UNIVAR SOLUTIONS

Binding Corporate Rules for Data Privacy and Data Protection

Version:	V2
Supersedes:	V1
Effective date:	01.06.2021
Next review date:	01.06.2022
Distribution:	All employees
Owner: Global Privacy Counsel	Sabine Duyfjes
Approved date:	
Approved by: Global General Counsel	Noelle Perkins
Signature	

1. INTRODUCTION

Univar Solutions is a world leader in the distribution of chemistry and related products and services, and is more than just a distribution company; it is a global partner to customers and suppliers dedicated to:

- Earning customers for life
- Using its global network to provide market insight and expertise to grow its customers' business
- Uncompromising safety and compliance
- Creating enduring supplier relationships
- Providing an innovative suite of value-added services

Our scale, geographic reach, diversified distribution channels, industry expertise and comprehensive product portfolio enable us to develop strong and long-term relationships with our suppliers and provide a single-source solution for our customers.

Univar Solutions operates over 650 distribution sites globally and serves more than 100,000 customers in over 130 countries worldwide with 10,300 employees.

Univar Solutions maintains privacy principles designed to reflect Univar Solutions' continuing commitment to privacy and data protection compliance. The Information Security and Protection Policy (Annex 1) together with the Privacy Policy (Annex 2), other key documents and this document constitute Univar Solutions' Binding Corporate Rules for Data Privacy and Protection ("**BCRs**").

The BCRs express the commitment of our employees, Executive Management and Board of Directors to data privacy to protecting all information relating to identified or identifiable natural individuals (hereinafter referred as "**Data Subjects**"). Univar Solutions processes certain information about Data Subjects while performing its business (hereinafter referred as "**Personal Information or Personal Data**"). Univar Solutions is committed to ensuring adequate protection for the transfer of Personal Information between Univar Solutions entities. The BCRs set out Univar Solutions' overall approach to privacy and data protection and also emphasize the key role our employees play in protecting Personal Information.

Data Protection Laws and Regulations give Data Subjects certain rights as to how their Personal Information shall be handled. As a global company, Univar Solutions' use of Personal Information is subject to a variety of laws. Thus, the European General Data Protection Regulation does not allow the transfer of Personal Information to countries outside the European Economic Area (hereinafter referred as "**EEA**") that do not ensure an adequate level of data protection.

To avoid breaching the laws, the Univar Solutions entities take proper steps to ensure that the processing of Personal Information on an international basis is safe and hence lawful.

Univar Solutions' BCRs represent company-wide global privacy rules. The BCRs contain rules and other policies and procedures that are designed to implement the privacy principles that must be followed by all Univar Solutions employees and contractors.

In order to be fully compliant with the existing data protection laws, Univar Solutions must put proper measures in place that the use of Personal Information on an international level is safe and hence lawful.

The purpose of these BCRs is therefore to establish a framework to follow the regulations of the different jurisdictions and, as a result, provide an adequate level of protection for all Personal Information used and collected by Univar Solutions and transferred from one Univar Solutions entity to another.

Univar Solutions' BCRs apply to all its entities globally and all entities are legally bound to comply with these BCRs.

Univar Solutions has appointed a Global Privacy Counsel, located in EMEA as the appropriate person to oversee and ensure compliance with all aspects of the BCRs. The Global Privacy Counsel reports to the Global General Counsel. If required, the Global Privacy Counsel will be supported by local lawyers at a regional and country level. In addition, all Univar Solutions entities operating in EMEA have appointed a local data protection officer in order to support the Global Privacy Counsel.

If you have any questions regarding the BCRs, your rights under data protection laws or any other data protection issues, you may contact Univar Solutions' Global Privacy Counsel who will either deal with the matter or forward it to the appropriate person or department within Univar Solutions. The Global Privacy Counsel is responsible for ensuring that changes to these BCRs are notified to Univar Solutions entities and to individuals whose Personal Information is processed by Univar Solutions.

The Global Privacy Counsel can be contacted at sabine.duyfjes@univarsolutions.com / dataprivacy.emea@univarsolutions.com for EMEA and at or dataprivacy@univarsolutions.com for the US and the rest of the world.

2. SCOPE OF THE BCRs

The BCRs apply to all Personal Information used and collected by Univar Solutions entities wherever they are located. They are binding on all Univar Solutions entities. As a result, all Univar Solutions entities are under a legal duty to comply with the BCRs. An up-to-date list of these entities can be found in Annex 3.

The BCRs are communicated to all Univar Solutions employees and published on the internal website accessible at https://univar1.sharepoint.com/SitePages/UnivarHome.aspx.

The BCRs are as well published on our external website (http://www.univarsolutions.com/) in order to make them accessible for our business partners (suppliers, customers, logistic partners, contractors, etc.)

The BCRs define the rules applicable to Univar Solutions entities in relation to Personal Information

- that is processed by any of the Univar Solutions entities,
- the processing of which is subject to regulation by local legislation implementing the European General Data Protection Regulation.

The BCRs apply to

(i) the processing of Personal Information by Univar Solutions as Data Controller in the EEA

(ii) the processing of Personal Information in the EEA by Univar Solutions as Data Controller located outside of the EEA

(iii) any transfer of Personal Information out of the EEA by one Univar Solutions entity to another; and

(iv) any processing or onward transfer of Personal Information by one Univar Solutions entity in the EEA to another that is outside of the EEA

In relation to the above paragraph and the BCRs, United Kingdom is not considered part of the EEA after the 1 January 2021 when the transition period of United Kingdom leaving the European Union ended.

3. CATEGORIES OF DATA SUBJECTS AND PURPOSES OF PROCESSING AND TRANSFERS

Univar Solutions processes and transfers Personal Information including Sensitive Personal Information relating to the following types of Data Subjects:

- Customers
- Suppliers
- Logistic partners
- Contractors
- Consultants, advisors and professional experts
- Agents
- Univar Solutions' employees, former employees, dependents and beneficiaries of employees and former employees in connection with their work relationship or application for employment
- Other persons as appropriate to conduct its business with Univar Solutions

4. NATURE OF DATA TRANSFERRED

The processing and transfer of Personal Information undertaken by Univar Solutions entities relating to the types of Data Subjects discussed above include processing for the following business purposes:

- ***HR administration:*** recruitment, removals, payments, performance management, payroll and administration of employee benefits, training, discipline, work management or any other personal matters in relation to the employees

- ***Advertising, marketing, business and public relations:*** business development, maintaining and building upon customer and supplier relationships, business planning, etc.

- ***Accounts and records:*** keeping accounts related to any business or other activity carried on, decision as to whether to accept any person as a business partner, keeping records of purchases, sales or other transactions for the purpose of ensuring that the requisite payments and deliveries are made or services provided by them in respect of those transactions or for the purpose of making financial or management forecasts to assist them in the conduct of any such business or activity

Univar Solutions processes and transfers a broad range of Personal Information between Univar Solutions entities and third parties. The following types of Personal Information are distinguished:

- ***Business Related Information:*** is information needed to conduct business, including but not limited to, name, title, business address, business, business phone numbers, and business e-mail addresses. It also includes Personal Information that an employee or contractor voluntarily uploads into the business directory or directs Human Resources to do so, such as a personal mobile number.

- ***Employment Related Information:*** includes, but is not limited to, health records, benefit information, staff development records, attendance records (including any days off due to illness), salary remuneration and expenses information, expatriate information, equal opportunities management, grievance and disciplinary procedures, employee share equity holdings, employment termination information, names, addresses, date of birth, work location, employee performance, trade union membership and next of kin.

- ***Sensitive Personal Information:*** includes any information related to racial or ethnic origin, political opinions, religious or other similar beliefs, membership of trade unions, physical or mental health or condition, sexual life and convictions, proceedings and criminal acts.

  Univar Solutions collects and uses Sensitive Personal Information only if necessary for Health, Safety or Compliance purposes. This information deserves more stringent protection than other personal information, so Univar Solutions' standards of care clearly define when storage or use of this type of information is required. Univar Solutions always assesses whether Sensitive Personal Information is essential for the respective topic.

Information about race, religion and ethnics are stored for tax purposes as well as any purpose to avoid any discrimination. Those data are solely accessible for HR and the Compliance office.

Information about membership of trade unions is stored for legal reasons to assure compliance with the labour laws (as union members enjoy additional employment protection e.g.)

Information about physical health and condition are stored as far as disclosed to employers from a legal perspective, in order to comply with social security and labour law requirements as well as for statistical purposes to measure health of the company overall (the latter is anonymised).

Information about proceedings and criminal acts is collected and stored as far as legally permitted to fulfil cooperate legal requirements for legal representatives of the company, financial obligations imposed on employees, such as pledges on salaries and the like, to do background checks in countries where it is permitted, such as Russia and others.

5. APPLICABLE LAW

Univar Solutions handles Personal Information and Personal Sensitive Information in accordance with the BCRs and all applicable local data protection and privacy laws and regulations, including, but not limited to, the European Union General Data Protection Regulation (Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC) and the local data protection regulations in the different countries.

Where local data protection and privacy laws provide less protection than those set out in Univar Solutions' BCRs, the BCRs will apply. Whereas, where local data protection and privacy laws provide a higher protection, the local regulations will apply.

6. DEFINITIONS

Access Control	The process of limiting access to system resources and information based on job requirements or on a need-to-know basis.
Business Related Information	Information needed to conduct business including, but not limited to, name, title, business address, business phone numbers, and business emails. It also includes Personal Information that an employee or contractor voluntarily uploads into the business directory or directs to human resources to do so, such as a personal mobile number.
Data Controller	Natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data.
Data Processor	Natural or legal person, public authority, agency or any other body which processes personal data on behalf of the Data Controller.
Data Protection Officer	Any natural person responsible for data protection issues in specific entities across EMEA
Data Subject	A living identifiable person who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural, or social identity.
Entity	Any legal entity of the Univar Solutions Group that exports or imports Personal Information.
Information Security and Protection Policy and Standards	The total set of requirements with regards to protecting the confidentiality, integrity, and availability of company information and information systems for the Univar Solutions Group.
Personal Information / Personal Data	Any information relating to an identified or identifiable natural living person. This may or may not include Sensitive Personal Information, such as race, gender, or ethnicity, as well as Business Related Information and Special Handling Information.
Processing	Any operation or set of operations which is performed upon personal data, whether or not by automatic means, such as collection, recording, organization, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, blocking, erasure or destruction.
Security Incident / Breach Incident	A type of incident that involves (a) loss of company information, (b) loss of control of a system, or (c) loss of a type of data that requires special handling and disclosure procedures as defined by law or contract, such as the discovery of child pornography or a breach of credit card data.
Sensitive Personal Information	Includes any information related to racial or ethnic origin, political opinions, religious or other similar beliefs, membership of trade unions, physical or mental health or

	condition, sexual life and convictions, proceedings and criminal acts.
Special Handling Information	Is where data combinations trigger breach notification provisions of any state, province, or national government, with a SSN, bank account number, credit/debit card number, or medical or health information.
Third Country	A country that is not a member of the European Economic Area (EEA) that has not been recognised as having adequate laws to protect personal data. Considering that the transition period for United Kingdom to leave the European Union ended on 1 January 2021, United Kingdom is considered a Third Country until it has been recognised by the EU as having the adequate level of data protection.
Third Party	Means any natural or legal person, public authority, agency or any other body other than the data subject, the controller, the processor and the persons who, under the direct authority of the controller or the processor, are authorized to process the data.

7. UNIVAR SOLUTIONS' PRIVACY RULES

7.1 Complying with local laws

Univar Solutions will ensure Personal Information is collected and used in compliance with local laws.

Where the BCRs or Univar Solutions' guidelines differ from local laws or regulations, Univar Solutions will always follow the higher standard.

The BCRs also apply where Univar Solutions entities process Personal Information on behalf of other Univar Solutions entities.

7.2 Ensuring Transparency

Univar Solutions will explain to Data Subjects how their Personal Information will be used.

Univar Solutions will provide clear and comprehensive notice when Personal Information is collected describing how that information will be used and with whom it will be shared, unless there is a legitimate basis for not doing so, e.g. any criminal intention of the data subject, which can be proven by Univar Solutions.

7.3 Using Personal Information for a valid purpose

Univar Solutions will only collect and use Personal Information for purposes which are relevant to Univar Solutions and are known to the Data Subjects.

If Univar Solutions changes the purpose for which Personal Information is used, Univar Solutions will make individuals aware of the changes, unless the changes are within the individual's expectations and they can express their concerns or unless there is a legitimate basis for not doing so, e.g. any criminal intention of the Data Subject, which can be proven by Univar Solutions. If Univar Solutions changes the purpose for which Personal Information is used, Univar Solutions may be required to ask the individuals concerned for their consent. This is typically accomplished by posting an updated privacy notice or sending messages to individuals in order to gain their consent for using their Personal Information.

Univar Solutions will identify and clearly explain the purposes for which Personal Information will be used.

In order to reduce the risk of exposure, Univar Solutions should not keep data for longer than needed for the purposes for which it was collected. Once the retention period is over, the data can only be retained if anonymized.

7.4 Ensuring data quality

Univar Solutions will only collect and use Personal Information that is relevant and not excessive for the purpose. Univar Solutions will keep Personal Information accurate and up to date. Univar Solutions will only retain Personal Information for as long as is necessary to meet the purpose or other legal requirements.

The Data Subjects can always ask for their Personal Information held by Univar Solutions and they can ask for their Personal Information to be amended if that information is not accurate. The Data Subjects can do this by way of oral or written communication by contacting the appropriate departments within Univar Solutions or the Global Privacy Counsel.

7.5 Taking appropriate security measures

Univar Solutions takes reasonable precautions, including implementation of physical, administrative and technical safeguards, to protect Personal Information from loss, misuse, unauthorised access, disclosure, alteration or destruction. The specific requirements about implementing security measures are set out in Univar Solutions' global "Information Security and Protection Policy" (Annex 1)

7.6 Honouring individuals' rights

Data Subjects must be allowed to correct, amend, or delete their Personal Information when it is inaccurate. This can be achieved by having users send their update requests to the respective departments or to the Global Privacy Counsel (dataprivacy.emea@univarsolutions.com or dataprivacy@univarsolutions.com).

Univar Solutions will respond to inquiries or requests made by individuals about their Personal Information within one month as of receipt. If the inquire or request is complex or if multiple requests are received from the same Data Subject, Univar Solutions may extend its response time for additional two months. Univar Solutions will reply to requests to rectify, delete, block or cease processing Personal Information.

Univar Solutions will respond to requests from individuals whose information is collected and used by Univar Solutions, in accordance with the Privacy Access Request Procedure (more details about this procedure can be found in Annex 4)

7.7 Protecting Personal Information transferred to third parties

Univar Solutions will ensure that Personal Information transferred to third parties is adequately protected according to Articles 28, 32, 44, 45, 46 and 49 of the General Data Protection Regulation.

Transfers of Personal Information to third parties outside Univar Solutions are not allowed without appropriate steps being taken to ensure that there is a legal basis for the transfer, and to protect the Personal Information being transferred, such as contractual clauses and whether the third party is a Data Controller or a service provider.

For example, where a third party service provider processes Personal Information on behalf of Univar Solutions, Univar Solutions will enter into a contract with that provider which states that the third party service provider is a Data Processor of Univar Solutions, will act only on its instructions and will adopt proportionate technical and organisational security measures to safeguard the Personal Information.

However, before Univar Solutions starts to do any business with a third party that touches its sensitive data, Univar Solutions' data security department undertakes a full audit of the

third party to address those concerns. The audit questionnaire has to be completed by the third party as the first step. This is followed by an interview with Univar Solutions' data security managers and approval of that department is a condition precedent to start working with the third party.

The contract mentioned above will refer to full adherence of data privacy rules and data security as well as to allow regular audits as appropriate.

Univar Solutions will assure its counterparts also have BCRs or adequate measure embedded in their policies. The contracts are not unilateral as being signed by both parties at the beginning of the business relation. Univar Solutions undertakes a full fletch due diligence of the data protection tools of any company it plans to exchange sensitive data with and will only start such exchange after its IT security officer has approved the security level of such company.

Appropriate technical and organisational measures to protect Personal Information are also applied during the transfer of the Personal Information to a third party.

Validation of security measures implemented by third parties takes place during the procurement process and is repeated periodically as required, for example in response to contract renewal or changes in business, legal or regulatory requirements.

7.8 Safeguarding the use of Sensitive Personal Information

Univar Solutions will only use Sensitive Personal Information if it is absolutely necessary, unless Univar Solutions has an alternative legitimate basis for using the information.

Univar Solutions classifies Personal Information based upon its sensitivity. Univar Solutions implements appropriate technical and organisational measures to protect Sensitive Personal Information, based on its classification.

Univar Solutions will only collect and use Sensitive Personal Information where the Data Subject's express consent has been obtained unless Univar Solutions has a legitimate basis for doing so, e.g. any criminal intention of the Data Subject, which can be proven by Univar Solutions.

The permissions of Data Subjects to use Sensitive Personal Information by Univar Solutions must be genuine and freely given.

7.9 Using Personal Information for direct marketing

Univar Solutions will not use Personal Information for direct marketing to a consumer unless the consumer has at the point of collecting the data agreed to that use. Univar Solutions will give all individuals the opportunity to opt out from receiving direct marketing from Univar Solutions. Univar Solutions will honour the "opt out" requests it receives.

7.10 Training

All Univar Solutions employees shall take privacy training in order to improve their practical skills and knowledge that relate to data protection issues. This privacy training is part of everyone's professional development with Univar Solutions.

Furthermore, all employees shall be required to take Privacy training on an annualbasis. All employees must take the online training course and pass the knowledge check included in that training and confirm at the end of the online training their knowledge and skills on privacy issues.

New employees shall be required to take an online privacy compliance training course within 30 days after the day they are hired.

Univar Solutions will offer a privacy training to all new and current HR and IT personnel who handle Sensitive Personal Information on an annual basis.

BCRs and all related guidelines, procedures and policies shall be uploaded on Univar Solutions' intranet page and permanently accessible to every Univar Solutions employee.

Access to the BCRs and all related guidelines, procedures or policies shall be granted to every Univar Solutions new employee.

Internal Privacy Notices shall also be communicated and made available within the group to raise awareness on the BCRs.

At the local level each Data Protection Officer shall feel free to enhance the privacy training courses described above by adding any appropriate training material. They may also develop and offer additional training in countries where the laws are more stringent.

Privacy training programs shall be reviewed and approved by experienced Univar Solutions employees and senior management in coordination with the local Data Protection Officers and the Global Privacy Counsel.

7.11 Auditing

Univar Solutions will be accountable for measuring and reporting compliance with BCRs.

Univar Solutions will regularly audit, using appropriately skilled internal or external resources, Univar Solutions' systems that process Personal Data on compliance with the BCRs.

Under specific circumstances (i.e. data protection incidents, complaints by data subjects, etc.), Univar Solutions' Global General Counsel and the Global Privacy Counsel can request additional ad-hoc BCR audits outside the regular audit plan for BCR audits.

If a BCR audit concludes that corrective actions are needed to maintain compliance with the BCR, the BCR audit team shall also conduct necessary monitoring and follow-up and ensure that the necessary corrective actions are implemented.

Univar Solutions' Global General Counsel and the Global Privacy Counsel shall receive the full BCR audit report. The results of the BCR audit are made available to the competent

data protection authority upon request. Univar Solutions may redact parts of the audit data to the extent necessary to protect confidential company information.

7.12 Handling Complaints

In accordance with global privacy rules, all employees, contractors, customers, and suppliers have the right to submit a complaint to Univar Solutions or supervisory authority related to how Univar Solutions handles the Personal Information it collects about them.

Univar Solutions will follow the Privacy Complaint Procedure set out in Annex 4.

The Privacy Complaint Procedure describes the process used to respond to a complaint from an employee, contractor, customer, or supplier or any other individual who believes that Univar Solutions has interfered with their privacy and/or Univar Solutions denied their request to access or modify their Personal Information.

In addition, any Data Subject has the right to lodge a complaint before a competent data protection authority or to lodge a complaint before the courts with the choice of jurisdiction.

7.13 Handling Breach Incidents

Univar Solutions will follow the Privacy Incident Response Procedure set out in Annex 4

The Privacy Incident Response Procedure describes the process used to Breach Incidents. Breach Incidents involve the knowledge or reasonable belief that there may have been an unauthorized or inappropriate collection, use, access, disclosure, modification, and/or exposure of Personal Information.

7.14 Liability

Each participating entity within the EEA is liable for any breach of the BCR committed by the participating company.

In addition, Univar Solutions B.V., based in the Netherlands accepts liability for non-compliance with the BCRs by participating entities established outside the EEA, including the undertaking to pay compensation for the damages in the event of a proven breach of the BCRs and a resulting violation of a Data Subject's rights caused by such non-compliance of a non-EEA participating entity. It furthermore agrees to take the necessary corrective actions to remedy breaches of the BCRs of entities established outside the EEA.

The burden of proof in case of a breach of the BCRs resides with the member of Univar Solutions at the origin of the transfer or with that part of the company with delegated data protection responsibilities. In case of any denial of responsibility by a group member, Univar Solutions BV will step in as the ultimate liable member. Univar Solutions BV as the company with delegated data protection responsibilities will always be jointly responsible for the burden of proof and any consequences resulting of any breach.

The burden of proof lies with Univar Solutions. Univar Solutions shall demonstrate that no breach of the BCRs has taken place or that the participating entity established outside the EEA is not responsible for the breach of the BCRs on which the Data Subject's claim for damages is based.

7.15 Univar Solutions intragroup co-operation and co-operation with Data Protection Authorities

The purpose of Univar Solutions' BCRs is to establish Univar Solutions' approach to compliance with privacy laws.

Univar Solutions has designated a Data Protection Officer for each EEA country and UK and each of them is responsible for monitoring compliance of the BCRs for his/her country. Globally, the Global Privacy Counsel is responsible for compliance of Univar Solutions' BCRs by its employees.

Univar Solutions' Global General Counsel and the Global Privacy Counsel can request ad-hoc BCR audits from Univar Solutions' Internal Audit Department.

Co-operation between the Univar Solutions entities:

Univar Solutions entities will co-operate and assist each other and the the Global Privacy Counsel and/or local Data Protection Officers when handling requests or complaints regarding the BCRs from individuals or national Data Protection Authorities.

Univar Solutions entities will comply with any instructions requiring the remedy of a breach of the BCRs.

Co-operation with Data Protection Authorities:

Where required, Univar Solutions will make the necessary personnel available for dialogues with the Data Protection Authorities in relation to the BCRs.

Univar Solutions will actively review and consider:

- any decisions made by relevant data protection authorities on any data protection law issues that may affect the BCRs; and
- Univar Solutions will abide by any decision of the applicable data protection authority on any issue related to the interpretation and application of the BCRs where a right to appeal is not exercised.

Audit by Data Protection Authorities:

Univar Solutions will, upon request by a data protection authority of competent jurisdiction, provide the authority with a copy of the results of any audit of the BCRs conducted under the Audit Protocol.

Where any Univar Solutions entity subject to the BCRs is located within the jurisdiction of a data protection authority based in the EEA, Univar Solutions agrees that the data protection authority may audit that Univar Solutions entity for the purpose of reviewing compliance with the BCRs.

Any audit by a data protection authority will be carried out in accordance with the applicable law of the country in which the Univar Solutions entity is located. In the case of a Univar Solutions entity located outside EEA, the audit will be carried out in accordance with the applicable law of the EEA country from which the Personal Information is transferred under the BCRs.

Where appropriate, the relevant data protection authority will provide Univar Solutions with reasonable prior written notice of its intention to carry out an audit. Audits will be conducted with full respect to the confidentiality of the information obtained and to the trade secrets of Univar Solutions.

7.16 Updating the BCRs

Communicating changes to data protection authorities:

Univar Solutions will inform the Dutch Data Protection Authority and any other relevant EEA data protection authority of any substantial changes to the BCRs or to the list of members at least once a year. The Global Privacy Counsel is responsible for communicating changes to the BCRs, and will also provide a brief explanation of the reasons for any notified changes to the BCRs. However, Univar Solutions is not obliged to communicate changes to the BCRs which are administrative in nature or which have occurred as a result of a change of applicable data protection law in any EEA country through any legislative, court or supervisory authority measure unless they

- result in change to the BCRs, or
- affect the authorisation of the BCRs by EEA data protection authorities.

Communicating changes to the Univar Solutions entities and individuals:

The Global Privacy Counsel will communicate the amended BCRs to the Univar Solutions entities bound by the BCRs through its internal communication channels and will publish the amended BCRs on Univar Solutions' intranet and external webpage.

Inclusion of new Univar Solutions entities:

Univar Solutions will ensure that all new Univar Solutions entities are considered for inclusion in the list of Univar Solutions entities bound by the BCRs. Univar Solutions will also ensure that the necessary legal, administrative, operational and technical measures are in place before a transfer of Personal Information to or from a new Univar Solutions

entity takes place. Hence, no transfer will be made to a new Univar Solutions entity until that new entity is effectively bound by the BCRs and can deliver compliance.

Tracking of any changes to the BCRs:

The Global Privacy Counsel is responsible for keeping a fully updated list of the members of the group and for keeping track of and record any updates to the BCRs and provide the necessary information to the Data Subjects or the Dutch Data Protection Authority.

7.17 Conflicting legal requirements

If Univar Solutions becomes aware of a conflict between national laws and the BCRs which would prevent Univar Solutions from complying with the BCRs, the Global General Counsel will be promptly informed of the conflict. The Global General Counsel will decide how to resolve the issue and will consult with the appropriate data protection authority if necessary.

ANNEX 1

INFORMATION SECURITY AND PROTECTION POLICY

ANNEX 2

PRIVACY POLICY

ANNEX 3

UNIVAR SOLUTIONS ENTITIES

Univar Solutions entities operating in the European Economic Area:

Belgium	Univar Solutions Belgium NV/SA
Czech Republic	Univar Solutions s.r.o.
Denmark	Univar Solutions Denmark A/S
Finland	Univar Solutions Oy
France	Univar Solutions SAS
Germany	Univar Solutions GmbH
Greece	Univar Solutions Hellas EPE
Hungary	Univar Solutions Hungary Sales Limited Liability Company
Ireland	Univar Solutions Ireland Limited
Italy	Univar Solutions S.p.A.
Netherlands	Univar Solutions B.V. Univar Solutions Netherlands B.V. Chempoint.com-EMEA BV
Norway	Univar Solutions AS
Poland	Univar Solutions Sp. Z.o.o
Portugal	Univar Solutions Portugal SA
Spain	Univar Solutions Spain SA
Sweden	Univar Solutions AB
Switzerland	Univar Solutions AG

Univar Solutions entities operating outside the European Economic Area:

Brazil	Univar Solutions Brasil Ltd.
Canada	Univar Canada Limited
Dubai	Univar Solutions Middle East & Africa FZE
Egypt	Univar Egypt LLC
Mexico	Univar de Mexico, S.A. de C.V.
Tunisia	Univar Tunisia SARL
Turkey	Univar Solutions Kimya Sanayi Limited Şirketi
Russia	Univar Solutions LLC
United Kingdom	Univar Solutions UK Limited Univar Specialty Consumables Limited
United States of America	Univar Solutions Inc. Univar Solutions USA Inc. Chempoint.com Inc.

ANNEX 4
Privacy Access Request Procedure
Privacy Complaint Procedure
Privacy Incident Procedure