

AkzoNobel

Binding Corporate Rules (BCR)

(Binding Corporate Rules for the transfer of personal data outside the EEA under Article 47 GDPR)

Introduction

AkzoNobel has committed itself to the protection of personal data of AkzoNobel employees, customers, business partners, and other individuals in the AkzoNobel Code of Conduct. This BCR describes how this principle shall be implemented.

This BCR constitutes Binding Corporate Rules for the transfer of personal data to a third country outside the EEA under Article 47 GDPR and is legally binding and shall apply to and be enforced by AkzoNobel and its Group Companies, including Employees.

Capitalized terms have the meaning set out in **Annex 1** (Definitions). Capitalized terms that are not defined in this BCR have the meanings given to them in the GDPR.

Article 1. Scope

This BCR applies to the Processing of Personal Data by Akzo Nobel N.V. and its wholly or majority-owned affiliates (each a **Group Company**, collectively **AkzoNobel**).

1.1 Scope

The BCR addresses the Processing of personal data of: (a) Customers, Suppliers, and Business Partners (**CSB Data**); and (b) Employees and their dependents (**Employee Data**) (jointly referred to as **Personal Data**), by AkzoNobel or a Third Party Processor on behalf of AkzoNobel, that are: (i) subject to EEA Data Protection Laws (or were subject to EEA Data Protection Laws prior to the Transfer to a Group Company), and (ii) are transferred to a Group Company in a Third Country. The Transfers under this BCR are described in more detail in Annex 2. Customers, Suppliers, Business Partners, and Employees are jointly referred to as **Individuals**.

Individuals will keep any rights and remedies they may have under applicable local law. For the avoidance of doubt (i) where applicable local law provides more protection than this BCR, local law will apply in addition to this BCR and (ii) where this BCR provides more protection than

applicable local law or provides additional safeguards, rights or remedies for Individuals, this BCR for Personal Data will apply in addition to applicable local law.

Article 2. Purposes for Processing Personal Data

AkzoNobel only Processes Personal Data for appropriate business purposes or with the Individual's consent.

2.1 Fair and Lawful processing

Personal Data shall be Processed fairly and lawfully. Lawful Processing means that AkzoNobel will not Process Personal Data, unless one of the following conditions applies:

- (i) AkzoNobel needs to Process Personal Data to:
 - (a) Perform a contract to which the Individual is a party or in order to take steps at the request of the Individual prior to entering into a contract;
 - (b) comply with a legal obligation to which AkzoNobel is subject;
 - (c) protect the vital interests of the Individual;
- (ii) AkzoNobel needs to carry out such Processing to pursue AkzoNobel's legitimate interests, and these interests do not prejudice the interests or fundamental rights and freedoms of the Individual concerned; or
- (iii) the Individual concerned has consented to the Processing, by providing a freely given, specific, informed and unambiguous indication of the Individual's wishes by a clear affirmative action.

AkzoNobel will not use Personal Data for new purposes without following our internal procedures to verify that such Processing can take place lawfully.

2.2 Purposes for Processing Personal Data

AkzoNobel Processes Personal Data for one or more of the business purposes set out in Annex 2 (**Business Purposes**). These processing purposes can generally be based on one of the legal bases listed above but remain subject to any applicable requirements and restrictions under EEA Data Protection Law.

In deviation of the above, AkzoNobel will only Process Employee Data of dependents if:

- (i) the Personal Data were provided with the consent of the Employee or the Dependent;
- (ii) Processing of the Personal Data is reasonably necessary for the performance of a contract with the Employee or for managing the employment-at-will relationship; or
- (iii) Processing is required or permitted by applicable local law.

Employee Data of dependents will be considered Employee Data for the purposes of this BCR and dependents shall have the same rights as Employees under this BCR.

2.3 Secondary Purposes for Processing Personal Data

Personal Data may be Processed for a purpose other than those specified in **Annex 2** (a Secondary Purpose) only if the additional purpose is closely related to (or compatible with) a specified Business Purpose taking into account the link between the original and additional

purpose, the context in which the Personal Data are collected, the nature of the relevant Personal Data and the implementation of appropriate safeguards set out below. Examples of Processing for Secondary Purposes that may be permissible include:

- (i) anonymization of Personal Data;
- (ii) internal audits or investigations;
- (iii) implementation of business controls and operational efficiency;
- (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, including archiving Personal Data for these purposes;
- (vi) enforcement of contracts or dispute resolution;
- (vii) legal advice or business consulting; or
- (viii) insurance purposes.

Depending on the sensitivity of the relevant Personal Data and the possible consequences for the Individual, the Processing for a Secondary Purpose may require additional safeguards (such as limiting access to the Personal Data or taking additional security measures) to mitigate the consequences. If the consequences cannot be appropriately mitigated, AkzoNobel may need to provide the Individual the opportunity to object to the Processing or obtain the Individual's consent.

The Business Purposes and Secondary Purposes together constitute the **Processing Purposes**.

2.4 Processing of Sensitive Data

AkzoNobel respects the sensitivity of Sensitive Data, and the Processing thereof will be prohibited, with the following exceptions:

- **Criminal data.** AkzoNobel may Process Sensitive Data relating to criminal convictions and offences or related security measures where such Processing is carried out under the control of official authority or is authorized by EEA Law for one of the purposes specified in Annex 2; and
- **Other categories.** AkzoNobel may Process other categories of Sensitive Data:
 - a) as required or allowed by EEA Law (e.g., in the field of employment and social security and social protection law, the assessment of the working capacity of employees, for reasons of public interest, and for archiving, scientific or historical research purposes or statistical purposes);
 - b) as necessary for the establishment, exercise or defence of a legal claim;
 - c) as necessary to protect a vital interest of an Individual, but only where it is impossible to obtain the Individual's consent first;
 - d) relating to Sensitive Data that have been manifestly made public by the Individual (e.g., posted or otherwise shared at the Individual's own initiative on AkzoNobel social media); or
 - e) based on the Individual's explicit consent.

Sensitive Data may be Processed for Secondary Purposes in accordance with Articles 2.3 and 2.4.

2.5 Consent for Processing of Personal Data

If a legal ground as set forth in article 2.1(i),(ii) and (iii) does not exist or if EEA Law so requires AkzoNobel shall (also) seek consent from the Individual for the Processing.

When seeking consent, AkzoNobel shall in addition to the information about inform the Individual about:

- (i) the purposes of the Processing;
- (ii) the Group Company that is responsible for the Processing;
- (iii) the right to withdraw consent at any time without detriment and for Employee Data, that this will be without consequence to the Employees' employment relationship; and
- (iv) the fact that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal.

If an Individual withdraws consent, AkzoNobel will discontinue Processing as soon as reasonably possible. The withdrawal of consent will not affect (i) the lawfulness of the Processing based on such consent before its withdrawal or (ii) the lawfulness of Processing for Processing Purposes not based on consent after withdrawal.

In relation to Employee Data, Employee consent cannot be used as a legitimate basis for Processing. One of the Business Purposes must exist for any Processing of Employee Data. If none of the Business Purposes apply, AkzoNobel may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee. A request for Employee consent requires the authorization of the appropriate I&C Business Partner prior to seeking consent.

2.6 Automated Decisions

Individuals have the right not to be subject to a decision based solely on automated decision-making, including profiling, that produces legal or similarly significant effects on the individual. This restriction does not apply if:

- (i) the use of automated tools is authorized by EEA law; or
- (ii) the decision is made by AkzoNobel for purposes of (i) entering into or performing a contract, including assessing creditworthiness or eligibility or for fraud prevention purposes or (ii) managing the contract or employment-at-will relationship, provided the underlying request leading to a decision by AkzoNobel was made by the individual; or
- (iii) the decision is made based on the explicit consent of the individual.

Items (ii) and (iii) apply only if suitable measures are taken to safeguard the legitimate interests of the Individual (including by providing the Individual with an opportunity to express his or her point of view and the right to obtain human intervention on the part of the Controller).

AkzoNobel will only base automated decisions on Sensitive Data with the Individual's explicit consent or where processing is necessary for reasons of substantial public interest on the basis of EEA law.

Article 3. Quantity and Quality of Personal Data

AkzoNobel takes measures to collect and process only Personal Data relevant to the Processing Purposes, to retain them only as long as needed for these purposes and to keep them up-to-date during Processing. AkzoNobel is further committed to 'privacy by design and by default' principles.

3.1 No Excessive Personal Data

AkzoNobel will only Process those elements of Personal Data that are adequate, relevant and limited to what is necessary for the applicable Processing Purposes and only as long as needed for its Processing Purposes, including as needed to comply with law. AkzoNobel will take steps to (i) delete, de-identify, or otherwise destroy Personal Data that are not needed for a Processing Purpose, and (ii) rectify Personal Data that is inaccurate without undue delay.

3.2 Storage Period

AkzoNobel specifies – e.g. in a policy, statement, records retention schedule or in new systems via 'privacy by design' - a time period for which certain categories of Personal Data may be kept, which means not for longer than necessary for the applicable Processing Purpose.

Upon the end of the storage period, the Personal Data shall be:

- (i) securely deleted or destroyed;
- (ii) anonymized; or
- (iii) kept as necessary for litigation purposes or compliance with legal record keeping obligations.

3.3 Quality of Personal Data

Personal Data will be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Processing Purpose. AkzoNobel shall take reasonable steps to rectify or erase Personal Data that is inaccurate without delay.

Article 4. Information Requirements

AkzoNobel informs Individuals about the Processing of their Personal Data, including through privacy policies or notices.

4.1 Information Requirements

At the time when Personal Data is obtained from the Individual, or prior to Processing such Personal Data for a Secondary Purpose, AkzoNobel shall inform Individuals through a privacy policy or privacy notice of the following:

- (i) the nature and categories of Personal Data Processed;
- (ii) the Group Company or Group Companies that are solely or jointly responsible for the Processing and their contact details;

- (iii) the contact details of the Corporate Privacy Officer or designated central point of contact for privacy and data protection matters;
- (iv) the Processing Purposes for which their Personal Data are Processed;
- (v) the legal basis for the Processing of their Personal Data and, if the Processing is based on the legitimate interests of AkzoNobel, of the legitimate interests pursued by AkzoNobel;
- (vi) the categories of recipients to which the Personal Data are disclosed (if any);
- (vii) if applicable, the fact that Personal Data will be transferred to an international organization, Processor, or other Third Party located in a Third Country, including the safeguards in place to protect the Personal Data; and
- (viii) and to the extent applicable, any other relevant information such as:
 - (a) the retention period of the Personal Data or the criteria to determine the retention period;
 - (b) the Individual's rights under this BCR and how these rights may be exercised, including the right to obtain compensation;
 - (c) the right to withdraw consent;
 - (d) the right to lodge a complaint to a Data Protection Authority or a competent court;
 - (e) whether an Individual is required to provide Personal Data;
 - (f) the existence of automated decision making, including profiling, and about the logic behind and envisaged consequences of this automated decision making; and
 - (g) if the Personal Data were not collected from the Individual, the source from which the Personal Data originate.

4.2 Personal Data not Obtained from the Individual

Where Personal Data has not been obtained directly from the Individual, AkzoNobel shall provide the Individual with the information as set out in Article 4.1(i)-(viii):

- (i) within a reasonable period after obtaining Personal Data but at the latest within one month, having regard to specific circumstances of the Personal Data Processed;
- (ii) if Personal Data are used for communication with an Individual, at the latest at the time of the first communication with the Individual;
- (iii) if a disclosure to another recipient is envisaged, at the latest when Personal Data are first disclosed.

4.3 Exceptions

The requirements of Articles 4.1 and 4.2 may be inapplicable if:

- (i) the Individual already has the relevant information;
- (ii) it would be impossible or would involve a disproportionate effort to provide the information to the Individual, in which case AkzoNobel will take appropriate measures to protect the Individual's rights and freedoms and legitimate interests, including making the information publicly available;
- (iii) obtaining Personal Data is expressly laid down in EEA Law that is necessary and

proportionate in a democratic society to protect one of the objectives listed in Article 23(1) GDPR; or

- (iv) Personal Data must remain confidential subject to an obligation of professional secrecy regulated by applicable local law, including a statutory obligation of secrecy.

Article 5. Rights of Individuals

AkzoNobel provides Individuals with the ability to request access to Personal Data Processed about them, and to request correction, deletion, restriction of such Personal Data, or to object to Processing thereof.

5.1 Right of Access

Every Individual has the right to request confirmation of whether or not his or her Personal Data are Processed, request a copy thereof, as well as request access to the information listed in Article 4.1.

5.2 Right to Rectification, Erasure, and Restriction

If Personal Data are incorrect, incomplete, or not Processed in compliance with EEA Data Protection Law or this BCR, the Individual has the right to have his or her Personal Data:

- (i) Rectified or completed, if such Personal Data are incorrect or incomplete;
- (ii) Erased or anonymized, if such Personal Data are not Processed in compliance with, or erasure is required by, EEA Data Protection Law or this BCR. If the Personal Data has been made public by AkzoNobel, and the Individual is entitled to erasure of Personal Data, in addition to erasing or anonymizing the relevant Personal Data, AkzoNobel shall, taking account of available technology and the cost of implementation, take reasonable steps to inform recipients with whom the Personal Data has been shared or who are linking to the relevant Personal Data, that the Individual has requested the erasure of Personal Data;
- (iii) Restricted from other Processing than storage, pending verification in case the accuracy of such Personal Data are contested or if the Individual objects to such Processing under Article 5.3(i), or where the Processing is unlawful or no longer needed, but the Individual prefers restriction to erasure of the Personal Data. AkzoNobel will only Process the restricted Personal Data with the Individual's consent or as permitted by EEA Data Protection Law. AkzoNobel will inform the Individual before the restriction is lifted.

AkzoNobel shall communicate any rectification, erasure, or restriction in accordance with the rights sub (i)-(iii) above, to any Third Party to whom the relevant Personal Data have been disclosed, unless this proves impossible or involves disproportionate effort. AkzoNobel will inform the Individual about those recipients upon request.

5.3 Right to Object

The Individual has the right to object to:

- (i) the Processing of his or her Personal Data on grounds relating to his or her particular situation, unless AkzoNobel can demonstrate prevailing compelling legitimate grounds for the Processing; and

- (ii) receiving marketing communications (including any profiling related thereto).

5.4 Restrictions to Rights of Individuals

The rights of Individuals set out in Articles 5.1-5.3 are subject to any applicable exceptions provided under EEA Data Protection Law. Depending on the relevant right of the Individual, exceptions may be available in cases where:

- (i) the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of AkzoNobel;
- (ii) the Processing is required by or allowed for a task carried out in the public interest, including in the area of public health and for archiving, scientific or historical research or statistical purposes;
- (iii) the Processing is necessary for exercising the right of freedom of expression and information;
- (iv) for the establishment, exercise or defence of legal claims;
- (v) the exercise of the rights adversely affects the rights and freedoms of AkzoNobel or others; or
- (vi) in case a specific restriction of the rights applies under EEA Law.

The right of access as set out in Article 5.1 can only be restricted by the circumstances under the circumstances listed in items (iii), (iv), and (v) above.

5.5 Procedure

An Individual may exercise rights under this Article 5, and lodge any other requests, by following the procedure outlined in **Annex 3** (Procedure for Data Subject Requests by Individuals).

5.6 No Requirement to Process Identifying Information

AkzoNobel is not obliged to Process additional information in order to be able to identify the Individual for the sole purpose of facilitating the rights of the Individual under this BCR. In this case, the rights under Article 5.1 through 5.3 shall not apply, except where the Individual, for the purpose of exercising those rights, provides additional information enabling his or her identification.

Article 6. Restrictions under EEA law

In certain cases, rights of Individuals and obligations of AkzoNobel under this BCR may be subject to lawful restrictions, e.g., to protect fundamental rights of others or to prevent, investigate or prosecute criminal offenses.

6.1 Restrictions under EEA law

Certain rights of Individuals and obligations of AkzoNobel in this BCR may in specific cases be subject to restrictions provided by EEA Law, as specified and applied in accordance with EEA Data Protection Law, such as to:

- (i) prevent or investigate criminal offences (including cooperating with law enforcement);

- (ii) Enforce civil law claims; or
- (iii) protect Individuals, or the rights and freedoms of other persons.

6.2 Consultation with Global Privacy Officer

Setting aside obligations of AkzoNobel or rights of Individuals based on a restriction under EEA law requires prior consultation of the Corporate Privacy Officer. The Corporate Privacy Officer shall document his or her advice.

Article 7. Security and Confidentiality Requirements

AkzoNobel takes appropriate measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition, or access, and to provide notification in the event of a Data Security Breach.

7.1 Information Security

AkzoNobel shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Individuals, take appropriate reasonable technical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, AkzoNobel has developed and implemented the information security policies and other policies relating to the protection of Personal Data.

7.2 Staff Access

Staff will be authorized to access Personal Data as necessary to serve the applicable Processing Purpose and to perform their job as instructed by AkzoNobel.

7.3 Staff Confidentiality

Staff who access Personal Data will meet their confidentiality obligations.

7.4 Data Security Breach Notification

Group Companies outside of the EEA shall notify Data Security Breaches without undue delay to the relevant I&C Business Partner and Akzo Nobel Nederland B.V. in accordance with AkzoNobel's established incident response procedures. Group Companies that act as internal Processors will notify the relevant Group Company that is the Controller of the affected Personal Data without undue delay upon becoming aware of the Data Security Breach. AkzoNobel shall notify the Competent Supervisory Authority of a Data Security Breach without undue delay, and where feasible within 72 hours after becoming aware of it, unless the Data Security Breach is unlikely to result in a risk to the rights and freedoms of Individuals.

If the Data Security Breach is likely to result in a high risk to the rights and freedoms of Individuals, AkzoNobel shall notify the affected Individuals of the Data Security Breach without undue delay following its determination that such a Data Security Breach has occurred.

AkzoNobel shall respond promptly to inquiries of Individuals relating to such Data Security Breach. Group Companies shall document Data Security Breaches (comprising the facts

relating to the personal data breach, its effects and the remedial action taken) and the documentation should be made available to the Competent Supervisory Authority on request.

Article 8. Disclosure of Personal Data to Third Parties

AkzoNobel may transfer Personal Data to Controllers or Processors to the extent necessary to serve the applicable Processing Purpose and provided data transfer safeguards are in place.

8.1 Transfers by AkzoNobel

Each Group Company may disclose Personal Data to Third Parties or other Group Companies for Processing as needed for the Business Purpose or with the Individual's consent in accordance with Article 2.5.

Disclosures to Third-Party Controllers. AkzoNobel shall seek to contractually safeguard the data protection interests of its Individuals when Personal Data are transferred to Third Party Controllers. This will include the safeguards set forth in Article 8.2.

Disclosures to Processors. Third Party Processors as well as internal Processors may Process Personal Data only if they have a written contract with AkzoNobel that describes the Processing. The contract with a Processor will include the following provisions:

- (i) the Processor shall Process Personal Data only in accordance with AkzoNobel's documented instructions and for the purposes authorized by AkzoNobel, including in relation to transfers of Personal Data to Third Countries;
- (ii) the Processor shall, and have persons it authorizes to Process Personal Data, keep the Personal Data confidential;
- (iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;
- (iv) the Processor shall not permit subcontractors and affiliates to Process Personal Data in connection with its obligations to AkzoNobel without (a) the prior specific or generic consent of AkzoNobel, and (b) a validly entered into written contract between the Processor and the subcontractor, which imposes data protection obligations that shall be no less protective than those imposed on the Processor, and provided that the Processor remains liable to AkzoNobel for the performance of the subcontractors. In case AkzoNobel gives generic consent, the Processor shall provide notice to AkzoNobel of any changes in its subcontractors and will provide AkzoNobel the opportunity to object to such changes based on reasonable grounds;
- (v) taking into account the nature of the processing, the Processor shall assist AkzoNobel by appropriate technical and organizational measures, insofar as this is possible, with the fulfilment of AkzoNobel's obligation to respond to Individuals' requests under Articles 5.1 – 5.3 and Individuals' rights under Article 2.6 and AkzoNobel's obligation to conduct Data Protection Impact Assessments in accordance with Article 9.7.
- (vi) AkzoNobel may review the security measures taken by the Processor and the Processor shall submit its relevant data processing facilities to audits and inspections by AkzoNobel, a Third Party on behalf of AkzoNobel or any relevant government authority. This may also

be done by means of a statement issued by a qualified independent third party assessor certifying that the information processing facilities of the Processor used for the Processing of Personal Data comply with the requirements of the contract;

- (vii) the Processor shall promptly inform AkzoNobel of any actual or suspected security breach involving Personal Data;
- (viii) the Processor shall take adequate remedial measures as soon as possible and shall promptly provide AkzoNobel with all relevant information and assistance as requested by AkzoNobel regarding the security breach;
- (ix) at the choice of AkzoNobel, the Processor shall delete or return all Personal Data to AkzoNobel at the end of the provision of services relating to the Processing of Personal Data, and shall delete all copies of the Personal Data, unless storing the Personal Data is required by law applicable to the Processor. The Processor shall continue to Process the Personal Data in accordance with the requirements of the contract as long as it has not returned or deleted all Personal Data (including copies), and will only retain the Personal Data to the extent and for as long as required under the relevant law.

8.2 Transfer to a Third Country

This Article sets forth additional rules for a Transfer to a Third Country (including onward transfers). Personal Data may be transferred to a Third Party in a Third Country only:

- (i) in accordance with a data transfer mechanism for the lawful Transfer of Personal Data recognized under EEA Data Protection Law;
- (ii) if item (i) does not apply, the Transfer is subject to an applicable derogation for specific situations under EEA Data Protection Law (e.g., the Transfer is necessary for the performance of a contract with the Individual, to protect a vital interest of the Individual, for the establishment, exercise, or defence of a legal claim, or for important reasons of public interest).

Item (ii) above requires the prior consultation of the Corporate Privacy Officer.

Prior to a Transfer under (i), AkzoNobel will conduct a Transfer Impact Assessment in accordance with Article 9.11.

Article 9. Accountability

This BCR is binding on AkzoNobel. AkzoNobel has created a privacy governance structure to oversee and manage compliance with this BCR and has implemented policies and procedures to comply with this BCR.

9.1 Role of Akzo Nobel Nederland B.V.

Akzo Nobel N.V. has tasked Akzo Nobel Nederland B.V. with the oversight, coordination and implementation of this BCR.

9.2 Binding Effect

This BCR is legally binding and shall apply to and be enforced by AkzoNobel and its Group Companies, including Employees. The responsible executives and the Controllers within AkzoNobel will be accountable for compliance with the BCR.

9.3 Privacy Governance

AkzoNobel has implemented a global compliance organization to oversee and manage compliance with this BCR as described in **Annex 4** (Privacy Governance Structure).

9.4 Policies and Procedures

This BCR supplement all AkzoNobel privacy policies, guidelines and notices that exist on the Effective Date. AkzoNobel has developed and will continue to develop policies and procedures to comply with this BCR.

9.5 Staff Training

AkzoNobel will provide appropriate and up-to-date training on the obligations and principles set forth in this BCR to its Staff. This training includes the following elements:

- (i) Basic privacy training for all Staff (i) with permanent or regular access to Personal Data; (ii) involved in the collection of Personal Data; (iii) and involved in the development of tools used to process Personal Data upon joining AkzoNobel and bi-annually thereafter;
- (ii) Annual privacy training for Staff directly involved in managing Disclosure Requests;
- (iii) Continuous education on privacy- and data protection-related skills and competences for Staff with specific privacy-related tasks; and
- (iv) Ad-hoc training conducted where a need for extra training is identified, for example to reinforce existing trainings or when a new law affects a particular role's activities.

9.6 Records of Processing Activities

AkzoNobel shall maintain Records of Processing Activities. A copy will be provided to the Competent Supervisory Authority upon request.

9.7 Data Protection Impact Assessment

AkzoNobel will maintain a procedure to conduct and document Data Protection Impact Assessments in accordance with EEA Data Protection Law. Where a Data Protection Impact Assessment shows that, despite mitigating measures taken by AkzoNobel, the Processing still presents a residual high risk for the rights and freedoms of the Individuals, the Competent Supervisory Authority will be consulted prior to such Processing taking place.

9.8 Monitoring and Audits

AkzoNobel shall monitor and audit compliance with this BCR in accordance with the procedures set forth in **Annex 5** (Procedures for Monitoring and Auditing Compliance).

Akzo Nobel Nederland B.V. shall take the necessary actions to remedy violations of this BCR by Group Companies outside the EEA that are identified during monitoring, auditing of compliance, or are otherwise brought to its attention. Akzo Nobel Nederland B.V. shall compensate Individuals who suffer damages as a consequence of such violation in accordance with Article 10.3.

9.9 Annual Privacy Report

The Corporate Privacy Officer shall produce an annual privacy report for the Executive Committee on compliance with this BCR, privacy protection risks and other relevant issues.

9.10 Sanctions for Non-Compliance

Non-compliance of Staff with this BCR may result in disciplinary action in accordance with AkzoNobel policies and local law, up to and including termination of employment or contract.

9.11 Transfer Impact Assessment

AkzoNobel will perform a Transfer Impact Assessment prior to a Transfer under this BCR and maintain it for the duration of the Transfer.

Where a Transfer Impact Assessment shows gap(s) in protection for Individuals under this BCR, AkzoNobel, with the involvement of Akzo Nobel Nederland B.V. and the Corporate Privacy Officer, will implement supplementary measures, such as contractual, technical, or organizational safeguards to be applied by the Data Exporter and/or Data Importer to enable them to fulfil their obligations under this BCR, including measures applied during transmission and to the Processing of Personal Data in the country of destination to ensure compliance with the BCR. Supplementary measures are not required in relation to laws and practices applicable to the Data Importer that respect the essence of fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) GDPR.

Each Group Company shall monitor its local laws and practices. If a Group Company learns of local laws or practices that prevent it from complying with this BCR or that have a substantial effect on its protection offered by this BCR, it will promptly notify the Data Exporter and Akzo Nobel Nederland B.V. Upon verification of such notification, the Data Exporter, with the involvement of Akzo Nobel Nederland B.V. and the Corporate Privacy Officer will promptly identify supplementary measures such as those outlined above. This requirement shall also apply where a Data Exporter has reasons to believe that a Data Importer can no longer fulfil its obligations under this BCR.

The Transfer shall not take place or will be suspended where: (i) compliance with this BCR cannot be assured (including where the Data Importer is in substantial or persistent breach of this BCR), (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent Supervisory Authority or in case of the Data Importer's non-compliance with a binding decision of a competent court or Competent Supervisory Authority. Any Transfer will be ended if compliance with the BCR is not restored within one month of the suspension of such Transfer. In this case, Personal Data Transferred prior to the suspension and any copies thereof should, at the choice of the Data Exporter, be returned or destroyed in their entirety.

AkzoNobel will conduct and document the Transfer Impact Assessment with the involvement of Akzo Nobel Nederland B.V. and the Corporate Privacy Officer and will notify the Data Exporter and Data Importer thereof. Akzo Nobel Nederland B.V. and the Corporate Privacy Officer will make the Transfer Impact Assessment, including any applicable supplementary measures, available to all Group Companies, so that the same supplementary measures and/or suspensions are applied to the same types of Transfers or where effective supplementary measures could not be put in place, the transfers at stake are suspended or ended, and to any Competent Supervisory Authority upon request.

9.12 'Privacy by Design and Default'

AkzoNobel uses, both at the time of determination of the means for Processing and at the time of the Processing itself, and taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of individuals, take appropriate technical and organizational steps to ensure that data protection principles are considered in the design of new systems and processes that Process Personal Data, consistent with privacy by design and privacy by default principles under applicable EEA Data Protection Laws.

Article 10. Complaints and Enforcement of Rights

This BCR provide enforceable rights to Individuals.

10.1 Complaints

Individuals may file a written (including by email) complaint in respect of or any violation of their rights under EEA Data Protection Law, or any claim under this BCR, in accordance with Annex 3. Individuals may also file a complaint or claim with the SAs or the courts in accordance with Article 10.3.

If AkzoNobel's response to the complaint is unsatisfactory to the Individual (e.g., the complaint is rejected) or AkzoNobel does not observe the conditions of the complaints procedure set out in this Article 10.1, the Individual can file a complaint with the Corporate Privacy Officer or a complaint or claim with the SAs or the courts in accordance with Article 10.3.

10.2 Enforcement Rights of Individuals

The rights contained in this Article are in addition to, and shall not prejudice, any other rights or remedies that these Individuals may otherwise have under EEA Data Protection Law.

Individuals are encouraged, but not required, to first file a complaint with AkzoNobel before filing any complaint or claim with a Supervisory Authority or court.

If AkzoNobel violates this BCR with respect to the Processing of Personal Data where such Processing is subject to EEA Data Protection Law (or was subject to EEA Data Protection Law prior to a Transfer of such Personal Data), the affected Individual can, as a third-party beneficiary, enforce Articles 2 - 5, 7, 8, 9.7, 9.11, 9.12, 10.1 - 10.4, 10.5, 10.6, 11, 12.1 and 12.2.

10.3 Jurisdiction for Complaints or Claims

The Individual may, at his or her choice, submit a complaint or a claim under Article 10.2 to:

- (i) The courts in the EEA country (a) where the Individual has his or her habitual residence, or (b) where the Group Company being the Controller or Processor of the relevant Personal Data is established, against the Group Company being the Controller or Processor of the relevant Personal Data or Akzo Nobel Nederland B.V.;
- (ii) The SA in the EEA country where (a) the Individual has his or her habitual residence or place of work, or (b) the alleged infringement took place, against the Group Company being the Controller or Processor of the relevant Personal Data or Akzo Nobel Nederland B.V.; or

(iii) The Lead SA or the courts in the Netherlands, against Akzo Nobel Nederland B.V.

Akzo Nobel Nederland B.V. accepts liability for a breach of this BCR by a Group Company located outside the EEA, although Akzo Nobel Nederland B.V. may assert any defense that the relevant non-EEA Group Company could have asserted. In such case, the courts or other judicial authorities in the Netherlands will have jurisdiction, and Individuals will have the rights and remedies against Akzo Nobel Nederland B.V. as if Akzo Nobel Nederland B.V. caused the breach of this BCR in the Netherlands.

Individuals may be represented by a not-for-profit body, organization, or association under the conditions set out in EEA Data Protection Laws.

10.4 Right of Individuals to Claim Damages

In case an Individual has a claim under Article 10.2, such Individual shall be entitled to compensation of material and non-material damages suffered by such Individual resulting from a violation of this BCR to the extent provided by applicable law of the relevant EEA country.

To bring a claim for damages, the Individual must demonstrate that he or she has suffered the relevant damages and to establish facts which show it is plausible that the damage has occurred because of a violation of this BCR. AkzoNobel must then prove that the damages suffered by such Individual are not attributable to AkzoNobel or a Processor or assert other applicable defenses.

10.5 Mutual Assistance and Redress

All Group Companies shall co-operate with and assist each other to handle a request, complaint or claim made by an Individual and investigations or inquiries by a Competent Supervisory Authority or public authority.

The Group Company that receives a request, complaint or claim from an Individual is responsible for promptly notifying the appropriate Privacy Coordinator thereof and handling any communication with such Individual regarding his or her request, complaint or claim as instructed by the appropriate I&C Business Partner, 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 Akzo Nobel Nederland B.V.

10.6 Cooperation with Competent Supervisory Authority

AkzoNobel shall cooperate with, and accept audits or inspection (including where necessary on-site) of the systems and facilities used by AkzoNobel to Process Personal Data by, the Competent Supervisory Authority in respect of any inquiry or investigation with regard to this BCR. AkzoNobel will also: (i) provide to the Competent Supervisory Authorities, upon request, information in relation to the Processing of Personal Data subject to this BCR; and (ii) take into account the advice of, and abide by decisions of, a Competent Supervisory Authority regarding issues related to this BCR.

Any dispute relating to the Competent Supervisory Authority's supervision of AkzoNobel's compliance with this BCR will be resolved by the courts of the EEA Country of that Supervisory Authority, in accordance with applicable local procedural law. AkzoNobel agrees to submit itself to the jurisdiction of these courts, insofar as the dispute relates to the Competent Supervisory Authority's supervision of AkzoNobel's compliance with this BCR.

Article 11. Conflicts and Notification Duties

11.1 Notification of Conflicts

Each Group Company shall monitor its local laws and practices. If a Group Company becomes aware that it cannot comply with this BCR, including if it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with this BCR or that have a substantial effect on the protection offered by this BCR (including on any Data Protection Impact Assessments or Transfer Impact Assessments performed thereunder), the relevant Group Company will promptly notify the relevant Data Exporter and Akzo Nobel Nederland B.V.

If a Group Company learns of local laws or practices that prevent it from complying with this BCR or that have a substantial effect on its protection offered by this BCR, it will determine, in consultation with the business and the Corporate Privacy Officer, how to comply with this BCR and address a potential conflict, including by promptly implementing appropriate supplementary measures in accordance with Article 9.11.

The Data Exporter will monitor, on an ongoing basis, and where appropriate in collaboration with the Data Importer, developments in the Third Country that could affect the initial Transfer Impact Assessment performed under Article 9.11.

11.2 Notification of Conflicts and Requests for Disclosure

Subject to the following paragraph, the Data Importer shall inform the affected Individual (where possible and with the help of the Data Exporter) and the Data Exporter, if the Data Importer receives a Disclosure Request. Notifications of a Disclosure Request shall include information about the Personal Data requested, the requesting body, the legal basis for the disclosure and the provided response or, in case of direct access, the notification shall include all relevant information available to the Data Importer.

The Data Importer will assess the legality of a Disclosure Request, in particular whether it remains within the powers granted to the requesting authority. The Data Importer will challenge Disclosure Requests that it considers unlawful under the laws of the Destination Country, applicable obligations under international law, or principles of international comity, and under the same conditions shall pursue possibilities to appeal. When challenging a Disclosure Request, the Data Importer shall seek interim measures with a view to suspending the effects of the Disclosure Request until the competent judicial authority has decided on its merits. The Data Importer shall not disclose the Personal Data requested until required to do so under the applicable procedural rules and will only provide the Personal Data that are strictly necessary when complying with a Disclosure Request, based on a reasonable interpretation thereof. The Data Importer will document this assessment and provide it to the Data Exporter and, upon request, to any Competent Supervisory Authority.

If notification of a Disclosure Request is prohibited, such as in case of a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation, the Data Importer will inform the Data Exporter to the maximum extent permitted by the relevant law, and will use its best efforts to waive this prohibition, will document these efforts, and demonstrate them upon request to the Data Exporter. The Data Importer will at regular intervals provide the Data Exporter with as much relevant information as possible on the requests received (such as the number of requests, type of Personal Data requested, requesting authority, whether requests have been challenged and the outcome of such challenges). This information will be preserved

and provided to any Supervisory Authority upon request. If the Data Importer is or becomes partially or completely prohibited from providing the Data Exporter with the aforementioned information, it will, without undue delay, inform the Data Exporter accordingly, to the maximum extent permitted.

The Data Importer will provide the minimum amount of information permissible when responding to a Disclosure Request. In any event, any disclosures by Data Importers of Personal Data to any authority in response to a Disclosure Request will not be massive, disproportionate or indiscriminate in a manner that would go beyond what is necessary in a democratic society.

Article 12. Adoption and Modification of this BCR

AkzoNobel has adopted this BCR and any changes will be made in accordance with the procedure set forth in this BCR.

12.1 Effective Date

This BCR has been adopted by the Management Board. It has entered into force as of 25 August 2014 (**Effective Date**). The BCR will be published on the AkzoNobel website. They will further be made available to Individuals upon request.

12.2 Changes

This BCR will be kept up to date in order to reflect any changes to the Processing of Personal Data or the regulatory obligations that apply thereto. Any changes to this BCR will require the prior approval of the Corporate Privacy Officer. All Group Companies will be informed of changes to this BCR and AkzoNobel will publish the new version of this BCR without undue delay. The Corporate Privacy Officer shall keep a record of any changes made to the BCR and will notify any changes including any updates to the list of Group Companies or the fact that no changes were made, to the relevant Supervisory Authorities via the Lead Supervisory Authority on an annual basis, including a brief explanation of the reasons justifying the update. The Corporate Privacy Officer will further provide the necessary information to Individuals. Where a change affects the protection offered by the BCR or significantly affects the BCR itself (e.g., changes to the binding character), the Corporate Privacy Officer will communicate these to the relevant Supervisory Authorities and the Lead Supervisory Authority in advance.

12.3 Transition Periods

(i) **Transition Period for New Group Companies**

Any entity that becomes a Group Company after the Effective Date shall comply with this BCR within two years of becoming a Group Company. During this transition period, no Personal Data will be transferred under this BCR until (a) the relevant Group Company has achieved compliance with this BCR or (b) an alternative data transfer mechanism has been implemented, such as standard contractual clauses.

(ii) **Transition Period for Divested Entities**

A Divested Entity (or specific parts thereof) may remain covered by this BCR after its divestment for such period as may be required by AkzoNobel to disentangle the Processing of Personal Data relating to such Divested Entity. If a Data Importer in a Third Country ceases to be a Group

Company or ceases to be bound by this BCR, it must delete the Personal Data received under these BCR unless: (i) it continues to comply with this BCR, or (ii) it implements and complies with another legal basis for data transfer under EEA Data Protection Law, such as standard contractual clauses.

Contact Details:

Akzo Nobel Nederland B.V.
c/o Corporate Privacy Officer
Christian Neefestraat 2
1077 WW Amsterdam

ANNEX 1 - DEFINITIONS

ADEQUACY DECISION means a decision issued by the European Commission under Article 45(3) of the GDPR that a country or region outside the EEA or a category of recipients in such country or region is deemed to provide an “adequate” level of data protection..

AKZONOBEL means Akzo Nobel N.V. and its Group Companies.

ARTICLE means an article in this BCR.

BCR means these AkzoNobel Binding Corporate Rules for Customer, Supplier, and Business Partner Data and any amendments thereto.

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

BUSINESS PURPOSE means a purpose for Processing Personal Data or for Processing Sensitive Data as specified in Article 2.

CORPORATE PRIVACY OFFICER means the officer as referred to in Section 1 of Annex 4.

COMPETENT SUPERVISORY AUTHORITY means the Supervisory Authority competent for the Data Exporter(s) of the specific Transfer.

CUSTOMER means any organization that purchases, may purchase or has purchased an AkzoNobel product or service, any Third Party that provides goods or services to AkzoNobel (e.g. an agent, consultant or vendor), or any Third Party that has or had a business relationship with AkzoNobel.

CSB DATA means the Personal Data of any (employee of or person working for) Customer, Supplier or Business Partner and any other individual that AkzoNobel processes in the context of the provision of its services.

DATA EXPORTER means the Group Company that Transfers Personal Data under this BCR.

DATA IMPORTER means the Group Company that is the recipient of a Transfer under this BCR.

DATA PROTECTION IMPACT ASSESSMENT (DPIA) means a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Personal Data, where such Processing is likely to result in a high risk for the rights and freedoms of Individuals, in particular where new technologies are used. A DPIA shall contain:

- a description of:
 - the scope and context of the Processing;
 - the Processing Purposes for which Personal Data are Processed;
 - the specific purposes for which Sensitive Data are Processed;
 - categories of recipients of Personal Data, including recipients not covered by an

- Adequacy Decision;
- Personal Data storage periods;
- an assessment of:
 - the necessity and proportionality of the Processing;
 - the risks to the privacy rights of Individuals; and
 - the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Personal Data.

DATA SECURITY BREACH means 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.

DESTINATION COUNTRY means Third Country to which Personal Data are transferred.

DEPENDENT means the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee.

DISCLOSURE REQUEST means a legally binding request for disclosure of (or direct access to) Personal Data from a public authority of a Destination Country or a public authority of another Third Country. This does not include a request that is necessary and proportionate in a democratic society to protect one of the objectives listed in article 23(1) of the GDPR.

DIVESTED ENTITY means the divestment by AkzoNobel of a Group Company or business by means of:

- a sale of shares that results in the divested Group Company no longer qualifying as a Group Company; and/or
- a demerger, sale of assets, or any other manner or form.

EEA or **EUROPEAN ECONOMIC AREA** means all Member States of the European Union, Norway, Iceland and Liechtenstein and, for the purposes of this BCR, Switzerland. AkzoNobel' General Counsel can decide to include other countries in this definition, provided that such country is subject to an Adequacy Decision.

EEA COUNTRIES means the countries in the EEA.

EEA DATA PROTECTION LAW means the provisions of mandatory law of an EEA country containing rules for the protection of Individuals with regard to the Processing of Personal Data including security requirements for and the free movement of such Personal Data.

EEA LAW means the laws and regulations of the EEA applicable to AkzoNobel as the case may be from time to time.

EFFECTIVE DATE means the date on which this BCR becomes effective as set forth in Article 12.1.

EMPLOYEE means any natural person in the context of the person's employment or similar relationship with AkzoNobel, such as:

- an Individual, job applicant or former Individual of AkzoNobel including temporary workers working under the direct supervision of AkzoNobel (e.g., independent contractors and trainees). This term does not include people working at AkzoNobel as consultants or Individuals of Third Parties providing services to AkzoNobel;
- a (former) executive or non-executive director of AkzoNobel or (former) member of the supervisory board or similar body to AkzoNobel.

EMPLOYEE DATA means shall mean any information relating to an identified or identifiable Employee (and their dependents).

GDPR means Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

GENERAL COUNSEL means the General Counsel of AkzoNobel.

GROUP COMPANY means Akzo Nobel N.V. and any company or legal entity of which Akzo Nobel N.V., directly or indirectly owns more than 50% of the issued share capital, has 50% or more 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 (i) as long as a liaison and/or relationship exists, and (ii) as long as it is covered by the AkzoNobel Policy Book and AkzoNobel Code of Business Conduct.

INDIVIDUAL means (i) any (person working for a) Customer and any other individual whose Personal Data AkzoNobel processes in the context of the manufacturing of its products and the sale of these products and the provision of related services; and/or (ii) an Employee.

LEAD SA means the Supervisory Authority of the Netherlands (*Autoriteit Persoonsgegevens*).

ORGANIZATIONAL UNIT means a unit that is delivering services, responsible for business or regional or functional tasks within AkzoNobel.

ORIGINAL PURPOSE means the purpose for which Personal Data were originally collected.

PERSONAL DATA means any information relating to an identified or identifiable Individual.

PROCESSING means 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.

PROCESSING PURPOSES means the Business Purposes and in respect of Sensitive Data, the specific or general purpose for Processing Sensitive Data listed in **Annex 2** (Purposes of Processing) as well as the Secondary Purposes.

PROCESSOR means Internal Processor or Third Party Processor.

PROCESSOR CONTRACT means any contract for the Processing of Personal Data entered into by AkzoNobel and a Third Party Processor.

RECORDS OF PROCESSING ACTIVITIES means a record of Processing activities maintained in writing, including in electronic form, by AkzoNobel that contains the following information:

- a. the name and contact details of the Group Company that is the Controller;
- b. the Processing Purposes;
- c. the categories of Personal Data and the categories of Individuals;
- d. the categories of recipients to whom Personal Data have been disclosed;
- e. where applicable, information about Transfers of Personal Data to a country not subject to an Adequacy Decision;
- f. where possible, the envisaged retention periods; and
- g. where possible, a general description of the measures under Article 7.1.

Where a Group Company acts as an internal Processor, the Records of Processing Activities shall:

1. in addition to the above, include the name and contact details of the Group Company that is the Processor, and
2. instead of item b through – d above, include the categories of Processing carried out on behalf of the Group Company that is the Controller.

SUPPLIER means any Third Party that provides goods or services to AkzoNobel (e.g. an agent, consultant, vendor, or contingent worker).

SECONDARY PURPOSE means any purpose other than the Original Purpose for which Personal Data are further Processed.

SENSITIVE DATA means Personal Data that reveal an Individual's racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning an Individual's sex life or sexual orientation, along with Personal Data relating to criminal convictions and offences or social security numbers issued by the government.

STAFF means all Individuals and other persons who Process Personal Data as part of their respective duties or responsibilities using AkzoNobel information technology systems or working primarily from AkzoNobel's premises.

SUPERVISORY AUTHORITY means an EEA supervisory authority, duly constituted and competent in accordance with applicable EEA Data Protection Law.

THIRD COUNTRY means a country outside the EEA to which Personal Data are transferred, where such Transfer is not covered by an Adequacy Decision.

THIRD PARTY means any person or entity (e.g., an organization or public authority) outside AkzoNobel.

THIRD PARTY CONTROLLER means a Third Party that Processes Personal Data and determines the

purpose and means of the Processing.

THIRD PARTY PROCESSOR means a Third Party that Processes Personal Data on behalf of AkzoNobel and at its direction as a Controller.

TRANSFER means a transfer (or set of transfers) of, including disclosure of, or remote access to, Personal Data that are subject to EEA Data Protection Law to a Third Country.

TRANSFER IMPACT ASSESSMENT means an assessment on whether, taking into account the specific circumstances of the Transfer, the laws and practices of the third country of destination to which Personal Data are Transferred (**Third Country**), including those requiring the disclosure of Personal Data to public authorities or authorizing access by such authorities, prevent AkzoNobel from fulfilling its obligations under this BCR.

In assessing the laws and practices of the Third Country, AkzoNobel shall take into account in particular:

- a. the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Third Country or to another Third Country, including:
 - i. purposes for which the data are Transferred and Processed;
 - ii. types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
 - iii. economic sector in which the Transfers occur;
 - iv. categories and format of the Personal Data Transferred;
 - v. location of the Processing including storage;
 - vi. transmission channels used.
- b. the laws and practices of the Third Country relevant in light of the circumstances of the Transfers, including requirements to disclose Personal Data to public authorities or authorizing access by such authorities as well as the applicable limitations and safeguards. This also includes laws and practices providing for access to Personal Data during transit between the country of the Data Exporter and the Third Country;
- c. any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under this BCR, including measures applied during transmission and to the Processing of Personal Data in the Third Country.

INTERPRETATION OF THIS BCR:

- 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;
- headings are included for convenience only and are not to be used in construing any provision of this BCR;

- if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- 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;
- a reference to a document (including, without limitation, a reference to this BCR) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this BCR or that other document; and
- 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.
- Terms that are not defined in this BCR have the meanings given to them in the GDPR.

ANNEX 2 - DESCRIPTION OF PROCESSING

The tables below describe the categories Personal Data, the type of Processing and their purposes, the categories of Individuals, and the Third Countries for AkzoNobel's Transfers under this BCR. As a global group of companies, AkzoNobel continuously transfers Personal Data between its various Group Companies for the purposes set out below. A list of the Group Companies is available [here](#).

I. CSB Data

1. Categories of CSB Data

Category of Personal Data	Examples of Data Elements
Basic Personal details	Name, business addresses and telephone numbers, e-mail address, mobile telephone numbers.
Other Personal details	Home addresses and telephone numbers, website login and passwords, internal identification number.
Business communications	Information included in requests from, or correspondence with, a (prospective) customer
Order information	Ordered products or services, order history, data generated during the performance of the agreement
Payment information	Bank account number or credit card number
Analytics information	Information about the use of AkzoNobel's websites, apps, or other services, IP address, device information, click and surf behaviour, session length, and responses to customer satisfaction surveys
Sanctions information	Information included on publicly available government and/or law enforcement sanctions lists.
Company information	Chamber of commerce details, VAT details, tax details, which may include personal data for independent contractors or other small businesses
Photo and video	A copy of an identity document including a photo, CCTV footage, or video in relation to videoconferences.
Criminal data	Information relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour.
Health and religion information	Information regarding religion, dietary preferences or disability that can be accommodated during a visit to AkzoNobel offices.

2. Purposes for which CSB Data are Processed

Purpose of Processing	Examples of Processing Activities
Business communication	Communicating with (prospective) customers, such as, answering questions or replying to communications.
Customer assessment and acceptance	Customer assessment and acceptance processes, such as, confirming and verifying identity, due diligence, and screening against publicly available government and/or law enforcement agency sanctions lists.

Concluding and executing agreements	Administrative processes, such as, sending invoices, making payments, delivering or receiving services, including related customer services.
Monitoring and investigating compliance	Monitoring and/or investigating compliance with applicable laws, regulations, and/or AkzoNobel policy or conditions, anti-money laundering and anti-terrorism screening.
Website and/or mobile app usage	Providing functionalities of websites and mobile apps, including administering user accounts, improving performance, saving preferences or products, enabling sharing functionalities.
Compliance with law	Complying with obligations under applicable laws and regulations, such as, tax or business conduct related obligations.
Protecting health, safety, security and ensuring integrity	Safeguarding the health and safety of Employees, customers, suppliers and business partners, such as, via access controls to AkzoNobel's systems and premises, sanctions checks against publicly available sanctions lists, protecting premises using CCTV cameras, and using road-facing cameras on trucks transporting hazardous materials.
Business process execution and internal management	General management, order management and asset management, such as, leveraging central processing facilities in order to work more efficiently, conducting audits and investigations, implementing business controls, managing and using customer, supplier and business partner directories, finance, accounting, archiving, insurance, legal and business consulting, and dispute resolution.
Organizational analysis and development, management reporting, and acquisitions and divestitures	Aggregating or anonymizing Personal Data to prepare and perform management reporting and analysis, conducting customer, supplier and business partner surveys, processing Personal Data in the context of mergers, acquisitions and divestitures and in order to manage such transactions.
Development and improvement of products and services	Assessing, analysing and improve products and (customer) services, using and combining Personal Data to analyse customer behaviour and to adjust our products and services accordingly, compiling analytics reports on the use of company websites or apps, assessing (online) campaigns and adjusting products and services accordingly, to ensure that it is relevant to customers, including analysing how often customers read newsletters, how often they visit company websites or apps, which pages they click on what goods or services they purchase through company websites or apps.
Relationship management and marketing	Sending newsletters, offers, or other relationship management or marketing communications, including promotions or invitations to events, administering events or promotions, providing customer services, perform account management, and communicate recalls, developing, executing and analysing marketing strategies.
Administering events and promotions	Communicating about promotions and inviting (prospective) customers to participate in events, organizing and administering events, and measuring response to events and/or promotions.

Social media connections	Communicating with (prospective) customers on social media, if connected with the company social media account, processing 'likes' on company websites and mobile apps, other social media interaction, such as liking the company social media page.
--------------------------	---

3. Purposes for which Sensitive Data are Processed

Purpose of Processing	Examples of Processing Activities
Security and facility access	In some countries photos and video images of Individuals qualify as Sensitive Data. AkzoNobel may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of (the interests and assets of) AkzoNobel, its Employees, joint ventures, participations, Customers, Suppliers and Business Partners (including safeguarding the integrity of AkzoNobel and monitoring of Customers, Suppliers and Business Partners), site access and security reasons, the identification and the authentication for compliance with financial regulatory laws, anti-money laundering and financing of terrorism laws of Customer, Supplier or Business Partner status and access rights, demographic reporting under applicable anti-discrimination laws and to record decisions made in the course of business for future reference (e.g. when Individuals participate in video conferencing which is recorded).
Customer assessment and acceptance	<p>Criminal data, including data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour, may be used insofar as necessary for assessment and acceptance of a Customer, Supplier or Business Partner, including the identification and authentication of Customers, Supplier or Business Partners (including confirming and verifying the identity of relevant Individuals).</p> <p>Physical or mental health data may be used insofar as necessary for the assessment and acceptance of a Customer, Supplier and Business Partner, including assessing and making decisions on (continued) eligibility for projects or scope of responsibilities, the execution of an agreement with a Customer, and compliance with AkzoNobel's duty of care towards Customers and Individuals.</p>
Protecting health, safety, security and ensuring integrity	<p>Criminal data, including data relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour, may be used for protecting the interests of AkzoNobel, its Employees, joint ventures, participations and Customers with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against AkzoNobel, its Employees, joint ventures, participations and Customers.</p> <p>Biometric data may be used for security and access management purposes in relation to AkzoNobel's premises and systems.</p>

Customer accommodation	Data on religious or philosophical beliefs may be used insofar as necessary for accommodating specific products or services for a Customer, dietary requirements or religious holidays.
------------------------	---

4. Third Countries to which CSB Data are Transferred

Third Country		
Argentina	Honduras	Qatar
Aruba	Hong Kong	Russia
Australia	India	Saudi Arabia
Bolivia	Indonesia	Singapore
Botswana	Kenya	South Africa
Brazil	Kuwait	Sri Lanka
Cayman Islands	Malaysia	Taiwan
Chile	Mauritius	Thailand
China	Mexico	Tunisia
Colombia	Morocco	Turkey
Costa Rica	Myanmar	Uganda
Curacao	Nicaragua	Ukraine
Ecuador	Oman	United Arab Emirates
Egypt	Pakistan	United States of America
El Salvador	Panama	Uruguay
Eswatini	Papua New Guinea	Vietnam
Guatemala	Peru	Zambia

II. Employee Data

1. Categories of Employee Data

Category of Employee Data	Examples of Employee Data Elements
Basic personal details	Name, Employee identification number, work and home contact details (email, phone numbers, physical address), language(s) spoken, gender, date and place of birth, marital status, national identification and passport number, tax identification and social security or national insurance number, next of kin, information to verify identity (including mother's maiden name), emergency contact information, photograph, Employee number, information about spouses, dependents and beneficiaries, birth certificate, marriage certificate and will in case of death in service situation.
Documentation required under immigration laws	Citizenship, passport data, details of residency or work permit.
Compensation, benefits and payroll	Base salary, bonus, benefits, compensation type, pay grade, salary step within assigned grade, details on shares options, shares schemes and other awards, currency, pay frequency, effective date of current compensation, salary reviews, driver's licence details, company car details and registration and driver numbers, including information relating to driver eligibility, parking and entry permits, banking and bank account

	details, corporate credit card, working time records (including pay data and payment history), time and attendance data, previous salaries, national insurance or other number, marital/civil partnership status, domestic partners and dependents.
Position information	Previous positions held, description of current position, job title, corporate status, management category, job code, job function(s) and subfunction(s), company name and code (legal employer entity), branch/unit/department, location, employment status and type, full-time/part-time, terms of employment, employment contract, work history, hire/re-hire and termination date(s) and reason, length of service, retirement eligibility, promotions and disciplinary records, Employee-benefits related information, date of transfers, and reporting manager(s) and supervisors information.
Talent management information	Details contained in letters of application and CV (previous employment background, education history (including institutions attended and performance), employment history such as date of hire, professional qualifications, language and other relevant skills, certification, certification expiration dates, information necessary to complete a background check, details on performance management ratings, development programmes planned and attended, e-learning programmes, (Trade Union) memberships in case of reimbursement of membership fees, job performance, conduct and development information, willingness to relocate or driver's license information.
Management records	Details of any shares of ordinary shares or directorships.
System and application access data	Information required to access company systems and applications such as System/User ID, LAN ID, email account, instant messaging account, mainframe ID, previous Employee ID, previous manager Employee ID, system passwords, branch, state, country code, previous company details, previous branch details, previous department details, information collected through automated means, and electronic content containing personal information produced by you using company systems or accounts, including documents, emails and telephone conversations and voicemails, including information concerning use of and personal information transmitted through AkzoNobel information systems, information arising from access badge.
Racial or ethnic data	Photos (e.g., a copy of a passport containing a photo) and video images which, in some countries, qualify as racial or ethnic data.
Physical or mental health data	Any information or opinion of physical or mental health and data relating to disabilities, disability status, (work-related) incident and or personal injury information, medical certificates, occupational health reports, health surveillance screening, return to work forms and absence due to illness or pregnancy and/or adoption of employee or partner, drugs and alcohol testing (in certain circumstances, depending on role and local requirements).
Criminal data	Information relating to criminal behaviour, criminal records or proceedings regarding criminal or unlawful behaviour.
Sexual preference	Information on sexual preference.

Biometric data	Data resulting from specific technical processing relating to the physical, physiological or behavioural characteristics of a natural person, which allow or confirm the unique identification of that natural person.
----------------	--

2. Purposes for which Employee Data are Processed

Purpose of Processing	Examples of Processing Activities
Managing Workforce	Managing work activities and personnel generally, including recruitment, appraisals, performance management, promotions and succession planning, rehiring, administering salary, and payment administration and reviews, wages and other awards such as stock appreciation rights and bonuses, healthcare, medical insurance, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honouring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing employee surveys, performing background checks, monitoring compliance with internal policies, rules and procedures, internal investigations and managing disciplinary matters, grievances and terminations, reviewing employment decisions, making business travel arrangements, managing business expenses and reimbursements, planning and monitoring of training requirements and career development activities and skills, workforce reporting and data analytics/ trend analysis, and creating and maintaining one or more internal employee directories.
Workforce Analytics	Analytics for succession planning, workforce management, and data security, such as, analytics to assist in planning succession and to ensure business continuity, to design employee retention programs and diversity initiatives (e.g. Gender Gap Pay report), to offer training opportunities and to identify patterns in the use of technology systems to information entrusted to AkzoNobel as well as to protect AkzoNobel's people and property.
Communications, IT/Cybersecurity, Facilities and Emergencies	Facilitating communication with employees, ensuring business continuity and crisis management, providing references, protecting the health and safety of employees and others, safeguarding and maintaining IT infrastructure, office equipment, facilities and other property, facilitating communication with employees and their nominated contacts in an emergency.

3. Purposes for which Sensitive Data are Processed

Purpose of Processing	Examples of Processing Activities
Security and facility access	In some countries photos and video images of Employees qualify as Sensitive Data. AkzoNobel may process photos (e.g. a copy of a passport containing a photo) and video images for the protection of (the interests and assets of) AkzoNobel, its Employees, joint ventures, participations, customers, suppliers and business partners (including safeguarding the integrity of AkzoNobel, pre- and in- employment screening of Employees

Purpose of Processing	Examples of Processing Activities
	and monitoring of Employees), to record decisions made in the course of business for future reference (e.g. when Employees participate in video conferencing which is recorded), for site access and security reasons, demographic reporting under applicable anti-discrimination laws, for obtaining visa's, permits and technology export licenses and for inclusion in Employee directories.
Preferential status based on ethnicity or culture	Providing preferential status to persons from particular ethnic or cultural minorities to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Sensitive Data allows for an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection against the relevant Processing.
Health services	Providing health services to an Employee provided that the relevant health data is processed by or under the supervision of a health professional who is subject to professional confidentiality requirements.

4. Third Countries to which Employee Data are Transferred

Third Country		
Argentina	Honduras	Qatar
Aruba	Hong Kong	Russia
Australia	India	Saudi Arabia
Bolivia	Indonesia	Singapore
Botswana	Kenya	South Africa
Brazil	Kuwait	Sri Lanka
Cayman Islands	Malaysia	Taiwan
Chile	Mauritius	Thailand
China	Mexico	Tunisia
Colombia	Morocco	Turkey
Costa Rica	Myanmar	Uganda
Curacao	Nicaragua	Ukraine
Ecuador	Oman	United Arab Emirates
Egypt	Pakistan	United States of America
El Salvador	Panama	Uruguay
Eswatini	Papua New Guinea	Vietnam
Guatemala	Peru	Zambia

ANNEX 3 - PROCEDURE FOR DATA SUBJECT REQUESTS AND COMPLAINTS BY INDIVIDUALS

1. Procedure

Individuals may send their request to the appropriate customer service representative or submit a request through the DSAR webform that is accessible through the Privacy Statement. Individuals may also send their request to the office of the Corporate Privacy Officer via email to compliance@akzonobel.com or using the contact details included in the BCR. In addition, Employees may send their request to the appropriate HR representative as set out in the Employee Privacy Statement.

Each request or complaint will be assigned to the appropriate Integrity & Compliance (**I&C**) Business Partner. The appropriate I&C Business Partner will:

- (i) promptly acknowledge receipt of the request or complaint;
- (ii) analyze the request or complaint and, if needed, initiate an investigation;
- (iii) in case of a complaint, if it is well-founded, advise the applicable Corporate Privacy Officer so that a remediation plan can be developed and executed; and
- (iv) maintain records of all requests and complaints received, responses given, and – where relevant – remedial actions taken by AkzoNobel.

Prior to fulfilling an Individual's request, AkzoNobel may request the Individual to:

- (i) if AkzoNobel Processes a large quantity of Personal Data relating to the Individual:
 - (a) specify the categories of Personal Data to which he or she is seeking access;
 - (b) specify, to the extent reasonably possible, the data system in which the Personal Data are likely to be stored;
 - (c) specify, to the extent reasonably possible, the circumstances in which AkzoNobel obtained the Personal Data;
- (ii) provide proof of his or her identity; and
- (iii) in the case of a request for rectification, deletion, or restriction, specify the reasons why the Personal Data are incorrect, incomplete or not Processed in accordance with EEA Law or the BCR.

2. Response Period

Within one calendar month of AkzoNobel receiving the request or complaint and any information necessary under Section 1 above, the relevant contact person or Corporate Privacy Officer shall inform the Individual in writing or electronically (i) of AkzoNobel's position with regard to the request or complaint and any action AkzoNobel has taken or will take in response; (ii) a specification of the information necessary for AkzoNobel to comply with the request in accordance with Section 1 above; or (iii) the ultimate date on which he or she will be informed of AkzoNobel's position and the reasons for the delay. AkzoNobel may extend the original one-month response period by two calendar months where necessary, taking into account the complexity and number of the requests or complaints.

3. Denial of Requests

The rights set out in Articles 5.1 – 5.3 are subject to any applicable exceptions provided under

EEA Data Protection Law. Depending on the relevant right of the Individual, exceptions may be available in cases where:

- (i) if the request does not meet the requirements of Articles 5.1 – 5.3 or a restriction under Article 5.4 applies;
- (ii) AkzoNobel can demonstrate that the request is manifestly unfounded, excessive or not sufficiently specific (and the Individual was given the opportunity to specify his/her request);
- (iii) the identity of the relevant Individual cannot be established by reasonable means, including after receipt of additional information provided by the Individual; or
- (iv) the request is made within an unreasonable time interval of a prior request or otherwise constitutes an abuse of rights.

ANNEX 4 - PRIVACY GOVERNANCE STRUCTURE

1. Corporate Privacy Officer

AkzoNobel has appointed a Corporate Privacy Officer who is, to the extent this does not result in a conflict of interest, responsible for:

- Supervising compliance with this BCR;
- Coordinating, communicating and consulting with the Integrity & Compliance (**I&C**) Business Partner network on central data protection;
- Advising on the information management processes, systems and tools to implement the privacy compliance framework;
- Providing annual reports to the Executive Committee on privacy protection risks and compliance issues as described in Article 9.9;
- Coordinating, in conjunction with the I&C Business Partner network, official investigations or inquiries into the Processing of Personal Data by a public authority;
- Advising in respect of conflicts between this BCR and applicable law as described in Article 12.1 of this BCR;
- Advising on transfers as described in Articles 11.1 and 8.2 of this BCR;
- Monitoring the performance and periodic review of a Data Protection Impact Assessment (DPIA) before a new system or a business process involving Processing of Personal Data is implemented as described in Article 9.7 of this BCR; and
- Maintaining a fully updated list of the Group Companies and keep track and records of updates to this BCR.
- Being available for Individuals' questions and ensuring that the Corporate Privacy Officer's contact details are made publicly available as part of this BCR.
- Devising the data management processes, systems and tools to implement the framework for data protection management as established by the Privacy Council, including:
 - to maintain, update and publish this BCR and related sub-policies;
 - tools to collect, maintain and update information regarding the structure and functioning of all systems that process personal data;
 - data privacy training and awareness for Individuals to comply with their responsibilities under this BCR;
 - appropriate processes to monitor, audit and report compliance with this BCR and ensure that AkzoNobel Internal Audit can verify and certify such compliance in line with the yearly AkzoNobel Audit Program;
 - procedures regarding data protection inquiries, concerns and complaints; and
 - determine and update appropriate sanctions for violations of this BCR (e.g. disciplinary standards).

The Corporate Privacy Officer enjoys the highest management support for the fulfilling of the

above-mentioned tasks and, where appropriate, may delegate any of the above responsibilities to the I&C Business Partners or Privacy Counsel, to be carried out under the Corporate Privacy Officer's responsibility.

2. Privacy Council

AkzoNobel shall establish a Privacy Council. The Privacy Council includes the most senior representatives of the following functions, or their delegates: CPO (Chair), Director Internal Audit, Director Group Control, Director CIO Office, Global Business Services Director, Director HR, Digital Marketing Director and Senior Legal Counsel Privacy (Secretary). The Privacy Council monitors progress on the implementation and continuous improvement of the framework for:

- Development, implementation and updating of local Personal Data protection policies and procedures;
- Maintaining, updating and publishing of this BCR and related sub-policies;
- Creating, maintaining and updating information regarding the structure and functioning of all systems that process personal data (as required by Article 14);
- Development, implementation and updating of the relevant data protection training and awareness programs;
- Monitoring, auditing and reporting on compliance with this BCR to the management board;
- Collecting, investigating and resolving privacy inquiries, concerns and complaints; and
- Determining and updating appropriate sanctions for violations of this BCR (e.g. disciplinary standards).

3. Regional support by I&C Business Partners, ICGC, Legal Counsels, and Privacy Counsels

Each Organizational Unit shall designate an I&C Business Partner. The I&C Business Partner acts as a local point of contact for privacy matters and assists the region with handling privacy incidents, investigations and complaints. The Corporate Privacy Officer shall act as the I&C Business Partner for Akzo Nobel N.V.

An I&C Business Partner works together with the regional Integrity & Compliance Governance Committee (ICGC), Legal Counsel(s), Privacy Counsel(s) and relevant representatives of the business and function(s) in the region to help the business and/or function(s) implement the framework for data protection management in their day-to-day activities in their respective region. This regional support structure of I&C Business Partners, ICGC, Legal Counsels and Privacy Counsels shall perform the following tasks for their respective Organizational Unit:

- Implement the data management processes, systems and tools, devised by the Corporate Privacy Officer to implement the framework for data protection management established by the Privacy Council in their respective Organizational Unit;
- Support and assess overall data protection management compliance within their Organizational Unit;
- Regularly advise their Responsible Executive and the Corporate Privacy Officer on

privacy risks and compliance issues;

- Maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that process personal data;
- Be available for requests for privacy advice;
- Provide information relevant to the annual privacy report of the Corporate Privacy Officer;
- Assist the Corporate Privacy Officer in the event of official investigations or inquiries by government authorities;
- Own and authorize all appropriate privacy sub-policies in their organizations;
- Direct that stored data be erased or anonymized;
- Decide on and notify the Corporate Privacy Officer of complaints; and
- Cooperate with the Corporate Privacy Officer and the other I&C Business Partners to:
 - ensure that the instructions, tools and training are in place to enable the Organizational Unit, to comply with this BCR;
 - share and provide guidance on best practices for data protection management within their Organizational Unit;
 - ensure that data protection requirements are taken into account whenever new technology is implemented in their Organizational Unit;
 - notify the Responsible Executive of the involvement of external service providers with data processing tasks for their Organizational Unit.

4. Responsible Executive

The Responsible Executive of each Organizational Unit is accountable that effective data protection management is implemented in his Organizational Unit, is integrated into business practices, and that adequate resources and budget are available.

Responsible Executives are accountable for:

- Ensuring overall data protection management compliance within their Organizational Unit, also during and following organizational restructuring, outsourcing, mergers and acquisitions and divestures;
- Implementing the data management processes, systems and tools, devised by the Corporate Privacy Officer to implement the framework for data protection management established by the Privacy Council in their respective Organizational Unit;
- Ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements (as advised by the I&C Business Partners);
- Ensuring and monitoring ongoing compliance of third parties with the requirements of this BCR in case personal data are transferred by the relevant Organizational Unit to a third party (including entering into a written contract with such third parties and obtaining a sign off of such contract from the legal department);

- Ensuring that relevant Individuals in their Organizational Unit follow the prescribed data protection training courses; and
- Directing that stored data be deleted or anonymized.

Responsible Executives are responsible for:

- Consulting with the Corporate Privacy Officer in all cases where there is a conflict between applicable local law and this BCR; and
- Informing the Corporate Privacy Officer of any new legal requirement that may interfere with AkzoNobel's ability to comply with this BCR (after consultation with the local legal department).

5. Default I&C Business Partner

If at any moment in time there is no I&C Business Partner designated for a relevant Organizational Unit, the Corporate Privacy Officer shall act as I&C Business Partner for that Organizational Unit.

6. Data Protection Officer with Statutory Position

Where a Data Protection Officer holds his or her position pursuant to relevant (local) law, he or she shall carry out his or her job responsibilities to the extent they do not conflict with his or her statutory position.

ANNEX 5 - PROCEDURES FOR MONITORING AND AUDITING COMPLIANCE

1. Internal Audits

AkzoNobel internal audit and external auditors (if any) shall audit business processes and procedures that involve the Processing of Personal Data for compliance with all aspects of this BCR, including methods of ensuring that corrective actions will take place. BCR topics will be part of AkzoNobel's internal audit, for which Internal Audit determines the exact scope, and all BCR topics will be audited during internal audit's five-year audit cycle. The audits may be carried out in the course of the regular activities of AkzoNobel internal audit or initiated by the Corporate Privacy Officer. The Corporate Privacy Officer may request to have an audit as specified in this Section 1 conducted by an external auditor. AkzoNobel internal audit may include privacy aspects in every individual audit even if the main subject of the audit does not relate to privacy (meaning that an audit into HR may also include a check of privacy aspects, e.g., a check of data subject access requests). All corrective action plans resulting from the audit will be followed up and reported upon by Internal Audit.

Applicable professional standards of independence, integrity and confidentiality will be observed when conducting an audit. The Corporate Privacy Officer, the board of AkzoNobel Nederland B.V., where appropriate, AkzoNobel N.V. and the relevant I&C Business Partners will be informed of the results of the audits. AkzoNobel shall provide a copy of the audit results to the Competent Supervisory Authority upon its request.

2. Mitigation

AkzoNobel shall, if so indicated, ensure that adequate steps are taken to address breaches of this BCR identified during the monitoring or auditing of compliance pursuant to this Annex 5.