

## Privacy Regulations

The purpose of these Privacy Regulations is to provide data subjects with information on the way in which ENNIA processes Personal Data.

### Article 1. Definitions

- a. Personal Data: all data regarding an identified or identifiable natural person.
- b. Personal Data Processing: any act or body of acts related to Personal Data, which in any event includes the collection, recording, organisation, storage, updating, amendment, retrieval, consultation, use, provision by means of forwarding, distribution or any other form of making available, combination, association, protection, exchanging or destruction of data.
- c. Recipient: the person to whom the Personal Data are made available, both within and outside the Controller's organisation.
- d. Data Subject: the person to whom Personal Data relate.
- e. Controller: the legal entity that, solely or together with others, determines the purpose of and the means used for the Personal Data Processing.
- f. Administrator: the party that is entrusted under the Controller's responsibility with the day-to-day care for the Personal Data Processing.
- g. Processor: the party that processes Personal Data for the Controller's benefit, without being subject to its direct authority.
- h. Third Party: any party, not being the Data Subject, the Controller, the Processor or any person who is authorised to process Personal Data under the direct authority of the Controller or the Processor.
- i. Permission of the Data Subject: any freely given, specific and informed indication of intent by means of which the Data Subject accepts that his or her Personal Data are processed.
- j. File: any structured body of Personal Data, irrespective of whether that body of data is centralised or is spread in a functionally or geographically specific manner, that is accessible in accordance with certain criteria and relates to different persons.
- k. Provision of Data: the disclosure or making available of Personal Data.
- l. Special Personal Data: Personal Data within the meaning of Section 16 of the BES Personal Data Protection Act.
- m. ENNIA: ENNIA Caribe Holding N.V., ENNIA Caribe Schade N.V., ENNIA Caribe Leven N.V., ENNIA Caribe Zorg N.V., ENNIA Caribe Holding (Aruba) N.V., ENNIA Caribe Leven (Aruba) N.V. and ENNIA Caribe Schade (Aruba) N.V.

### Article 2. Scope

These Regulations apply to:

- a. all fully or partially automated Personal Data Processing in the context of the Controller's business tasks; and
- b. the processing of documents that form part of a File.

### Article 3. Management of the Personal Data

1. The Controller must draw up a separate statement per separate processing act or related processing acts.
2. The Controller must make the statement referred to in paragraph 1 available for inspection by any party that wishes to inspect it. Any party may request the Controller to send him or her a copy or copies of one or more separate statements.
3. The Controller must state the name of the Administrator and – if applicable – the name of the Processor of the processing act or related processing acts in the statement referred to in paragraph 1.

#### Article 4. Purpose of the processing

1. The purpose of the processing is to promote the joint interests of ENNIA and the insured with a view to:
  - a. assessing and managing risks in general;
  - b. limiting the cost of claims, in particular by means of a sound acceptance policy;
  - c. discovering, preventing and controlling insurance fraud;
  - d. exchanging factual data between insurers and with the police/judicial authorities and other institutions acknowledged by the Controllers.
2. The data may also be used for statistical analyses with a view to fraud and crime prevention and risk analyses.
3. The data recorded will be used only for purposes that are compatible with the purpose of the processing.

#### Article 5. Lawful ground for the processing

The Controller must state the ground for the processing in the statement referred to in Article 3(1).

#### Article 6. Categories of persons whose Personal Data are processed

In the statement referred to in Article 3(1) the Controller must identify categories of persons whose Personal Data are processed.

#### Article 7. Types of Personal Data recorded and manner of collection

1. The Controller must indicate in the statement referred to in Article 3(1) the extent of the types of Personal Data that it processes.
2. The Controller must collect Personal Data to the extent possible from the Data Subject himself/herself, unless that is impossible because it would require a disproportionate effort.
3. The Controller must process Personal Data in accordance with the statutory rules and with due care.
4. The Controller may process Personal Data insofar as they are adequate, relevant and non-excessive in light of the purposes of the statement referred to in Article 3(1).
5. The Controller must process Special Personal Data with due observance of the provisions of Sections 16 to 24 of the BES Personal Data Protection Act.
6. The Controller must take the necessary measures to promote the correctness and completeness of the Personal Data.

#### Article 8. Internal advice on Personal Data Processing

1. ENNIA's management board will set up a working group that advises the management board on request and of its own accord about the manner in which the protection of Personal Data is organised and the Data Processing acts are secured within ENNIA's organisation.
2. The working group referred to in paragraph 1 will in any event include:
  - a. a chairperson, being a board member or corporate staff member entrusted with the internal organisation;
  - b. a member of the Automation department; and
  - c. a lawyer of the Legal Affairs department.
3. The working party must meet at least once a year and furthermore as often as necessary.
4. The members of the working group may not in any manner be disadvantaged by their participation in and advising of the working group.
5. If that is necessary in order to perform their tasks, the members of the working group may request anyone to cooperate in the provision of information on the nature of the Personal Data and the manner in which those Personal Data are processed within ENNIA, the purpose and the necessity of the Personal Data Processing, the manner in which that processing is secured and the parties with which data are exchanged.

6. If there is any statutory obligation to report to a duly authorised body, the management board will report the registration of Personal Data to that body.
7. The working party will investigate the Data Processing acts referred to in paragraph 6 and prepare the report to the competent body.
8. The working group will provide assistance in drawing up the statements referred to in Article 3(1).
9. The working group will advise the management board on how to increase the knowledge and awareness of privacy aspects of ENNIA employees in their day-to-day work.

#### Article 9. Retention period and removal of Personal Data recorded

1. The Controller must as soon as possible remove Personal Data that are no longer required for the purpose for which they were collected. Such removal need not take place if:
  - a. it may reasonably be assumed that retaining the information is of great importance to a party other than the Data Subject;
  - b. sound record-keeping necessitates the retaining of the Personal Data;
  - c. a statutory regulation prescribes the retaining of Personal Data;
  - d. the Data Subject and the Controller have so agreed.
2. The Controller may remove Personal Data by destroying them or by taking such action that it is no longer possible to trace the data to the person in question.

#### Article 10. Access to and provision of Personal Data

1. The Controller designates the heads of departments as Administrators of the Files and Data Processing acts that come under their departments.
2. Only the Administrator or the Processor and the employees or persons designated by the Administrator or Processor have direct access to Personal Data, with a view to the day-to-day care for the sound functioning of the processing. That authority pertains only to the use of the recorded data for purposes that are compatible with the purpose of the Personal Data registration in question.
3. The Controller must obligate any persons referred to in paragraph 1 who are not already under a duty of confidentiality on the grounds of their position, profession or a statutory regulation to observe confidentiality in respect of the Personal Data that come to their knowledge, except insofar as any statutory regulation obligates them to disclose or the necessity of disclosure follows from their tasks.
4. Internal and external accountants have access to the Personal Data registration insofar as that is strictly necessary in the context of their assignment.
5. The Controller may provide a Third Party with Personal Data only insofar as that follows from the purpose of the registration or is possible on the grounds of the statutory regulation.
6. If Personal Data are in an anonymous form in such a way that it is reasonably impossible to trace them to individual persons, the Controller may decide to make them available to third parties for purposes that are compatible with the purpose of the registration.
7. Notwithstanding paragraph 5, Third Parties may be provided with data on request for the benefit of scientific research, for statistical purposes or on the grounds of compelling or urgent reasons, insofar as the Data Subject's privacy is not disproportionately harmed.
8. Within the Controller's organisation Personal Data out of the records are made available to the following persons only insofar as those data are necessary for the performance of their tasks:
  - a. persons entrusted with or in charge of records management;
  - b. persons entrusted with handling disputes or advising on disputes in the context of a statutory regulation;
  - c. persons insofar as that is necessary with a view to their performance of scientific, statistical or historical research.
9. The Controller must state the name of the Recipient of Personal Data in the statement referred to in Article 3(1), insofar as applicable.

#### Article 11. Further processing of Personal Data

1. The Controller may further process Personal Data only in a manner that is compatible with the purpose for which the data were obtained. In doing so it must in any event take into account the connection between the purposes, the nature of the data, the consequences of further processing for the Data Subject, the manner in which the data were obtained and the safeguards for protection of privacy.
2. The Controller may further process Personal Data if that is necessary in order to comply with a statutory obligation that applies to the Controller or if it takes place with the unequivocal Permission of the Data Subject.

#### Article 12. Security

1. The Controller must draw up guidelines in a protection plan for the technical and organisational protection of the Personal Data Processing and must present that plan to the current employee representatives insofar as it relates to the processing of Personal Data of employees.
2. The Controller must send the adopted protection plan to the Administrator. The Administrator must comply with the protection plan in performing his or her work.
3. If the Controller uses the services of a Processor, the Controller must record both parties' obligations regarding the handling of Personal Data in writing in an agreement with that Processor.

#### Article 13. Obligation to inform

If the Controller obtains Personal Data from the Data Subject himself/herself, it must inform him/her of its identity and of the purpose of the processing for which the data are intended before obtaining the Personal Data, unless the Data Subject already has that information.

#### Article 14. Data Subject's rights: general

1. Each Data Subject has the right to be informed, the right of inspection, the right of correction and the right to object.
2. Employees of ENNIA may also exercise the rights referred to in paragraph 1 during working hours.
3. If in its opinion special circumstances occur, the Controller may charge costs to the Data Subjects for exercising the rights referred to in paragraph 1, with due observance of the relevant statutory provisions.
4. The Data Subjects may be assisted in exercising the rights referred to in paragraph 1.
5. The chairperson referred to in Article 8(2) is the contact for Data Subjects who wish to exercise their rights and must draw their attention to the possibilities of legal protection and supervision, and to the role of the Personal Data Protection Authority.

#### Article 15. Right to be informed

The Controller must inform the Data Subject at his or her request in a timely manner and in full about the purposes for which and the ways in which Personal Data of the Data Subject are processed, about the applicable rules, about the rights that the Data Subject has in that respect and about the manner in which he or she can exercise those rights. The Data Subject must then also be informed about the place where the documents in which those rules are recorded can be inspected or obtained.

#### Article 16. Right of inspection

1. The Controller must inform any party at his or her request in writing, as soon as possible but no later than four weeks after receipt of the request, whether any Personal Data concerning him or her are being processed.
2. If the Controller processes Personal Data concerning the applicant, the Administrator must provide the applicant at his or her request in writing, as soon as possible but no later than four weeks after receipt of the request, with a full statement of the Personal

Data processed in respect of the Data Subject, together with information on the purpose or purposes of the Data Processing, the data or categories of data to which the processing relates, the Recipients or categories of Recipients of the data, and the origin of the data. If the applicant so desires, the Controller must also provide information on the system used for the automated data processing.

3. If a compelling interest of the applicant so requires, the Controller must comply with the request in a manner other than in writing, in keeping with that interest.
4. The Controller must arrange for sound identification of the applicant.

#### Article 17. Right of correction: correction, supplementation, removal and/or protection

1. At the written request of a Data Subject, the Controller must correct, supplement, remove and/or protect the Personal Data processed in respect of the applicant, if and insofar as the data are factually incorrect or are incomplete, irrelevant or excessive for the purpose of the processing, or are otherwise being processed in violation of a statutory regulation. The request must state the changes to be made.
2. The Controller must state in writing as soon as possible but no later than four weeks after receipt of the request whether it will comply. If it does not wish to comply, or to comply in full, it must state the reasons.
3. The Controller must ensure that a decision to correct, supplement, remove and/or protect is implemented as soon as possible.
4. In the event of correction, supplementation, removal and/or protection, the Controller must inform Third Parties accordingly and ensure that those Third Parties change their Files accordingly. The Controller must inform the applicant of the names of the third parties to which it has provided that information.
5. The Controller must draw the attention of the Data Subject who is informed of a decision on his or her request of the possibilities of filing an appeal with the (administrative) court.

#### Article 18. Right to object

1. If the lawful ground for a specific processing act is the Controller's legitimate interest, the Data Subject may at any time object to the Controller to the processing on the grounds of special personal circumstances.
2. Within four weeks of receipt of the objection the Controller must state whether the objection is justified.
3. The Controller must immediately put an end to the processing if the Controller considers the objection to be justified. Objection to processing for commercial or charity purposes is legitimate at all times.

#### Article 19. Complaints procedure

1. If in the Data Subject's opinion the provisions of these Regulations are not observed or if he or she has other reasons to complain about the processing of his or her Personal Data by the Controller, he or she may contact ENNIA's complaints coordinator. The complaints coordinator has a duty of confidentiality in respect of all information that comes to his or her attention in that context, except insofar as the Data Subject agrees to disclosure. The complaints coordinator can mediate between the Controller and the Data Subject in the event of a complaint.
2. If that does not give rise to a result that is acceptable to the Data Subject, the Data Subject has the following possibilities:
  - a. the Data Subject may file a complaint. The Controller must then handle the complaint in accordance with the ENNIA complaints procedure; or
  - b. the Data Subject may contact ENNIA's legal counsel and request him or her to mediate or advise in the dispute with the Controller. This must be done within six weeks of receipt of a reply from the Controller.

#### Article 20

These Privacy Regulations enter into force on 1 January 2011.

Article 21

These Privacy Regulations may be cited as the “ENNIA Privacy Regulations”.

## **EXPLANATION**

### **General**

By means of these Privacy Regulations ENNIA wishes to emphasise the importance that it attaches to careful handling of personal data by the organisation. ENNIA also wishes to ensure that the organisation processes personal data in accordance with any statutory requirements that apply to registration.

It plays an important part in this context that ENNIA has decided to set up a working group in its internal organisation in order to increase awareness of privacy protection within the organisation. The working group will advise on the organisation's policy in the field of administration and protection in personal data processing.

ENNIA also wishes to clarify what personal data it processes in the context of its tasks.

Although ENNIA has a complaints procedure, it does not specifically relate to personal data processing. These Privacy Regulations are a further elaboration of the guarantees regulated by law for persons who wish to safeguard their interests and expressly assigns the implementation of that law to ENNIA's organisation.

These Privacy Regulations set out the rules that ENNIA observes in personal data processing in the context of its operations. These Privacy Regulations provide for a statement related to data processing acts that are necessary for the staff records.

### **Per Article**

#### **Article 1**

Article 1 explains a number of terms that are used in these Privacy Regulations. Where necessary, these Privacy Regulations have been based on the legal statutory terminology. The Controller is ENNIA when it processes personal data. The Administrator is in all cases a head of one of ENNIA's departments who is responsible within the organisation and serves as a contact for the personal data processing in question. The department head ensures that only those employees who are in charge of technical maintenance or data processing have access to the personal data in question.

#### **Article 2**

These Privacy Regulations relate to all the personal data processing acts that take place at ENNIA or under ENNIA's responsibility.

#### **Article 3**

Articles 3 to 7 regulate the minimum content of the statements drawn up by ENNIA per data processing act on the grounds of these Privacy Regulations. Article 3 provides that it must be clear in respect of each data processing act which employee is responsible at ENNIA.

#### **Article 4**

In order to protect personal data it is essential to establish the purpose of the data processing, *i.e.* the collection and further use of the data, because that purpose determines the minimum and maximum data that ENNIA may process and for what purpose ENNIA may use those data (limitation of purpose).

ENNIA may not process any more data than is necessary for the purpose. The data may not be excessive, may not be too detailed and must be relevant. ENNIA may not process any data that, due to an error or misunderstanding on the part of the data subject, exceed the data that were requested or that are relevant for the purpose of that request. If it is

unnecessary to process personal data for that purpose, *i.e.* if ENNIA can achieve that purpose by means of a different approach, the data processing is not permitted. The data that ENNIA processes for a specific purpose must be adequate. If ENNIA processes insufficient data to achieve the purpose, that data processing is an unsuitable means of achieving the end, and is therefore not permitted. ENNIA may not commence the collection of data before the purpose of the data collection has been determined. ENNIA may not change the purpose in the interim without a valid reason.

#### Article 5

All personal data processing must have a lawful ground. Briefly stated, at least one of the following grounds must exist:

- a. unequivocal permission of the data subject;
- b. necessity for the performance of an agreement to which the data subject is a party;
- c. necessity to comply with a statutory obligation of the controller;
- d. necessity to protect a vital interest of the data subject; or
- e. necessity to promote a legitimate interest of the Controller, unless the interests or fundamental rights of the data subject prevail. ENNIA must always ensure that there is a valid ground for the processing of personal data.

#### Article 6

By means of this provision ENNIA wishes to clarify on what persons ENNIA processes personal data in performing its tasks.

#### Article 7

The controller must obtain as many personal data as possible from the data subject himself/herself. However, this does not apply if that requires a disproportionate effort of the controller. In light of the number of persons whose personal data ENNIA processes, for instance, it may be impracticable to obtain those data directly from the data subjects.

Paragraph 4 provides that the personal data that ENNIA processes must be relevant and may not be excessive. This means that ENNIA does not process any personal data if ENNIA can also achieve the purpose of the data processing with less intrusion on the data subject's privacy. In many cases it may suffice for ENNIA to have quantitative data at its disposal, whereby the data cannot or can no longer be traced to the person in question. This also means that ENNIA must always wonder whether certain personal data are really necessary for the purpose for which the data are processed.

In paragraph 5 ENNIA regulates that it observes statutory provisions for the processing of special personal data. Special personal data are data regarding a person's religion or personal beliefs, race, political orientation, health and sexual life, and personal data regarding the membership of a trade union. Such data may not be processed, except for certain exceptions. Those exceptions are the same as those in Sections 17 to 23 of the (Dutch) Personal Data Protection Act, but may also be based on provisions in other Acts.

Caring for the correctness and completeness of personal data, as promoted by paragraph 8, is also important in carefully handling personal data. That way ENNIA cannot draw any incorrect conclusions from certain data.

#### Article 8

ENNIA attaches great importance to correct personal data processing within its organisation, in accordance with the applicable statutory provisions. By setting up a working group that can advise ENNIA's management board on request and of its own accord about all policy aspects related to privacy with which ENNIA is faced, ENNIA believes it can introduce a safeguard in its organisation.



The working group consists of employees with different expertise. This means that the legal, organisational and security aspects of personal data processing will form part of its advice.

Employees of ENNIA must assist the members of the working group and cooperate in any questions and investigations of the working group. The members of the working group obviously do not actually inspect personal data in order to perform their tasks.

#### Article 9

ENNIA may not retain personal data any longer than is necessary for the purpose for which ENNIA collects or processes the data. ENNIA may, however, retain certain data e.g. on the grounds of the law. This particularly applies, for instance, to statutory provisions regarding the storage of records. Data may also be kept without being processed any longer. Destruction of data usually means the physical destruction of the data carriers on which they are recorded or the deletion of data on data carriers.

#### Article 10

The access to personal data must be properly arranged and forms part of the manner in which ENNIA has organised the protection of personal data files. Only persons who are required to cooperate on the grounds of their position and tasks at ENNIA have access to certain personal data. ENNIA must ensure that employees cannot gain access to personal data if they have no business doing so. That will usually be done by securing the access to automated systems using passwords and other automation measures. However, the physical locking of cabinets and files are also among the measures that must be taken to protect personal data. Article 12 of these Regulations addresses this issue.

Article 10 primarily regulates the parties to which and the cases in which ENNIA provides personal data.

Article 21 of the BES Health Insurance Decree provides that ENNIA must provide the organisations named in that decree with all the information and data that are necessary for the implementation of the BES Health Insurance Decree. Article 21(1) of the BES Health Insurance Decree also classifies personal data as defined in the BES Personal Data Protection Act as such data. On the ground of that provision, ENNIA can provide personal data if that is necessary for the implementation of the BES Health Insurance Decree.

Data that ENNIA retains in the context of records management may be inspected only by persons who have access to those data on the grounds of statutory provisions. Data from the records may also be retrieved in the event of legal proceedings (disputes).

#### Article 11

Personal Data are collected for a specific purpose. In principle, they may not be used for any purpose other than that for which they were collected. That is permitted, however, if their use for another purpose is not incompatible with the original purpose. It depends on a number of factors whether further processing is incompatible. One of those factors is the expectation that the data subject has of the use of his or her personal data. Another factor is the degree of connection between the original purpose and the purpose of the further processing. The closer those purposes are connected, the more likely it is that further processing is compatible with the purpose for which the data were collected.

The nature of the data is also important. The more sensitive the data, the less likely it is that the data may also be used for another purpose. Name, address and place of residence data, for instance, may be used for another purpose more easily than salary data.

The consequences of the proposed processing (or further processing) for the data subject are also relevant. If those consequences would mean that a certain decision is made about

the data subject, incompatibility is likely. For instance, a medical expenses insurer who has obtained data about the data subject may not use those data in deciding whether or not to enter into a life insurance agreement with the data subject.

#### Article 12

In the protection plan the controller must state not only how the processed personal data are technically protected, but also how they are physically protected. An example is the use of shredders and locked cabinets, but also, for instance, rules about providing information by telephone, if necessary. The controller must implement the provisions of the protection plan.

#### Article 13

The legal principle is full openness regarding all processing that takes place. This Article prescribes that if the data subjects are not yet aware of the data processing, they must be actively informed about its purposes.

The controller may assume after the information has been sent or presented that the data subjects have been informed.

It does not suffice that the data subjects could reasonably have been informed, for instance because it could be established by means of an investigation who the controller is and for what purposes the data are being processed. An express reference by the controller to information that is available elsewhere is also insufficient.

Further information must be provided if that is necessary in relation to the data subject in order to safeguard proper and careful data processing. Whether that is the case depends on the nature of the data, the circumstances in which they are or have been obtained, and the use made of those data. The more sensitive those data are for the data subject, the more reason there is to inform the data subject in detail about the data processing.

If the data are obtained from the data subject himself/herself, the controller must inform the data subject before obtaining the data. That information can be included, for instance, on the form to be completed by the data subject.

#### Article 14

This Article sets out a number of general rights of persons whose data ENNIA processes. Those rights are recorded in Articles 16 to 20 and are without prejudice to the statutory rights of the data subjects.

#### Article 15

Data subjects may at any time, at reasonable intervals, file a request with ENNIA to inspect the data that ENNIA processes on them. If ENNIA receives such a request, it must help the data subject to formulate his or her request and provide information on his or her rights.

#### Article 16

If ENNIA receives an application to inspect data, it may refuse such inspection (in full or in part) on the grounds of exceptional circumstances, for instance because such inspection would infringe the privacy of other persons.

#### Article 17

In addition to correction, supplementation and removal, "correction" also means protection or ensuring in some manner that the incorrect data are no longer used. If it is technically impossible to correct the data, for instance because they are stored on a CD-ROM, the administrator can, for instance, include a file containing supplementations and corrections on behalf of the controller.

### Article 18

In a number of cases the data subject may object to a data processing act. The BES Personal Data Protection Act refers to that right as the right of objection.

The data subject has a relative right of objection if the processing of his or her personal data takes place on the grounds that it is necessary with a view to a legitimate interest of the controller. That objection must be respected if special personal circumstances of the data subject outweigh the controller's interest.

The data subject has an absolute right of objection if the processing of his or her personal data takes place for direct marketing purposes. In that case ENNIA must definitely put an end to the processing.

Incidentally, a situation in which ENNIA processes personal data for direct marketing purposes is not at issue. However, that situation might arise when data are passed on to third parties for direct marketing purposes. ENNIA may do so only with the express permission of the data subjects.

### Article 19

ENNIA has a complaints procedure. That complaints procedure applies if anyone files a complaint with ENNIA regarding the manner in which ENNIA processes personal data or implements these Privacy Regulations. After the complaint has been handled, the complainant can apply to the national ombudsman.

A data subject from Bonaire, Sint Eustatius and Saba can also directly apply to the BES Personal Data Protection Supervision Committee under the BES Personal Data Protection Act.

Incidentally, a data subject who receives an unwelcome decision from ENNIA in response to a request or an objection may object to that decision and, if necessary, file an appeal with the court.