SNCB

General Data Protection Requirements for 3rd Parties & Suppliers

SNCB Data Protection Office

Table of Contents

Document Control / Change History 2

Document Referenced 2

Review List 2

1 Introduction 3

2 Data Protection 4

3 Data protection & Confidentiality Requirements 4

4 Data retention Requirements 6

5 Application Development Requirements 7

6 Authentication & Identity Management Requirements 7

7 Incident Response Requirements 7

8 Audit & Inspection Requirements 7

9 Investigation 7

10 Availability Requirements 7

11 Encryption Requirements 7

Appendix A 8

Data Protection Requirements Checklist 8

Data Retention Checklist 11

Appendix B 11

Document Control / Change History

Version	Date	Title	Status
V1.0	12/05/2020	SNCB GDPR Requirements for 3rd Parties & Suppliers	Final

Document Referenced

Ref	Title
DR1.1	SNCB Minimum Security Requirements for 3rd Parties & Suppliers
DR1.2	Cyber- & Information Security Policy

Review List

Name	Date	Version
CISO Office Tim Groenwals Olivier Verack Paul Standaert Lennart Lapage Bouke Stijns Nick van den Bergh Yannick Scheelen	06/05/2020	0.9
DPO Ypto Luc Seyssens	06/05/2020	0.9
DPO SNCB Tim Verdickt	07/05/2020	0.9
SNCB Legal Anaïs Kempeners Gerout Eevers	07/05/2020	0.9

1 Introduction

This document sets out Minimum General Data Protection Requirements to assist "3rd Parties" or "Suppliers" to identify and meet the listed GDPR requirements where applicable to perform or supply professional services, products or solutions to SNCB or to SNCB affiliated Enterprises.
In this document, SNCB will mean SNCB and SNCB affiliated Enterprises.
This document is an addendum that forms an integral part of the RFP with which all suppliers must comply on top of all other MUST HAVES (technical & functional requirements).

Through this requirement document, SNCB wants to maintain its current level of GDPR conformity, avoid compliance breaches and control its threat landscape, while at the same time provide the Supplier with the incentive to successfully fulfil, based upon pricing, the operational parameters set forth herein, the negotiations between the parties and a formal written agreement documenting the parties' relationship.

Purpose

The purpose of this document is to define the minimum General Data Protection requirements for suppliers who wish to provide professional services, products, solutions or support to SNCB. All suppliers awarded a contract to provide such services MUST comply with the minimum data protection requirements set forth in this document. At its discretion, SNCB may require the supplier to implement, comply with, and/or provide proof of one or more of the requirements laid out in this document.

The information provided in this RFP is the most accurate and quantifiable data presently available to SNCB, and is provided solely for the purpose of assisting the Supplier in submitting a proposal. In addition, all information contained in this RFP is confidential, proprietary to SNCB and:

1) shall not be used for any purpose other than in your preparation of the proposal.
2) may only be disclosed to your company's principals, directors, officers and employees on a need-to-know basis relating directly to the suppliers proposal, and only after they have been made aware of and agreed to the confidential nature and restrictions of the information.
3) may not be disclosed to any third party for any reason other than what is provided for herein or as is approved by SNCB in advance in writing.

2 Data Protection

SNCB recognizes the value of personal data and does all it can to protect it. SNCB is legally obliged to inform its customers, employees and suppliers what personal information it collected, for which purpose it uses this data and on what basis, with which parties SNCB shares it and how long it will be processed. SNCB can only process personal data on a lawful basis and for a specific purpose. All processing activities must be documented in the data processing register. SNCB also must inform the data subjects of their rights in relation to their personal data: among others, data subjects have the right to know what information SNCB holds about them, to receive a copy of it, to change incorrect data or have data deleted.

SNCB takes data protection serious and ensures that the personal data of its customer, employees and suppliers is kept secure and is used in compliance with the applicable regulations.

Suppliers MUST demonstrate their ability for complying with the GDPR and their local data protection rules and must demonstrate how they will fulfil their duty to work together with SNCB, or its representatives, so that SNCB can keep complying with the GDPR including its duty report data breaches within the legal time frames, to both the authority and to the involved data subjects if required.

3 Data protection & Confidentiality Requirements

(a) The supplier MUST maintain a policy setting out all rules and responsibilities of its staff and employees, suppliers and contractors in order to achieve and maintain compliance with the GDPR and its local data protection rules

(b) The supplier should provide proof of how the data protection policy is put into practice, e.g., by way of internal guidelines and procedures

(c) The supplier MUST provide proof that it provided its staff and employees with sufficient training to enable them to honour the data protection policy.

(d) The supplier MUST provide:

   a. one single point of contact for SNCB to discuss matters regarding data protection, preferably a DPO

   b. a SPOC and contact procedures to report (24/7) incidents affecting personal data of SNCB employees, clients or suppliers

   c. an exit scenario, describing how SNCB will recover all personal information and how and when the supplier will destroy all personal information afterwards.

(e) The supplier MUST maintain procedures setting out how to:

a. handle data breaches within the legal time frames, including the required notification to SNCB under the DPA, to the data protection authority and the involved data subjects if required

b. keep and maintain a data processing register in accordance with the GDPR.

c. update his incident register.

d. execute DPIA's in its organisation

e. control and log the access to personal information.
Group accounts or predefined application accounts must not be used to access personal data, only personal accounts are allowed to access personal data.

f. keep personal data always up-to-date.

g. guarantee the integrity of the personal data.

h. ensure availability of the personal data.

i. limit the processing of personal data.

j. respect the applicable retention periods for personal data.

k. guarantee the data subject's rights (access, modification, deletion).

l. monitor and assess its own GDPR compliance and that of all suppliers and contractors that process personal data on its behalf.

m. guarantee compliance with all SNCB requirements regarding data protection.

n. execute background checks for staff that will have access to specific categories of personal data.

The supplier MUST be able to provide proof of the existing of these policies or procedures on the fact that these are kept up to date and that they are known by its staff and employees.

(f) The supplier MUST provide support to SNCB in case of:

a. A personal data breach

b. A requirement under the GDPR to fill in a DPIA for the processing activities that the supplier does on behalf of SNCB

c. Any audit SNCB will perform to check the supplier's compliance with the GDPR and these requirements.

(g) The Supplier MUST indicate in their policies the date of the most recent revision.

(h) The Supplier MUST ensure that the SPOC it provides under point (d) has sufficient knowledge and receives sufficient training to enable the SPOC's performance of its duty.

(i) The Supplier MUST hold SNCB Confidential Information in strict confidence and not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.

(j) The Supplier shall use all reasonable efforts to secure and defend any System hosting SNCB Confidential Information against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.

(k) The Supplier shall protect and secure all SNCB Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.

(l) The Supplier shall maintain all copies or reproductions of SNCB Confidential Information with the same security it maintains the originals. At the point in which SNCB Confidential Information is no longer useful for its primary or retention purposes, as specified by SNCB, the Supplier MUST destroy such Data, making it unusable and unrecoverable. SNCB reserves the right to request for the method of data sanitisations or hardware destruction.

(m) For all Application screens, front pages of reports, and landing pages of web Applications that contain Confidential Information, the Supplier MUST include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).

(n) Suppliers development, test and QA environments shall not use real SNCB Confidential Information and shall never run on production systems.

(o) The provider MUST ensure that the policies and processes it puts in place can at least ensure the requirements set out above. If the Supplier cannot make such certification for any reason (e.g. the Supplier's policies do not address an element listed above) at the moment it replies to the RFP, the Supplier MUST notify SNCB of the deficiency in its proposal/response to the RFP.

4 Data retention Requirements

(a) The Suppliers MUST maintain a procedure and the required processes to comply with the retention rules regarding Confidential Information including personal data that ensure that this information will be automatically erased after the pre-set retention period.

(b) Retention requirements for SNCB data may be specified in the RFP or changed by SNCB afterwards, depending on changing legislation or other criteria. If applicable, the Supplier MUST acknowledge in its proposal to the RFP that it can meet the requirements and, upon request by SNCB, demonstrate that retention requirements are being implemented.

(c) Record retention systems MUST comply with all security and data protection controls set forth in this document.

(d) The supplier will provide evidence on procedures for destroying end-of-life storage media. Data will be erased following the SNCB accepted procedures.

5 Application Development Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

6 Authentication & Identity Management Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

7 Incident Response Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

8 Audit & Inspection Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

9 Investigation

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

10 Availability Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

11 Encryption Requirements

For these requirements, SNCB refers to its document:
Minimum Security Requirements for 3rd Parties & Suppliers

Appendix A

Data Protection Requirements Checklist

Req. No	Requirements	Control	Compliant	
PC-01	The supplier MUST have a policy setting out all rules to ensure the supplier's compliance with the GDPR and its local data protection laws.	**MUST**	YES	NO
PC-02	The supplier should provide proof that processes are in place and used that enable the supplier to achieve and maintain GDPR compliance.	**SHOULD**	YES	NO
PC-03	The supplier should provide proof of GDPR data protection awareness campaigns for all staff, including support staff and their suppliers staff.	**SHOULD**	YES	NO
PC-04	The supplier MUST provide: (a) proof of GDPR data protection trainings for their staff, including support and sub supplier staff having access to personal information. (b) one single point of contact to enable SNCB to discuss and obtain all required information regarding the supplier's compliance with the data protection rules and regulations, preferably a DPO. (c) a SPOC and contact procedures to report (24/7) data breaches. (d) an exit scenario, describing how SNCB will recover all personal data and how and when the supplier will destroy all personal data afterwards.	**MUST**	YES	NO
PC-05	The supplier MUST maintain procedures setting out how to: (a) handle data breaches within the legal time frames, including the required notification to SNCB under the DPA, to the data protection authority and the involved data subjects if required (b) keep and maintain a data processing register in accordance with the GDPR (c) update his incident register (d) execute DPIA's in its organisation (e) control and log the access to personal information. Group accounts or predefined application accounts must	**MUST**	YES	NO

	not be used to access personal data, only personal accounts are allowed to access personal data (f) keep personal data always up-to-date (g) guarantee the integrity of the personal data (h) ensure availability of the personal data (i) limit the processing of personal data (j) respect the applicable retention periods for personal data (k) guarantee the data subject's rights (access, modification, deletion, …) (l) monitor and assess its own compliance GDPR and that of all suppliers and contractors that process personal data on its behalf (m) guarantee compliance with all SNCB requirements regarding data protection (n) execute background checks for staff that will have access to specific categories of personal data The supplier MUST be able to provide proof of the existing of these policies or procedures on the fact that these are kept up to date and that they are known by its staff and employees			
PC-06	The supplier MUST provide support to SNCB in case of: (a) A personal data breach (b) A requirement under the GDPR to fill in a DPIA for the processing activities that the supplier does on behalf of SNCB (c) Any audit SNCB will perform to check the supplier's compliance with the GDPR and these requirements.	**MUST**	YES	NO
PC-07	The Supplier MUST indicate in its policies the date of the most recent revision.	**MUST**	YES	NO
PC-08	The Supplier MUST ensure that the SPOC it provides under point (d) has sufficient knowledge and receives sufficient training to enable the SPOC's performance of its duty.	**MUST**	YES	NO
PC-09	The Supplier MUST hold SNCB Confidential Information in strict confidence and not disclose it to any third parties nor make use of such data for its own benefit or for the benefit of another, or for any use other than the purpose agreed upon.	**MUST**	YES	NO
PC-10	The Supplier shall use all reasonable efforts to secure and defend any System hosting SNCB Confidential Information	**MUST**	YES	NO

	against third parties who may seek to breach the security thereof, including, but not limited to breaches by unauthorized access or making unauthorized modifications to such System.			
PC-11	The Supplier shall protect and secure all SNCB Confidential Information in transit (collected, copied and moved) and at rest (stored on the physical servers), including during any electronic data transmission or electronic or physical media transfer.	**MUST**	YES	NO
PC-12	The Supplier shall maintain all copies or reproductions of SNCB Confidential Information with the same security it maintains the originals. At the point in which SNCB Confidential Information is no longer useful for its primary or retention purposes, as specified by SNCB, the Supplier **MUST** destroy such Data, making it unusable and unrecoverable. SNCB reserves the right to request for the method of data sanitisations or hardware destruction.	**MUST**	YES	NO
PC-13	The Supplier must enter into the standard SNCB agreement with SNCB setting out all applicable rules for processing data on SNCB behalf or if the Supplier will act as a separate data controller for receiving data from SNCB and processing data on its own behalf.	**MUST**	YES	NO
PC-14	For all Application screens, front pages of reports, and landing pages of web Applications that contain Confidential Information, the Supplier MUST include prominent confidentiality notices in legible-sized font on each page (e.g. a prominent notice that the information on such screen or report is confidential on the bottom of a web screen or the footer of a report page).	**MUST**	YES	NO
PC-15	Supplier's development, test and QA environments must not use real SNCB Confidential Information and must never run on production systems.	**MUST**	YES	NO

Data Retention Checklist

Req. No	Requirements	Control	Compliant	
DR-01	The Supplier's may be required to support retention of Confidential Information.	**MUST**	YES	NO
DR-02	Retention requirements for SNCB data may be specified in the RFP. If applicable, the Supplier MUST acknowledge in its proposal to the RFP that it can meet the requirements and, upon request by SNCB, or its representatives, demonstrate that retention requirements are being implemented.	**MUST**	YES	NO
DR-03	Record retention systems MUST comply with all security and privacy controls set forth in this document.	**MUST**	YES	NO

Appendix B

Document Name	Copy
Minimum Security Requirements for 3rd Parties & Suppliers	 SNCB Minimum Security Requirements for 3rd Parties Suppliers v1.0.pdf