Binding Corporate Rules – Controller Policy

Introduction

Arcadis N.V. and its group companies ("**Arcadis**") has committed itself to the protection of personal data it processes of its employees, clients, suppliers, business partners and other individuals in its Arcadis Risk & Control Framework ("**ARC Framework**").

This Privacy Policy indicates how this principle shall be implemented in respect of personal data of:(i) clients, suppliers, business partners, contingent workers and other individuals that are processed by Arcadis in the context of its business activities; and (ii) employees and other individuals working at Arcadis. This Privacy Policy 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 Arcadis, including its Employees.

Capitalized terms have the meaning set out in **Annex 1** (Definitions). Capitalized terms that are not defined in this Privacy Policy have the meanings given to them in the EU General Data Protection Regulation (Regulation (EU) 2016/679) (**GDPR**).

Article 1 – Scope, Applicability and Implementation

Scope	1.1.	This Policy applies to the Processing by Arcadis as a Controller of Personal Data (as described in Annex 2) that are (a) subject to data transfer restrictions under EEA Data Protection Laws (or were subject to data transfer restrictions under EEA Data Protection Laws prior to their Transfer), and (b) transferred to an Arcadis Group Company in a Third Country acting as a Controller or Internal Data Processor.
Electronic and paper-based Processing	1.2.	This Policy applies to the Processing of Personal Data by electronic means and in systematically accessible paper-based filing systems.
Applicability of local law and Policy	1.3.	Individuals keep any rights and remedies they may have under applicable local law. This Policy shall apply only where it provides supplemental protection for Personal Data. Where applicable local law provides more protection than this Policy, local law shall apply in addition to this Policy. Where this Policy provides more protection than applicable local law or provides additional safeguards, rights or remedies for Individuals, this Policy shall apply in addition to applicable local law. Article 20.1 applies to conflicts between applicable local law and this Policy,
Sub-policies and notices	1.4.	Arcadis may supplement this Policy through standards, rules, procedures, manuals, guidelines or notices that are consistent with this Policy.
Accountability	1.5.	This Policy is legally binding and shall apply to and be enforced by Arcadis, including its Employees. The Responsible Executives shall be accountable for compliance with this Policy.
Effective Date	1.6.	This Policy has been adopted by the Executive Board of ANV and has entered into force as of 24 May 2018 (**Effective Date**) and has applied from that day on to all Group Companies. This Policy (including a list of

Group Companies) shall be published on the Arcadis websites and intranet and be made available to Individuals upon request. A notice shall be published on the Arcadis internet site that this Policy will be made available to Individuals upon request and how a copy can be obtained.

Policy supersedes prior policies

1.7. This Policy supersedes all Arcadis privacy policies and notices that exist on the Effective Date to the extent they are in contradiction with this Policy.

Role of Arcadis International B.V.

1.8. Arcadis N.V. has appointed Arcadis International B.V. as the Group Company within the EU with delegated data protection responsibilities for the purposes of this Policy. These responsibilities include the oversight, coordination and implementation of this Policy on a global basis and further accepting liability for breaches of this Policy by Group Companies outside of the EEA as described more fully in Article 18 of this Policy.

Article 2 – Purposes for Processing Personal Data

Legitimate Business Purposes

2.1. Personal Data shall be Processed lawfully. Lawful processing means that Arcadis will not Process Personal Data, unless Arcadis needs to Process Personal Data for:

(a) the performance of a contract to which the relevant Individual is a party, or in order to take steps at the request of the relevant Individual prior to entering into a contract;

(b) the compliance with a legal obligation to which Arcadis is subject;

(c) the protection of the vital interests of Individuals or others;

(d) the performance of a task carried out in the public interest;

(e) the pursuit of a legitimate interest, except where this interest is overridden by the interests or fundamental rights and freedoms of the Individual concerned; or

(f) where applicable, in accordance with Article 2.2.

The Processing of Personal Data for the purposes set out in **Annex 2** (**Business Purposes**) can generally be based on one of the main legal bases set out in this Article 2.1, but remains subject to any applicable requirements and restrictions under EEA Data Protection Law.

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

Consent

2.2. In addition to the Business Purposes listed in Article 2.1, Personal Data may be Processed if the Individual has given his or her consent to the Processing. If applicable EEA law requires that Arcadis requests consent of the Individual for the relevant Processing, Arcadis shall, in addition to ensuring that a Business Purpose exists for the Processing, also seek consent of the Individual for the Processing.

When seeking consent for Processing Personal Data, Arcadis must inform the Individual:

(i) of the categories of Personal Data and the purposes of the Processing for which consent is requested;

(ii) which Group Company is responsible for the Processing;

(iii) of the possible consequences of automated decision-making, including profiling, for the Individual of the Processing;

(iv) that they are free to refuse or withdraw consent at any time (and for Employee Data, that this will be without consequence to the Employees' employment relationship); and

(v) that withdrawal of consent does not affect the lawfulness of the relevant Processing before such withdrawal and the lawfulness of Processing of the relevant Personal Data after withdrawal for other Processing Purposes not based on consent.

Additional requirements for Employee Data

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. If none of the Business Purposes apply, Arcadis 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 Privacy Officer prior to seeking consent.

Denial or withdrawal of consent

2.3. The Individual may both deny consent and withdraw consent at any time. The withdrawal of consent shall not affect the lawfulness of the Processing based on such consent before its withdrawal or the lawfulness for the Processing for other Processing Purposes not based on consent. Arcadis will discontinue such Processing without undue delay.

Limitations on Processing Personal Data of Dependents

2.4. Arcadis will Process Personal 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 of for managing the employment-at-will relationship; or

(iii) Processing is required or permitted by applicable EEA law.

Personal Data of Dependents will be considered Employee Data for the purposes of this Policy and Dependents shall have the same rights as Employees under this Policy.

Article 3 – Use for Other Purposes

Use of Personal Data for Secondary Purposes

3.1. Personal Data may be Processed for a legitimate purpose other than the Business Purpose(s) for which the Personal Data was originally collected, only if the additional purpose is compatible with the relevant Business Purpose(s), taking into account the link between the original and additional purpose, the context in which the Personal Data is collected, the nature of the relevant Personal Data and the implementation of appropriate safeguards set out below (**Secondary**

Purpose).

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 safeguarding measures such as limiting access to Personal Data or taking additional security measures to mitigate the consequences. If the consequences cannot be appropriately mitigated, Arcadis may need to provide the Individual an opt-out opportunity or obtain an Individual's consent.

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

To the extent not already covered by Article 2.1 and subject to the compatibility test referred to above, below are a number of examples of Processing for Secondary Purposes that may be permissible:

- anonymization of Personal Data;
- transfer of Personal Data to an archive;
- internal audits or investigations;
- implementation of business controls and operational efficiency;
- IT systems and infrastructure related Processing such as for maintenance, support, life-cycle management, and security (including resilience and incident management);
- statistical, historical or scientific research;
- dispute resolution;
- legal or business consulting; or
- insurance purposes.

Article 4– Purposes for Processing Privacy Sensitive Data

Purposes for Processing Privacy Sensitive Data

4.1. Arcadis (i) will not Process Privacy Sensitive Data relating to criminal convictions and offences or related security measures, unless such Processing is carried out under the control of official EEA authority or is authorized by EEA law for one of the purposes specified in **Annex 2**, and (ii) will not Process other categories of Privacy Sensitive Data unless one of the conditions in Article 4.2 applies. Arcadis shall Process Privacy Sensitive Data only to the extent necessary to serve one or more of the purposes specified in **Annex 2** or as otherwise provided by EEA law.

Conditions for Processing of Privacy Sensitive Data

4.2. In addition to the specific purposes listed in Article 4.1, Privacy Sensitive Data shall be Processed lawfully. Lawful Processing means that Arcadis will not Process Privacy Sensitive Data unless one of the following conditions applies:

(i) Processing is 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);

(ii) Processing is necessary for the establishment, exercise or defence of a legal claim;

(iii) Processing is necessary to protect a vital interest of an

Individual, but only where it is impossible to obtain the Individual's consent first;

(iv) Privacy Sensitive Data have manifestly been made public by the Individual.

Consent, and the denial or withdrawal of consent

4.3. In addition to the purposes listed in Article 4.1 and the conditions listed in Article 4.2, all categories of Privacy Sensitive Data may be Processed if the Individual has given their explicit consent to the Processing thereof. If one of the conditions listed in Article 4.2 applies, Arcadis shall in addition seek consent if applicable EEA law so requires. The information requirements set out in Article 2.2 and Article 2.3 apply to the granting, denial or withdrawal of consent.

Requirements for Employee consent for Processing Privacy Sensitive Data

Employee consent generally cannot be used as a legitimate basis for Processing Privacy Sensitive Data. One of the grounds listed in Article 4.2 must exist for any Processing of Privacy Sensitive Data. If applicable EEA law so requires, in addition to having one of the conditions listed in Article 4.2 for the relevant Processing, Arcadis shall also seek Employee consent for the Processing. If none of the conditions listed in Article 4.2 apply, Arcadis may request Employee consent for Processing Privacy 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). The information requirements set out in Articles 2.2 and 2.3 apply to the granting, denial or withdrawal of Employee consent.

Prior consultation of Privacy Officer

4.4. Where Privacy Sensitive Data are Processed based on the consent of an Individual, the Processing requires the prior consultation of the appropriate Privacy Officer.

Use of Privacy Sensitive Data for Secondary Purposes

4.5. Privacy Sensitive Data of Individuals may be Processed for Secondary Purposes in accordance with Article 3 and only if one of the conditions of Article 4.1 – 4.3 applies.

Article 5– Quantity and Quality of Personal Data

No excessive Personal Data

5.1. Arcadis shall limit the Processing of Personal Data to those Personal Data that are necessary and adequate for and relevant to the applicable Processing Purpose. Arcadis shall take reasonable steps to delete Personal Data that are not required for the applicable Processing Purpose.

Storage period

5.2. Arcadis shall not retain Personal Data longer than the period necessary for the applicable Processing Purpose. Arcadis may specify (e.g., in a sub-policy, notice or records retention schedule) a time period for which certain categories of Personal Data may be kept.

Promptly after the applicable storage period has ended, the Privacy Officer shall direct that the Personal Data be:

(i) securely deleted or destroyed, or

(ii) anonymized.

Quality of Personal Data

5.3. Personal Data should be accurate, complete and kept up-to-date to the extent necessary for the applicable Processing Purpose. Where Personal Data are inaccurate, Arcadis shall take reasonable steps to rectify or erase such Personal Data without delay.

Accurate, complete and up-to-date Data

5.4. Arcadis encourages Individuals to keep their Personal Data accurate, complete and up-to-date. Individuals shall inform Arcadis regarding any changes in accordance with Article 7. Where Arcadis requires an Employee to update their own Employee Data, Arcadis shall remind them at least once a year to do so.

'Privacy by Design and by Default'

5.5. Arcadis shall, both at the time of determination of the means of 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 the requirements of this Article 5 are implemented consistent with privacy by design and privacy by default principles under EEA Data Protection Law, when implementing new systems and processes that Process Personal Data.

Article 6– Individual Information Requirements

Information requirements

6.1. At the time when Personal Data are obtained, or prior to Processing Personal Data for a Secondary Purpose, Arcadis shall inform Individuals through a privacy policy or notice about:

(i) the Processing Purposes for which Personal Data are Processed;

(ii) which Group Company is responsible for the Processing as well as the contact information of the relevant Privacy Officer;

(iii) the categories of Third Parties to which the Personal Data are disclosed (if any); and

(iv) if applicable, the fact that Personal Data will be transferred to an international organization or a Third Party located in a Third Country, including the safeguards in place to protect the Personal Data;

Arcadis will also inform Individuals about other relevant information e.g.:

(a) the nature and categories of the Processed Personal Data;

(b) the legal basis for Processing of their Personal Data and, if the Processing is based on the legitimate interests of Arcadis, of the legitimate interests pursued by Arcadis;

(c) the period for which the Personal Data will be stored or (if not possible) the criteria used to determine this period;

(d) the rights of Individuals under this Policy and how these can be exercised, including the right to obtain compensation and the

right to lodge a complaint with a Supervisory Authority;

(e) 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 Individual;

(f) whether the provision of Personal Data is a statutory or contractual requirement, or a requirement necessary to enter into a contract, as well as whether the Individual is obliged to provide the Personal Data and of the possible consequences of failure to provide such Personal Data; and

(g) the source of the Personal Data (where the Personal Data have not been obtained from the Individual), including whether the Personal Data came from a public source.

Personal Data not obtained from the Individual

6.2. Where Personal Data have not been obtained directly from the Individual, Arcadis shall provide the Individual with the information as set out in Article 6.1:

(i) within 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 the 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.

Exceptions

6.3. The requirements of Articles 6.1 and 6.2 are inapplicable if the Individual already has the information as set out in Article 6.1. Where Personal Data has not been obtained directly from the Individual, the requirements of Article 6.1 and 6,2 are inapplicable if:

(i) it would be impossible or would involve a disproportionate effort to provide the information to Individuals, in which case Arcadis will take additional measures to mitigate potential negative consequences for the Individual, such as those listed in Article 3.1; or

(ii) obtaining Personal Data is expressly laid down in applicable EEA law.

Article 7– Rights of Individuals

Right to access

7.1. Individuals have the right to request confirmation whether or not their Personal Data are Processed, request a copy thereof as well as request access to the information listed in Article 6.1.

Right to rectification, deletion, and restriction

7.2. Where Personal Data are incorrect, incomplete, or not Processed in compliance with EEA Data Protection Law, the Individual has the right to have their Personal Data:

(i) rectified or completed, if such Personal Data are incorrect or incomplete;

(ii) deleted, if such Personal Data are not Processed in compliance with EEA Data Protection Law or this Policy, or

deletion is required by EEA law; or

(iii) restricted from Processing other than for storage, pending verification in case the accuracy of such Personal Data are contested or if the Individual objects to such Processing under Article 7.3, or where the Processing is unlawful or no longer needed, but the Individual prefers restriction to erasure of the Personal Data. Arcadis will only Process the restricted Personal Data with the Individual's consent or as permitted by EEA Data Protection Law. Arcadis will inform the Individual before the restriction is lifted.

Arcadis shall communicate any rectification, deletion, or restriction in accordance with the rights in 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. Arcadis will inform the Individual about those recipients upon request.

Right to object

7.3. The Individual has the right to object to the Processing of their Personal Data on the basis of compelling grounds related to their particular situation, unless Arcadis can demonstrate a prevailing legitimate interest for the Processing.

Restrictions to rights of Individuals

7.4. The rights of Individuals set out in Articles 7.1 – 7.3 are subject to any applicable exceptions provided under EEA Data Protection Law. Applying exceptions requires the prior consultation of the relevant Privacy Officer. Depending on the relevant rights of the Individual, exceptions may be available in the following cases.

All requests:

(i) a specific restriction of the rights of Individuals applies under applicable EEA law.

Requests for erasure:

(ii) the Processing is necessary for compliance with a legal obligation of Arcadis;

(iii) the Processing is necessary 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;

(iv) the Processing is necessary for exercising the right of freedom of expression and information;

Requests for erasure and to opt out (right to object):

(v) for dispute resolution purposes;

(vi) the Processing is required by or allowed for a task carried out in the public interest;

Requests for access:

(vii) the exercise of the rights by the Individual adversely affects the rights and freedoms of others.

Procedure

7.5. Individuals that are not Employees should send their request to the contact indicated in the relevant privacy statement or notice. They may also send their request to the office of the Global Privacy Officer via email to **[privacy@arcadis.com]**. Employees should send their request to the appropriate Privacy Officer. The contact details of the

Privacy Officers are available at the Arcadis Intranet.

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

(i) specify the categories of Personal Data to which they are seeking access;

(ii) specify, to the extent reasonably possible, the data system in which the Personal Data are likely to be stored;

(iii) specify, to the extent reasonably possible, the circumstances in which Arcadis obtained the Personal Data;

(iv) provide proof of their identity when Arcadis has reasonable doubts concerning such identity or to provide additional information enabling their identification;

(v) pay a reasonable fee to compensate Arcadis for the reasonable costs relating to fulfilling the request of the Individual, provided that Arcadis can reasonably demonstrate that the request is manifestly unfounded or excessive, e.g., because of its repetitive character, or additional copies are requested in the exercise of the right to access; and

(vi) 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 applicable EEA Data Protection Law or this Policy.

Response period

7.6. Within one month of Arcadis receiving the request, the contact person or Privacy Officer shall inform the Individual in writing either (i) of Arcadis' position with regard to the request and any action Arcadis has taken or will take in response or (ii) the ultimate date on which they will be informed of Arcadis' position. Arcadis may extend the original one-month response period by two months where necessary, taking into account the complexity and number of requests. Arcadis shall explain the reasons of this delay.

Complaint

7.7. Where an Individual has the right to lodge a request under Articles 7.1-7.3, the Individual also has the right to file a complaint in accordance with Article 17.3 and/or file a complaint or claim with the Supervisory Authorities or the courts in accordance with Article 18 if:

(i) the response to the request is unsatisfactory to the Individual (e.g., the request is denied);

(ii) the Individual has not received a response as required by Article 7.6; or

(iii) the time period provided to the Individual in accordance with Article 7.6 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which they will receive a response.

Denial of requests

7.8. Arcadis may deny an Individual request if:

(i) the request does not meet the requirements of Articles 7.1-7.3 or an exemption under Article 7.4 applies;

(ii) the identity of the relevant Individual cannot be established by reasonable means, including additional information provided

by the Individual; or

(iii) Arcadis 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.

No requirement to Process identifying information

7.9. If the Processing Purposes do not or do no longer require the identification of an Individual, Arcadis shall not be 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 Article 7. In this case, Article 7.1 through 7.4 shall not apply, except where the Individual, for the purpose of exercising those rights, provides additional information enabling his or her identification.

Article 8– Security and Confidentiality Requirements

Data security

8.1. Arcadis shall appropriate take technical, physical and organizational measures to protect Personal Data from misuse or accidental, unlawful, or unauthorized destruction, loss, alteration, disclosure, acquisition or access. These measures shall, taking into account the state of the art ("*stand van de techniek*") and the costs of the implementation and execution of the measures, ensure an adequate level of protection taking into account the risks involved in the Processing and the nature of the Personal Data to be secured. To achieve this, Arcadis has developed and implemented the Arcadis IT framework and policies, available and updated from time to time through the Arcadis intranet and other policies relating to the protection of Personal Data, as integrated in the ARC Framework.

Staff access

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

Confidentiality obligations

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

Internal data Processing

8.4. Where a Group Company acts as Internal Data Processor, it shall only do so on the instruction of the Arcadis Data Controller.

Data Security Incident notification requirement

8.5. Group Companies outside the EEA shall notify Data Security Incidents without undue delay to Arcadis International B.V. and the Global Privacy Office in accordance with Arcadis' established incident response procedures. Group Companies that act as Internal Data Processors will notify the relevant Group Company that is the Data Controller of the affected Personal Data without undue delay upon becoming aware of the Data Security Incident.

Arcadis shall notify the Competent Supervisory Authority(s) of a Data Security Incident without undue delay, and where feasible within 72 hours after becoming aware of it, unless the Data Security Incident is unlikely to result in a risk to the rights and freedoms of Individuals. In addition, if the Data Security Incident is likely to result in a high risk to the rights and freedoms of Individuals, Arcadis shall notify the affected Individuals of the Data Security Incident without undue delay following

its determination that such a Data Security Incident has occurred.

Arcadis shall respond promptly to inquiries of Individuals relating to such Data Security Incident. Group Companies shall document any Data Security Incidents, comprising the facts relating to the Data Security Incident, its effects and the remedial actions taken. Documentation pertaining to Data Security Incidents will be made available to the Competent SA upon request.

Article 9– Direct Marketing

Consent for direct marketing (opt-in)

9.1. If applicable EEA law so requires, Arcadis shall send directed marketing communications to an Individual only with the Individual's opt-in consent. If applicable EEA law does not require prior opt-in consent of the Individual, Arcadis shall offer the Individual the opportunity to opt-out of such directed marketing communications.

Objection to direct marketing

9.2. If an Individual objects to receiving direct marketing communications from Arcadis, or withdraws their consent to receive such communications, Arcadis will take steps to refrain from sending further direct marketing communications as specifically requested by the Individual. Arcadis will do so without undue delay.

Personal Data of Children

9.3. Arcadis shall not use any Personal Data of Children for direct marketing, without the prior consent of the holders of parental responsibility over Children. Arcadis shall make reasonable efforts to verify that consent is given or authorized by the holders of parental responsibility over the Children.

Article 10– Automated Decision Making

Automated decisions

10.1. Individuals have the right not to be subject to a decision based solely on automated decision-making, including profiling, which produces legal effects or similarly significantly affects them. This restriction does not apply if:

(i) the use of automated tools is authorized by EEA law;

(ii) the decision is necessary for purposes of (a) entering into or performing a contract between the Individual and Arcadis, or (b) managing the contract or employment-at-will relationship (as applicable) between the Individual and Arcadis, provided the underlying request leading to a decision by Arcadis was made by the Individual (e.g., where automated tools are used to filter promotional game submissions or job applications); or

(iii) the decision is made based on the explicit consent of the Individual.

Arcadis will only Process Privacy Sensitive Data for automated decision-making purposes with the Individual's explicit consent or where the Processing of an Individual's Privacy Sensitive Data is necessary for reasons of substantial public interest on the basis of EEA law.

Suitable measures

10.2. The items (ii) and (iii) in Article 10.1 only apply if suitable measures are taken to safeguard the legitimate interests of the Individual, including at least the right for the Individual to obtain human intervention and to express their point of view. The requirements set out in Articles 2.2 and 2.3 apply to the requesting, denial or withdrawal of consent.

Article 11– Disclosure and Transfer of Personal Data to Third Parties

Disclosures to Third Parties

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

Third Party Controllers and Third Party Processors

11.2. There are two categories of Third Parties:

(i) **Third Party Controllers**: these are Third Parties that Process Personal Data and determine the purposes and means of the Processing (e.g., Arcadis Business Partners that provide their own goods or services directly to Clients, or government authorities or service providers that provide their services directly to Employees);

(ii) **Third Party Processors**: these are Third Parties that Process Personal Data on behalf of Arcadis and at its direction (e.g., Third Parties that Process online registrations made by Clients or Employee salaries on behalf of Arcadis).

Disclosure for applicable Processing Purposes only

11.3. Arcadis shall disclose Personal Data to a Third Party to the extent necessary to serve the applicable Processing Purpose (including purposes for which the Individual has provided consent in accordance with Article 2).

Third Party Controller safeguards

11.4. Third Party Controllers (other than government agencies or bodies) may Process Personal Data only if they have validly entered into an electronic or written contract with Arcadis. In the contract, Arcadis shall seek to contractually safeguard the data protection interests of Individuals when Personal Data are disclosed to Third Party Controllers. All such contracts shall be drafted in consultation with the appropriate Privacy Officer. Individual Business Contact Data may be disclosed to a Third Party Controller without a contract if it is reasonably expected that such Business Contact Data will be used by the Third Party Controller to contact the Individual for legitimate business purposes related to Individual's job responsibilities.

Third Party Processor contracts

11.5. Third Party Processors may Process Personal Data only if they have validly entered into an electronic or written contract with Arcadis. The contract with a Third Party Processor must include the following provisions:

(i) the Third Party Processor shall Process Personal Data only for the purposes authorized by Arcadis and in accordance with Arcadis' documented instructions, including on Transfers to any Third Party Processor in a Third Country, unless the

Third Party Processor is required to Transfer under mandatory requirements applicable to the Third Party Processor and has notified Arcadis thereof;

(ii) the Third Party Processor shall keep the Personal Data confidential and shall impose confidentiality obligations on staff with access to Personal Data;

(iii) the Third Party Processor shall take appropriate technical, physical and organizational security measures to protect the Personal Data;

(iv) the Third Party Processor shall only permit subcontractors to Process Personal Data in connection with its obligations to Arcadis (a) with the prior specific or generic consent of Arcadis 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 Third Party Processor contract and provided that the Third Party Processor remains liable to Arcadis for the performance of the subcontractors in accordance with the terms of the Third Party Processor contract. In case Arcadis provides generic consent for involvement of subcontractors, the Third Party Processors shall provide notice to Arcadis of any changes in its subcontractors and will provide Arcadis the opportunity to object to such changes based on reasonable grounds;

(v) Arcadis should be able to verify the above-mentioned security measures taken by the Third Party Processor (a) by an obligation of Third Party Processor to submit its relevant facilities used to Process Personal Data to audits and inspections by Arcadis, a Third Party on behalf of Arcadis, or any relevant public authority; or (b) by means of a statement issued by a qualified independent third party assessor on behalf of Third Party Processor certifying that the facilities of the Third Party Processor used for the Processing of Personal Data comply with the requirements of the Third Party Processor contract;

(vi) the Third Party Processor shall promptly inform Arcadis of any actual or suspected security incident involving Personal Data;

(vii) the Third Party Processor shall promptly and appropriately deal with:

(a) requests for information necessary to demonstrate compliance of the Third Party Processor with its obligations under the Third Party Processor contract and will inform Arcadis if any instructions of Arcadis in this respect violate applicable law;

(b) requests and complaints of Individuals as instructed by Arcadis;

(c) requests for assistance of Arcadis as reasonably required to ensure compliance of the Processing of the Personal Data with EEA Data Protection Law; and

(viii) upon termination of the Third Party Processor contract, the Third Party Processor shall, at the option of Arcadis, return the Personal Data and copies thereof to Arcadis or shall securely delete such Personal Data, except to the extent the

Third Party Processor contract or EEA Data Protection Law provides otherwise.

Transfer to a Third Country

11.6. This Article sets forth additional rules for Transfers to a Third Party located in a Third Country.

Transfers to a Third Party in a Third Country may only take place:

(i) in accordance with a data transfer mechanism that is recognized under EEA Data Protection Law as providing an adequate level of data protection; or

(ii) if (i) does not apply, the Transfer is subject to an applicable derogation for specific situations under EEA Data Protection Law (e.g., the processing 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, or the Individual has given his or her explicit consent to the Transfer in accordance with Article 11.7).

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

Prior to a Transfer under (i), Arcadis will conduct a Transfer Impact Assessment in accordance with Article 14.4.

Consent for Transfer

11.7. If applicable local law so requires, in addition to having one of the grounds listed in Article 11.6, Arcadis shall (also) seek consent from the Individual for the Transfer to a Third Party located in a Third Country.

Prior to requesting consent, the Individual shall be provided with the following information:

(i) the purpose of the Transfer;

(ii) the identity of the transferring Group Company;

(iii) the identity or categories of Third Parties to which the Personal Data will be transferred;

(iv) the categories of Personal Data that will be transferred;

(v) the country to which the Personal Data will be transferred; and

(vi) the fact that the Personal Data will be transferred to a Third Country.

Article 2.3 applies to the denial or withdrawal of consent.

Requirements for Employee consent

Arcadis generally shall not seek Employee consent for a Transfer to a Third Party located in a Third Country. 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, Arcadis shall also seek Employee consent for the relevant Transfer. If none of the grounds listed in Article 11.6 exists, Arcadis may request Employee consent for a Transfer to a Third Party located in a Third Country, but only if:

1. the Transfer has no foreseeable adverse consequences for the Employee; or

2. the consent is requested prior to the participation of the Employee in specific projects, assignments or tasks that require the Transfer.

Requesting Employee consent for a Transfer requires the prior consultation of the appropriate Privacy Officer.

Internal Data Processors

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

Article 12– Restrictions under EEA law

Restrictions under EEA law

12.1. Certain rights of Individuals and obligations of Arcadis in this Policy 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 (including cooperating with law enforcement) criminal offences, or non-compliance with the Arcadis Code of Conduct or other Arcadis policies or procedures;

(ii) enforce civil law claims; and/or

(iii) protect Individuals or the rights or freedoms of others.

Applying such restrictions requires the prior consultation of the relevant Privacy Officer and will be documented.

Article 13– Supervision and Compliance

Global Privacy Officer

13.1. The Executive Board of ANV has appointed a Global Privacy Officer who is supported by a global network of Privacy Officers, sufficient to direct compliance with this Policy. Where required under EEA Data Protection Law, Arcadis will appoint a data protection officer (**DPO**) who shall have the tasks and responsibilities in accordance with EEA Data Protection Law, including reporting on privacy compliance to the board of directors of the relevant Group Company.

The Global Privacy Officer is responsible for ensuring the following occurs:

(i) Establishing a Global Privacy Committee as described in Article 13.2;

(ii) Establishing a global network of Privacy Officers;

(iii) Supervising compliance with this Policy;

(iv) Coordinating, communicating and consulting with the Privacy Officers network on central data protection issues;

(v) Providing annual privacy reports, as appropriate, to the Global Privacy Committee on data protection risks and compliance issues as described in Article 16.3;

(vi) Coordinating, in conjunction with the Privacy Officers network official investigations or inquiries into the Processing of Personal Data by a government authority;

(vii) Dealing with conflicts between this Policy and applicable law as described in Article 20.2;

(viii) Being available for consultation in relation to Transfers as described in Article 11.6;

(ix) 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 14.3;

(x) Informing Employee representatives on the Processing of Employee Data;

(xi) Monitoring the documentation, notification and communication of Data Security Incidents;

(xii) Deciding on complaints as described in Article 17; and

(xiii) Devising the data management processes, systems and tools to implement the framework for data protection management as established by the Global Privacy Committee, including:

(a) To maintain, update and publish this Policy 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 this Policy;

(d) Appropriate internal audit systems to monitor, audit and report compliance with this Policy and ensure that Arcadis' internal audit department can verify and certify such compliance in line with its annual audit process;

(e) Procedures regarding data protection inquiries, concerns and complaints; and

(f) Determine and update appropriate sanctions for violations of this Policy (e.g. disciplinary standards).

Global Privacy Committee

13.2. The Global Privacy Officer shall establish a Global Privacy Committee. The Global Privacy Committee shall create and maintain a framework for:

(i) the development, implementation and updating of local Personal data protection policies and procedures;

(ii) the maintaining, updating and publishing of this Policy and related sub-policies;

(iii) the creating, maintaining and updating of the records of processing activities (as required by Article 14);

(iv) the development, implementation and updating of the relevant data protection training and awareness programs;

(v) the monitoring, auditing and reporting on compliance with this Policy throughout Arcadis to the Executive Board of ANV;

(vi) the collecting, investigating and resolving privacy inquiries, concerns and complaints; and

(vii) determining and updating appropriate sanctions for violations

of this Policy (e.g., disciplinary standards).

Privacy Officers

13.3. Each Business Unit shall have a Privacy Officer who will report to the Global Privacy Officer. The Global Privacy Officer may, in consultation with the relevant Responsible Executive, direct the appointment of additional Privacy Officers as it deems necessary or appropriate. The Global Privacy Officer shall act as the Privacy Officer for ANV.

The Privacy Officers shall perform the following tasks within the scope of their appointment:

(i) Implement the data management processes, systems and tools, devised by the Global Privacy Officer to implement the framework for data protection management established by the Global Privacy Committee;

(ii) Support and assess overall data protection management compliance;

(iii) Regularly advise their Responsible Executive and the Global 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 consultation or advice as described in Article 7;

(vi) Provide information relevant to the annual privacy reports of the Global Privacy Officer (as required in Article 16);

(vii) Assist the Global Privacy Officer in the event of official investigations or inquiries by government authorities;

(viii) Own and authorize all appropriate privacy sub-policies;

(ix) Direct that stored data be deleted, destroyed, or anonymized as required by Article 5.2;

(x) Maintain a record of requests or complaints received under Articles 7.5 and 17.1;

(xi) Decide on and notify the Global Privacy Officer of complaints as described in Article 17; and

(xii) Cooperate with the Global Privacy Officer, other Privacy Officers, and the Global Privacy Committees to:

- Ensure that the instructions, tools and training are in place to enable compliance with this Policy;
- Share and provide guidance on best practices for data protection management;
- Ensure that data protection requirements are taken into account whenever new technology is implemented;
- Notify the Responsible Executive of the involvement of external service providers with data processing tasks within their area of responsibility.

Responsible Executive

13.4. The Responsible Executive is accountable that effective data protection management is implemented in their area of responsibility, is integrated into business practices, and that adequate resources and budget are available.

Responsible Executives are accountable for the following within their area of responsibility:

(i) Ensuring overall data protection management compliance, also during and following organisational restructuring, outsourcing, mergers and acquisitions and divestures;

(ii) Implementing the data management processes, systems and tools, devised by the Global Privacy Officer to implement the framework for data protection management established by the Global Privacy Committee;

(iii) Ensuring that the data protection management processes and systems are maintained up to date against changing circumstances and legal and regulatory requirements;

(iv) Ensuring and monitoring ongoing compliance of third parties with the requirements of this Policy in case Personal Data are disclosed by Arcadis 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 individuals follow the prescribed data protection training courses; and

(vi) Directing that stored data be deleted or destroyed, or anonymized as required by Article 5.2.

Responsible Executives are responsible for:

(i) Having appointed a Privacy Officer for their area of responsibility as directed by the Global Privacy Officer;

(ii) Consulting with the Global Privacy Officer in all cases where there is a conflict between applicable local law and this Policy as described in Article 20.2; and

(iii) Informing the Global Privacy Officer of any new legal requirement that may interfere with Arcadis' ability to comply with this Policy as required by Article 20.3.

Default Privacy Officer

13.5. If at any moment in time there is no Privacy Officer designated for a Business Unit, the Global Privacy Officer is responsible for supervising compliance with this Policy. The Global Privacy Officer may designate a Privacy Officer of another Business Unit (ad interim) until a new Privacy Officer has been appointed for the relevant Business Unit.

Article 14– Policies and Procedures

Policies and procedures

14.1. Arcadis shall develop and implement sub-policies and procedures to comply with this Policy.

Records of Processing Activities

14.2. Arcadis shall maintain in writing, including in electronic form, records of its Processing activities of Personal Data in compliance with EEA Data Protection Law, which records will include (i) name and contact details of the Group Company that is the Data Controller of Personal Data and, where applicable, the data protection officer, (ii) the Processing Purposes, (iii) a description of the categories of Personal Data and data subjects, (iv) information about categories of recipients and Transfers, (v) where possible, retention periods, and (vi) where possible, a general description of security measures.

Where an Arcadis Group Company acts as an internal Data Processor, the records of Processing Activities shall: (1) in addition include the name and contact details of the Arcadis Group Company that is the Data Processor, and (2) instead of (ii) – (iv) above, include the categories of Processing carried out on behalf of the Arcadis Group Company that is the Data Controller.

A copy of this information will be provided to the Competent SA upon request.

Data Protection Impact Assessment

14.3. Arcadis 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 Individuals, in particular where new technologies are used (**Data Protection Impact Assessment**). Where the Data Protection Impact Assessment shows that, despite mitigating measures taken by Arcadis, the Processing of Personal Data still presents a residual high risk for the rights and freedoms of Individuals, the Competent SA will be consulted prior to such Processing taking place.

Transfer Impact Assessment

14.4. The Arcadis Group Company that undertakes a Transfer under this Policy will perform a Transfer Impact Assessment prior to the Transfer to a Third Country and maintain it for the duration of the Transfer.

Where a Transfer Impact Assessment shows gap(s) in protection for Individuals under this Policy, Arcadis will implement supplementary measures, such as contractual, technical, or organizational safeguards, including measures applied during transmission and to the Processing of Personal Data in the country of destination to ensure compliance with the Policy. 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.

Transfers shall not take place or will be suspended where: (i) compliance with this Policy cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent SA.

Arcadis will conduct and document the Transfer Impact Assessment with the involvement of Arcadis International B.V. and the Global Privacy Officer and will notify the Data Exporter and Data Importer thereof. Arcadis International B.V. and the Global 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), and to any Competent SA upon request.

Article 15– Training

Staff training

15.1. Arcadis shall provide appropriate and up-to-date annual training on this Policy and related confidentiality obligations to Staff members who have access to Personal Data, who are involved in the collection of Personal Data or in the development of tools used to Process Personal Data.

Article 16– Monitoring and Auditing Compliance

Monitoring 16.1. Arcadis' management shall monitor compliance with this Policy as part of their regular business processes and procedures.

Audit 16.2. Arcadis Internal Audit shall audit business processes and procedures that involve the Processing of Personal Data for compliance with all aspects of this Policy, including methods of ensuring that corrective actions will take place. The audits shall be carried out annually in the course of the regular activities of Arcadis Internal Audit or at the request of the Global Privacy Officer. The Global Privacy Officer may request to have an audit as specified in this Article 16.2 conducted by an external accredited auditor. Applicable professional standards of independence, integrity and confidentiality shall be observed when conducting an audit. The Global Privacy Officer and the appropriate Privacy Officers shall be informed of the results of the audits. Reported violations of the Privacy Policies will be reported back to the Responsible Executive. A copy of the audit results will be provided to the Competent SA upon request.

Annual privacy report 16.3. The Global Privacy Officer shall implement appropriate processes to monitor compliance with this Policy and produce annual Personal Data privacy reports for the Executive Board on compliance with this Policy, data protection risks and other relevant issues.

Each Privacy Officer shall provide information relevant to the reports to the Global Privacy Officer.

Mitigation 16.4. Arcadis shall, if so indicated, ensure that adequate steps are taken to address breaches of this Policy identified during the monitoring or auditing of compliance pursuant to this Article 16.

SA audit or inspection 16.5. The Competent SA may request an audit or to carry out an inspection (including where necessary on-site) of the facilities used by Arcadis for the Processing of Personal Data for compliance with this Policy. Arcadis shall cooperate with the Competent SA in respect of such audit or inspection

Article 17– Complaints Procedure

Complaints 17.1. Customers, Suppliers and Business Partners may file a complaint regarding compliance with this Policy or violations of their rights under EEA Data Protection Law in accordance with the complaints procedure set forth in the relevant privacy policy or contract.

Employees may file such complaints:

(i) in accordance with the AGBP Issue Reporting and Handling Procedure; or

(ii) With the appropriate Privacy Officer.

Unless the complaint was filed directly with the appropriate Privacy Officer, the receiver of the complaint shall promptly forward the complaint to the appropriate Privacy Officer.

The appropriate Privacy Officer shall:

(a) notify the Global Privacy Officer;

(b) initiate an investigation; and

(c) when necessary, advise the business on the appropriate measures for compliance and monitor, through to completion, the steps designed to achieve compliance.

Reply to Individual

17.2. Arcadis will use reasonable efforts to resolve complaints without undue delay, and in any event within one month of the date that the complaint was filed. After receiving a complaint, the appropriate Privacy Officer shall inform the Individual in writing either (i) of Arcadis position with regard to the complaint and any action Arcadis has taken or will take in response or (ii) when they will be informed of Arcadis' position, which date shall be no later than two months thereafter, taking into account the complexity and number of requests. The appropriate Privacy Officer shall send a copy of the complaint and their written reply to the Global Privacy Officer.

Complaint to Global Privacy Officer

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

(i) the resolution of the complaint by the appropriate Privacy Officer is unsatisfactory to the Individual (e.g., the complaint is rejected);

(ii) the Individual has not received a response as required by Article 17.2;

(iii) the time period provided to the Individual pursuant to Article 17.2 is, in light of the relevant circumstances, unreasonably long and the Individual has objected but has not been provided with a shorter, more reasonable time period in which they will receive a response; or

(iv) in one of the events listed in Article 7.7.

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

An Individual may at all times file a complaint or claim with the SA or the competent court in accordance with Article 18.2, including if the handling of the complaint by the Global Privacy Officer is not satisfactory to the Individual (e.g., the request is denied).

Article 18– Legal Issues

Complaints procedure and Third Party Beneficiary Rights

18.1. Individuals are encouraged, but not required, to first follow the complaints procedure set forth in Article 17 of this Policy before filing any complaint or claim with the competent SAs or the courts. If Arcadis violates the Policy with respect to the Personal Data of an Individual covered by this Policy (**Affected Individual**), the Affected Individual can as a third party beneficiary enforce any claim as a result of a breach of the following elements in accordance with Article 18.2:

(i) Data protection principles (Articles 2, 3, 4, 5, 6, 8 and 11);

(ii) Transparency and easy access to this Policy (Articles 1.6 and 6)

(iii) Rights of access, rectification, erasure, restriction, objection to

processing, right not to be subject to decisions based solely on automated Processing, including profiling (Articles 7 and 10);

(iv) Obligations in case of local laws and practices affecting compliance with this Policy and in case of Disclosure Requests (Article 20 and 14.4);

(v) Right to complain through the internal complaint mechanism (Article 17);

(vi) Privacy by design and default (Article 5.5)

(vii) Cooperation duties with Supervisory Authorities (Article 16.5 and 18.3);

(viii) Liability and jurisdiction provisions, including this third-party beneficiary clause and the right to judicial remedies, redress and compensation (Article 18);

(ix) Duty to inform of updates to this Policy and the Group Companies (Article 21.1 and 21.3).

The rights contained in this Article 18.1 are in addition to, and shall not prejudice, any other rights or remedies that an Individual may otherwise have by law.

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

Local law and jurisdiction

18.2. This Policy provides for supplemental rights and remedies only, and nothing in this Policy will be construed to take away any rights or remedies under applicable local law.

In case an Individual has a claim under Article 18.1, the Individual may, at their choice, submit a complaint or a claim 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 Data Controller or the internal Data Processor of the relevant Personal Data is established, against the Group Company being the Data Controller or the internal Data Processor of the relevant Personal Data, or Arcadis International B.V.;

(ii) The SA in the EEA country where (a) the Individual has his/her habitual residence or place of work, or (b) the infringement took place, against the Group Company being the Data Controller or the internal Data Processor of the relevant Personal Data, or Arcadis International B.V.; or

(iii) The Lead SA or the courts in the Netherlands, against Arcadis International B.V.

Arcadis International B.V. accepts liability for a breach by a Group Company located outside the EEA, although Arcadis International B.V. may assert any defense that such Group Company or could have asserted.

The SAs and courts shall apply their own substantive and procedural laws to the dispute. Any choice made by the Individual will not prejudice the substantive or procedural rights they may have under EEA Data Protection Law.

Cooperation

18.3. Arcadis shall: (a) provide to the Competent SA, upon request,

with Competent SAs		information in relation to the Processing of Personal Data which is subject to this Policy; and (b) take into account the advice of, and abide by binding decisions of, the Competent SA, issued on the interpretation and application of this Policy. Any dispute related to the Competent SA's exercise of supervision of compliance with this Policy will be resolved by the courts of the Member State of that SA, in accordance with that Member State's procedural law.
Right to claim damages	18.4.	In case an Individual has a claim under Article 18.1, such Individual shall be entitled to compensation of material and non-material damages suffered by an Individual resulting from a violation of this Policy to the extent provided by applicable EEA law.
Burden of proof in respect of claim for damages	18.5.	To bring a claim for damages under Article 18.2, the Individual must demonstrate that they have suffered damages and establish facts which show it is likely that the damage has occurred because of a violation of the Policy. It will subsequently be for the relevant Group Company to prove that the damages suffered by the Individual due to a violation of the Policy are not attributable to Arcadis.
Mutual assistance and redress	18.6.	All Group Companies shall co-operate with and assist each other to the extent reasonably possible to handle: (i) a request, complaint or claim made by an Individual; or (ii) a lawful investigation or inquiry by a competent SA or public authority. The Group Company that receives a request, complaint or claim from an Individual is responsible for handling any communication with the Individual regarding their 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 the respective Group Company or Group Companies.
Mitigation	18.7.	Arcadis International B.V. shall ensure that necessary actions are taken to remedy violations of this Policy by a Group Company.

Article 19– Sanctions for Non-compliance

Non-compliance	19.1.	Non-compliance of Employees with this Policy may result in disciplinary action in accordance with applicable law up to and including termination of employment.

Article 20– Conflicts Between this Policy and Applicable Local Law

Conflict between Policy and law	20.1.	Each Data Importer shall monitor its local laws and practices and, if it becomes aware that it is or has become subject to laws or practices (including Disclosure Requests) that prevent it from complying with this Policy or that have a substantial effect on the protection offered by this Policy (including on any Data Protection Impact Assessments or Transfer Impact Assessments performed thereunder), the relevant Data Importer will promptly notify the relevant Data Exporter and Arcadis International B.V. The relevant Data Exporter and Arcadis

International B.V. shall, upon verification of the notification, promptly determine – in consultation with the Responsible Executive and the Global Privacy Officer – how to comply with this Policy and address the conflict, including by implementing appropriate supplementary measures in accordance with Article 14.4. The same applies if the Data Exporter has reasons to believe that the Data Importer can no longer fulfil its obligations under this Policy.

Laws and practices that respect the essence of the fundamental rights and freedoms, and do not exceed what is necessary and proportionate in a democratic society to protect one of the objectives listed in article 23(1) of the GDPR, are not considered to prevent Arcadis from complying with this Policy or to have a substantial effect on the protection offered by this Policy.

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 14.4.

Consequences of a Termination of a Transfer

20.2. The Data Importer shall – at the Data Exporter's option – immediately return or delete Personal Data that were received under this Policy in its entirety (including any copies thereof), and certify to the Data Exporter that it has done so, where: (i) the Transfer has been suspended for a period longer than one month, (ii) the Data Importer is in substantial or persistent breach of this Policy, (iii) the Data Importer fails to comply with a binding decision of a Competent SA or court, or (iv) the Data Importer ceases to be bound by this Policy. If local laws applicable to the Data Importer prevent the return or deletion of Personal Data, the Data Importer will only process the Personal Data to the extent and for as long as required under that local law. Until the Personal Data are deleted or returned, the Data Importer will continue to ensure compliance with the Policy to the extent possible.

Requests for disclosure of Personal Data

20.3. The Data Importer shall inform the affected Individual (where possible and, if necessary, with the help of the Data Exporter) and the Data Exporter, if it 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. In case of direct access to Personal Data by a public authority in the Destination Country, the notification will include all 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 SA.

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 applicable 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 for as long as the Personal Data are subject to the safeguards provided by this Policy and provided to any Competent SA upon request.

The Data Importer will provide the minimum amount of information permissible when responding to a Disclosure Request. In any event, any disclosures by the Data Importer of Personal Data 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 21– Changes to this Policy

Approval for changes	21.1.	Any changes to this Policy require the prior approval of the Global Privacy Officer and the Executive Board and shall thereafter be communicated by Arcadis International B.V. to the Group Companies. The Global Privacy Officer shall notify the relevant SAs via the Lead SA in advance of changes to this Policy that have a material impact on the protection offered by this Policy or the Policy itself (including a brief explanation justifying the change) and will be responsible for coordinating Arcadis' responses to questions of the relevant SAs submitted through the Lead SA in respect thereof. The Global Privacy Officer shall inform the appropriate Privacy Officers of the effect of such responses. Other non-material changes (if any), as well as any updates to the list of Group Companies subject to this Policy, will be notified by the Global Privacy Officer to the relevant SAs via the Lead SA on a yearly basis, including a brief explanation justifying the update. Local law including works council and other employees' representation regulations shall apply.
Individual's consent	21.2.	This Policy may be changed by Arcadis International B.V. without Individual's consent even though an amendment may relate to a benefit conferred on Individuals.
Effective date of changes	21.3.	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 Arcadis website and intranet.
Prior versions	21.4.	Any request, complaint or claim of an Individual involving this Policy shall be judged against the version of this Policy that is in force at the time the request, complaint or claim is made.

Article 22 – Transition Periods

General transition period	22.1.	During any transition period, any Transfer to a Group Company or Divested Entity located in a Third Country may only take place to the extent (i) such Group Company complies with this Policy, or (ii) the Transfer meets one of the grounds for Transfers listed in Articles 11.6 – 11.7.
Transition period for new Group Companies	22.2.	Any entity that becomes a Group Company after the Effective Date shall comply with this Policy within two years of becoming a Group Company.
Transition period for Divested Entities	22.3.	Arcadis may decide (and shall in such case ensure) that a Divested Entity (or specific parts thereof) will remain covered by this Policy for such period as is required by Arcadis to separate the Processing of Personal Data relating to such Divested Entity (e.g., until such time that the Personal Data are returned or deleted or the Divested Entity no longer has (remote) access). If local laws applicable to the Divested Entity prevent the return or deletion of Personal Data, the Divested Entity will only process the Personal Data to the extent and for as long as required under that local law. Until the Personal Data are deleted or returned, the Divested Entity will continue to ensure compliance with the Policy.
Contact details	22.4.	Arcadis Privacy Office c/o Arcadis International B.V. Gustav Mahlerplein 97-103 1082 MS Amsterdam The Netherlands

ANNEX 1 - Definitions

Adequacy Decision	ADEQUACY DECISION shall mean 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.
ANV	ANV shall mean Arcadis N.V., having its registered seat in Amsterdam and its business address at Gustav Mahlerplein 97-103, 1082MS Amsterdam.
Arcadis	ARCADIS shall mean ANV and its Group Companies.
Arcadis Data Controller	ARCADIS DATA CONTROLLER shall mean a Group Company that Processes Personal Data and determines the purposes and means of the Processing.
Article	ARTICLE shall mean an article in this Policy.
Business Contact Data	BUSINESS CONTACT DATA shall mean any data typically found on a business card and used by the Individual in their contact with Arcadis.
Business Partner	BUSINESS PARTNER shall mean any Third Party, other than a Client or Supplier, that has or had a business relationship or strategic alliance with Arcadis (e.g. joint marketing partner, joint venture or joint development partner).
Business Purpose	BUSINESS PURPOSE shall mean a purpose for Processing Personal Data as specified in Article 2 or 3 or for Processing Privacy Sensitive Data as specified in Article 4 or 3.
Business Unit	BUSINESS UNIT shall mean the Arcadis global businesses or a country.
Children	CHILDREN shall mean Individuals under the age of thirteen (13) years.
Client	CLIENT shall mean any Third Party that purchases, may purchase or has purchased an Arcadis project or service.
Client Services	CLIENT SERVICES shall mean the services provided by Arcadis to Clients to support Arcadis projects and services offered to or in use with their employees or clients. These services may include the maintenance, upgrade, replacement, inspection and related support activities aimed at facilitating continued and sustained use of Arcadis projects and services.
Competent SA or Competent Supervisory Authority	COMPETENT SA or COMPETENT SUPERVISORY AUTHORITY shall mean the Supervisory Authority in the EEA competent for the Data Exporter(s) of the specific Transfer.
CSB Data	CSB DATA shall mean the Personal Data of any (employee of or any person working for) Client, Supplier or Business Partner and any other Individual that Arcadis Processes in the context of the provision of its Client Services.
Data Exporter	DATA EXPORTER shall mean the Group Company that transfers Personal Data to a Third Country under this Policy.
Data Importer	DATA IMPORTER shall mean the Group Company in a Third Country that is the recipient of Personal Data.
Data Protection Impact Assessment (DPIA)	DATA PROTECTION IMPACT ASSESSMENT (DPIA) shall mean 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:

(i) a description of:

(a) the scope and context of the Processing;

(b) the Business Purposes for which Personal Data are Processed;

(c) the specific purposes for which Privacy Sensitive Data are Processed;

(d) categories of Personal Data recipients, including recipients not covered by an Adequacy Decision;

(e) Personal Data storage periods;

(ii) an assessment of:

(a) the necessity and proportionality of the Processing;

(b) the risks to the privacy rights of Individuals; 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 Personal Data.

Data Security Incident DATA SECURITY INCIDENT shall mean the unauthorized acquisition, access, use or disclosure of unencrypted Personal Data that compromises the security or privacy of such data to the extent the compromise poses a high risk of financial, reputational, or other harm to the Individual.

Dependent DEPENDENT shall mean the spouse, partner of child belonging to the household of the Employee or emergency contact of the Employee.

Destination Country DESTINATION COUNTRY shall mean the Third Country to which Personal Data are transferred.

Disclosure Request DISCLOSURE REQUEST shall mean a legally binding request for disclosure of (or direct access to) Personal Data from a public authority of a Destination 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 DIVESTED ENTITY shall mean the divestment by Arcadis of a Group Company or business by means of:

(a) a sale of shares as a result whereof the Group Company so divested no longer qualifies as a Group Company and/or

(b) a demerger, sale of assets, or any other manner or form.

EEA EEA or EUROPEAN ECONOMIC AREA shall mean all Member States of the European Union, plus Norway, Iceland, and Liechtenstein.

EEA Data Protection Law EEA DATA PROTECTION LAW shall mean 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.

Effective Date EFFECTIVE DATE shall mean the date on which this Policy becomes effective as set forth in Article 1.6.

Employee EMPLOYEE shall mean the following persons:

(a) employees, job applicants or former employees of Arcadis.

(b) temporary workers who are individuals engaged by Arcadis through a third-party agency whereby the third-party agency has the responsibility for salary, tax and social security obligations of the temporary worker. This term does not include Contingent

	Workers. (c) (former) executive or non-executive directors of Arcadis or (former) members of the supervisory board or similar body to Arcadis.
Employee Data	EMPLOYEE DATA shall mean any Personal Data of an Employee (and/or their Dependents).
Employment-at-will	EMPLOYMENT-AT-WILL means an employment relationship in which either the employer or employee can terminate the employment relationship at any time for any reason, with or without advance notice.
GDPR	GDPR shall mean the Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 of 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).
Global Privacy Committee	GLOBAL PRIVACY COMMITTEE shall mean the Global Privacy Committee as referred to in Article 13.2.
Global Privacy Officer	GLOBAL PRIVACY OFFICER shall mean the officer as referred to in Article 13.1.
Group Company	GROUP COMPANY shall mean ANV and any company or legal entity of which ANV 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 where the ARC Framework has been implemented by the management of such company or legal entity and it is included in the list of legal entities in Annex 3 of this Policy.
Head of Legal	HEAD OF LEGAL shall mean the General Counsel and Corporate Secretary of ANV.
Lead SA	LEAD SA shall mean the SA of the Netherlands, *Autoriteit Persoonsgegevens*.
Individual	INDIVIDUAL shall mean (as relevant) (i) an Employee, or (ii) any (employee of or any person working for) Client, Supplier or Business Partner and any other individual whose Personal Data Arcadis Processes in the context of the provision of its Client Services.
Internal Data Processor	INTERNAL DATA PROCESSOR shall mean a Group Company that Processes Personal Data on behalf of another Group Company being the Arcadis Data Controller.
Original Purpose	ORIGINAL PURPOSE shall mean the purpose for which Personal Data was originally collected.
Personal Data	PERSONAL DATA shall mean any information relating to an identified or identifiable Individual.
Policy	POLICY shall mean this Privacy Policy.
Privacy Officer	PRIVACY OFFICER shall mean the privacy officer as referred to in Article 13.3.
Privacy Sensitive Data	PRIVACY SENSITIVE DATA shall mean Personal Data that reveal an Individual's racial or ethnic origin, political opinions or membership in political parties or similar organizations, religious or philosophical beliefs, membership in a professional or trade organization or union, physical or

	mental health including any opinion thereof, disabilities, genetic code, biometric data for identification purposes, addictions, sex life, criminal offenses, criminal records, proceedings with regard to criminal or unlawful behavior, or social security numbers issued by the government.
Processing	PROCESSING shall mean any operation that is performed on Personal Data, whether or not by automated means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of Personal Data.
Responsible Executive	RESPONSIBLE EXECUTIVE shall mean each head of a Business Unit or the board of directors.
SA or Supervisory Authority	SA or SUPERVISORY AUTHORITY shall mean any supervisory authority of one of the countries in the EEA.
Secondary Purpose	SECONDARY PURPOSE shall mean any purpose other than the Original Purpose for which Personal Data are further Processed.
Staff	STAFF shall mean all Employees and other persons who Process Personal Data as part of their respective duties or responsibilities using Arcadis information technology systems or working primarily from Arcadis' premises.
Supplier	SUPPLIER shall mean any Third Party that provides goods or services to Arcadis (e.g. an agent, consultant, vendor or Contingent Worker).
Third Country	THIRD COUNTRY shall mean a country outside the EEA to which Personal Data are transferred, where such Transfer is not covered by an Adequacy Decision.
Third Party	THIRD PARTY shall mean any person, private organization or government body outside Arcadis.
Third Party Controller	THIRD PARTY CONTROLLER shall mean a Third Party that Processes Personal Data and determines the purposes and means of the Processing.
Third Party Processor	THIRD PARTY PROCESSOR shall mean a Third Party that Processes Personal Data on behalf of Arcadis that is not under the direct authority of Arcadis.
Transfer	TRANSFER shall mean a transfer (or set of transfers) of, including disclosure of, or remote access to, Personal Data that are subject to EEA Data Protection Law (or were subject to EEA Data Protection Law prior to their transfer outside the EEA) to a country outside the EEA.
Transfer Impact Assessment	TRANSFER IMPACT ASSESSMENT shall mean an assessment on whether there are any gap(s) in protection, i.e., whether, taking into account the specific circumstances of the Transfer, the laws and practices of the Destination Country, including those requiring the disclosure of Personal Data to public authorities or authorizing access by such authorities, prevent Arcadis from fulfilling its obligations under this Policy. Laws and practices that respect the essence of the 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, are understood not to be in contradiction with this Policy. In assessing the laws and practices of the Destination Country, Arcadis shall take into account in particular: (i) the specific circumstances of the Transfers, and any envisaged onward Transfers within the same Destination Country or to another Destination country, including:

- purposes for which data are transferred and Processed (e.g., marketing, HR, storage, IT support);
- types of entities involved in the Processing (the Data Importer and any further recipient of any onward Transfers);
- sector in which the Transfers occur;
- categories and format of the Personal Data transferred;
- location of the Processing including storage;
- transmission channels used.

(ii) the laws and practices of the Destination 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 Destination Country;

(iii) any relevant contractual, technical or organizational safeguards put into place to supplement the safeguards under this Policy, including measures applied during transmission and to the Processing of Personal Data in the Destination Country.

Interpretations

INTERPRETATION OF THIS POLICY:

(i) Unless the context requires otherwise, all references to a particular Article or Annex are references to that Article or Annex in or to this document, as they may be amended from time to time

(ii) headings are included for convenience only and are not to be used in construing any provision of this Policy

(iii) if a word or phrase is defined, its other grammatical forms have a corresponding meaning

(iv) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa and

(v) a reference to a document (including, without limitation, a reference to this Policy) is to the document as amended, varied, supplemented or replaced, except to the extent prohibited by this Policy or that other document and

(vi) a reference to law or legal obligation includes any regulatory requirement, sectorial recommendation, and best practice issued by relevant national and international supervisory authorities or other bodies.

ANNEX 2 - Description of Processing of Personal Data

As a global group of companies, Arcadis continuously transfers Personal Data between its various Group Companies. As such, Personal Data may be transferred between the various Group Companies for the purposes, and in relation to the categories of Personal Data, included in this **Annex 2**. A list of Arcadis Group Companies is available as Error! Reference source not found. to this Policy.

1. Categories of Employee Data

Category of Employee Data	Examples of Employee Data Elements
Basic personal details	Name, employee identification number, work contact details (email, phone numbers, physical address).
Other personal Details	Home contact details (email, phone numbers, physical address), language(s) spoken, gender, date of birth, national identification number, social security number, marital/civil partnership status, domestic partners, dependents, emergency contact information.
Documentation required under immigration laws	Citizenship, passport data, details of residency or work permit.
Compensation and payroll	Base salary, bonus, benefits, compensation type, salary step within assigned grade, details on stock appreciation rights and other awards, currency, pay frequency, effective date of current compensation, salary reviews, banking details, working time records (including vacation and other absence records, leave status, hours worked and department standard hours), pay data and termination date.
Position information	Description of current position, job title, corporate status, management category, job code, salary plan, pay grade or level, 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, date of transfers, and reporting manager(s) information.
Talent management information	Details contained in letters of application and resume/CV (previous employment background, education history, professional qualifications, language and other relevant skills, certification, certification expiration dates), details on performance management ratings, development programs planned and attended, e-learning programs, performance and development reviews, willingness to relocate, driver's license information, and information used to populate Employee biographies.
Management records	Details on directorships and appointments, board minutes, board decisions.
System and application access data	Information required to access company systems and applications such as user and system IDs for company network or servers, email account, instant messaging account, passwords, access logs, activity logs, and electronic content produced by individuals using company systems.
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, and absence due to illness or pregnancy.

Trade union membership	Information relating to Employees' trade union membership.
Criminal data	Information relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior.
Sexual preference	Information on sexual preference.
Biometric data	Data resulting from specific technical processing relating to the physical, physiological or behavioral characteristics of a natural person, which allow or confirm the unique identification of that natural person.

2. Categories of CSB Data

Category of Personal Data	Examples of Personal Data Elements
Basic Personal details	Name, organization, business addresses and telephone numbers, e-mail address, mobile telephone numbers.
Other Personal details	Home addresses and telephone numbers, date of birth, age, gender, region, profession, login and passwords, internal identification number.
Business communications	Information included in requests from, or correspondence with, a (prospective) Client, Supplier or Business Partner and online interactions with Arcadis.
Order information	Terms of contract, ordered or delivered products or services, order history, and other data generated during the performance of the agreement.
Payment and transaction information	(Outstanding) invoices, bank account number or credit card number, wire transfer details, payment history, information about transactions, billing and shipping information
Analytics information	Information about the use of and interactions with Arcadis' websites, apps, newsletter, and online advertisements or other services, including, IP address, device information, click and surf behavior, 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.
Security information	Security, authentication, fraud prevention, and risk-management related data.
Compliance information	Records related to Individuals' preferences (marketing preferences, consent documentation) and data subject rights requests.
Racial or ethnic data	Pictures and moving images of an Individual. In some countries photos and video images of Individuals qualify as racial or ethnic data.
Criminal data	Criminal data including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior.
Religious or philosophical beliefs	Information related to dietary requirements or religious holidays.

3. 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, pensions and savings plans, training, leave, managing sickness leave, promotions, transfers, secondments, honoring other contractual benefits, providing employment references, loans, performing workforce analysis and planning, performing Employee surveys, performing background checks, 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, to offer training opportunities and to identify patterns in the use of technology systems to information entrusted to Arcadis as well as to protect Arcadis's people and property.
Communications, 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.
Business Operations	Operating and managing the IT, communications systems and facilities, managing product and service development, improving products and services, managing company assets, allocating company assets and human resources, strategic planning, project management, business continuity, compilation of audit trails and other reporting tools, maintaining records relating to business activities, budgeting, financial management and reporting, communications, managing mergers, acquisitions, sales, re-organizations or disposals and integration with upon mergers or acquisitions.
Monitoring	Monitoring compliance with Arcadis internal policies and procedures, including pursuant to Arcadis's policies and procedures with regard to monitoring of telephone, email, Internet and other company resources, and other monitoring activities as permitted by applicable law.

4. Purposes for which CSB Data are Processed

Purpose of Processing	Examples of Processing Activities
Assessment and acceptance of a Client, Supplier or Business Partner, conclusion and execution of agreements with Clients, Suppliers and Business Partners	Processing of Personal Data that are necessary in connection with the assessment and acceptance of Clients, including confirming and verifying the identity of relevant Individuals (this may involve the use of a credit reference agency or other Third Parties) and conducting due diligence, screening against publicly available government and/or law enforcement agency sanctions lists. This activity also includes the Processing of Personal Data necessary to conclude and execute agreements with Clients, Suppliers and Business Partners, including required screening activities (e.g. for access to Arcadis' premises or systems), delivery of Client Services, and to record and financially settle delivered services, projects and materials to and from Arcadis.
Development and improvement of projects and/or	Processing of Personal Data that is necessary for the development and improvement of Arcadis projects and/or services, research and development.

services	
Relationship management and marketing	Activities such as maintaining and promoting contact with Clients, Suppliers and Business Partners, account management, client service, recalls and the development, execution and analysis of market surveys and marketing strategies.
Business process execution, internal management and management reporting	Such as the management of company assets, conducting audits and investigations; finance and accounting; implementing business controls, provision of central processing facilities for efficiency purposes; Processing Personal Data for management reporting and analysis, creating business insights, archive and insurance purposes, legal or business consulting, and preventing, preparing for or engaging in dispute resolution.
Organizational analysis and development, management reporting, and acquisitions and divestures	Aggregating or anonymizing Personal Data to prepare and perform management reporting and analysis, conducting Client, Supplier and Business Partner surveys, processing Personal Data in the context of mergers, acquisitions and divestitures and in order to manage such transactions.
Health, safety, security and integrity	Such as the protection of the interests of Arcadis and its Employees, Clients, Suppliers and Business Partners and activities such as those involving safety and health, the protection of Arcadis and Employee assets, and the authentication of Client, Supplier or Business Partner status and access rights.
Compliance with law	Processing of Personal Data necessary for the performance of a task carried out to comply with a legal obligation to which Arcadis is subject, including the disclosure of Personal Data to government institutions or supervisory authorities in relation thereto.
Protection of the vital interests of Individuals	Where Processing is necessary to protect the vital interests of an Individual.

5. Purposes for which Privacy 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 racial or ethnic data. Arcadis may process photos (e.g., a copy of a passport containing a photo) and video images: (i) for the protection of the interests and assets of Arcadis, its Employees, joint ventures, participations, Clients, Suppliers and Business Partners (including safeguarding the integrity of Arcadis, pre- and in-employment screening and monitoring of Employees); (ii) for site access and security reasons, assessment and acceptance of Clients, including the identification and authentication of Clients (including confirming and verifying the identity of relevant Individuals), Supplier or Business Partner status and access rights, (iii) to verify and confirm advice or record decisions made in the course of business for future reference (e.g., when Individuals participate in video conferencing which is recorded); (iv) for obtaining visas, permits and technology export licenses; and (v) for inclusion in Employee directories.
Protecting health, safety, security and ensuring integrity	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 Arcadis, its Employees, joint ventures, participations and Clients, Suppliers and Business Partners with respect to criminal offences that have been or, given the relevant circumstances are suspected to be or have been, committed against Arcadis, its Employees, joint ventures, participations and Clients, Suppliers and

Purpose of Processing	Examples of Processing Activities
	Business Partners, and further for pre- and in-employment screening and monitoring of Employees.
Accommodation	Religious or philosophical beliefs may be Processed: (i) to accommodate specific projects or services for a Client; or (ii) insofar as necessary for accommodating religious or philosophical practices, dietary requirements or religious holidays.
Employee Data only	
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 Privacy 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.
Communications or marketing	Enabling Employees to voluntarily join video or photo shoots used for Arcadis communications and promotional marketing materials.
Health services	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.
Affinity groups	Administering Employee affinity groups.
Administering pensions and benefits	Administering pensions, health and welfare benefit plans, maternity, paternity or family leave programmes, or collective agreements (or similar arrangements) that create rights depending on the state of health of the Employee, or the payment of trade union membership.
Preferential status based on health status	Providing preferential status to persons with a particular disability to remove or reduce inequality or to ensure diversity in staffing, provided that use of the relevant Privacy Sensitive Data allows for an objective determination that an Employee belongs to the relevant category and the Employee has not filed a written objection against the relevant Processing.
Re-integration and support	Reintegrating or providing support for Employees entitled to benefits in connection with illness or work incapacity.
Pre- and in-employment screening	Pre- and in-employment screening and monitoring of Employees and for assessing and making decisions on (continued) eligibility for positions, projects or scope of responsibilities.
Facility management	Providing facilities in the workplace to accommodate health problems or disabilities.
Background checks	Assessing an application by an Employee to make a decision about the Employee or provide a service to the Employee.
Administering Employee pensions, benefits, and memberships	Processing data on sexual preference (including data relating to partners of Employees) for the purpose of administering Employee pensions, benefits programs, and memberships.
CSB Data only	
Client, Supplier, Business Partner assessment and acceptance	Criminal data (including data relating to criminal behavior, criminal records or proceedings regarding criminal or unlawful behavior) may be Processed as necessary for assessment and acceptance of Clients, including the identification and authentication of Clients (including confirming and verifying the identity of relevant Individuals), the execution of an agreement with Clients, and to protect the interests of Arcadis, its

Purpose of Processing	Examples of Processing Activities
	Employees and Clients.