ii) when he will be informed of DSM's position, which date shall be no later than four (4) weeks thereafter. The appropriate Privacy Officer

shall send a copy of the complaint and his written reply to the Chief Privacy Officer.

Complaint to Chief Privacy Officer

17.3 An Individual may file a complaint with the Chief Privacy Officer if:

(i) the resolution of the complaint by the appropriate Privacy Officer 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 will receive a response; or

(iv) in one of the events listed in Article 7.4.

The procedure described in Articles 17.1 through 17.2 shall apply to complaints filed with the Chief Privacy Officer.

Article 18 – Legal issues

Local law and jurisdiction

18.1 Any Processing by DSM of Personal Data shall be governed by applicable local law. Individuals keep their own rights and remedies as available in their local jurisdictions. Local government authorities having jurisdiction over the relevant matters shall maintain their authority.

Law applicable to Code; Code has supplemental character

18.2 This Code shall be governed by and interpreted in accordance with Dutch law. This Code shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Code, local law shall apply. Where this Code provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Code shall apply.

Lead authority for supervision of rules

18.3 Compliance with this Code shall be exclusively supervised by the Dutch Data Protection Authority in the Netherlands, which is also exclusively authorized to advise Koninklijke DSM N.V. on the application of this Code at all times. The Dutch Data Protection Authority shall have investigative powers based on the Dutch Data Protection Act. To the extent the Dutch Data Protection Authority has discretionary powers related to enforcement of the Dutch Data Protection Act, it shall have similar discretionary powers for enforcement of this Code.

Exclusive jurisdiction under Code

18.4 Any complaints or claims of an Individual concerning any supplemental right the Individual may have under this Code shall be directed to Koninklijke DSM N.V. only and shall be brought before the Dutch Data Protection Authority in the Netherlands or the competent court in Amsterdam, the Netherlands. The Dutch Data Protection Authority and courts in Amsterdam, the Netherlands have exclusive jurisdiction over any supplemental rights provided by this Code. Complaints and claims shall be admissible only if the Individual has

first followed the complaints procedure set forth in Article 17 of this Code.

Code enforceable against Koninklijke DSM N.V.

18.5 Any additional safeguards, rights or remedies granted to Individuals under this Code are granted by and enforceable in the Netherlands against Koninklijke DSM N.V. only.

Available remedies and limitation of damages

18.6 Individuals shall only be entitled to remedies available to data subjects under the Dutch Data Protection Act, the Dutch Civil Code and the Dutch Code on Civil Procedure. However, Koninklijke DSM N.V. shall be liable only for direct damages suffered by an Individual resulting from a violation of this Code. Where an Individual can demonstrate that it has suffered damage and establish facts which show it is plausible that the damage has occurred because of a violation of the Code, it will be for Koninklijke DSM N.V. to prove that the damages suffered by the Individual due to a violation of the Code are not attributable to the relevant Group Company.

Mutual assistance and redress

18.7 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 who receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding his 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 Koninklijke DSM N.V.

Article 19 – Sanctions for non-compliance

Non-compliance

19.1 Non-compliance of Staff with this Code may result in disciplinary action up to and including termination of employment.

Article 20 – Conflicts between the Code and applicable local law

Conflict of law when transferring Data

20.1 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 Chief Privacy Officer. The Chief Privacy Officer has to seek the advice of the Director DSM Legal Affairs. The Chief Privacy Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.

Conflict between Code and law

20.2 In all other cases, where there is a conflict between applicable local law and the Code, the Responsible Executive shall consult with the Chief Privacy Officer to determine how to comply with this Code and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.

New conflicting legal requirements

20.3 The Responsible Executive shall promptly inform the Chief Privacy Officer of any new legal requirement that may interfere with DSM's ability to comply with this Code.

Article 21 – Changes to the Code

21.1 Any changes to this Code require the prior approval of the Director DSM Legal Affairs. Koninklijke DSM N.V. shall notify the Dutch Data Protection Authority in case of significant changes to the Code on a yearly basis.

21.2 This Code may be changed without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.

21.3 Any amendment shall enter into force after it has been approved and published on the DSM website and DSM Intranet.

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

Article 22 – Transition Periods

General transition period

22.1 Except as indicated below, there shall be a two-year transition period for compliance with this Code. Accordingly, except as otherwise indicated, within two years of the Effective Date, all Processing of Personal Data shall be undertaken in compliance with the Code. During any transition period, DSM shall strive to comply with the Code.

Transition period for new Group Companies

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

Transition Period for Divested Entities

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

Transition period for IT Systems

22.4 Where implementation of this Code requires updates or changes to information technology systems (including replacement of systems), the transition period shall be four 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.

Transition period for existing agreements 22.5 Where there are existing agreements with Third Parties that are affected by this Code, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.

Transitional period for local-for-local systems 22.6 Processing of Personal Data that were collected in connection with activities of a Group Company located in a Non-Adequate Country shall be brought into compliance with this Code within five years of the Effective Date.

Contact details

DSM Legal Affairs
Ms. Carola Beaumont – senior legal counsel
c/o Head office Koninklijke DSM N.V.
PO 6500
6401 JH Heerlen
The Netherlands
Tel: +31 45-578 2439
E-mail: carola.beaumont@dsm.com

ANNEX 1 Definitions

Archive	ARCHIVE shall mean a collection of Personal Data that are no longer necessary to achieve the purposes for which the 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 this Code.
Business Contact Data	BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Individual in his contact with DSM.
Business Partner	BUSINESS PARTNER shall mean any Third Party, other than a Customer or Supplier, that has or had a business relationship or strategic alliance with DSM (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Chief Privacy Officer	CHIEF PRIVACY OFFICER shall mean the officer as referred to in Article 13.1.
Code	CODE shall mean this Privacy Code for Customer, Supplier and Business Partner Data.
Customer	CUSTOMER shall mean any Third Party that purchases, may purchase or has purchased a DSM product or service.
Director DSM Legal Affairs	DIRECTOR DSM LEGAL AFFAIRS shall mean the Corporate Director DSM Legal Affairs.
Divested Entity	DIVESTED ENTITY shall mean the divestment by DSM of a Group Company or business by means of: (a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or (b) a demerger, sale of assets, or any other manner or form.
DSM	DSM shall mean Koninklijke DSM N.V. and its Group Companies.
Effective Date	EFFECTIVE DATE shall mean the date on which this Code becomes effective as set forth in Article 1.6.
Employee	EMPLOYEE shall mean an employee, job applicant or former employee of DSM. This term does not include people working at DSM as consultants or employees of Third Parties providing services to DSM.

Employee Data	EMPLOYEE DATA shall mean any information relating to an identified or identifiable Employee.
EEA	EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
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.
Exporting Group Company	EXPORTING GROUP COMPANY shall mean the Group Company located within the EEA that transfers Personal Data to a Group Company located in a Non-Adequate Country.
Group Company	GROUP COMPANY shall mean Koninklijke DSM N.V. and any company or legal entity of which Koninklijke DSM N.V. directly or indirectly owns more than 50% of the issued share capital, has more than 50% of the voting power at general meetings of shareholders, has the power to appoint a majority of the directors, or otherwise directs the activities of such other legal entity; however, any such company or legal entity shall be deemed a Group Company only as long as a liaison and/or relationship exists.
Head of Compliance	HEAD OF COMPLIANCE shall mean the Head of Compliance of Koninklijke DSM N.V.
Individual	INDIVIDUAL shall mean any (employee of or any person working for) Customer, Supplier or Business Partner.
Personal Data or Data	PERSONAL DATA shall mean any information relating to an identified or identifiable Individual.
Managing Board	MANAGING BOARD shall mean the managing board of Koninklijke DSM N.V.
Non-Adequate Country	NON-ADEQUATE COUNTRY shall mean a country that under applicable local law (such as Article 25 of the EU Data Protection Directive) is deemed not to provide an "adequate" level of data protection.
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 DSM or rights of Individuals set forth in Article 12.2 and 12.3 may, under specific circumstances, be overridden if this pressing interest outweighs the interest of the Individual.

Privacy Council	PRIVACY COUNCIL shall mean the council referred to in Article 13.2.
Privacy Officer	PRIVACY OFFICER shall mean a privacy officer appointed by the Chief Privacy Officer pursuant to Article 13.3.
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.
Koninklijke DSM N.V.	KONINKLIJKE DSM N.V. shall mean Koninklijke DSM N.V., having its registered seat in Heerlen (Netherlands).
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean the Business Group Director, the Service Group Director and the Corporate Staff Director.
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 that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic code, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Supplier	SUPPLIER shall mean any Third Party that provides goods or services to DSM (e.g. an agent, consultant or vendor).
Staff	STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using DSM information technology systems or working primarily from DSM's premises.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside DSM.
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 DSM that is not under the direct authority of DSM.

Interpretations

INTERPRETATION OF THIS CODE:
(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 this Code
(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning
(iv) the male form shall include the female form
(v) 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 and
(vi) a reference to a document (including, without limitation, a reference to this Code) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Code or that other document.

Heerlen, February 17, 2014