**Appendix X**

**PROCESSOR AGREEMENT**

accompanying the [………] Agreement

The Undersigned:

1. **Alliander N. V.**, a public limited liability company incorporated under Dutch law [*naamloze vennootschap*] having its registered office and place of business at Utrechtseweg 68 in (NL‑6812 AH) Arnhem, The Netherlands, and registered with the Central Gelderland Chamber of Commerce under number 34108286, duly represented in this matter by Mr R.A. Hof, [manager purchase and facilities], hereinafter also referred to as “Controller”,

and

2. {name of entity B}, having its registered office in {town/city} and place of business at {address, postcode, and town/city}, duly represented in this matter by [name, position], hereinafter referred to as “Processor”;

Controller and Processor will also be referred to jointly hereinafter as “**Parties**” and separately as a “**Party**”;

WHEREAS:

1. Controller concluded a {….. Agreement} with Processor on [date], hereinafter referred to as the “Agreement”. Based on said Agreement, Processor will carry out {brief description of services}. In performing the Agreement, Processor, acting at the behest of and on the instructions of Controller, will process Personal Data;
2. Parties attach importance to the careful handling of Personal Data. Alliander is Controller for the Processing of the Personal Data and {B} is Processor on behalf of Alliander;
3. As a processor of Personal Data, Processor provides effective guarantees that appropriate technical and organisational measures are in place to ensure that the Processing complies with the requirements of the Applicable Law and to ensure protection of the rights of Data Subjects.
4. In the present Processor Agreement, Parties wish to record what they have agreed regarding Processing of the Personal Data by Processor at the behest of Controller in accordance with the Applicable Law;

**DECLARE THAT THEY HAVE AGREED AS FOLLOWS:**

1. Definitions

As regards this Processor Agreement, the same definitions shall apply as in the body of the Agreement and in the Applicable Law, unless otherwise provided herein and supplemented by the definitions in the present Clause 1.

* 1. Personal Data: any information relating to an identified or identifiable natural person (the “Data Subject”). An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier, or one or more factors specific to the physical, physiological, genetic, mental, economic, cultural, or social identity of that natural person, as further defined in Clause 3.1 of this Processor Agreement;
  2. Processing: any operation or set of operations which is performed on Personal Data or on a set of Personal Data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or deletion;
  3. Controller: a natural person, legal entity, public authority, agency, or other body who/which, alone or jointly with others, determines the purposes and means of the Processing of Personal Data.
  4. Processor: a natural or legal person, public authority, agency, or other body which processes Personal Data on behalf of Controller;
  5. Appendix: An appendix to this Processor Agreement, which, after having been signed by both Parties, forms part of this Processor Agreement;
  6. Data Breach(es): any incident resulting in (possible) unintentional or unlawful destruction, loss, alteration, unauthorised disclosure of or access to the Personal Data transmitted, stored or otherwise processed, regardless of whether such incident occurred in connection with the Processing facilities or elsewhere;
  7. Processor Agreement: the present Processor Agreement, which forms part of the Agreement, including recitals and Appendix/Appendices, as well as any alteration, replacement, update, or other subsequent versions thereof;
  8. Employees: the employees and other (auxiliary) persons engaged by Processor for the performance of this Processor Agreement who are subject to Processor’s responsibility;
  9. Applicable Law: the applicable Dutch and/or European legislation or regulations, the General Data Protection Regulation (EU) 2016/679 that is applicable as of 25 May 2018, or any other guidelines, policy rules, instructions, or recommendations of any competent Dutch and/or European government authority that apply to the Processing of the Personal Data, including any amendments, replacements, updates or other subsequent versions thereof.

1. Subject of this Processor Agreement
   1. In the context of performance of the Agreement and the Appendices thereto, Alliander is to be regarded as Controller for Processing of the Personal Data pursuant to the Applicable Law, and {B) as Processor of the Personal on behalf of Alliander.
   2. This Processor Agreement forms an Appendix to the body of the Agreement, and replaces all previous arrangements, whether oral or written, that may have been made by Controller and Processor regarding the Processing of the Personal Data.
   3. In the event of any conflict between the provisions of this Processor Agreement and the body of the Agreement and the other Appendices, the provisions of this Processor Agreement shall prevail, unless expressly provided otherwise in this Processor Agreement.
   4. Processor guarantees that it will process the Personal Data in accordance with the Applicable Law. Processor shall immediately notify Controller if it considers that any instruction violates the Applicable Law.
   5. Processor shall only process the Personal Data at the behest of Controller and in accordance with the latter’s written instructions, including with regard to the transfer of Personal Data to a third country. Provider shall have no independent controlling authority [*zeggenschap*] over the Data that it processes. The Agreement and the present Processor Agreement shall be deemed to be a written instruction from Controller. Processor shall not process the Personal Data for its own benefit, for the benefit of third parties, or for other purposes unless pursuant to different mandatory obligations to which it is subject under the Applicable Law.
   6. Processor shall not retain the Personal Data in a form that can traced to Data Subjects any longer than necessary in order to provide the service. [The maximum retention period for the Personal Data shall in any case be ….].
   7. If, contrary to this Processor Agreement and/or the Applicable Law, Processor determines the purpose and means of/for the Processing of the Personal Data, Processor shall be considered to be the controller for such Processing operations within the meaning of the Applicable Law.
2. Processing of the Personal Data
   1. For the purposes of the Agreement and the Appendices, Processor shall process the “Personal Data” as further specified in Appendix A.
   2. Taking into account the nature of the Processing and the information available to Processor, Processor shall provide Controller with all necessary assistance to ensure compliance with the obligations of Parties under the Applicable Law, in particular the obligations relating to the security of the Personal Data, the obligations regarding notification of Data Breaches, the obligations relating to the performance of data protection impact assessments (DPIAs), and the obligations regarding prior consultation by one or more competent public authorities. Processor shall keep a register of all categories of Processing operations that it has performed or is performing on behalf of Controller. Said register shall in any case contain the information referred to in Article 30(2) GDPR. Said register shall be made available by Processor to the supervisory authority and Controller on request.
   3. Processor shall only disclose the Personal Data to those Employees who require the Personal Data in order to carry out their work or who must necessarily be aware of the Personal Data for performance of the Agreement and the Appendices, and shall otherwise keep said Personal Data confidential, unless Processor is subject to differing statutory obligations under the Applicable Law.
   4. Appendix A lists which Employees (or groups of Employees) may have access to which Personal Data and describes which Processing operations such persons may carry out with which type of Personal Data. Processor is expressly prohibited from (i) providing access to the Personal Data to persons or groups of persons other than those listed in Appendix A, and (ii) to perform, or give instructions for, Processing operations with the Personal Data other than those specified in Appendix A.
   5. Processor shall impose the obligations laid down in this Processor Agreement and in the Agreement, including the security and confidentiality obligations, on the Employees whom it deploys. Processor shall ensure that such Employees comply with the relevant obligations arising from this Processor Agreement, the Agreement, and the Appendices.
3. Sub-Processors
   1. Processor shall not provide the Personal Data to third parties other than to a Sub‑Processor approved in advance by Controller in writing, in so far as Personal Data is concerned that is necessary for optimum service provision by such Sub‑Processor. The name and address of such Sub-Processor shall be given in Appendix C.
   2. Processor shall conclude a written Sub-Processor Agreement with any other processor that it engages as a Sub-Processor and in doing so shall impose the same obligations on such other processor as those to which it is itself subject pursuant to this Processor Agreement, including but not limited to its own notification obligations regarding Data Breaches. In said Sub-Processor Agreement, Processor shall also prohibit the other processor from engaging processors or sub-processors.
4. Security
   1. Processor shall be responsible for implementing technical and organisational security measures. Processor shall observe and implement at least the technical and organisational security measures set out in Appendix B in order to ensure the availability, integrity, and confidentiality of the Personal Data and to protect the Personal Data effectively against unauthorised access or loss, or any other form of unlawful Processing of the Personal Data.
   2. The technical and organisational security measures to be implemented by Processor shall ensure an appropriate level of protection, including in view of Controller’s obligation as regards dealing with requests from Data Subjects who exercise their rights. Said measures shall take account of the state of technology, the costs associated with the implementation, nature, extent, context, and purposes of the Processing, as well as the varying risks to the rights and freedoms of individuals in terms of probability and seriousness. Said measures shall in any case include, where appropriate:
      1. pseudonymisation and encryption of the Personal Data;
      2. the ability to permanently ensure the confidentiality, integrity, availability, and resilience of the Processing facilities and Services;
      3. appropriate preventive measures which enable Processor to immediately identify and/or prevent a Data Breach and to inform Controller of such in good time, for example intrusion detection, future-proof encryption, and the possibility to restore the availability of the Personal Data in good time;
      4. a process for regularly testing, assessing, and evaluating the technical and/or organisational security measures in order to guarantee the efficiency and effectiveness and security of the Processing of the Personal Data;
   3. When implementing any security measure, Processor shall comply with the Applicable Law.
   4. Processor shall, at least annually, review and if necessary update the technical and organisational security measures.
5. Security Reports
   1. Without prejudice to Controller’s right to carry out an audit, or to have such carried out, Processor shall have the Processing of the Personal Data, Processing facilities, and security measures evaluated regularly at its own expense, at least annually, and on that basis shall submit an annual written security report to Controller. Processor shall in any case provide said written security report to Controller within two weeks after completion of the evaluation. Said evaluation shall be carried out by an independent (expert) third party according to appropriate audit standards accepted in writing by Controller.
   2. The security report shall cover all Processing of the Personal Data and shall address at least the status of the Processing facilities and security measures, the recorded down time of the technical security measures, the established compliance (or non‑compliance) with the organisational security measures, Data Breaches that have occurred, perceived threats to security and the Personal Data, and the necessary and/or recommended improvements.
   3. Processor shall implement all (immediate) measures to effectively remedy any perceived threats, weaknesses, and other problems identified, as well as any necessary and/or recommended improvements contained in the security report. Alternative measures may also be decided upon in consultation with Controller, provided that Processor can demonstrate that they have at least the same mitigating effect.
6. Notification of Data Breaches
   1. Processor shall maintain effective procedures for detecting and taking action against all possible Data Breaches, including procedures for preventive and corrective action, as well as for preventing the recurrence of any Data Breaches. Said procedures shall have been designed by Processor in such a way that both Controller and Processor are able to comply with the notification obligations concerning Data Breaches pursuant to the Applicable Law.
   2. As soon as Processor detects or reasonably suspects that a Data Breach has occurred or may occur, Processor shall immediately notify Controller to that effect, and in any case within 8 hours of detection or suspicion of a Data Breach. Such notification shall be made through the e-mail address for security incidents [meldpuntdatalekken@alliander.com](https://contentserver.alliander.com/csdav/nodes/165234090/meldpuntdatalekken%40alliander.com) as listed in Appendix C. If Processor is unable to reach Controller immediately and directly, Processor shall make all reasonable efforts to ultimately contact Controller directly.
   3. In the event of a Data Breach, Processor shall implement effective rectification measures as soon as possible. In addition, Processor shall provide Controller with all relevant information requested by Controller in relation to the Data Breach. Said information shall in any case comprise:
      1. a description of the nature and extent of the Data Breach, an estimate of the number or potential number of persons affected, and an indication of the nature of the affected Personal Data, and whether such Personal Data was encrypted or otherwise protected or rendered inaccessible or incomprehensible;
      2. a description of the preventive and corrective measures that have been and will be implemented, planned measures, and recommended measures to reduce damage, including an emergency plan and the expected time for resolution and workaround;
      3. information about which third parties, such as government authorities and the media/social media, are or may be aware of the Data Breach;
      4. the contact details of Processor’s authorised representative(s) from whom Controller can obtain immediate and regular updates on the status of the Data Breach; and
      5. any other information that can assist in limiting the damage to Controller’s organisation and the privacy of the Data Subject(s) affected.
   4. Processor shall also provide all reasonably foreseeable assistance to Controller and share with Controller all necessary information or information requested by Controller, so that Controller, in good time, can inform the affected (and potentially affected) Data Subject(s) and/or the relevant government authorities or supervisory authorities that are competent to adjudicate regarding the Processing of Personal Data about the Data Breach and is able to comply with the reporting obligations regarding Data Breaches pursuant to the Applicable Law. Processor shall not be permitted to communicate with supervisory authorities and Data Subjects in the context of a Data Breach, except on the basis of instructions from Controller.
   5. Processor shall carry out an audit in order to establish and implement appropriate rectification measures so as to prevent the recurrence of a similar situation, without prejudice to any audit rights of Controller.
7. Audit Right of Controller
   1. Subject to a prior notification period of 2 weeks, Controller may have the Processing activities and Processing facilities audited in order to investigate, or have investigated, the technical and organisational measures implemented with regard to the Personal Data.
   2. Controller may also carry out an audit of the Processing operations and Processing facilities, or have such carried out, in order to verify whether Processor has correctly informed Controller, in good time, of all Data Breaches and of the preventive and rectification measures implemented in that regard, including any measures to prevent the recurrence of a Data Breach.
   3. Processor shall provide all reasonably necessary cooperation so that Controller can exercise its audit rights and can demonstrate compliance with the Applicable Law, and Processor shall ensure that sub-contractors engaged by it do so also.
   4. Controller may engage (expert) third parties for the exercise of its audit rights. The performance of an audit by Controller or on behalf of Controller shall not lead to any delay in the work of Processor or one of Processor’s sub-contractors. If such delay is likely to occur, Parties shall enter into consultations on the matter.
8. Transfer of Personal Data
   1. Unless with the express written consent of Controller, Processor shall not transfer Personal Data to, make it accessible from, or otherwise process it in any country outside the European Economic Area (EEA).
   2. If Processor intends Processing Personal Data outside the EEA or transferring Personal Data otherwise to a country outside the EEA, Processor – without prejudice to the provisions of paragraph 1 of this clause – shall inform Controller in writing of such intention in good time and shall also indicate which country or countries is/are concerned. Transfer of Personal Data to a country outside the EEA also includes making Personal Data accessible from such other country or from an entity in such other country.
   3. Processor shall cooperate fully at all times, at its own expense, to ensure that any transfer to a country outside the EEA takes place in accordance with the Applicable Law.
9. Requests by Data Subjects
   1. Processor shall cooperate fully in order to ensure that Controller can comply with its statutory obligations if a Data Subject exercises its rights pursuant to the Applicable Law.
   2. As soon as Processor receives a request to that effect, as referred to in the previous paragraph of this clause, from a Data Subject, Processor shall immediately inform Controller in writing thereof, and shall provide Controller with a copy of all correspondence received in that regard. Controller shall inform Processor as to whether Processor, acting on behalf of Controller, can respond to the request and if so, in what manner.
   3. Without prejudice to its obligations under the Agreement, Processor shall, where applicable, immediately correct or otherwise amend the Personal Data, in accordance with the instructions of Controller.
10. Requests by Government Authorities
    1. If Processor receives a request from a government authority to provide Personal Data (or to inspect Personal Data), Processor shall immediately inform Controller in writing thereof before providing such Personal Data (or enabling inspection thereof), and shall provide Controller with a copy of all correspondence received in that regard. Processor shall only comply with a request to that effect if it is obliged to do so pursuant to the Applicable Law. Controller may issue Processor with reasonable instructions in this regard, in so far as such does not prevent the performance of the aforementioned statutory obligation.
    2. If it is possible to take legal action against the request for the provision of Personal Data or against any prohibition on informing third parties about such request, Contracting Party shall make full use of such possibility (at its own expense).
    3. To guarantee protection of the Personal Data, Processor shall ensure that it does not provide the government authority with any more Personal Data than is strictly necessary to comply with the latter’s request.
    4. If Processor is not permitted – on the basis of the request to provide Personal Data that it has received – to inform third parties, including Controller, about said request and the possible subsequent provision of Personal Data to a government authority, then Processor shall be the controller for Processing the Personal Data solely as regards compliance with said request. As soon as Processor is permitted to do so, it shall immediately inform Controller about requests received and any subsequent provision of Personal Data, and in doing so shall provide Controller with a copy of all correspondence received in that regard.
11. Costs
    1. The costs involved in the performance of this Processor Agreement are included in the prices and fees as agreed in the Agreement.
12. Liability and Indemnification

13.1 The liability of Processor for loss/harm arising from or in connection with failure to comply with this Processor Agreement or action contrary to the Applicable Law shall be limited in accordance with the provisions of the Agreement.

13.2 Processor indemnifies Controller in respect of all claims, penalties, proceedings, or claims by third parties, including public supervisory authorities and Data Subjects, that may be brought against Controller due to a contravention of the Applicable Law that is attributable to Processor, the Employees or other persons whom Processor has engaged, or Processor’s sub-contractors. The extent of said indemnification obligation shall be limited to a maximum of 5 million euros per event, unless the situation involves an intentional act or omission or deliberate recklessness. [Coordinate alternative with Legal Affairs department]: The extent of said indemnification obligation shall be limited to the maximum within the meaning of the first paragraph of this clause, unless the situation involves an intentional act or omission or deliberate recklessness.

13.3 Processor shall ensure that it has adequate liability insurance during the term of this Processor Agreement. Processor shall provide Controller with a copy of the relevant policy and the associated policy conditions at Controller’s first request.

1. Term and Termination
   1. This Processor Agreement shall enter into force at the same time as the Agreement.
   2. This Processor Agreement shall remain in force for as long as the Agreement is in force. Upon termination of the Agreement, this Processor Agreement shall terminate by operation of law without any further (legal) act being required, on the understanding, however, that as long as Processor has not yet returned all Personal Data to Controller or has deleted it and/or has failed to comply with the provisions of Clause 14.5, all provisions of this Processor Agreement which by their nature continue to apply shall remain in force until such time as said return, delivery, or deletion and the provisions of Clause 14.5 have been complied with. Such shall be on the understanding that the duration of the confidentiality obligation of Processor and its Employees within the meaning of Clause 3.5 shall be unlimited.
   3. Premature termination of this Processor Agreement by Processor shall not be possible.
   4. Unless such ensues otherwise in accordance with the Applicable Law, if this Processor Agreement terminates or on an earlier date, Processor shall ensure, as soon as Controller indicates that the Processing of some or all of the Personal Data is no longer relevant for the performance of the Services (i) that the Personal Data is immediately returned or provided, in a manner that Controller considers suitable, to Controller or to a substitute service provider designated by Controller or (ii) that the Personal Data is immediately deleted if Controller so requests in writing.
   5. Processor shall ensure that after such return, provision, or deletion Processor shall immediately cease and desist from all Processing of (the relevant) Personal Data.
2. Changes and Renegotiation
   1. Parties shall implement changes in the processed Personal Data, Processor’s Processing activities on behalf of Controller, the applicable reliability requirements, and/or changes in the contact details in Appendix/Appendices A, B, and/or C. The relevant changes shall take effect after both Parties have signed the amended appendix/appendices.
   2. If a change in circumstances justifies such, Controller shall be entitled to renegotiate this Processor Agreement. If Parties fail to reach Agreement during the renegotiations, Controller shall be entitled to terminate the Agreement, without being liable for any resulting loss/harm.
   3. Processor hereby consents in advance to amendments to this Processor Agreement that are necessary, due to changed circumstances, for compliance with the Applicable Law.

THUS AGREED AND SIGNED,

|  |  |  |
| --- | --- | --- |
| Alliander N.V. |  | {B} |
| Name:  Position:  Date: |  | Name:  Position:  Date: |
|  |  |  |

**Appendix A  
Overview of the Services and Related Processing Operations**

**Description of the Processing Operations**

|  |  |  |  |  |  |
| --- | --- | --- | --- | --- | --- |
| **Categories of Data Subjects** | **Categories of Personal Data that Processor will process**  If necessary differentiated according to sensitivity. | **Purposes for which Personal Data will be processed** | **Duration of Processing** | **Employees (or groups of Employees) to be engaged by Processor who have, or may have, access to the Personal Data** | **Operations that said persons may carry out regarding said Personal Data** |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |
|  |  |  |  |  |  |

**Appendix B**

**Security Measures**

Where applicable differentiated according to the sensitivity of the categories of Personal Data listed in Appendix A.

**Implementation in the form of specific technical and organisational measures**

Processor shall implement at least the following measures as referred to in Clause 5:

Section 1

Processor shall establish and implement information security policy and procedures based on commonly accepted standards. Said information security policy shall be aimed at protecting the confidentiality, integrity, and availability of the Personal Data.

Section 2

Within its organisation, Processor shall establish the responsibilities for information security and shall deploy sufficient personnel and resources to secure the Personal Data against loss or unauthorised access or use.

Section 3

Processor shall ensure that the personnel who have access to the Personal Data are trustworthy. Processor shall impose a duty of confidentiality on personnel who have access to the Personal Data.

Section 4

Processor shall oblige its personnel to conform to Processor’s information security policy, the specific instructions of Controller in the area of security and the confidentiality of the Personal Data, and all obligations arising from the applicable legislation and regulations.

Section 5

Processor shall make the personnel who have access to the Personal Data or who are otherwise involved in the Processing of the Personal Data aware of the security risks and of their obligations regarding the security of Personal Data. Processor shall require its personnel to report any observed or suspected Data Breach immediately in accordance with the procedure laid down by Processor regarding the notification of Data Breaches.

Section 6

Processor shall have procedures in place to prevent unauthorised access to Personal Data and shall deploy appropriate measures for that purpose, including in any case:

1. use of secure authentication procedures on information systems;
2. closing off of areas containing servers or computers on which Personal Data is stored or with which Personal Data is processed;
3. encryption of the Personal Data during its transport via a network;
4. encryption of the Personal Data when it is stored on a laptop, USB stick, smartphone, or other portable storage medium;
5. logging of access to the information systems and/or the Personal Data;
6. use of antivirus software.

**Appendix C**

**Contact Persons**

[to be filled in by Parties]

|  |  |  |  |
| --- | --- | --- | --- |
| **Controller** | | | |
|  | Name and position | Phone number | **E-mail adress** |
| Contact person |  |  |  |
| Substitute |  |  |  |
| E-mail address for security incidents: [meldpuntdatalekken@alliander.com](https://contentserver.alliander.com/csdav/nodes/165234090/meldpuntdatalekken%40alliander.com) | | | |

|  |  |  |  |
| --- | --- | --- | --- |
| **Processor** | | | |
|  | Name and position | Phone number | **E-mail adress** |
| Contact person |  |  |  |
| Substitute |  |  |  |

**Sub-Processors**

[to be completed by Parties if relevant]

The Personal Data is processed by the following party (ies):

|  |  |  |  |
| --- | --- | --- | --- |
| **Sub-Processors** | | | |
| NAME | ADDRESS | PLACE | **explanation** |
|  |  |  |  |
|  |  |  |  |