Rinus Football Data Processing Agreement v1. (hereinafter: “DPA”)

Article 1: Definitions

In addition to the definitions set out in the TCs, the following definitions apply to the DPA:

a. Data Subject, Data Processor, Third Party, Personal Data, Processing of Personal Data, Data Protection Impact Assessment and Data Controller: the descriptions referred to in the GDPR.
b. Data Breach: a Personal Data Breach, as referred to in Article 4(12) of the GDPR.
c. Subprocessor: the party engaged by the KNVB as subprocessor as well as any party engaged by a Subprocessor for the Processing of Personal Data under the DPA and the Agreement.

Article 2: Subject and instructions under the DPA

1. The DPA applies to the Processing of Personal Data in connection with the performance of the Agreement.
2. The Customer instructs the KNVB to Process Personal Data for the purpose of performing the Agreement.

Article 3: Division of roles

1. With regard to the Processing of Personal Data on its behalf, the Customer is the Data Controller and the KNVB is the Data Processor for the Data Controller in relation to the Services. The KNVB does not make independent decisions about the Processing of Personal Data for (other) purposes, including the provision thereof to Third Parties and the duration of the storage of Personal Data. The control over Personal Data provided to the KNVB by the Data Controller under the DPA or other agreements between the Parties, as well as over the data processed by the KNVB in that context, rests with the Data Controller. Consequently, the Data Controller has and retains independent control over the purpose and means of the Processing of Personal Data.
2. The KNVB will ensure that the Data Controller is sufficiently informed about the Service(s) it provides and the activities to be carried out in this regard prior to the conclusion of the DPA.
3. The Parties will provide each other with all the necessary information so as to allow proper compliance with the relevant privacy laws and regulations. If the KNVB reasonably suspects that the Data Controller’s instructions are contrary to statutory provisions on the Processing of Personal Data, the KNVB will immediately inform the Data Controller of this in writing.
4. Upon request, the KNVB will provide assistance to the Data Controller in the event that a Data Protection Impact Assessment is carried out. If the KNVB incurs any reasonable costs in doing so, it will be allowed to invoice Data Controller for these at its then current standard consultancy rates.

Article 4: Use of Personal Data

1. The KNVB undertakes not to use the Personal Data obtained from the Data Controller for any other purposes or in any other way than for the purpose of the Services. The KNVB is therefore not permitted to carry out any other processing with regard to the Personal Data than that which the Data Controller has instructed the KNVB (either in writing or electronically) to carry out under the DPA. This obligation applies both during the term of the DPA and after its expiry.
2. An overview of the categories of Data Subjects, the types of Personal Data, the background, the purpose and the duration of the Processing Operations is provided in Annex 1.
3. The KNVB will refrain from providing Personal Data to a Third Party, unless this exchange takes place on the written instructions of the Data Controller or if this is necessary to fulfil a statutory obligation of the KNVB. In case of a statutory obligation, the KNVB will verify the basis of the request and the identity of the applicant prior to providing the information. In addition, the KNVB will inform the Data Controller - if permitted by law and if possible - prior to the provision.
4. The KNVB and all staff acting under its authority have access to Personal Data only to the extent necessary for the performance of their duties.
5. Intellectual property rights or similar claims that rest on the Personal Data or that arise as a result of and in connection with the processing of Personal Data by the KNVB on the instructions of the Data Controller under the DPA are and remain the property of the Data Controller.
6. In the event that the KNVB also processes Personal Data for the KNVB's own purposes or on behalf of Parties other than the Data Controller and other than under the DPA, the KNVB will ensure that the Processing of Personal Data on behalf of the Data Controller is carried out separately and in a protected manner, unless the Data Controller has granted written permission to make an exception. Furthermore, the KNVB will ensure that Personal Data processed on behalf of the Data Controller is not used in any way for or combined with Personal Data processed for the KNVB's own purposes or processed on behalf of Parties other than the Data Controller, unless the Data Controller has granted written permission for this.

Article 5: European Economic Area

1. The KNVB is permitted to store Personal Data in countries within the European Economic Area (hereinafter referred to as the "EEA").
2. Personal Data could only be transferred by the KNVB to a country outside the EEA, where:

i. this transfer of Personal Data is required based on the documented instructions of the Data Controller for the purpose of performing the services under the Agreement, given that these instructions are permitted by Union and Member State law; and

ii. is in accordance with the requirements for the transfer of Personal Data outside the EEA based on the GDPR.

The assessment whether the transfer of Personal Data outside the EEA is allowed under the GDPR and/or other applicable laws and regulations, should be assessed by and is the sole responsibility

of the Data Controller. Notwithstanding the notification duty of the KNVB pursuant to Article 28(3) of the GDPR, the KNVB is not obliged to verify whether the intended transfer is in accordance with the GDPR and/or any other applicable laws and regulations. Transferring Personal Data outside the EEA is also possible if it is required to do so by Union or Member State law to which the KNVB is subject; in such a case, the KNVB shall inform the Data Controller of that legal requirement before processing, unless that law prohibits such information on important grounds of public interest.

Article 6: Confidentiality

1. The KNVB will ensure that it and anyone else involved in the Processing of Personal Data, including its staff, representatives and/or a Subprocessor, treats this data confidentially. The KNVB ensures that a confidentiality agreement or clause is concluded with anyone involved in the Processing of Personal Data.
2. The obligation of confidentiality referred to in this article does not apply:

- to the extent that the Data Controller has explicitly given permission to provide the Personal Data to a Third Party;
- if the provision of the Personal Data to a Third Party is necessary in view of the nature of the services to be provided to the Data Controller by the KNVB; or
- if there is a statutory obligation to provide the Personal Data to a Third Party.

Article 7: Security and control/audit

1. The KNVB, as well as the Data Controller, will take appropriate technical and organisational measures to protect Personal Data against loss or any form of unlawful Processing of Personal Data. These measures will ensure an appropriate level of protection, taking into account the state of the art, the costs involved in the implementation of the measures, the risks involved in the Processing of Personal Data and the nature thereof.
2. The measures referred to in Article 7.1 will in any event include:

- measures that guarantee that only authorised staff have access to the Personal Data processed under the Agreement;
- measures to protect Personal Data against, in particular, accidental or unlawful destruction, loss, accidental alteration, unauthorised or unlawful storage, access or disclosure;
- measures that identify the weaknesses with regard to the Processing of Personal Data in the systems that are used for the provision of services under the DPA;
- an appropriate information security policy for the Processing of Personal Data.

3. The KNVB will evaluate and tighten, supplement or improve the information security measures it has taken insofar as the requirements or (technological) developments give cause to do so.
4. Annex 2 lays down the arrangements made between the Parties about the technical and organisational security measures, as well as about the content and frequency of the reports that

the KNVB provides to the Data Controller about the security measures. These measures are an extension of the security measures that the Data Controller must take.

5. The KNVB enables the Data Controller to fulfil its statutory obligation to supervise the KNVB's compliance with the technical and organisational security measures as well as the fulfilment of the obligations with regard to Data Breaches referred to in Article 8. In addition to reports by the KNVB, this can be done on the basis of a valid certification or any equivalent means of verification or proof.
6. In addition to Article 7.5, the Data Controller is at all times entitled, in consultation with the KNVB and with due observance of a reasonable period of time, to have the technical and organisational security measures taken by the KNVB tested at its own expense by an independent Register EDP Auditor. The Parties may agree that the audit is carried out by a certified and independent auditor engaged by the KNVB, who will issue a third-party statement (TPM). The Data Controller will be immediately informed of the results of the audit.
7. The Parties will consult each other on the findings of the audit report at their earliest convenience. The Parties will implement the measures for improvement suggested in such report insofar as they can be reasonably expected to do so. The KNVB will implement the proposed measures for improvement insofar as it feels these are appropriate, taking into account the processing risks associated with its product or service, the state of the art, the costs of implementation, the market in which it operates, and the intended use of the Website. The KNVB will be entitled to invoice Data Controller at its then current standard consultancy rates for any costs it incurs for facilitating the audit and/or in implementing the measures referred to in this article.

Article 8: Data Breaches

1. The KNVB has an appropriate policy in place for dealing with Data Breaches, which policy has been communicated to everyone involved in the Processing of Personal Data at the KNVB.
2. If the KNVB or the Data Controller identifies a Data Breach, it will immediately inform the other Party. In the event of a Data Breach, the KNVB will provide the Data Controller with all relevant information relating to the Data Breach, including information about any developments concerning the Data Breach, and the measures that the KNVB takes to limit the consequences of the Data Breach on its part and to prevent recurrence. The KNVB will also provide all the information that the Data Controller deems necessary to be able to assess the incident. The information to be provided to the Data Controller by the KNVB is described in Annex 3.
3. In addition, Parties will inform each other immediately if the security breach is likely to have adverse consequences for the privacy of the Data Subjects referred to in Article 34(1) of the GDPR.
4. In the event of a Data Breach, the KNVB will enable the Data Controller to take or have a third party take appropriate follow-up steps with regard to the Data Breach. In doing so, the KNVB must seek to link up with the existing processes that the Data Controller has set up for this purpose.

The Parties will take all reasonably necessary measures as soon as possible to prevent or limit (further) violations or infringements relating to the Processing of Personal Data, and more specifically (further) violations of the GDPR or other regulations relating to the Processing of Personal Data.

5. In the event of a Data Breach, the Data Controller will fulfil any statutory reporting obligations. At the request of the Data Controller, the KNVB can assist and advise the Data Controller in this respect. The Parties may determine in mutual consultation whether and, if so, how, the KNVB can notify the Dutch Data Protection Authority. If required by law, the Data Controller will inform the Data Subjects about such an infringement. If the KNVB incurs any reasonable costs in doing so, it will be allowed to invoice Data Controller for these at its then current standard consultancy rates.

Article 9: Procedure for Data Subjects

1. A complaint or request from a Data Subject, including a request to exercise the Data Subject's rights as referred to in the GDPR, with regard to the Processing of Personal Data will be immediately forwarded by the KNVB to the Data Controller, which is responsible for handling the request.
2. Insofar as reasonably possible, the KNVB will cooperate fully with the Data Controller in order to fulfil the obligations under the GDPR with regard to the rights of the Data Subject set out in Articles 15, 16, 17, 18, 20 and 21 of the GDPR within the statutory periods of time. If the KNVB incurs any reasonable costs in doing so, it will be allowed to invoice Data Controller for these at its then current standard consultancy rates.
3. The Parties can determine whether and, if so, how the KNVB can handle a complaint or a request from a Data Subject as referred to in Article 9.1 on behalf of the Data Controller.

Article 10: Engaging a Subprocessor

1. Where the KNVB engages Subprocessors, it ensures that they are bound by at least the same conditions with regard to the Processing of Personal Data as stated in the DPA. The KNVB reserves the right to switch to another Subprocessor if it sees reason to do so, and the Data Controller gives permission to this in advance. The KNVB will inform the Data Controller of this in good time. If the Data Controller has objections to the new Subprocessor, it can make its objections known to the KNVB within 30 days of notification. The Parties will then enter into consultation about the most suitable solution. Appendix 1 contains a list of the current Subprocessors appointed by the KNVB.

2. The KNVB will contractually oblige each Subprocessor to process Personal Data only in accordance with and during the DPA.

3. At the request of the Data Controller, the KNVB will provide the following information about each Subprocessor:

a) the name and address details of the Subprocessor;

b) the services for which the Subprocessor carries out activities and the activities carried out;
c) information on information security at the Subprocessor;
d) information about the manner in which the KNVB has arranged with the Subprocessor that the latter must comply with the DPA;
e) information on an appropriate policy of the Subprocessor regarding the handling of Data Breaches.

4. The KNVB remains responsible and liable for the actions of the Subprocessors engaged by the KNVB with due observance of the other provisions of the DPA.

Article 11: Retention periods and destruction of Personal Data

1. The Data Controller will duly inform the KNVB about (statutory) retention periods that apply to the Processing of Personal Data and ensure that Personal Data that no longer needs to be stored is deleted. Upon request, the KNVB will provide assistance to the Data Controller in the event that Personal Data that no longer needs to be stored has to be deleted. If the KNVB incurs any reasonable costs in doing so, it will be allowed to invoice Data Controller for these at its then current standard consultancy rates.
2. The Data Controller obliges the KNVB to destroy the Personal Data processed on the instructions of the Data Controller upon termination of the Agreement, unless the Personal Data has to be stored for a longer period of time, as part of (statutory) obligations or at the request of the Data Controller, for example. The Data Controller may check or have a third party check at its own expense whether destruction has taken place.
3. The KNVB will confirm to the Data Controller (in writing or electronically) that the processed Personal Data has been destroyed.
4. The KNVB will notify all Subprocessors involved in the Processing of Personal Data of any termination of the Agreement and will guarantee that all Subprocessors destroy or have a third party destroy the Personal Data.

Article 12: Inconsistency and amendment to the DPA

1. In the event of any conflict between the provisions of the DPA and the provisions of the Agreement, the provisions of the DPA will take precedence.
2. In the event of significant changes to the product and/or the (additional) services that affect the Processing of Personal Data, the KNVB will inform the Data Controller of the possible consequences of these changes. Significant changes are in any case understood to mean the following: the addition of or modification to a functionality that leads to an expansion with regard to the Processing of Personal Data, the purposes for which the Personal Data is processed and the engagement of a (different) Subprocessor. A change is only legally valid if and insofar as it is agreed in accordance with Article 15.1.

3. If regulations change or if the interpretation of regulations changes, the Parties will consult with each other to determine the effect of this change on the DPA and, if necessary, to amend or supplement the DPA in accordance with Article 15.1.
4. In the event that any provision of the DPA is or becomes void, voidable or otherwise unenforceable, the remaining provisions of the DPA will remain in full force and effect. In that case, the Parties will consult with each other to replace the void, voidable or otherwise unenforceable provision by an enforceable alternative provision. In doing so, the Parties will as much as possible allow for the purpose and purport of the invalid, voidable or otherwise unenforceable provision.

Article 13: Liability

1. If the KNVB fails to fulfil its obligations under the DPA, the Data Controller may hold the KNVB liable for this. If Data Controller fails to fulfil its obligations under the DPA, the KNVB may hold the Data Controller liable for this.
   Provided that, the Parties' liability and indemnification obligations under the DPA shall be fully subject to the limitations of liability set forth in the Agreement.

Article 14: Duration and termination

1. The term of the DPA is equal to the term of the Agreement concluded between the Parties.
2. The DPA ends by operation of law upon termination of the Agreement.
3. The Parties are not permitted to terminate the DPA prematurely.
4. Upon termination of the DPA on whatever grounds or in whatever manner, the KNVB will, at the Data Controller's request:

- make all Personal Data and other data to which the Data Controller is entitled available to the Data Controller in a commonly used machine-readable format;
- immediately suspend the Processing of Personal Data;
- permanently remove all Personal Data from data storage media in such a manner that it can no longer be used or is no longer accessible to the KNVB and third parties unless the Personal Data must be kept for a longer period of time pursuant to a statutory obligation of the KNVB or at the Data Controller's request. As soon as the statutory obligation of the KNVB to keep the Personal Data for a longer period of time has ended, the KNVB will remove all Personal Data from data storage media in such a manner that it can no longer be used or is no longer accessible to the KNVB and third parties.

5. The KNVB will notify all Subprocessors involved in the Processing of Personal Data of any termination of the DPA and will guarantee that all Subprocessors accept with the consequences as described in Article 14.4.
6. At the Data Controller's request, the KNVB will confirm in writing that all the obligations under this article have been fulfilled and will, where applicable, inform the Data Controller in writing of its

statutory obligations or those of a Subprocessor on the basis of which Personal Data must be retained for a longer period.

7. The KNVB is entitled to invoice its reasonable costs regarding the implementation of Articles 14.4, 14.5 and 14.6 at its then current standard consultancy rates.
8. The Data Controller can, at its own expense, have a check carried out to see whether destruction has taken place. The costs of such a check will be payable by the KNVB if it transpires that destruction has not taken place or has not taken place correctly.
9. The termination of the DPA will not relieve the Parties of their obligations under the DPA that by their nature are deemed to continue to apply after termination.

Article 15: Other provisions

1. Amendments and additions to the DPA will only be valid if and insofar as they are agreed in writing between the Parties.
2. The Annexes to the DPA form an integral part of the DPA.
3. The Parties acknowledge that the applicability of their own (purchase or sales/delivery) conditions or other conditions is explicitly excluded and accept the provisions of the DPA explicitly and exclusively with regard to the Processing of Personal Data.
4. The Parties are not entitled to transfer rights and obligations under the DPA to a third party in whole or in part without the prior written permission of the other Party.
5. The DPA supersedes all previous processing agreements between the Parties.
6. The DPA and its performance are governed by the laws of the Netherlands. Any and all disputes and agreements that may arise between the Parties in connection with the DPA and its performance will be brought before the competent Court of Midden-Nederland (location: Utrecht).

Annex 1.

Description of the categories of Data Subjects, the types of Personal Data processed for each service, the background, the purpose and the duration of the Processing Operations and Subprocessors:

A. General information

Name of product and/or service	: KNVB – Rinus Football
Name of Processor and location details	: KNVB, Woudenbergseweg 52-56, Zeist
Concise explanation and operation of product and service	: Digital Trainer Platform
Link to supplier and/or product page	: www.rinusfootball.com
Target Group	: (con)federations
Users	: Authorised persons of the (con)federations

B. Purposes of data processing

The KNVB is a supplier of a digital product and/or digital service. In the context of these products and services, the following applies:

Applicable		Purpose
X	A	The following possible purposes of data processing in the context of these products and services apply: • Provide coaches with high-quality training programmes; • Connect all coaches to a national football methodology; • Combine Rinus Football with coach education; • Provide a solid foundation for player development; • Create a national database of coaches; • Communication with (con)federations.
X	B	The delivery of / ability to use Digital Information Resources in accordance with the arrangements made between the (con)federation and the Supplier.
X	C	Obtaining access to the Digital Service offered, including identification, authentication and authorisation.
X	D	The security, control and prevention of misuse and improper use, and the prevention of inconsistency and unreliability in the Personal Data Processed using the Digital Service.
X	E	The continuity and proper operation of the Digital Service in accordance with the arrangements made between the (con)federation and the Supplier, including having maintenance carried out, making a back-up, making

		improvements after errors or inaccuracies have been detected and receiving support.
X	F	Research and analysis based on strict conditions, comparable to existing codes of conduct in the field of research and statistics, for the purpose of (optimising) the process or policy of the (con)federation.
X	G	The (con)federation can make completely anonymised Personal Data available for research and analysis purposes in order to improve the quality of the sport.
X	H	Making Personal Data available to the extent necessary to comply with legal requirements for Digital Resources.

The diagram included under D shows for each module which Personal Data is Processed (included under C) and for which purposes (included under B).

C. Categories and types of Personal Data

The KNVB specifies below the categories of Personal Data that may (optionally or otherwise) be processed by the KNVB.

1. Description of the categories of Data Subjects about whom Personal Data is Processed and the categories of Personal Data of the Data Subjects

Applicable	Category	Explanation
X	1. Contact details	surname, first names, initials, email
X	2. Sports association participant number	an administration number that identifies sport participants
X	3. (Con)federation	data relating to the organisation and provision of matches and training sessions
X	4. Image material	photographs and video footage, with or without sound, of activities of the (con)federation
X	5. Other data, namely ….	data other than that referred to in points 1 to 4 whose processing is required by or necessary for the purposes of another law. However, the data in question must be specified.

2. Type of Personal Data

a. The KNVB ~~does/~~does not* process special Personal Data.

b. The KNVB ~~does/~~does not* process sensitive Personal Data.

3. Specific retention periods of Personal Data to be used by the KNVB (or assessment criteria for determining this)

Category of Personal Data	Retention period or assessment criterion
Contact details	Up to 12 months after the end of the contract
Sports association participant number	Up to 12 months after the end of the contract
Etc.	Up to 12 months after the end of the contract

*The basic principle remains that the (con)federation must not keep personal data for longer than necessary for the purpose of processing.

D. Details of Personal Data Processing and purposes per purchased module

Below the function for which and module in which this Personal Data is Processed in the context of KNVB - Rinus Football, and on the basis of which of the above-mentioned this occurs, are specified for each category of Personal Data:

Category of Personal Data (1 to 4): 1. Contact details

Purchased module	Function	Product reference	Purpose
Basic Rinus Football	Digital trainer platform	KNVB - Rinus Football	A
Drawing module	Creating own training sessions	KNVB - Rinus Football + Drawing module	A
Match module	Add team line-up	KNVB - Rinus Football + Match module	A

Category of Personal Data (1 to 4): 2. Sports association participant number

Purchased module	Function	Product reference	Purpose
Basic Rinus Football	Digital trainer platform	KNVB - Rinus Football	A
Drawing module	Creating own training sessions	KNVB - Rinus Football + Drawing module	A

Category of Personal Data (1 to 4): 3. (Con)federation

Purchased module	Function	Product reference	Purpose
Basic Rinus Football	Digital trainer platform	KNVB – Rinus Football	A
Drawing module	Creating own training sessions	KNVB - Rinus Football + Drawing module	A

Match module	Add team line-up	KNVB - Rinus Football + Match module	A

Category of Personal Data (1 to 4): 4. Image material

Purchased module	Function	Product reference	Purpose
Basic Rinus Football	Digital trainer platform	KNVB – Rinus Football	A
Drawing module	Creating own training sessions	KNVB - Rinus Football + Drawing module	A

E. Subprocessors

At the time of entering into the Processing Agreement, the KNVB uses the following Subprocessors:

Name + location	Description of task/service	Country of storage + Processing
.....	Web hosting	

F. Contact details

For questions or comments about this leaflet or the operation of this product or service, please contact: Joeri Houniet via info@rinusfootball.com.

G. Version

Version 1 – 1 February 2021

Annex 2. Security

Description of the measures referred to in Article 7

I. Description of the measures to guarantee that only authorised staff have access to the Personal Data Processing.

The KNVB has an internal privacy and ICT policy. This internal ICT and privacy policy (hereinafter referred to as 'policy') serves as a guideline for the way in which its organisation deals with Personal Data. This policy has been drawn up by the KNVB partly as a handle on the use of Personal Data, but also to demonstrate to the outside world that the KNVB handles Personal Data with care.

Below the (groups of) employees of the KNVB who have access to which Personal Data are specified, including a description of the operations that these employees are authorised to perform with the Personal Data.

Groups of employees and Personal Data	Operations
Primary help desk, employees of the local support department act as the point of contact. They answer 'basic questions', refer people elsewhere and, if necessary, report substantive questions.	End-user support.
Secondary help desk, employees of the KNVB support department answer both basic and substantive questions from the primary help desk, analyse and solve incidents, and provide feedback to the primary help desk.	Support of the primary help desk.
Tertiary support, employees of the KNVB support department and R&D are the experts and/or the developer of the application. They provide support in the analysis of incidents and their resolution, and also provide feedback to the secondary help desk.	Analysing the incident.
Analysts / experts in the field of development of the product have access to anonymised sets of results of use of the product, any problems/errors during use.	Analysis of the use, aimed at improving the functionality, development and optimisation of detection and improvement of errors in the operation of the product.

IT database administrators have access to the databases. They may include Subprocessors.	The operations of IT database administrators are aimed at continuity and optimisation of ICT systems.

II. Description of the measures to protect the Personal Data against accidental or unlawful destruction, accidental loss or alteration, unauthorised or unlawful storage, Processing, access or disclosure.

The KNVB has the Certification Scheme with AIC (Availability, Integrity and Confidentiality) classification as an assessment framework and for creating a solid basic level of information security and privacy for its products and services.

Below are the report of the AIC classification, the degree of compliance and the explanation of any deviations from the standards.

Assessment form	Self-assessment		
Assessment performed by	KNVB		
AIC Classification	[Availability = 1, Integrity = 1, Confidentiality = 2		
Category	Measures	Compliance	Explanation
		[Completed/ not completed/alt ernative measure]	[If not completed, indicate how/when this will be corrected. In case of alternative measure, describe it]
Availability	Overload	Completed	
	Business continuity	Completed	
	Design	Completed	
	Monitoring	Completed	
	Testing	Completed	
	Software	Completed	
	Current threats	Completed	
Integrity	Traceability (users)	Completed	
	Backup	Completed	
	Application controls	Completed	
	Irrefutability of data	Completed	
	Traceability (technical management)	Completed	
	Integrity check	Completed	
	Irrefutability of application	Completed	
	Current threats	Completed	

Confidentiality	Data life cycle	Completed	
	Logical access	Completed	
	Physical access	Completed	
	Network Access	Completed	
	Separation of environments	Completed	
	Transport and physical storage	Completed	
	Logging	Completed	
	Review	Completed	
	Current threats	Completed	

Organisation of information security and communication processes

- The KNVB has an active information security policy in place.
- The KNVB has an information security coordinator (security officer) to identify risks relating to the Personal Data Processing, promote security awareness, monitor facilities and take measures to ensure compliance with the information security policy.
- The KNVB has set up a process for communicating about information security incidents.

Staff

- Non-disclosure agreements are concluded with staff and information security arrangements are made.

III. Description of the measures to identify vulnerabilities with regard to the Personal Data Processing in the systems used for the provision of the services to the (con)federation.

To secure the data of the users in a correct way, several measures are applied within the organisation that are in line with the certification schedule for information security.

- These can be technical measures, such as the use of Secure Socket Layer on the websites where the service is made available. The R&D department ensures that these security measures are properly implemented and are up to date.
- Another way to protect users' data is to restrict access to the data. Staff only have access to the systems and data required to do their jobs. Access can also be obtained by requesting a temporary password after permission from the (con)federation and the manager.

- In addition to authorisation, jobs have been explicitly separated. Access is based on verified authorisation, making it possible to trace exactly who has been granted access. In this way, abuse and/or fraud with data is kept to minimum.
- The systems of the KNVB are periodically checked against (inter)nationally recognised norms and standards for information security. In addition, the KNVB's security policy provides for internal processes to identify vulnerabilities.

Reporting

The KNVB constantly updates this information and informs the Data Controller about changes in the measures taken to protect Personal Data against misuse via a specific role in the application.
If the Data Controller identifies a security risk, the Data Controller must contact the help desk of the KNVB via info@rinusfootball.com.

Version 1 – 1 February 2021

Annex 3. Data Breaches

If the KNVB or the Data Controller identifies a Data Breach, it will immediately inform the other Party. In the event of a Data Breach, the KNVB will provide the Data Controller with all relevant information relating to the Data Breach, including information about any developments concerning the Data Breach, and the measures that the KNVB takes to limit the consequences of the Data Breach on its part and to prevent recurrence. The KNVB will also provide all the information that the Data Controller deems necessary to be able to assess the incident.

At least the following information will be provided:

- the nature of the infringement;
- the (alleged) cause of the infringement;
- the (as yet known and/or expected) consequences;
- the (proposed) solution;
- the number of Data Subjects whose data is involved in the infringement (if no exact number is known: the minimum and maximum number of Data Subjects whose data is involved in the infringement);
- a description of the categories of Data Subjects whose data is involved in the infringement;
- the type or types of Personal Data involved in the infringement;
- the date on which the infringement took place (if no exact date is known: the period during which the infringement took place);
- the date and time at which the infringement became known to the KNVB or to a third party or subcontractor engaged by it;
- whether the data was encrypted, hashed or otherwise made incomprehensible or inaccessible to unauthorised persons;
- the measures already taken to end the infringement and to limit its effects.

Version 1 - 1 February 2021