Binding Corporate Rules – Processor Policy

Introduction

In its Arcadis Risk & Control Framework ("**ARC Framework"**) Arcadis N.V. and its group companies ("**Arcadis"**) has committed itself to the protection of personal data it processes.

This Privacy Policy for Processing Personal Data of Client Individuals ("**Processor Policy"**) indicates how this principle shall be implemented in respect of processing of personal data by Arcadis on behalf of Arcadis' clients. This Processor 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.

For the privacy rules applicable to the processing of personal data by Arcadis in its role as a data controller, refer to the Privacy Policy for Employee Data and Client, Supplier and Business Partner Data.

Capitalized terms have the meaning set out in Annex 1 (Definitions).

ARTICLE 1
– SCOPE, APPLICABILITY AND IMPLEMENTATION

Scope Arcadis as Data Processor	1.1	This Processor Policy applies to the worldwide processing of CI Information by Arcadis in its role as a Data Processor in the course of delivering Client Services, where such CI Information is: (a) subject to EEA Data Transfer Restrictions, or was subject to EEA Data Transfer Restrictions prior to the Transfer of such CI Information to a Group Company in a Third Country; and (b) is Processed by Arcadis in a Third Country pursuant to a Services Contract that specifically provides that this Processor Policy shall apply to such CI Information. The Processor Policy covers all types of CI Information that Arcadis processes in the context of its business activities as a Data Processor.
Electronic and paper-based Processing	1.2	This Processor Policy applies to the Processing by Arcadis by electronic means and in any systematically accessible paper-based filing systems.
Applicability of local law and this Processor Policy	1.3	Client Individuals keep any rights and remedies they may have under applicable local law. This Processor Policy shall apply only where it provides supplemental protection for CI Information. Where applicable local law provides more protection than this Processor Policy, local law shall apply in addition to this Policy. Where this Processor Policy

provides more protection than applicable local law or provides additional safeguards, rights or remedies for Client Individuals, this Processor Policy shall apply in addition to applicable local law. Article 13.1 applies to conflicts between applicable local law and this Processor Policy.

Sub-policies and procedures 1.4 Arcadis may supplement this Processor Policy through sub-policies and procedures that are consistent with this Processor Policy.

Accountability 1.5 This Processor Policy is legally binding and shall apply to and be enforced by Arcadis, including its Employees. The Responsible Executive is accountable for his/her business organization's compliance with this Processor Policy. Arcadis Staff must comply with this Processor Policy.

Effective Date 1.6 This Processor Policy has been adopted by the Executive Board of ANV and has entered into force as of 2 March 2026 ("**Effective Date**").

Processor Policy supersedes prior policies 1.7 This Processor Policy supersedes all Arcadis privacy processes and procedures 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 Processor Policy. These responsibilities include the oversight, coordination and implementation of this Processor Policy on a global basis and further accepting liability for breaches of this Processor Policy by Group Companies outside of the EEA as described more fully in Article 11 of this Processor Policy.

Privacy Officer advice 1.9 Where there is a question as to the applicability of this Processor Policy, Staff shall seek the advice of the appropriate Privacy Officer prior to the relevant Processing.

ARTICLE 2 – SERVICES CONTRACT

Services Contract 2.1 Arcadis shall Process CI Information only on the basis of a validly entered into written or electronic Services Contract which complies with Data Protection Law.

The Arcadis Contracting Entity may use Sub-Processors, both Arcadis Sub-Processors and Third Party Sub-Processors, in the regular performance of Services Contracts. The standard Services Contract

shall authorize the use of such Sub-Processors, provided that the Arcadis Contracting Entity remains liable to the Client for the performance of the contract by the Sub-Processors in accordance with the terms of the Services Contract. The provisions of Article 7 shall further govern the use of Third Party Sub-Processors.

Termination of Services Contract

2.2 Upon termination of the Services Contract, Arcadis shall fulfill its obligations with regard to return of CI Information as set forth in the Services Contract. When Arcadis's obligations under the Services Contract have been fulfilled, Arcadis shall (i) delete or otherwise render unrecoverable such CI Information as set forth in the Services Contract, unless the Services Contract or applicable law provides otherwise, and (ii) (upon request of the Client) confirm to Client that Arcadis has done so. In case the Services Contract or applicable law provides that CI Information shall not be deleted or rendered unrecoverable, Arcadis shall no longer Process the CI Information, unless specified otherwise by the Services Contract or as required by applicable law.

Audit of termination measures

2.3 Upon termination of the Services Contract, Arcadis shall, at the request of the Client, allow its Processing facilities to be audited in accordance with Article 10.1, 10.2 and 10.3 (as applicable) to verify that Arcadis has complied with its termination-related obligations under Article 2.2.

ARTICLE 3 – COMPLIANCE OBLIGATIONS OF ARCADIS

Instructions of the Data Controller

3.1 Each Group Company, including their Employees, shall Process CI Information only (i) on behalf of the Client and in accordance with any documented instructions received from the Client (including with regards to data transfers to a country outside the EEA), which instructions shall be consistent with the terms of the Services Contract, or (ii) as needed to comply with applicable law (subject to Article 13.1). Arcadis shall immediately inform the Client if in its opinion, an instruction infringes Data Protection Law.

Compliance with Applicable Data Processor and Data Controller Law

3.2 Arcadis shall Process CI Information in accordance with this Code and shall deal promptly and appropriately with requests for assistance of the Client as reasonably required and possible to enable the Client's compliance with the Applicable Data Controller Law in accordance with the Services Contract.

Request for disclosure of CI

3.3 The Data Importer shall inform the affected Client Individual (where possible and, if necessary, with the help of the Data Exporter or Client)

Information

and the Data Exporter if it becomes aware that any applicable local law of a Third Country is likely to prevent Data Importer from fulfilling the instructions of the Client, or its obligations under this Processor Policy or the Services Contract, including if it receives a Disclosure Request. Notifications of a Disclosure Request shall include information about the CI Information requested, the requesting authority, the legal basis for the disclosure and the provided response. In case of direct access to CI Information by a public authority in the Destination Country, the notification will include all information available to the Data Importer. The Data Exporter shall forward the notification to the Client.

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 CI Information requested until required to do so under the applicable procedural rules and will only provide the CI Information 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. The Data Exporter shall forward the assessment to the Client.

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 CI Information requested, requesting authority, whether requests have been challenged and the outcome of such challenges). This information will be preserved for as long as the CI Information is subject to the safeguards provided by this Policy and provided to any Competent SA upon request. The Data Exporter shall forward the information to the Client.

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 CI Information 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.

Inquiries of the Client

3.4 Arcadis shall deal promptly and appropriately with inquiries of the Client related to the Processing by Arcadis pursuant to the terms of the Services Contract.

ARTICLE 4 – PROCESSOR PURPOSES

Legitimate business purposes

4.1 As a Data Processor, Arcadis may Process CI Information only for providing the following Client Services or as otherwise instructed by Client in accordance with Article 3.1:

(a) Design, Consultancy and Engineering Services

(b) Business Advisory and Strategic Environmental Consultancy Services

(c) Program, Project and Cost Commercial Management Services

(d) Environmental Restoration Services

(e) Asset Management Services.

(f) Construction with procurement and validation services

(g) Digital services including granting software licences and support and maintenance services in respect of Arcadis' digital offerings

The Client Services may include the following processing activities:

(a) **Client data management information technology services** including:

(i) Hosting, storage, backup, or archiving and providing digital software solutions, e.g. for infrastructure;

(ii) Reporting on the use of Client Services by customers of the Client;

(iii) Security maintenance (e.g., implementing access controls, auditing use, managing servers, managing network security, managing incidents, pro-active management for security);

(iv) Account management of third-party use of Client-specific Arcadis products or services (e.g., use reporting and billing of customers of a Client on behalf of the Client).

(b) **Client support services** including:

(i) Providing (local and remote) assistance to a Client in relation

to the use or repair of Arcadis services or products;

(ii) Generation of service level reports or other reports on the use by a Client of Arcadis services or products for Client information management purposes; or

(iii) Life-cycle management of Arcadis services or products (e.g., planning, evaluation, demonstration, installation, calibration, training, maintenance, decommissioning) to facilitate continued and sustained use by a Client of Arcadis services or products.

(c) **Client-specific services** including:

(i) Device or system tuning for the purpose of adjusting the service or product to meet the specifications of a Client (e.g., by engaging application specialists, undertaking project management activities, modifying of device or system);

(ii) Stakeholder management in respect of any of the purposes listed under (i) – (v) of this Article 4.1, including collecting and processing stakeholder feedback through Arcadis managed (online) platforms;

(iii) Analytics services, e.g. analysis and use of data collected in respect of the use of assets of a Client, e.g. tunnels, airports or railways, or CCTV cameras footage and data from other sources to assist the Client in monitoring and managing crowd flows, to report trends, such as specific status reports, management reporting and the general improvement of the internal or external operations of a Client);

(iv) Assistance of the Client in rights management (such as managing and evaluating claims and supporting documents as instructed by Client, e.g., stakeholder management);

(v) The purchase of services or products on behalf of a Client (e.g., contract broadband network service for device placement and data acquisition, third-party hardware integration); or

(vi) The provision of training for staff of the Client or third parties (e.g., equipment training).

(d) **Arcadis internal business process execution and management** leading to incidental Processing for:

(i) Internal auditing of Arcadis Processor-related activities;

(ii) Activities related to compliance with applicable law or regulation (e.g., Data Processor Law);

(iii) Data de-identification and aggregation of de-identified data for

data minimization; and

(iv) Use of de-identified, aggregate data to facilitate continuity, sustainability, and improvement of Arcadis services or products.

ARTICLE 5
SECURITY AND CONFIDENTIALITY REQUIREMENTS

Information Security

5.1 Arcadis shall, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of Processing as well as the risk of varying likelihood and severity for the rights and freedoms of Client Individuals, take appropriate technical, physical and organizational measures to protect CI Information from misuse or accidental, unlawful or unauthorized destruction, loss, alteration, disclosure, acquisition or access during the Processing (including Transfer). Arcadis shall in any event take the measures specified in **Annex 2** of this Processor Policy, which Annex may be revised by Arcadis, provided that such changes do not in any material manner diminish the level of security provided to CI Information under **Annex 2**.

Data access and confidentiality

5.2 Arcadis shall provide Arcadis Staff access to CI Information only to the extent necessary to perform the Processing and to perform their job. Arcadis shall impose confidentiality obligations on Staff with access to CI Information.

Data Security Incident notification requirement

5.3 Arcadis shall notify the Client of a Data Security Incident without undue delay after becoming aware that a Data Security Incident has occurred.

ARTICLE 6
– TRANSPARENCY TO CLIENT INDIVIDUALS

Other requests of Client Individuals

6.1 Arcadis shall promptly notify the Client of requests or complaints that are received directly from a Client Individual regarding the Processing without responding to such requests or complaints, unless otherwise instructed by the Client in the Services Contract.

If Arcadis is generally instructed by the Client in the Services Contract to respond to requests and complaints of Client Individuals, Arcadis shall ensure that all information will be made available to Client Individuals that is reasonably required for the Client Individual to be

able to effectively make a request or lodge a complaint (including about the point of contact and procedure).

If the Client has disappeared factually or has ceased to exist in law or became insolvent, Arcadis will handle the Client Individual's request or complaint.

Arcadis will handle claims and complaints in accordance with Article 11.2.

ARTICLE 7 – THIRD PARTY SUB-PROCESSORS

Third Party Sub-Processor contracts

7.1 Third Party Sub-Processors may Process CI Information only if the Third Party Sub-Processor has a binding contract with Arcadis. The contract shall impose data protection-related Processing terms on the Third Party Sub-Processor that will be no less protective than those imposed on the Arcadis Contracting Entity by the Services Contract and this Processor Policy.

Overview of Third Party Sub-Processors

7.2 Arcadis shall maintain a list of the Third Party Sub-Processors involved in the performance of the relevant Client Services. This overview shall be made available in the Services Contract and upon request, and it shall be promptly updated in case of changes.

Notification new Third Party Sub-Processors and right to object

7.3 Arcadis shall provide notice to the Client of any new Third Party Sub-Processors engaged by Arcadis for the delivery of the Client Services. Within fourteen days of receiving such notice, the Client may object to the involvement of such Third Party Sub-Processor in the delivery of the Client Services by providing objective justifiable grounds related to the ability of such Third Party Sub-Processor to protect CI Information or comply with applicable data protection or security requirements. In the event the objection is not unreasonable, Arcadis and the Client will work together in good faith to find a solution to address such objection, including but not limited to reviewing additional documentation supporting the Third Party Sub-Processors' compliance or making the Client Services available without the involvement of such Third Party Sub-Processor. To the extent the parties cannot reach a mutually acceptable solution, both parties shall have the right to terminate the relevant Client Services (i) in accordance with the terms of the Services Contract; (ii) without either party incurring any liability towards the other; and (iii) without relieving the Client from its payment obligations under the Services Contract up to the date of termination.

Onward

7.4 Arcadis may Transfer CI Information to a Third Party Sub-Processor

Transfers

located in a Third Country:

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

(b) if item (a) does not apply, the Transfer is subject to a derogation for specific situations under Data Protection Law (i.e., the Processing is necessary for the conclusion or performance of a contract with or in the interest of the Client Individual or the implementation of pre-contractual measures taken at the Client Individual's request, to protect a vital interest of an individual, for the establishment, exercise, or defence of a legal claim, or for important reasons of public interest (as recognized by the EEA law to which the Data Exporter is subject), or the Client Individual has given explicit consent to the Transfer).

Prior to a Transfer under (a), Arcadis will conduct a Transfer Impact Assessment in accordance with Article 9.3.

ARTICLE 8 – PRIVACY GOVERNANCE

Global Privacy Officer

8.1 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 Processor Policy. Where required under Data Protection Law, Arcadis will appoint a data protection officer ("**DPO**") who shall have the tasks and responsibilities in accordance with 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:

(a) Establishing a Global Privacy Committee as described in Article 8.2;

(b) Establishing a global network of Privacy Officers;

(c) Supervising compliance with this Processor Policy;

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

(e) Providing annual privacy reports, as appropriate, to the Global Privacy Committee on data protection risks and compliance issues as described in Article 10.4;

(f) Coordinating, in conjunction with the Privacy Officers network, official investigations or inquiries into the Processing by a

government authority;

(g) Dealing with conflicts between this Processor Policy and Applicable Data Processor Law as described in Article 13.1;

(h) Approving changes to this Processor Policy as required under Article 14.1;

(i) Monitoring the documentation, notification and communication of Data Security Incidents as described in Article 5.3;

(j) Deciding on complaints as described in Article 11.2;

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

(i) To maintain, update and publish this Policy and related sub-policies;

(ii) Tools to collect, maintain and update information regarding the structure and functioning of all systems that process CI Information;

(iii) Data privacy training and awareness for Staff to comply with their responsibilities under this Policy;

(iv) 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;

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

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

Global Privacy Committee

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

(a) The development, implementation and updating of local data protection policies and procedures;

(b) The maintaining, updating and publishing of this Processor Policy and related sub-policies;

(c) The creating, maintaining and updating of the records of processing activities (as required by Article 9.2);

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

(e) The monitoring, auditing and reporting on compliance with this

Processor Policy throughout Arcadis to the Executive Board of ANV;

(f) The collecting, investigating and resolving privacy inquiries, concerns and complaints; and

(g) Determining and updating appropriate sanctions for violations of this Processor Policy (e.g., disciplinary standards).

Privacy Officers

8.3 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:

(a) 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;

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

(c) Regularly advise their Responsible Executive and the Global Privacy Officer on privacy risks and compliance issues;

(d) Maintain (or ensure access to) an inventory of the system information about the structure and functioning of all systems that process CI Information (as required by Article 9.2);

(e) Be available for consultation or advice;

(f) Provide information relevant to the annual privacy report of the Global Privacy Officer (as required in Article 10.4)

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

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

(i) Direct that stored CI Information is returned or securely deleted after termination of the Services Contract (as required by Article 2.2);

(j) Decide on and notify the Global Privacy Officer of complaints as described in Article 11.2;

(k) Cooperating with the Global Privacy Officer, other Privacy Officers and the Global Privacy Committee to:

(i) Ensure that the instructions, tools and training are in place to

enable compliance with this Policy;

(ii) Share and provide guidance on best practices for data protection management;

(iii) Ensure that data protection requirements are taken into account whenever new technology is implemented.

Responsible Executive

8.4 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:

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

(b) 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;

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

(d) Ensuring and monitoring ongoing compliance of third parties with the requirements of this Processor Policy in case CI Information is disclosed by Arcadis to a Third Party (including entering into a written contract with such Third Party and obtaining advice on such contract from the legal department);

(e) Ensuring that relevant individuals follow the prescribed data protection training courses; and

(f) Directing that CI Information is returned or securely deleted after termination of the Services Contract (as required by Article 2.2);

Responsible Exectives are responsible for:

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

(h) consulting with the Global Privacy Officer in all cases where there is a conflict between Applicable Data Processor Law and this Processor Policy as decribed in Article 13.1;

(i) informing the Global Privacy Officer of the involvement of Third Party Sub-Processors with data processing tasks for their Region;

and

(j) informing the Global Privacy Officer of any new legal requirement that may interfere with Arcadis' ability to comply with this Processor Policy as required by Article 13.1.

Default Privacy Officer

8.5 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 9 – POLICIES, PROCEDURES AND TRAINING

Sub-policies and procedures

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

Records of Processing Activity

9.2 Arcadis shall maintain in writing, including in electronic form, records of its Processing activities of CI Information Processed on behalf of Clients in compliance with Data Protection Law, which records will include (i) name and contact details of the relevant Group Companies acting as a Data Processor, where applicable, the data protection officer, and the Client on whose behalf Arcadis Processes CI Information, (ii) the categories of Processing, (iii) where applicable, information about Transfers of CI Information to Third Countries, and (iv) where possible, a general description of security measures. A copy of this information relating to CI Information will be provided to the Competent SA upon request.

Transfer Impact Assessment

9.3 The Group Company that undertakes a Transfer under this Processor 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 Client Individuals under this Processor Policy, Arcadis will implement supplementary measures, such as contractual, technical, or organizational safeguards, including measures applied during transmission and to the Processing of CI Information in the country of destination to ensure compliance with the Processor 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 Processor Policy cannot be assured, (ii) no appropriate supplementary measures can be taken, or (iii) so instructed by any Competent SA or the Client.

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 or Client upon request.

Staff training

9.4 Arcadis shall provide appropriate and up-to-date annual training on the obligations and principles laid down in this Processor Policy and related confidentiality and other privacy and data security obligations to Staff who have access to CI Information or who are involved in the collection of CI Information or in the development of tools used to Process CI Information.

ARTICLE 10 – MONITORING AND AUDITING COMPLIANCE

Internal audits

10.1 Arcadis Internal Audit shall audit business processes and procedures that involve the Processing of CI Information for compliance with all aspects of this Processor 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 10.1 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. Any violations of this Processor Policy identified in the audit report will be reported to the Responsible Executive. A copy of the audit results related to compliance with this Processor Policy will be provided upon request to the Competent SA.

Client audit

10.2 Arcadis shall, at its option, either

(a) Make available the facilities it uses for the Processing for an audit

by a qualified independent third party auditor selected by the Client, provided such auditor is (i) reasonably acceptable to Arcadis and (ii) has executed a written confidentiality agreement reasonably acceptable to Arcadis before conducting the audit. In accordance with the audit provisions of the applicable Services Contract, audits shall be conducted no more than once per year per Client and during regular business hours, and shall be subject to (I) a written request submitted to Arcadis at least six weeks in advance of the proposed audit date, (II) a detailed written audit plan reviewed and approved by Arcadis's security organization and (III) Arcadis's on-site security policies. In case of a reasoned and duly substantiated urgent need, for example, a demonstrable violation of this Processor Policy that leads to a material risk to CI Information (an "**Urgent Audit**"), the Client may submit a written request no less than one week in advance of the proposed audit date. Arcadis will reasonably consider and accommodate Urgent Audits. Upon completion of an audit, the Client shall provide Arcadis with a copy of the audit report, which shall be treated as confidential information pursuant to the terms of the Services Contract; or

(b) Provide to the Client a statement issued by a qualified independent third party assessor certifying that the Arcadis business processes and procedures that involve the Processing comply with the principles set forth in this Processor Policy.

SA audit or inspection

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

Annual privacy report

10.4 The Global Privacy Officer shall implement appropriate processes to monitor compliance with this Processor Policy and produce an annual CI Information privacy report for the Executive Board on compliance with this Processor Policy, data protection risks and other relevant issues.

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

Mitigation

10.5 Arcadis shall, if so indicated, ensure that adequate steps are taken to remedy breaches of this Processor Policy identified during the monitoring or auditing of compliance pursuant to this Article 10.5.

Data Accuracy 10.6 The Arcadis Group Company that is the Data Importer shall inform the Data Exporter without undue delay if it becomes aware that the CI Information it has received is or has become inaccurate. The Data Importer shall cooperate with the Data Exporter to rectify or erase the relevant CI Information.

ARTICLE 11 – LEGAL ISSUES

Rights of Client Individuals 11.1 Client Individuals are encouraged, but not required, to first follow the complaints procedure set forth in Article 11.2 of this Processor Policy before filing any complaint or claim with the competent SAs or the courts in accordance with Article 11.3. If Arcadis violates the Processor Policy with respect to the CI Information of a Client Individual covered by this Processor Policy ("**Affected Individual**"), the Affected Individual can as a third party beneficiary enforce any claim as a result of a breach of:

(a) Duty to respect the instructions from the Client (Article 2.1, 2.2, 3.1 and 4.1);

(b) Duty to implement appropriate technical and organizational security measures and to notify Data Security Incidents to the Client (Article 5);

(c) Duty to respect the conditions when engaging a Sub-Processor (Article 2.1 and 7);

(d) Duty to cooperate with and assist the Client in complying and demonstrating compliance with Applicable Data Controller Law (Articles 3.2, 3.4, 6.1, 9.2 and 10.2);

(e) Easy access to the Processor Policy (Article 1.6 and 14.2);

(f) Right to complain through internal complaint mechanisms (Article 11.2);

(g) Duty to cooperate with the Competent SA (Articles 10.3, 11.6 and 11.7);

(h) Liability, compensation and jurisdiction provisions (Articles 11.1, 11.3 and 11.4); and

(i) National legislation preventing respect of the Processor Policy (Article 3.3, 9.3 and 13).

Complaints Procedure 11.2 Affected Individuals may file a written complaint in respect of any claim they have under Article 11.1 or violations of their rights under Data

Protection Law with the Privacy Officer. Affected Individuals may also file a complaint or claim with the authorities or the courts in accordance with Article 11.3.

The appropriate Privacy Officer shall:

(a) notify the Global Privacy Officer;

(b) initiate an investigation;

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

(d) maintain records of complaints received, responses given and remedial actions taken.

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 Affected 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, taking into account the complexity and number of the requests, be no later than two months thereafter. The appropriate Privacy Officer shall send a copy of the complaint and their written reply to the Global Privacy Officer.

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

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

(b) the Affected Individual has not received a response as required by this Article 11.2; or

(c) the time period provided to the Affected Individual pursuant to this Article 11.2 is, in light of the relevant circumstances, unreasonably long and the Affected Individual has objected but has not been provided with a shorter, more reasonable time period in which they will receive a response.

The procedure described above shall also apply to complaints filed with the Global Privacy Officer.

An Affected Individual may at all times file a complaint or claim with the SA or the competent court in accordance with Article 11.3, including if the handling of the complaint by the Global Privacy Officer is not satisfactory to the Affected Individual (e.g., the request is denied).

Jurisdiction for claims of Client Individuals

11.3 In case an Affected Individual has a claim under Article 11.1, the Affected Individual may, at their choice, submit a complaint or claim to the following SAs or the courts (as applicable):

(a) The courts in the EEA country (a) where the Affected Individual has his or her habitual residence, or (b) where the Arcadis Contracting Entity is established, against the Arcadis Contracting Entity, or Arcadis International B.V.;

(b) The SA in the EEA country where (a) the Affected Individual has his/her habitual residence or place of work, or (b) the infringement took place, against the Arcadis Contracting Entity, or Arcadis International B.V.; or

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

Arcadis may not avoid liability as a result of a breach by a Sub-Processor of its obligations, although Arcadis may assert any defense that such Sub-Processor could have asserted.

Arcadis may assert any defenses or rights that would have been available to the Client. Notwithstanding Article 11.4, Arcadis also may assert any defenses that Arcadis could have asserted against the Client (such as contributory negligence), in defending against the Affected Individual's claim.

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

Affected Individuals may be represented by a not-for-profit body, organization, or association in accordance with article 80(1) GDPR.

Right to Claim damages, reversal of burden of proof

11.4 In case an Affected Individual has a claim under Article 11.1, such Affected Individual shall be entitled to compensation of material and non-material damages suffered by the Affected Individual resulting from a violation of this Processor Policy in accordance with article 82(2) GDPR ("**Claim for Damages"**).

To bring a Claim for Damages, the Affected 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 this Processor Policy. It will subsequently be for the Arcadis Contracting Entity or Arcadis International B.V. to prove that the damages suffered by the Affected Individual due to a violation of this Processor Policy are not attributable to a Group Company or a Sub-Processor or to assert other applicable defenses.

To the extent the Claim for Damages concerns a Processing which involves both the Client and Arcadis and both are found responsible for the damage caused by such Processing in accordance with article 82(4) GDPR, the Affected Individual shall be entitled to receive compensation for the entire damage directly from Arcadis, in which case Arcadis shall be entitled to claim back from the Client that part of the compensation corresponding to the Client's part of responsibility for the damage, in accordance with article 82(5) GDPR.

Rights of Clients

11.5 The Client may enforce this Processor Policy against the Arcadis Contracting Entity or, if the Arcadis Contracting Entity is not established in an EEA Country, against Arcadis International B.V. Arcadis International B.V. shall ensure that adequate steps are taken to address violations of this Processor Policy by the Arcadis Contracting Entity or any other Group Company.

To bring a claim for damages, the Client must demonstrate that it has suffered damages and establish facts which show it is likely that the damage has occurred because of a violation of this Processor Policy. Arcadis International B.V. accepts liability for a breach by another Group Company or a Sub-Processor located outside of the EEA, although Arcadis International B.V. may assert any defense that such Group Company or Sub-Processor could have asserted.

Mutual assistance Group Companies and redress

11.6 All Group Companies shall co-operate with and assist each other to the extent reasonably possible to handle:

(a) a request, complaint or claim made by an Affected Individual; or

(b) a lawful audit, investigation or inquiry by a Competent SA or public authority, or the Client.

The Group Company that receives a request, complaint or claim is responsible for promptly informing the appropriate Privacy Officer thereof and handling any communication with the Client Individual regarding their request, complaint or claim as instructed by the appropriate Privacy Officer 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.

Cooperation with Competent SAs

11.7 Arcadis shall: (a) provide to the Competent SA, upon request, information in relation to the Processing of CI Information which is subject to this Processor Policy; and (b) take into account the advice of the Competent SA issued on the interpretation and application of this Processor Policy. Arcadis shall abide by binding decisions of the

Competent SA as instructed by Client in accordance with the Services Contract and Articles 3.1 and 3.2. Any dispute related to the Competent SA's exercise of supervision of compliance with this Processor Policy will be resolved by the courts of the Member State of that SA, in accordance with that Member State's procedural law.

ARTICLE 12 – SANCTIONS FOR NON-COMPLIANCE

Non-compliance

12.1 Non-compliance of Arcadis employees with this Processor Policy may result in disciplinary action in accordance with Arcadis policies and local law, up to and including termination of employment.

ARTICLE 13 – CONFLICTS BETWEEN THIS PROCESSOR POLICY AND APPLICABLE DATA PROCESSOR LAW

Conflict between Processor Policy and Applicable Data Processor Law

13.1 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 Processor Policy or that have a substantial effect on the protection offered by this Processor Policy (including on any 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 and, where appropriate, the Client – how to comply with this Processor Policy and address the conflict, including by implementing appropriate supplementary measures in accordance with Article 9.3. The same applies if the Data Exporter has reason to believe that the Data Importer can no longer fulfill its obligations under this Processor Policy. The Data Exporter will forward the notification to the Client.

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 Processor Policy or to have a substantial effect on the protection offered by this Processor Policy.

The Group Company that is 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 (including the identified supplementary

measures) performed under Article 9.3.

Consequences of Termination of a Transfer

13.2 The Data Importer shall – at the Client's choice (where relevant as communicated by the Data Exporter) – immediately return or delete CI Information that was received under this Processor 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 Processor 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 Processor Policy. If local laws applicable to the Data Importer prevent the return or deletion of CI Information, the Data Importer will only Process the CI Information to the extent and for as long as required under that local law. Until the CI Information is deleted or returned, the Data Importer will continue to ensure a level of protection no lower than that provided for in the Processor Policy.

ARTICLE 14 – CHANGES TO THIS PROCESSOR POLICY

Approval for changes

14.1 Any changes to this Processor Policy require the prior approval of the Global Privacy Officer and the Executive Board and shall thereafter be communicated to Group Companies.

Effective Date Of changes

14.2 Any change shall enter into force with immediate effect after it is approved in accordance with Article 14.1, published on the Arcadis Internet site and communicated to the relevant Clients.

Prior versions

14.3 Any request, complaint or claim of a Client Individual involving this Processor Policy shall be judged against the version of this Processor Policy that is in force at the time the request, complaint or claim is made.

Notification to Lead SA and Clients

14.4 The Global Privacy Officer shall notify the relevant SAs via the Lead SA in advance of changes to this Processor Policy that have a material impact on the protection offered by this Processor Policy or the Processor 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 Processor 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.

Where a change affects the Processing conditions of CI Information, Arcadis will provide notice of such change to the relevant Client. Within 30 days of receiving such notice, the Client may object to such change by providing written notice to Arcadis. In the event that the parties cannot reach a mutually acceptable solution, Arcadis shall put in place an alternative data transfer solution. In the event no alternative data transfer solution can be put in place, the Client will have the right to suspend the relevant Transfer to Arcadis. In the event a suspension of the relevant Transfers is not possible, Arcadis shall enable the Client to terminate the relevant Client Services in accordance with the terms of the Services Contract.

ARTICLE 15 – TRANSITION PERIODS

Transition period for new Group Companies

15.1 Any entity that becomes a Group Company after the Effective Date shall comply with this Processor Policy within two years of becoming a Group Company.

Transition period for Divested Entities

15.2 Arcadis may decide (and shall in such case ensure) that a Divested Entity (or specific parts thereof) will remain covered by this Processor Policy after its divestment for such period as is required by Arcadis to disentangle the Processing relating to such Divested Entity (e.g., until such time that the CI Information is 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 CI Information to the extent and for as long as required under that local law. Until the CI Information is deleted or returned, the Divested Entity will continue to ensure compliance with the Processor Policy.

Compliance during transition periods

15.3 During the transition periods set out in Article 15.1 – 15.2, no Transfer shall take place under this Processor Policy until the relevant Group Company is fully compliant.

Contact details

15.4 Office of the Global Privacy Officer: privacy@arcadis.com

Arcadis Privacy Office

c/o Arcadis International B.V.

Gustav Mahlerplein 97-103

1082 MS Amsterdam

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.
Affected Individual	AFFECTED INDIVIDUAL shall have the meaning set forth in Article 11.1 above.
ANV	ANV shall mean Arcadis N.V., having its registered seat in Amsterdam and its business address at Gustav Mahlerplein 97-103, 1082MS Amsterdam.
Applicable Data Controller Law	APPLICABLE DATA CONTROLLER LAW shall mean the Data Protection Laws applicable to the Client as the Data Controller of the CI Information.
Applicable Data Processor Law	APPLICABLE DATA PROCESSOR LAW shall mean the data protection laws that are applicable to Arcadis as the Data Processor of the CI Information.
Arcadis	ARCADIS shall mean ANV and its Group Companies.
Arcadis Contracting Entity	ARCADIS CONTRACTING ENTITY shall mean the Group Company that has entered into the Services Contract.
Arcadis International B.V.	ARCADIS INTERNATIONAL B.V. shall mean Arcadis International B.V., having its registered seat in Amsterdam and its business address at Gustav Mahlerplein 97-103, 1082MS Amsterdam.
Arcadis Sub-Processor	Any Group Company engaged by Arcadis as a Sub-Processor.
Article	ARTICLE shall mean an Article in this Processor Policy.
Business Unit	BUSINESS UNIT shall mean the Arcadis global businesses or a country.
CI Information	CI INFORMATION shall mean Personal Data of a Client Individual.
Client	CLIENT shall mean any Third Party who has entered into a contract with Arcadis for Client Services.
Client Individual	CLIENT INDIVIDUAL shall mean any individual whose Personal Data is Processed by Arcadis in its role as a Data Processor in the course of delivering Client Services to a Client.
Client Services	CLIENT SERVICES shall mean the services provided by Arcadis to Clients as described in Article 4.1.

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.
Data Exporter	DATA EXPORTER shall mean the Group Company that transfers CI Information to a Data Importer.
Data Importer	DATA IMPORTER shall mean the Group Company in a Third Country that is the recipient of CI Information.
Data Controller	DATA CONTROLLER shall mean the entity or natural person which alone or jointly with others determines the purposes and means of the Processing of Personal Data.
Data Processor	DATA PROCESSOR shall mean the entity or natural person that Processes Personal Data on behalf of a Data Controller.
Data Protection Law	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.
Data Security Incident	DATA SECURITY INCIDENT shall mean the unauthorized acquisition, access, use or disclosure of unencrypted CI Information 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 Client Individual.
Destination Country	DESTINATION COUNTRY shall mean the Third Country to which CI Information are transferred.
Disclosure Request	DISCLOSURE REQUEST shall mean a legally binding request for disclosure of (or direct access to) CI Information 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.
EEA or EEA Countries	EEA or EUROPEAN ECONOMIC AREA COUNTRIES shall mean all Member States of the European Union, plus Norway, Iceland, and Liechtenstein.
EEA Data Transfer Restriction	EEA DATA TRANSFER RESTRICTION shall mean any restriction under Data Protection Law to transfer Personal Data to a Third Country.
Effective Date	EFFECTIVE DATE shall mean the date on which this Processor Policy becomes effective as set forth in Article 1.6.
General Data	GENERAL DATA PROTECTION REGULATION or GDPR means the

Protection Regulation or GDPR	Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data or any successor or replacement thereof.
Global Privacy Officer	GLOBAL PRIVACY OFFICER shall mean the officer referred to in Article 8.1
Global Privacy Committee	GLOBAL PRIVACY COMMITTEE shall mean either the Global Privacy Committee as referred to in Article 8.2.
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 the Processor Policy.
Lead SA	LEAD SA shall mean the SA of the Netherlands, *Autoriteit Persoonsgegevens*.
Personal Data or Data	PERSONAL DATA shall mean any information relating to an identified or identifiable individual.
Privacy Officer	PRIVACY OFFICER shall mean a Privacy Officer appointed by the Global Privacy Officer pursuant to Article 8.3
Processing	PROCESSING shall mean any operation that is performed on CI Information, whether or not by automatic means, such as collection, recording, storage, organization, alteration, use, disclosure (including the granting of remote access), transmission or deletion of CI Information.
Processor Policy	PROCESSOR STANDARD shall mean this Processor Policy for Processing Personal Data of Client Individuals.
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.
Services Contract	SERVICES CONTRACT shall mean the contract for delivery of Arcadis Services entered into between a Group Company and the Client pursuant to Article 2.1.
Staff	STAFF shall mean all employees and other persons under the direct authority

	of Arcadis who Process CI Information as part of their respective duties or responsibilities towards Arcadis using Arcadis information technology systems or working primarily from Arcadis' premises.
Sub-Processor	SUB-PROCESSOR shall mean any Group Company or Third Party engaged by Arcadis to Process CI Information as a sub-processor.
Third Country	THIRD COUNTRY shall mean a country outside the EEA to which CI Information is transferred, where such Transfer is not covered by an Adequacy Decision.
Third Party	THIRD PARTY shall mean any person or entity (e.g., an organization or public authority) outside Arcadis.
Third Party Sub-Processor	THIRD PARTY SUB-PROCESSOR shall mean any Third Party engaged by Arcadis as a Sub-Processor.
Third Party Sub-Processor Contract	THIRD PARTY SUB-PROCESSOR CONTRACT shall mean the validly entered into written or electronic agreement between the Arcadis Contracting Entity and the Third party Sub-Processor pursuant to Article 7.2.
Transfer	TRANSFER shall mean a transfer (or set of transfers) of, including disclosure of, or remote access to, CI Information that is subject to Data Protection Law (or has been subject to Data Protection Law prior to its 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 CI Information to public authorities or authorizing access by such authorities, prevent Arcadis from fulfilling its obligations under this Processor 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 Processor 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 CI Information 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 CI Information 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 CI Information 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 Processor Policy, including measures applied during transmission and to the Processing of CI Information in the Destination Country.

Interpretations

INTERPRETATION OF THIS PROCESSOR STANDARD:

(a) 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;

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

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

(d) the male form shall include the female form(v) the words "include", "includes" and "including" and any words following them shall be construed without limitation to the generality of any preceding words or concepts and vice versa ;

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

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