

Rules

7.08.1 Privacy Rules for Employee Data			
Source Directive		Directive 7.08 Protection of Personal Data	
Content Owner		AkzoNobel Legal Group (ALG)	
Signed off by	Date	Executive Committee	April 16, 2018
Effective Date		April 16, 2018	
Purpose			
AkzoNobel has committed itself to the protection of personal data of AkzoNobel employees in Directive 7.08 Protection of Personal Data and the AkzoNobel Code of Conduct. These Privacy Rules for Employee Data indicate how this principle shall be implemented. For the rules applicable to customer, supplier and business partner data, refer to the <i>Privacy Rules for Customer, Supplier and Business Partner Data</i> .			
Scope and definitions			
These Rules address the Processing of Personal Data of AkzoNobel Employees (“Employee Data”) by AkzoNobel or a Third Party on behalf of AkzoNobel.			
Table of contents			
Article 1 – Scope, Applicability and Implementation 2			
Article 2 – Purposes for Processing Employee Data 3			
Article 3 – Use for other purposes..... 5			
Article 4 – Purposes for Processing Sensitive Data..... 6			
Article 5 – Quantity and Quality of Data 8			
Article 6 – Employee Information Requirements 9			
Article 7 –Rights of Employees 10			
Article 8 – Security and Confidentiality Requirements 12			
Article 9 – Intentionally left blank for consistency reasons..... 13			
Article 10 – Automated Decision Making..... 14			
Article 11 – Transfer of Employee Data to Third Parties and Internal Processors 14			

Article 12 – Overriding Interests	17
Article 13 – Privacy Governance	18
Article 14 – Policies and Procedures.....	22
Article 15 – Training.....	22
Article 16 – Monitoring and Auditing Compliance	22
Article 17 – Complaints Procedure.....	24
Article 18 – Legal Issues	25
Article 19 – Sanctions for Non-compliance	26
Article 20 – Conflicts between the Rules and Applicable Local Law.....	26
Article 21 – Changes to the Rules.....	27
Article 22 – Transition Periods	28
Article 23 – Interpretations	29
ANNEX 1	31
Definitions	31

Rules

Article 1 – Scope, Applicability and Implementation

Scope	1.1	These Rules address the Processing of Personal Data of AkzoNobel Employees (Employee Data) by AkzoNobel or a Third Party on behalf of AkzoNobel.
Electronic and Paper-based Processing	1.2	These Rules apply to the Processing of Employee Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Rules	1.3	Employees keep any rights and remedies they may have under applicable local law. These Rules shall apply only where it provides supplemental protection for Employee Data. Where applicable local law provides more protection than these Rules, local law shall apply. Where these Rules provide more protection than applicable local law or provides additional safeguards, rights or remedies for Employees, these Rules shall apply.
Sub-policies and notices	1.4	AkzoNobel may supplement these Rules through sub-policies or notices that are consistent with these Rules.
Accountability	1.5	These Rules are binding on AkzoNobel. The Responsible Executive shall be accountable for his or her business organization's compliance with these Rules. Staff must comply with these Rules.

Effective date	1.6	These Rules have been adopted by the Executive Committee of Akzo Nobel N.V. and shall enter into force as of August 25, 2014 (Effective Date) and shall be published on the AkzoNobel intranet and be made available to Employees upon request.
Rules supersede prior policies	1.7	These Rules supersede all AkzoNobel privacy policies and notices that exist on the Effective Date to the extent they address the same issues.
Implementation	1.8	These Rules shall be implemented in the AkzoNobel organization based on the timeframes specified in Article 22.
Role of AkzoNobel Nederland	1.9	Akzo Nobel N.V. has tasked Akzo Nobel Nederland with the coordination and implementation of these Rules.

Article 2 – Purposes for Processing Employee Data

Legitimate Business Purposes	2.1	<p>Employee Data shall be collected, used or otherwise Processed for one (or more) of the following purposes (Business Purposes):</p> <ul style="list-style-type: none"> (i) Human resources and personnel management. This purpose includes Processing that is necessary for the performance of an employment or other contract with an Employee (or to take necessary steps at the request of an Employee prior to entering into a contract), or for managing the employment-at-will relationship, e.g., management and administration of recruiting and outplacement, compensation and benefits (including pensions and special promotional offers for Employees), payments, tax issues, career and talent development, performance evaluations, training, travel and expenses, facilitating Employee group activities, and Employee communications; (ii) Business process execution and internal management. This purpose addresses activities such as scheduling work, recording time, managing company assets, provision of central processing facilities for efficiency purposes, conducting internal audits and investigations, implementing business controls, and managing and using Employee directories; (iii) Health, safety and security. This purpose addresses activities such as those involving occupational safety and health, the protection of company and Employee assets, and the authentication of Employee status and access rights; (iv) Organizational analysis and development and management reporting. This purpose addresses activities such as conducting Employee surveys, managing mergers, acquisitions and divestitures, and Processing Employee Data for management reporting and analysis; (v) Compliance with legal obligations. This purpose addresses the
-------------------------------------	-----	---

	Processing of Employee Data as necessary for compliance with a legal obligation to which AkzoNobel is subject or
	(vi) Protecting the vital interests of Employees. This is where Processing is necessary to protect the vital interests of an Employee.
	Where there is a question whether a Processing of Employee Data can be based on a purpose listed above, it is necessary to seek the advice of the appropriate Privacy Manager before the Processing takes place.
Employee consent	<p>2.2 Employee consent generally cannot be used as a legitimate basis for Processing Employee Data. One of the Business Purposes must exist for any Processing of Employee Data.</p> <p>Employee consent may be requested from Employees only in the following cases:</p> <ul style="list-style-type: none"> (i) If none of the Business Purposes applies, AkzoNobel may request Employee consent for Processing Employee Data, but only if the Processing has no foreseeable adverse consequences for the Employee. If the Processing is reasonably necessary to address a request of the Employee (e.g., he or she subscribes to a service or seeks a benefit), the Employee's consent is implied; or (ii) If Data Protection Law requires that AkzoNobel requests consent of the Employee for the relevant Processing, AkzoNobel shall, in addition to ensuring that a Business Purpose exists for the Processing, also seek Employee consent for the Processing. <p>When seeking Employee consent, AkzoNobel must inform the Employee:</p> <ul style="list-style-type: none"> (i) of the purposes of the Processing for which consent is requested; (ii) which Group Company is responsible for the Processing; (iii) of the possible consequences for the Employee of the Processing; (iv) of the right to withdraw his or her consent at any time without consequences to his or her employment relationship; (v) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal. <p>Where Processing is undertaken at the Employee's request (e.g., he or she subscribes to a service or seeks a benefit), he or she is deemed to have provided consent to the Processing.</p> <p>A request for Employee consent requires the authorization of the appropriate Privacy Manager prior to seeking consent.</p>
Denial or withdrawal of Employee consent	<p>2.3 The Employee may deny or withdraw consent at any time without consequence to his employment relationship. Upon withdrawal or consent, AkzoNobel will discontinue such Processing as soon as reasonably practical. The withdrawal of consent shall not affect (i) the lawfulness of the Processing based on such consent before its</p>

Limitations on Processing Data of Dependents of Employees	<p>withdrawal; and (ii) the lawfulness of Processing for Business Purposes not based on consent after withdrawal.</p> <p>2.4 AkzoNobel will Process Data of Dependents of an Employee if:</p> <ul style="list-style-type: none"> (i) the Data were provided with the consent of the Employee or the Dependent; (ii) Processing of the Data is reasonably necessary for the performance of a contract with the employee or for managing the employment-at-will relationship; or (iii) the Processing is required or permitted by applicable local law.
--	--

Article 3 – Use for other purposes

Use of Data for Secondary Purposes	<p>3.1 Generally, Employee Data shall be used only for the Business Purposes for which they were originally collected (Original Purpose). Employee Data may be Processed for a legitimate Business Purpose of AkzoNobel different from the Original Purpose (Secondary Purpose) only if the Original Purpose and Secondary Purpose are closely related. Depending on the sensitivity of the relevant Employee Data and whether use of the Data for the Secondary Purpose has potential negative consequences for the Employee, the secondary use may require additional measures such as:</p> <ul style="list-style-type: none"> (i) limiting access to the Data; (ii) imposing additional confidentiality requirements; (iii) taking additional security measures; (iv) informing the Employee about the Secondary Purpose; (v) providing an opt-out opportunity; or (vi) obtaining Employee consent in accordance with Article 2.2 or Article 4.3 (if applicable).
Generally permitted uses of Data for Secondary Purposes	<p>3.2 It is generally permissible to use Employee Data for the following Secondary Purposes provided appropriate additional measures are taken in accordance with Article 3.1:</p> <ul style="list-style-type: none"> (i) transfer of the Data to an Archive; (ii) internal audits or investigations; (iii) implementation of business controls and operational efficiency; (iv) statistical, historical or scientific research; (v) preparing for or engaging in dispute resolution; (vi) legal advice or business consulting; or (vii) insurance purposes.

Article 4 – Purposes for Processing Sensitive Data

Specific purposes for Processing Sensitive Data

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

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

(i) **Racial or ethnic data:**

- (a) in some countries photos and video images of Employees qualify as racial or ethnic data. AkzoNobel may process photos and video images for the protection of AkzoNobel and Employee assets, site access and security reasons, and for inclusion in Employee directories;
- (b) 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 an objective determination that an Employee belongs to a minority group and the Employee has not filed a written objection to the relevant Processing.

(ii) **Physical or mental health data** (including any opinion of physical or mental health and data relating to disabilities and absence due to illness or pregnancy):

- (a) providing health services to an Employee provided that the relevant health data are processed by or under the supervision of a health professional who is subject to professional confidentiality requirements;
- (b) administering pensions, health and welfare benefit plans, maternity, paternity or family leave programs or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee;
- (c) reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity;
- (d) assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities;
- (e) providing facilities in the workplace to accommodate health problems or disabilities.

(iii) **Criminal data** (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior):

- (a) assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee;
- (b) protecting the interests of AkzoNobel with respect to criminal offenses that have been or, given the relevant circumstances

		are suspected to have been, committed against AkzoNobel or its Employees.
		(iv) Sexual preference (including data related to partners of Employees):
		(a) administering Employee pensions and benefit programs;
		(b) administering Employee memberships.
		(v) Religious or philosophical beliefs:
		(a) accommodating religious or philosophical practices, dietary requirements or religious holidays.
General Purposes for Processing of Sensitive Data	4.2	<p>In addition to the specific purposes listed in Article 4.1 above, all categories of Sensitive Data may be Processed for one (or more) of the following:</p> <ul style="list-style-type: none"> (i) as required or allowed for a performance of a task carried out to comply with a legal obligation to which AkzoNobel is subject; (ii) as required by or allowed under applicable local law or a collective agreement; (iii) for dispute resolution and/or fraud prevention; (iv) to protect a vital interest of an Employee, but only where it is impossible to obtain the Employee's consent first; (v) to the extent necessary to comply with an obligation of public international law (e.g., a treaty); or (vi) if the Sensitive Data have been posted or otherwise shared at the Employee's own initiative on AkzoNobel social media or have manifestly been made public by the Employee.
Employee consent for Processing Sensitive Data	4.3	<p>Subject to the exceptions set forth below, Employee consent generally should not be used as a legitimate basis for Processing Sensitive Data. One of the grounds listed in Article 4.1 or 4.2 must exist for any Processing of Sensitive Data.</p> <p>Employee consent may be requested from Employees for Processing Sensitive Data only in the following cases:</p> <ul style="list-style-type: none"> (i) If none of the grounds listed in Article 4.1 or 4.2 applies, AkzoNobel may request Employee consent for Processing Sensitive Data, but only if the Processing has no foreseeable adverse consequences for the Employee (e.g., Employee diversity programs or networks, research, product development, selection of candidates in hiring or management development processes); or (ii) If Applicable Data Controller Law requires that AkzoNobel requests consent of the Employee for the relevant Processing, AkzoNobel shall, in addition to ensuring that one of the grounds listed in Article 4.1 or 4.2 for the Processing, also seek Employee consent for the Processing. <p>The requirements set out in Articles 2.2 and 2.3 apply to the</p>

		requesting, denial or withdrawal of Employee consent.
Prior Authorization of Privacy Manager	4.4	Where Sensitive Data are Processed based on a requirement of law other than the local law applicable to the Processing, or based on the consent of the Employee, the Processing requires the prior authorization of the appropriate Privacy Manager.
Use of Sensitive Data for Secondary Purposes	4.5	Sensitive Data of Employees or Dependents may be Processed for Secondary Purposes in accordance with Article 3.
Article 5 – Quantity and Quality of Data		
No Excessive Data	5.1	AkzoNobel shall restrict the Processing of Employee Data to those Data that are reasonably adequate for and relevant to the applicable Business Purpose. AkzoNobel shall take reasonable steps to delete or otherwise destroy (e.g., by scrambling) Employee Data that are not required for the applicable Business Purpose.
Storage period	5.2	<p>AkzoNobel generally shall retain Employee Data only for the period required to serve the applicable Business Purpose, to the extent reasonably necessary to comply with an applicable legal requirement or as advisable in light of an applicable statute of limitations. AkzoNobel may specify (e.g., in a notice or records retention schedule) a time period for which certain categories of Employee Data may be kept.</p> <p>Promptly after the applicable storage period has ended, the relevant Privacy Manager shall direct that the Data be:</p> <ul style="list-style-type: none"> (i) securely deleted or destroyed; (ii) anonymized; or (iii) transferred to an Archive (unless this is prohibited by law or an applicable records retention schedule).
Quality of Employee Data	5.3	Employee Data should be accurate, complete and kept up-to-date to the extent reasonably necessary for the applicable Business Purpose.
‘Privacy by Design’	5.4	AkzoNobel shall take commercially reasonable technical and organizational steps to ensure that the requirements of this Article 5 are implemented into the design of new systems and processes that Process Employee Data.
‘Self-service’	5.5	Where AkzoNobel requires an Employee to update his or her own Employee Data, AkzoNobel shall remind him or her periodically to do so.

Article 6 – Employee Information Requirements

Information requirements

- 6.1 AkzoNobel shall inform Employees through a privacy policy or notice of the following privacy information:
- (i) the Business Purposes (including Secondary Purposes) for which their Data are processed;
 - (ii) which Group Company is responsible for the Processing and the contact information of the responsible Privacy Manager;
 - (iii) the categories of Third Parties to which the Data are disclosed (if any); if the Third Party is located in a country outside the EEA, whether any such Third Party is covered by an Adequacy Decision and if not, information on the data transfer mechanism as referred to in Article 11.6 (ii), (iv) or (v) as well as the means to get a copy thereof or access thereto; and
 - (iv) other relevant information, e.g.,:
 - (a) the nature and categories of the Personal Data Processed;
 - (b) the period for which the Personal Data will be stored or (if not possible) the criteria used to determine this period;
 - (c) an overview of the rights of Employees under these Rules, how these can be exercised, including the right to obtain compensation;
 - (d) the existence of automated decision making referred to in Article 10 as well as meaningful information about the logic involved and potential negative consequences thereof for the Employee;
 - (e) the source of the Personal Data (where the Personal Data has not been obtained from the Employee), including whether the Personal Data came from a public source.

Employee Information not Obtained from the Employee

- 6.2 Where Employee Data have not been obtained directly from the Employee, AkzoNobel shall provide the Employee with the information as set out in Article 6.1:
- (i) within reasonable period after obtaining Employee Data but at the latest within one month, having regard to specific circumstances of the Employee Data Processed;
 - (ii) if Employee Data are used for communication with Employee, at the latest at the time of the first communication with the Employee;
 - (iii) if a disclosure to another recipient is envisaged, at the latest when Employee Data are first disclosed.

Exceptions

- 6.3 The requirements of Articles 6.1 and 6.2 may be inapplicable if:
- (i) the Employee already has the information as set out in

Article 6.1;

- (ii) it would be impossible or would involve a disproportionate effort to provide the information to Employees, in which case AkzoNobel will take additional measures to mitigate potential negative consequences for the Employee, such as those listed in Article 3.1;
- (iii) obtaining Employee Data is expressly laid down in applicable law; or
- (iv) the Employee Data must remain confidential subject to an obligation of professional secrecy regulated by applicable local law, including a statutory obligation of secrecy.

These exceptions to the above requirements qualify as Overriding Interests as set out in Article 12.

Article 7 –Rights of Employees

Right of Access	7.1	Every Employee has the right to request a copy of his or her Personal Data Processed by or on behalf of AkzoNobel, and further, where reasonably possible, access to the information listed in Article 6.1 and 6.2.
Right to Rectification, Deletion and Restriction	7.2	<p>If the Employee Data are incorrect, incomplete, or not Processed in compliance with Data Protection Law or these Rules, the Employee has the right to have his or her Personal Data rectified, deleted or the Processing thereof restricted (as appropriate).</p> <p>In case the Personal Data have been made public by AkzoNobel, and the Employee is entitled to deletion of the Personal Data, in addition to deleting the relevant Personal Data, AkzoNobel shall take commercially reasonable steps to inform Third Parties that are Processing the relevant Personal Data or linking to the relevant Personal Data, that the Employee has requested the deletion of the Personal Data by such Third parties.</p>
Right to Object	7.3	<p>The Employee has the right to object to:</p> <ul style="list-style-type: none"> (i) the Processing of his or her Personal Data on the basis of compelling grounds related to his or her particular situation, unless AkzoNobel can demonstrate a prevailing legitimate interest for the Processing; and (ii) receiving marketing communications on the basis of Article 9 (including any profiling related thereto).
Restrictions to Rights of	7.4	The rights of Employees set out in Articles 7.1 - 7.3 above do not apply in one or more of the following circumstances:

Employees		<ul style="list-style-type: none"> (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 dispute resolution purposes; (v) the exercise of the rights by the Employee adversely affects the rights and freedoms of AkzoNobel or others; or (vi) in case a specific restriction of the rights of Employees applies under Data Protection Law.
Procedure	7.5	<p>Employees should send their request to the appropriate Privacy Manager. Employees may also send their request to the office of the Corporate Privacy Officer via email to compliance@akzonobel.com.</p> <p>Prior to fulfilling the request of the Employee, AkzoNobel may require the Employee to:</p> <ul style="list-style-type: none"> (i) specify the type of Employee Data to which he or she is seeking access; (ii) specify, to the extent reasonably possible, the data system in which the Employee Data are likely to be stored; (iii) specify the circumstances in which AkzoNobel obtained the Employee Data; (iv) provide proof of his or her identity when AkzoNobel has reasonable doubts concerning such identity, or to provide additional information enabling his or her identification; (v) pay a fee to compensate AkzoNobel for the reasonable costs relating to fulfilling the request of the Employee provided AkzoNobel can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character; and (vi) in case of a request for rectification, deletion, or restriction, specify the reasons why the Employee Data are incorrect, incomplete or not Processed in accordance with applicable law or the Rules.
Response period	7.6	<p>Within one calendar month of AkzoNobel receiving the request, the Privacy Officer shall inform the Employee in writing either (i) of AkzoNobel position with regard to the request and any action AkzoNobel has taken or will take in response or (ii) the ultimate date on which he or she will be informed of AkzoNobel's position and the reasons for the delay, which shall be no later than two calendar months thereafter.</p>
Complaints	7.7	<p>An Employee may file a complaint in accordance with Article 17.3 and/or file a complaint or claim with the authorities or the courts in accordance with Article 18 if:</p> <ul style="list-style-type: none"> (i) the response to the request is unsatisfactory to the Employee (e.g. the request is denied);

		<ul style="list-style-type: none"> (ii) the Employee has not received a response as required by Article 7.6; or (iii) the time period provided to the Employee in accordance with Article 7.6 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response.
Denial of requests	7.8	<p>AkzoNobel may deny an Employee request if:</p> <ul style="list-style-type: none"> (i) the request does not meet the requirements of Articles 7.1 – 7.3 or meets the requirements of Article 7.5; (ii) the request is not sufficiently specific; (iii) the identity of the relevant Employee cannot be established by reasonable means including additional information provided by the Employee; (iv) AkzoNobel can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character. A time interval between requests of six months or less shall generally be deemed to be an unreasonable time interval; (v) the Processing is required or allowed for the performance of a task carried out to comply with a legal obligation of AkzoNobel; (vi) 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; (vii) the Processing is necessary for exercising the right of freedom of expression and information; (viii) for dispute resolution purposes; (ix) in so far as the request violates the rights and freedoms of AkzoNobel or others; or (x) In case a specific restriction of the rights of Employees applies under Data Protection Law.
No Requirement to Process Identifying Information	7.9	<p>AkzoNobel is not obliged to Process additional information in order to be able to identify the Employee for the sole purpose of facilitating the rights of the Employee under this Article 7.</p>
Article 8 – Security and Confidentiality Requirements		
Data security	8.1	<p>AkzoNobel shall take appropriate commercially reasonable technical, physical and organizational measures to protect Employee Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. To achieve this, AkzoNobel has developed and implemented the AkzoNobel information security policies and other sub-policies and guidelines</p>

		relating to the protection of Employee Data.
Staff access and Confidentiality	8.2	AkzoNobel shall provide AkzoNobel Staff access to Employee Data only to the extent necessary to serve the applicable Business Purpose and to perform their job. AkzoNobel shall impose confidentiality obligations on Staff with access to Employee Information.
Personal Data Breach Notification	8.3	AkzoNobel shall document any Personal Data Breach, comprising the facts relating to the Personal Data Breach, its effects and the remedial actions taken, which documentation will be made available to the Lead DPA and a DPA competent to audit under Article 16.2 upon request. Group Companies shall inform AkzoNobel Nederland of a Personal Data Breach without delay. If Data Protection Law so requires, AkzoNobel shall notify the Employees of an Personal Data Breach as soon as reasonably possible following its determination that an Personal Data Beach has occurred, unless otherwise prohibited such as if a law enforcement official or a supervisory authority determines that notification would impede a (criminal) investigation or cause damage to national security the trust in the relevant industry sector. In this case, notification shall be delayed as instructed by such law enforcement official or supervisory authority. AkzoNobel shall respond promptly to inquiries of Employees relating to such Personal Data Breach.
Article 9 – Direct Marketing		
Consent for Direct Marketing	9.1	If Data Protection Law so requires, AkzoNobel shall send direct marketing communications to an Employee only with the Employee's prior opt-in consent. If Data Protection Law does not require prior opt-in consent of the Employee, AkzoNobel shall offer the Employee the opportunity to opt-out of such direct marketing communications.
Objection to Direct Marketing	9.2	If an Employee objects to receiving direct marketing communications from AkzoNobel, or withdraws his or her consent to receive such communications, AkzoNobel will take steps to refrain from sending further direct marketing communications as specifically requested by the Employee. AkzoNobel will do so within the time period required by Data Protection Law.
Article 10 – Automated Decision Making		
Automated decisions	10.1	Automated tools may be used to make decisions about Employees but decisions with a negative outcome for the Employee may not be based solely on the results provided by the automated tool. This restriction does not apply if: <ul style="list-style-type: none"> (i) the use of automated tools is necessary for the performance of a task carried out to comply with a legal obligation to which

AkzoNobel is subject;

- (ii) the decision is made by AkzoNobel for purposes of (a) entering into or performing a contract or (b) managing the employment-at will relationship, provided the underlying request leading to a decision by AkzoNobel was made by the Employee (e.g., where automated tools are used to filter job applications); or
- (iii) the decision is made based on the explicit consent of the Employee.

Items (i) and (iii) only apply if suitable measures are taken to safeguard the legitimate interests of the Employee, e.g., the Employee has been provided with an opportunity to express his or her point of view.

The requirements set out in Articles 2.2 and 2.3 apply to the requesting, denial or withdrawal of Employee consent.

Article 11 – Transfer of Employee Data to Third Parties and Internal Processors

Transfer to Third Parties	11.1	This Article sets forth requirements concerning the transfer of Employee Data from AkzoNobel to a Third Party. Note that a transfer of Employee Data includes situations in which AkzoNobel discloses Employee Data to Third Parties (e.g. in the context of corporate due diligence) or where AkzoNobel provides remote access to Employee Data to a Third Party.
Third Party Controllers and Third Party Processors	11.2	<p>There are two categories of Third Parties:</p> <ul style="list-style-type: none"> (i) Third Party Processors: these are Third Parties that Process Employee Data solely on behalf of AkzoNobel and at its direction (e.g., Third Parties that Process Employee salaries on behalf of AkzoNobel); (ii) Third Party Controllers: these are Third Parties that Process Employee Data and determine the purposes and means of the Processing (e.g., government authorities or service providers that provide services directly to Employees).
Transfer for applicable Business Purposes only	11.3	AkzoNobel shall transfer Employee Data to a Third Party to the extent necessary to serve the applicable Business Purpose for which the Employee Data are Processed (including Secondary Purposes as per Article 3 or purposes for which the Employee has provided consent in accordance with Article 2).
Third Party Controller contracts	11.4	Third Party Controllers (other than government agencies) may Process Employee Data only if they have a written contract with AkzoNobel. In the contract, AkzoNobel shall seek to contractually protect the data protection interests of its Employees. All such contracts shall be drafted in consultation with the appropriate Privacy

<p>Third Party Processor contracts</p>	<p>Manager and/or Privacy Counsel.</p> <p>11.5 Third Party Processors may Process Employee Data only if they have a written contract with AkzoNobel. The contract with a Third Party Processor (Processor Contract) must include the following provisions:</p> <ul style="list-style-type: none"> (i) the Third Party Processor shall Process Employee Data only for the purposes authorized by Akzonobel in accordance with AkzoNobel's documented instructions including on transfers of Personal Data to any Third Party Processor not covered by an Adequacy Decision, unless the Third Party Processor is required to do so under mandatory requirements applicable to the Third Party Processor and notified to AkzoNobel; (ii) the Processor shall keep the Employee Data confidential and shall impose confidentiality obligations on Staff with access to Personal Data; (iii) the Processor shall take appropriate technical, physical and organizational security measures to protect the Employee Data; (iv) the Third Party Processor shall only permit subcontractors to Process Personal Data in connection with its obligations to AkzoNobel (a) with the prior specific or generic consent of AkzoNobel and (b) based on a validly entered into written or electronic contract with the subcontractor, which imposes similar privacy protection-related Processing terms as those imposed on the Third Party Processor under the Processor Contract and provided that the Third Party Processor remains liable to AkzoNobel for the performance of the subcontractor in accordance with the terms of the Processor Contract. In case AkzoNobel provides generic consent for involvement of subcontractors, the Third Party Processors 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) AkzoNobel has the right to review the security measures taken by the Third Party Processor and the Third Party Processor shall submit its relevant data processing facilities to audits and inspections by AkzoNobel, a Third Party on behalf of AkzoNobel, or any relevant government authority; (vi) the Third Party Processor shall promptly inform AkzoNobel of any actual or suspected security breach involving Employee Data; (vii) The Third Party Processor shall deal promptly and appropriately with (a) requests for information necessary to demonstrate compliance of the Third Party Processor with its obligations under the Processor Contract and will inform AkzoNobel if any instructions of AkzoNobel in this respect violate applicable law; (b) requests and complaints of Employees as instructed by AkzoNobel; and (c) requests for assistance of AkzoNobel as reasonably required to ensure compliance of the Processing of
---	---

**Transfer of Data
to Third Parties
outside the EEA
not covered by
an Adequacy
Decision**

11.6

the Personal Data with applicable law; and

(viii) Upon termination of the Processor Contract, the Third Party Processor shall, at the option of AkzoNobel, return the Personal Data and copies thereof to AkzoNobel or shall securely delete such Personal Data, except to the extent the Processor Contract or applicable law provides otherwise.

This Article sets forth additional rules for Employee Data that are (a) collected originally in connection with activities of a Group Company that is located in the EEA or covered by an Adequacy Decision; and (b) transferred to a Third Party that is located outside the EEA and not covered by an Adequacy Decision.

Employee Data may be transferred to a Third Party not covered by an Adequacy Decision only if:

- (i) the transfer is necessary for the performance of a contract with the Employee, for managing the employment-at-will relationship or to take necessary steps at the request of the Employee prior to entering into a contract or an employment-at-will relationship, e.g., for processing job applications;
- (ii) a contract has been concluded between AkzoNobel and the relevant Third Party that (a) such Third Party shall be bound by the terms of these Rules as were it a Group Company; (b) provides for safeguards at a similar level of protection as that provided by these Rules; or (c) that is recognized under Data Protection Law as providing an “adequate” level of privacy protection;
- (iii) the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the Employee between AkzoNobel and a Third Party (e.g. in case of the booking of an airline ticket);
- (iv) the Third Party has been certified under a ‘safe harbor’ program that is recognized under Data Protection Law as providing an “adequate” level of data protection;
- (v) the Third Party has implemented Binding Corporate Rules or similar transfer control mechanism that is recognized under Data Protection Law as providing an adequate level of protection;
- (vi) the transfer is necessary to protect a vital interest of the Employee;
- (vii) the transfer is necessary for the establishment, exercise or defense of a legal claim;
- (viii) the transfer is necessary to satisfy a pressing need to protect the public interests of a democratic society; or
- (ix) the transfer is necessary for the performance of a task carried out to comply with a legal obligation to which the relevant Group Company is subject.

Items (viii) and (ix) above require the prior approval of the Corporate Privacy Officer.

**Employee
consent for
transfer**

11.7 AkzoNobel generally shall not seek Employee consent for a transfer of Employee Data to a Third Party not covered by an Adequacy Decision. One of the grounds for transfer listed in Article 11.6 must exist. If applicable local law so requires, in addition to having one of the grounds listed in Article 11.6, AkzoNobel shall also seek Employee consent for the relevant transfer. If none of the grounds listed in Article 11.6 exists, AkzoNobel may request Employee consent for a transfer to a Third Party located in a Non-Adequate Country, but only if:

- (i) the transfer has no foreseeable adverse consequences for the Employee; or
- (ii) the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the transfer of the Data.

Requesting Employee consent for a transfer requires the prior approval of the appropriate Privacy Manager. Prior to requesting Employee consent, the Employee shall be provided with the following information:

- (i) the purpose of the transfer;
- (ii) the identity of the transferring Group Company;
- (iii) the identity or categories of Third Parties to which the Data will be transferred;
- (iv) the categories of Data that will be transferred;
- (v) the country to which the Data will be transferred; and
- (vi) the fact that the Data will be transferred to a Third Party not covered by an Adequacy Decision.

Article 2.3 applies to the requesting, denial or withdrawal of consent.

**Internal
Processors**

11.8 Internal Processors may Process Personal Data only if they have a validly entered into written or electronic contract with the Group Company being the Data Controller of the relevant Personal Data, which contract must in any event include the provisions set out in Article 11.5.

Article 12 – Overriding Interests
**Overriding
Interests**

12.1 Some of the obligations of AkzoNobel or rights of Employees under these Rules may be overridden if, under the specific circumstances at issue, a pressing need exists that outweighs the interest of the Employee (**Overriding Interest**). An Overriding Interest exists if there is a need to:

- (i) protect the legitimate business interests of AkzoNobel including
 - (a) the health, security or safety of Employees;

		<ul style="list-style-type: none"> (b) AkzoNobel's intellectual property rights, trade secrets or reputation; (c) the continuity of AkzoNobel's business operations; (d) the preservation of confidentiality in a proposed sale, merger or acquisition of a business; or (e) the involvement of trusted advisors or consultants for business, legal, tax, or insurance purposes;
		<ul style="list-style-type: none"> (ii) prevent or investigate (including cooperating with law enforcement) suspected or actual violations of law, breaches of the terms of employment, or non-compliance with the AkzoNobel Code of Conduct or other AkzoNobel policies or procedures; or (iii) otherwise protect or defend the rights or freedoms of AkzoNobel, its Employees or other persons.
Exceptions in the event of Overriding Interests	12.2	<p>If an Overriding Interest exists, one or more of the following obligations of AkzoNobel or rights of the Employee may be set aside:</p> <ul style="list-style-type: none"> (i) Article 3.1 (the requirement to Process Employee Data for closely related purposes); (ii) Article 5.2 (data storage or deletion); (iii) Article 6.1 and 6.2 (information provided to Employees); (iv) Article 7.1 – 7.3 (rights of Employees); (v) Articles 8.2 (Staff access limitations and confidentiality); and (vi) Articles 11.4, 11.5 and 11.6 (ii) (contracts with Third Parties).
Sensitive Data	12.3	<p>The requirements of Articles 4.1 and 4.2 (Sensitive Data) may be set aside only for the Overriding Interests listed in Article 12.1 (i) (a), (c) and (e), (ii) and (iii).</p>
Consultation with Corporate Privacy Officer	12.4	<p>Setting aside obligations of AkzoNobel or rights of Employees based on an Overriding Interest, requires the prior consultation of the Corporate Privacy Officer. The Corporate Privacy Officer shall document his or her advice.</p>
Information to Employee	12.5	<p>Upon request of the Employee, AkzoNobel shall inform the Employee of the Overriding Interest for which obligations of AkzoNobel or rights of the Employee have been set aside, unless the particular Overriding Interest sets aside the requirements of Articles 6.1 or 7.1 – 7.3, in which case the request shall be denied.</p>
Article 13 – Privacy Governance		
Corporate Privacy Officer	13.1	<p>Akzo Nobel Nederland shall appoint a Corporate Privacy Officer who is responsible for:</p> <ul style="list-style-type: none"> (i) Establishing a Privacy Council as described in article 13.2;

- (ii) Supervising compliance with these Rules;
- (iii) Coordinating, communicating and consulting with the Privacy Managers network on central data protection issues;
- (iv) Providing annual privacy reports, as appropriate, to the Head of Legal on data protection risks and compliance issues as described in article 16.2;
- (v) Coordinating, in conjunction with the Privacy Counsel and Privacy Managers network, official investigations or inquiries into the Processing of Employee Data by a government authority;
- (vi) Dealing with conflicts between these Rules and applicable law as described in article 20.2;
- (vii) Approving transfers as described in articles 20.1 and 11.6;
- (viii) Providing advice on Data Protection Impact Assessments as described in Article 14.3;
- (ix) Deciding on complaints as described in article 17; and
- (x) Devising the data management processes, systems and tools to implement the framework for data protection management as established by the Privacy Council, including:
 - (a) To maintain, update and publish these Rules and related sub-policies;
 - (b) Tools to collect, maintain and update information regarding the structure and functioning of all systems that process personal data;
 - (c) Data privacy training and awareness for Employees to comply with their responsibilities under these Rules;
 - (d) Appropriate processes to monitor, audit and report compliance with these Rules and ensure that AkzoNobel Internal Audit can verify and certify such compliance in line with the yearly AkzoNobel Audit Program;
 - (e) Procedures regarding data protection inquiries, concerns and complaints; and
 - (f) Determine and update appropriate sanctions for violations of these Rules (e.g. disciplinary standards).

Where appropriate, the Corporate Privacy Officer may delegate any of the above responsibilities to the Privacy Managers or other person, to be carried out under the Corporate Privacy Officer's responsibility.

- | | | |
|------------------------|------|---|
| Privacy Council | 13.2 | <p>AkzoNobel shall establish a Privacy Council. The Privacy Council shall create and maintain a framework for:</p> <ul style="list-style-type: none"> (i) the development, implementation and updating of local Employee data protection policies and procedures; (ii) the maintaining, updating and publishing of these Rules and related sub-policies; (iii) the creating, maintaining and updating information regarding the structure and functioning of all systems that process personal |
|------------------------|------|---|

	<p>data (as required by Article 14);</p> <ul style="list-style-type: none"> (iv) the development, implementation and updating of the relevant data protection training and awareness programs; (v) the monitoring, auditing and reporting on compliance with these Rules to the management board; (vi) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and (vii) determining and updating appropriate sanctions for violations of these Rules (e.g. disciplinary standards).
<p>Privacy Managers</p>	<p>13.3 Each Organizational Unit shall designate a Privacy Manager. The Corporate Privacy Officer shall act as the Privacy Manager for Akzo Nobel N.V.</p> <p>The Privacy Managers shall perform the following tasks for their respective Organizational Unit:</p> <ul style="list-style-type: none"> (i) 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; (ii) Support and assess overall data protection management compliance within their Organizational Unit; (iii) Regularly advise their Responsible Executive and the Corporate Privacy Officer on privacy risks and compliance issues; (iv) Maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that process personal data (as required by Article 14.2); (v) Be available for requests for privacy approvals or advice as described in article 7; (vi) Provide information relevant to the annual privacy report of the Corporate Privacy Officer (as required in Article 16); (vii) Assist the Corporate Privacy Officer in the event of official investigations or inquiries by government authorities; (viii) Own and authorize all appropriate privacy sub-policies in their organizations; (ix) Direct that stored data be deleted or destroyed, anonymized or transferred as required by article 5.2; (x) Decide on and notify the Corporate Privacy Officer of complaints as described in article 17; and (xi) Cooperate with the Corporate Privacy Officer and the other Privacy Managers to: <ul style="list-style-type: none"> (a) Ensure that the instructions, tools and training are in place to enable the Organizational Unit, to comply with these Rules; (b) Share and provide guidance on best practices for data protection management within their Organizational Unit; (c) Ensure that data protection requirements are taken into account whenever new technology is implemented in their

		Organizational Unit;
		(d) Notify the Responsible Executive of the involvement of external service providers with data processing tasks for their Organizational Unit.
Responsible Executive	13.4	<p>The Responsible Executive of each Organizational Unit is accountable that effective data protection management is implemented in his or her Organizational Unit, is integrated into business practices, and that adequate resources and budget are available.</p> <p>Responsible Executives are accountable for:</p> <ul style="list-style-type: none"> (i) Ensuring overall data protection management compliance within their Organizational Unit, also during and following organizational restructuring, outsourcing, mergers and acquisitions and divestures; (ii) 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; (iii) 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 Privacy Manager); (iv) Ensuring and monitoring ongoing compliance of third parties with the requirements of these Rules 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); (v) Ensuring that relevant Employees in their Organizational Unit follow the prescribed data protection training courses; and (vi) Directing that stored data be deleted or destroyed, anonymized or transferred as required by article 5.2. <p>Responsible Executives are responsible for:</p> <ul style="list-style-type: none"> (i) Appointing a Privacy Manager for their Organisational Unit; (ii) Consulting with the Corporate Privacy Officer in all cases where there is a conflict between applicable local law and these Rules as described in Article 20.2; and (iii) Informing the Corporate Privacy Officer of any new legal requirement that may interfere with AkzoNobel's ability to comply with these Rules as required by Article 20.3 (after consultation with the local legal department).
Default Privacy Manager	13.5	If at any moment in time there is no Privacy Manager designated for a relevant Organizational Unit, the Corporate Privacy Officer will be responsible for the Organizational Unit assigned to the Privacy Manager.
Data Protection Officer with a	13.6	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

statutory position	responsibilities to the extent they do not conflict with his or her statutory position.
---------------------------	---

Article 14 – Policies and Procedures

Policies and Procedures	14.1	AkzoNobel shall develop and implement policies and procedures to comply with these Rules.
--------------------------------	------	---

Records of Processing Activities	14.2	AkzoNobel shall maintain readily available information regarding the structure and functioning of all systems and processes that Process Employee Data (e.g. inventory of systems and processes). A copy of this information will be provided to the Lead DPA or to a DPA competent to audit under Article 16.2 upon request.
---	------	---

Data Protection Impact Assessment	14.3	AkzoNobel shall maintain 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 Employees, in particular where new technologies are used (Data Protection Impact Assessment). Where the 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 Employees, the Lead DPA will be consulted prior to such Processing taking place.
--	------	--

Article 15 – Training

Staff training	15.1	AkzoNobel shall provide training on these Rules and related confidentiality obligations to Staff members who have access to Employee Data.
-----------------------	------	--

Article 16 – Monitoring and Auditing Compliance

Internal Audits	16.1	AkzoNobel Internal Audit shall audit business processes and procedures that involve the Processing of Employee Data for compliance with these Rules. The audits shall be carried out in the course of the regular activities of AkzoNobel Internal Audit or at the request of the Corporate Privacy Officer. The Corporate Privacy Officer may request to have an audit as specified in this Article 16.1 conducted by an external auditor. Applicable professional standards of
------------------------	------	--

		<p>independence, integrity and confidentiality shall be observed when conducting an audit. The Corporate Privacy Officer and the appropriate Privacy Managers shall be informed of the results of the audits. Reported violations of the Rules will be reported to the Responsible Executive. A copy of the audit results related to compliance with these Rules will be provided to the Lead DPA and a DPA competent to audit under Article 16.2 upon request.</p>
DPA Audit	16.2	<p>Subject to Article 16.3, the Lead DPA may request an audit of the facilities used by AkzoNobel for the Processing of Personal Data for compliance with these Rules. In addition, the DPA of the EEA country at the origin of a data transfer under these rules will be authorized to audit the relevant data transfer for compliance with these Rules.</p>
DPA Audit Procedure	16.3	<p>If a DPA requests an audit based on Article 16.2, the following procedure will be followed:</p> <ul style="list-style-type: none"> (i) Information sharing: AkzoNobel will attempt to resolve the request using alternative methods of providing information to the DPA including AkzoNobel audit reports, discussion with AkzoNobel subject matter experts, and review of security, privacy, and operational controls in place. (ii) Examinations: If the DPA determines that the information available through these mechanisms is insufficient to address the DPA's stated objectives, AkzoNobel will provide the DPA with the opportunity to communicate with AkzoNobel's auditor and if required, a direct right to examine AkzoNobel's data processing facilities used to process the Personal Data on giving reasonable prior notice and during business hours, with full respect to the confidentiality of the information obtained and to the trade secrets of AkzoNobel. <p>The audits will otherwise be performed in accordance with the relevant DPAs own national procedural laws.</p> <p>Nothing in these rules will be construed to take away any audit rights that a DPA may have under Data protection Law. In the event of any conflict between this Article 16.3 and applicable law, the provisions of applicable law will prevail.</p>
Annual Privacy Report	16.4	<p>The Corporate Privacy Officer shall implement appropriate processes to monitor compliance with these Rules and produce an annual Employee Data privacy report for the Executive Committee on compliance with these Rules, data protection risks, and other relevant issues.</p> <p>Each Privacy Manager shall provide information relevant to the report to the Corporate Privacy Officer.</p>
Mitigation	16.5	<p>AkzoNobel shall, if so indicated, ensure that adequate steps are taken to address breaches of these Rules identified during the monitoring or auditing of compliance pursuant to this Article 16.</p>

Article 17 – Complaints Procedure

Complaint to Privacy Manager

17.1 Employees may file a complaint in respect of any claim they have under Article 18.1 or violations of their rights under applicable local law:

- (i) with the appropriate Privacy Manager; or
- (ii) in accordance with the complaints procedure set forth in the AkzoNobel Code of Conduct.

The appropriate Privacy Manager shall:

- (i) notify the Corporate Privacy Officer;
- (ii) analyze the complaint and, if needed, initiate an investigation;
- (iii) when necessary, advise the business on the appropriate measures for compliance and monitor, through completion, the steps designed to achieve compliance; and
- (iv) maintain records of all complaints received, responses given, and remedial actions taken by AkzoNobel.

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

Reply to Employee

17.2 AkzoNobel will use reasonable efforts to resolve complaints without undue delay, so that a response is given to the Employee within one calendar month of the date that the complaint was filed. The appropriate Privacy Manager shall inform the Employee in writing via the means that the Employee originally used to contact AkzoNobel (e.g., via mail or email) either (i) of AkzoNobel position with regard to the complaint and any action AkzoNobel has taken or will take in response or (ii) when he or she will be informed of AkzoNobel's position, which date shall be no later than two calendar months thereafter. The appropriate Privacy Manager shall send a copy of the complaint and his or her written reply to the Corporate Privacy Officer.

Complaint to Corporate Privacy Officer

17.3 An Employee may file a complaint with the Corporate Privacy Officer if:

- (i) the resolution of the complaint by the appropriate Privacy Manager is unsatisfactory to the Employee (e.g., the complaint is rejected);
- (ii) the Employee has not received a response as required by Article 17.2;
- (iii) the time period provided to the Employee pursuant to Article 16.2 is, in light of the relevant circumstances, unreasonably long and the Employee has objected but has not been provided with a shorter, more reasonable time period in which he or she will receive a response; or
- (iv) in the events listed in Article 7.7.

The procedure described in Articles 17.1 through 17.2 shall apply to

complaints filed with the Corporate Privacy Officer.

If the response of the Corporate Privacy Officer to the complaint is unsatisfactory to the Employee (e.g., the request is denied), the Employee can file a complaint or claim with the authorities or the courts in accordance with Article 18.2.

Article 18 – Legal Issues

Rights of Employees

- 18.1 If AkzoNobel violates the Rules with respect to the Personal Data of an Employee (**Affected Employee**) covered by these Rules, the Affected Employee can as a third party beneficiary enforce any claim as a result of a breach of Articles 1.6, 2 – 11, 12.5, 16.2, 17, 18 and 20.4 - 20.5 in accordance with Article 18.2.

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

Jurisdiction for Claims of Employees

- 18.2 Employees are encouraged to first follow the complaints procedure set forth in Article 17 of these Rules before filing any complaint or claim with a competent DPA or the courts.

In case of a violation of these Rules, the Affected Employee may, at his or her choice, submit a complaint or a claim to the DPA or the courts:

- (i) in the Netherlands, against Akzo Nobel Nederland; or
- (ii) in the EEA country where (a) the Employee has his or her habitual residence or place of work, or (b) the infringement took place, or (c) the Group Company being the Data Controller of the relevant Personal Data is established, against the Group Company being the data controller of the relevant Personal Data or Akzo Nobel Nederland.

The Group Company against which the complaint or claim is brought (relevant Group Company), may not rely on a breach by another Group Company or a Third Party Processor of its obligations to avoid liability except to the extent any defense of such other Group Company or Third Party Processor would also constitute a defense of the relevant Group Company.

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

Right to Claim Damages

- 18.3 In case an Employee has a claim under Article 18.2, and
- (i) the relevant Processing is governed by Data Protection Law, such Employee shall be entitled to compensation of damages suffered by an Employee resulting from a violation of these Rules to the

		<p>extent provided by Data Protection Law; or</p> <p>(ii) the relevant Processing is not governed by Data Protection Law, such Employee shall be entitled to compensation of actual direct damages (which exclude, without limitation, lost profits or revenue, lost turnover, cost of capital, and downtime cost), suffered by an Employee resulting from a violation of these Rules.</p>
Burden of Proof in Respect of Claim for Damages	18.4	<p>In case an Employee brings a claim for damages under Article 18.2, it will be for the Employee to 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 these Rules. It will subsequently be for the relevant Group Company to prove that the damages suffered by the Employee due to a violation of these Rules are not attributable to AkzoNobel.</p>
Mutual Assistance and Redress	18.5	<p>All Group Companies shall co-operate and assist each other to the extent reasonably possible to handle:</p> <p>(i) a request, complaint or claim made by an Employee; or</p> <p>(ii) a lawful investigation or inquiry by a competent DPA or public authority.</p> <p>The Group Company employing the Employee is responsible for handling any communication with the Employee regarding his or her request, complaint or claim except where circumstances dictate otherwise. The Group Company that is responsible for the Processing to which the request, complaint or claim relates, shall bear all costs involved and reimburse Akzo Nobel Nederland.</p>
Advice of the Lead DPA	18.6	<p>Akzo Nobel Nederland shall abide by the advice of the EEA DPAs competent pursuant to Article 18.2 issued on the interpretation and application of these Rules.</p>
Mitigation	18.7	<p>Akzo Nobel Nederland shall ensure that adequate steps are taken to address violations of these Rules by a Group Company.</p>
Law Applicable to this Code	18.8	<p>This Code shall be governed by and interpreted in accordance with Dutch law.</p>
Article 19 – Sanctions for Non-compliance		
Non-compliance	19.1	<p>Non-compliance of Employees with these Rules may result in appropriate measures in accordance with applicable local law up to and including termination of employment.</p>
Article 20 – Conflicts between the Rules and Applicable Local Law		

Conflict of law when transferring Data	20.1	Where a legal requirement to transfer Employee Data conflicts with the laws of the Member States of the EEA or the law of Switzerland, the transfer requires the prior approval of the Corporate Privacy Officer. The Corporate Privacy Officer shall seek the advice of the Head of Legal. The Corporate Privacy Officer may seek the advice of the Dutch Data Protection Authority or another competent government authority.
Conflict between Rules and law	20.2	In all other cases, where there is a conflict between applicable local law and these Rules, the relevant Responsible Executive shall consult with the Corporate Privacy Officer to determine how to comply with these Rules and resolve the conflict to the extent reasonably practicable given the legal requirements applicable to the relevant Group Company.
New conflicting legal requirements	20.3	The relevant Responsible Executive (after consultation with the local legal department) shall promptly inform the Corporate Privacy Officer of any new legal requirement that may interfere with AkzoNobel's ability to comply with these Rules.
Reporting to Lead DPA	20.4	If AkzoNobel becomes aware that applicable local law of a non-EEA country is likely to have a substantial adverse effect on the protection offered by these Rules, AkzoNobel will report this to the Lead DPA.
Requests for Disclosure of Personal Data	20.5	<p>If AkzoNobel receives a request for disclosure of Personal Data from a law enforcement authority or state security body of a non-EEA country (Authority), it will first assess on a case-by-case basis whether this request (Disclosure Request) is legally valid and binding on AkzoNobel. Any Disclosure Request that is not legally valid and binding on AkzoNobel will be resisted in accordance with applicable law.</p> <p>Subject to the following paragraph, AkzoNobel shall promptly inform the Lead DPA of any legally valid and binding Disclosure Requests, and will request the Authority to put such Disclosure Requests on hold for a reasonable delay in order to enable the Lead DPA to issue an opinion on the validity of the relevant disclosure.</p> <p>If suspension and/or 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, AkzoNobel will request the Authority to waive this prohibition and will document that it has made this request. In any event, AkzoNobel will on an annual basis provide to the Lead DPA general information on the number and type of Disclosure Requests it received in the preceding 12 month period, to the fullest extent permitted by applicable law.</p> <p>In any event, any transfers by AkzoNobel of Personal Data to any Authority in response to a Disclosure Request will not be massive, disproportionate or indiscriminate.</p>
Article 21 – Changes to the Rules		

Approval for Changes	21.1	Any changes to these Rules require the prior approval of the Head Legal and shall thereafter be communicated to the Group Companies. The Corporate Privacy Officer shall promptly inform the Lead DPA of changes to these Rules that have a significant impact on the protection offered by these Rules or the Rules themselves and will be responsible for coordinating AkzoNobel's responses to questions of the Lead DPA in respect thereof. Other changes (if any) will be notified by the Corporate Privacy Officer to the Lead DPA on a yearly basis.
Effective Date of Changes	21.2	Any material change shall enter into force with immediate effect after it has been approved in accordance with Article 21.1 and is published on the AkzoNobel intranet.
Prior Versions	21.3	Any request, complaint or claim of an Employee involving these Rules shall be judged against the version of the Rules that is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

Transition Period for New Group Companies	22.1	Any entity that becomes a Group Company after the Effective Date shall comply with these Rules within two years of becoming a Group Company.
Transition Period for Divested Entities	22.2	A Divested Entity may remain covered by these Rules after its divestment for such period as may be required by AkzoNobel to disentangle the Processing of Employee Data relating to such Divested Entity.
Transition Period for IT Systems	22.3	Where implementation of these Rules requires updates or changes to information technology systems (including replacement of systems), the transition period shall be three years from the Effective Date or from the date an entity becomes a Group Company, or any longer period as is reasonably necessary to complete the update, change or replacement process.
Transition Period for Existing Agreements	22.4	Where there are existing agreements with Third Parties that are affected by these Rules, the provisions of the agreements will prevail until the agreements are renewed in the normal course of business.
Transition Period for Local-for-Local Systems	22.5	Processing of Employee Data that were collected in connection with activities of a Group Company not covered by an Adequacy Decision shall be brought into compliance with these Rules within five years of the Effective Date.

Article 23 – Interpretations

Interpretation of these Rules

23.1 These Rules should be interpreted as follows:

- (i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time;
- (ii) headings are included for convenience only and are not to be used in construing any provision of these Rules;
- (iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning;
- (iv) the male form shall include the female form;
- (v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa; and
- (vi) a reference to a document (including, without limitation, a reference to these Rules) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by these Rules or that other document.

Contact Details

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

ANNEX 1**Definitions**

Adequate Decision	shall mean a decision issued by the European Commission under Data Protection Law that a country or region or a category of recipients in such country or region is deemed to provide an "adequate" level of data protection.
Akzo Nobel N.V.	shall mean Akzo Nobel N.V., having its registered seat in Amsterdam, The Netherlands.
AkzoNobel	shall mean Akzo Nobel N.V. and its Group Companies.
Archive	shall mean a collection of Employee Data that are no longer necessary to achieve the purposes for which the Data originally were collected or that are no longer used for general business activities, but are used only for historical, scientific or statistical purposes, dispute resolution, investigations or general archiving purposes. An archive includes any data set that can no longer be accessed by any Employee other than the system administrator.
Article	shall mean an article in these Rules.
Binding Corporate Rules	shall mean a privacy policy of a group of undertakings which under applicable local law (such as Article 47 of the European General Data Protection Regulation) is considered to provide an adequate level of protection for the transfer of Personal Data within that group of undertakings.
Business Purpose	shall mean a purpose for Processing Employee Data as specified in Article 2 or 3 or for Processing Sensitive Data as specified in Article 4 or 3.
Corporate Privacy Officer	shall mean the officer as referred to in Article 13.1.
Data Controller	shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Protection Impact Assessment	<p>shall mean a procedure to conduct and document a prior assessment of the impact which a given Processing may have on the protection of Employee Information, where such Processing is likely to result in a high risk for the rights and freedoms of Employees, in particular where new technologies are used.</p> <p>A DPIA shall contain:</p> <ul style="list-style-type: none"> (i) a description of: <ul style="list-style-type: none"> (a) the scope and context of the Processing; (b) the Business Purposes for which Employee Information is Processed; (c) the specific purposes for which Sensitive Information is Processed;

	<ul style="list-style-type: none"> (d) categories of Employee Information recipients, including recipients not covered by an Adequacy Decision; (e) Employee Information storage periods; (ii) an assessment of: <ul style="list-style-type: none"> (a) the necessity and proportionality of the Processing; (b) the risks to the privacy rights of Employees; and (c) the measures to mitigate these risks, including safeguards, security measures and other mechanisms (such as privacy-by-design) to ensure the protection of Employee Information.
Data Protection Law	shall mean the provisions of mandatory law of an EEA Country containing rules for the protection of Employees with regard to the Processing of Personal Information including security requirements for and the free movement of such Personal Information.
Dependent	shall mean the spouse, partner or child belonging to the household of the Employee or emergency contact of the Employee.
Divested Entity	<p>shall mean the divestment by AkzoNobel of a Group Company or business by means of:</p> <ul style="list-style-type: none"> (a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or (b) a demerger, sale of assets, or any other manner or form.
DPA	shall mean any data protection authority of one of the countries of the EEA.
EEA	or European Economic Area shall mean all Member States of the European Union, plus Norway, Iceland and Liechtenstein.
Effective Date	shall mean the date on which these Rules become effective as set forth in Article 1.6.
Employee	shall mean an employee, job applicant or former employee of AkzoNobel. This term does not include people working at AkzoNobel as consultants or employees of Third Parties providing services to AkzoNobel.
Employee Data or Data	shall mean any information relating to an identified or identifiable Employee (and his or her Dependants); an identifiable Employee is one who can be identified, directly, or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person..
Executive Committee	shall mean the Executive Committee of Akzo Nobel N.V.
Group Company	shall mean 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 has implemented the AkzoNobel Code of Conduct.
Head of Legal	shall mean the General Counsel of Akzo Nobel N.V..
Lead DPA	shall mean the DPA of the Netherlands.
Organizational Unit	shall mean a unit that is delivering services, responsible for business or regional or functional tasks within AkzoNobel.
Original Purpose	shall mean the purpose for which Employee Data was originally collected.
Overriding Interest	shall mean the pressing interests set forth in Article 12.1 based on which the obligations of AkzoNobel or rights of Employees under specific circumstances, be overridden if this pressing interest outweighs the interest of the Employee.
Personal Data Breach	<p>shall mean the unauthorized acquisition, access, use, unavailability or disclosure of unencrypted Personal Data that compromises the security or privacy of such data to the extent the compromise poses a significant risk of financial, reputational, or other harm to the Employee. A Personal Data Breach is deemed not to have occurred where there has been an unintentional acquisition, access or use of unencrypted Personal Data by an employee of AkzoNobel or Third party Processor or an Employee acting under their respective authority, if:</p> <ul style="list-style-type: none"> (i) the acquisition, access, or use of Personal Data was made in good faith and within the course and scope of the employment or professional relationship of such employee; and (ii) the Personal Data are not further acquired, accessed, used or disclosed by any person.
Privacy Council	shall mean the Council as referred to in Article 13.2.
Privacy Counsel	shall mean the Legal Counsel Privacy appointed by the Corporate Privacy Officer.
Privacy Manager	shall mean the privacy manager appointed by the Corporate Privacy Officer pursuant to Article 13.3.
Processing	shall mean any operation that is performed on Employee 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 Employee Data.
Processor Contract	shall mean any contract for the Processing of Personal Data entered into by AkzoNobel and a Third Party Processor.
Responsible	shall mean the executive of each Organizational Unit who is accountable that

Executive	effective data protection management is implemented in his or her Organizational Unit, is integrated into business practice, and that adequate resources and budget are available, as referred to in article 13.4.
Rules	shall mean these Privacy Rules for Employee Data.
Secondary Purpose	shall mean any purpose other than the Original Purpose for which Employee Data is further Processed.
Sensitive Data	shall mean Employee Data that reveal an Employee's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or mental health including any opinion thereof, disabilities, genetic data, biometric data for the purpose of uniquely identifying a natural person, addictions, sex life, sexual orientation, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Staff	shall mean all Employees and other persons who Process Employee Data as part of their respective duties or responsibilities using AkzoNobel information technology systems or working primarily from AkzoNobel's premises.
Third Party	shall mean any person, private organization or government body outside AkzoNobel.
Third Party Controller	shall mean a Third Party that Processes Employee Data and determines the purposes and means of the Processing.
Third Party Processor	shall mean a Third Party that Processes Employee Data on behalf of AkzoNobel that is not under the direct authority of AkzoNobel.
Related documents	
Directive 7.08 Protection of Personal Data	
7.08.2 Privacy Rules for Customer, Supplier and Business Partner Data	