SNCB

Exigences de la SNCB au regard du RGPD pour les tiers et fournisseurs

SNCB Data Protection Office

Table des matières

Document de contrôle/Historique des modifications

Version	Date	Titre	Statut
V1.0	12.5.2020	Exigences de la SNCB au regard du RGPD pour les tiers et fournisseurs	Version finale

Document référencé

Réf.	Titre
DR1.1	Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs
DR1.2	Politique en matière de cybersécurité et de sécurité de l'information

Liste des révisions

Nom	Date	Version
CISO Office Tim Groenwals Olivier Verack Paul Standaert Lennart Lapage Bouke Stijns Nick van den Bergh Yannick Scheelen	6.5.2020	0.9
DPO Ypto Luc Seyssens	6.5.2020	0.9
DPO SNCB Tim Verdickt	7.5.2020	0.9
SNCB Legal Anaïs Kempeners Gerout Eevers	7.5.2020	0.9

1 Introduction

Le présent document définit les exigences générales minimales en matière de protection des données afin d'aider les « tiers » ou « fournisseurs » à identifier et à respecter les exigences minimales du RGPD énoncées, le cas échéant pour fournir des services, solutions ou produits professionnels à la SNCB ou aux sociétés apparentées à la SNCB.

Dans ce document, SNCB désigne la SNCB et les sociétés apparentées à la SNCB.
Le présent document constitue un addenda qui fait partie intégrante de l'appel d'offres auquel tous les fournisseurs doivent se conformer en plus de tous les autres MUST-HAVES (exigences techniques et fonctionnelles).

À travers ce document qui précise les exigences à respecter, la SNCB entend maintenir son niveau actuel de conformité au RGPD, éviter la violation de règles de conformité et contrôler son paysage des menaces, tout en incitant le fournisseur à satisfaire pleinement, sur la base du tarif convenu, aux paramètres opérationnels définis dans le présent document. La SNCB entend également que ce document serve de base aux négociations entre les parties et à la conclusion d'un accord écrit officiel documentant la relation entre celles-ci.

Objectif

Le présent document a pour but de définir les exigences générales minimales en matière de protection des données pour les fournisseurs désireux d'offrir des services, produits, solutions, services ou soutien professionnels à la SNCB. Tous les fournisseurs bénéficiant d'un contrat de fourniture de services DOIVENT respecter les exigences minimales en matière de protection des données définies dans le présent document. La SNCB peut, à sa discrétion, exiger du fournisseur qu'il mette en œuvre, respecte et/ou prouve qu'il répond à une ou plusieurs exigences définies dans le présent document.

Les informations reprises dans cet appel d'offres sont les données les plus précises et quantifiables dont dispose présentement la SNCB et sont fournies dans l'unique but d'aider le fournisseur à soumettre une proposition. Par ailleurs, toutes les informations reprises dans cet appel d'offres sont confidentielles, constituent la propriété de la SNCB et :

1) ne seront pas utilisées à d'autres fins que l'élaboration d'une proposition ;
2) ne peuvent être divulguées aux directeurs, administrateurs, responsables et collaborateurs de votre entreprise, qu'en vertu du principe du « besoin d'en connaître » en lien direct avec la proposition des fournisseurs, et uniquement après qu'ils ont été sensibilisés et ont accepté la nature confidentielle des informations et les restrictions applicables à ces dernières ;

3) ne peuvent être divulguées à un tiers pour toute raison autre que celles prévues dans le présent ou approuvées au préalable par écrit par la SNCB.

2 Protection des données

La SNCB reconnaît la valeur des données à caractère personnel et met tout en œuvre pour les protéger. La SNCB est tenue légalement d'informer ses clients, collaborateurs et fournisseurs sur les informations à caractère personnel qu'elle recueille, la finalité de l'utilisation qu'elle en fait et la base sur laquelle celle-ci repose, ainsi que sur les parties avec lesquelles elle partage ces données et la durée de leur traitement. La SNCB ne peut traiter des données à caractère personnel que sur une base légale et dans un but spécifique. Toutes les activités de traitement doivent être documentées dans le registre des activités de traitement des données. La SNCB a également l'obligation d'informer les personnes concernées de leurs droits en matière de données à caractère personnel : entre autres le droit de savoir quelles informations la SNCB détient à leur sujet, d'en recevoir une copie, de rectifier des données incorrectes ou d'effacer des données.

La SNCB prend la protection des données au sérieux et veille à ce que les données à caractère personnel de ses clients, collaborateurs et fournisseurs soient conservées en toute sécurité et que leur utilisation soit conforme aux réglementations en vigueur.

Les fournisseurs DOIVENT démontrer leur capacité à se conformer au RGPD ainsi qu'aux règles applicables à l'échelon local en matière de protection des données, et démontrer qu'ils assumeront leur devoir de collaboration avec la SNCB ou ses représentants, permettant ainsi à la SNCB de rester conforme au RGPD, y compris son devoir de communiquer toute fuite de données dans les délais légaux, tant à l'égard de l'autorité compétente que des personnes concernées, le cas échéant.

3 Exigences en matière de protection des données et de confidentialité

(a) Le fournisseur DOIT tenir à jour une politique qui définit l'ensemble des règles et responsabilités de son personnel et de ses collaborateurs, fournisseurs et sous-traitants en vue du respect et du maintien de la conformité au RGPD et ses règles applicables à l'échelon local en matière de protection des données.

(b) Le fournisseur devrait prouver la façon dont il met en pratique sa politique en matière de protection des données, par exemple au moyen de directives et procédures internes.

(c) Le fournisseur DOIT prouver qu'il a dispensé à son personnel et ses collaborateurs une formation suffisante pour leur permettre de respecter la politique en matière de protection des données.

(d) Le fournisseur DOIT prévoir :

a. un point de contact unique à la SNCB, de préférence un DPO, pour examiner des questions relatives à la protection des données ;

b. un SPOC et des procédures de contact pour signaler (24 heures sur 24 et 7 jours sur 7) les incidents affectant les données à caractère personnel des collaborateurs, clients ou fournisseurs de la SNCB ;

c. un scénario de sortie décrivant comment la SNCB récupérera toutes les données à caractère personnel ainsi que comment et quand le fournisseur détruira toutes les informations à caractère personnel après coup.

(e) Le fournisseur DOIT maintenir des procédures fixant la manière de :

a. gérer les fuites de données dans les délais légaux, y compris les notifications requises à la SNCB en vertu du DPA, à l'autorité de protection des données et aux personnes concernées le cas échéant ;

b. tenir et conserver un registre de traitement des données conformément au RGPD ;

c. mettre à jour son registre d'incidents ;

d. réaliser les analyses d'impact (DPIA) au sein de son organisation ;

e. contrôler et enregistrer l'accès aux données à caractère personnel.
Les comptes de groupe ou les comptes prédéfinis dans des applications ne doivent pas être utilisés pour accéder à des données à caractère personnel, seuls les comptes personnels sont autorisés à y accéder.

f. veiller à mettre à jour en permanence les données à caractère personnel ;

g. garantir l'intégrité des données à caractère personnel ;

h. assurer la disponibilité des données à caractère personnel ;

i. limiter le traitement des données à caractère personnel ;

j. respecter les périodes de conservation en vigueur pour les données à caractère personnel ;

k. garantir les droits des personnes concernées (accès, rectification, effacement) ;

l. contrôler et évaluer sa propre conformité au RGPD ainsi que celle de l'ensemble des fournisseurs et entreprises qui traitent des données à caractère personnel pour son compte ;

m. garantir la conformité avec toutes les exigences de la SNCB en matière de protection des données ;

n. vérifier les antécédents du personnel qui aura accès à des catégories spécifiques de données à caractère personnel.

Le fournisseur DOIT être en mesure de prouver à l'aide d'éléments tangibles que ces politiques ou procédures sont mises à jour et connues de son personnel et de ses collaborateurs.

(f) Le fournisseur DOIT apporter son aide à la SNCB dans les cas suivants :

a. une fuite de données à caractère personnel ;

b. une obligation en vertu du RGPD de remplir un DPIA pour les activités de traitement que le fournisseur effectue pour le compte de la SNCB ;

c. tout audit réalisé par la SNCB pour vérifier le respect par le fournisseur du RGPD et de ces exigences.

(g) Le fournisseur DOIT indiquer dans ses politiques la date de la dernière révision.

(h) Le fournisseur DOIT s'assurer que le SPOC qu'il fournit en vertu du point (d) possède des connaissances suffisantes et bénéficie d'une formation suffisante pour lui permettre d'accomplir sa mission.

(i) Le fournisseur DOIT respecter la stricte confidentialité des informations confidentielles de la SNCB et ne pas les divulguer à des tiers, ni les utiliser pour son propre intérêt ou l'intérêt d'autrui ou pour tout autre usage que celui qui a été convenu.

(j) Le fournisseur consentira tous les efforts raisonnables pour sécuriser et protéger tout système hébergeant des informations confidentielles de la SNCB contre des tiers qui pourraient tenter d'en violer la sécurité, y compris, mais sans s'y limiter, les violations par accès non autorisé ou les modifications non autorisées apportées audit système.

(k) Le fournisseur protégera et sécurisera toutes les informations confidentielles de la SNCB qui sont en transit (recueillies, copiées et déplacées) et au repos (stockées sur des serveurs physiques), y compris lors de toute transmission électronique de données ou de tout transfert de support électronique ou physique.

(l) Le fournisseur conservera toutes les copies ou reproductions des informations confidentielles de la SNCB en appliquant le même degré de sécurité que pour les originaux. Au moment où les informations confidentielles de la SNCB n'auront plus d'utilité pour leur but premier ou leur conservation, le fournisseur DOIT, comme spécifié par la SNCB, détruire ces données en les rendant inutilisables ou irrécupérables. La SNCB se réserve le droit de s'enquérir de la méthode de nettoyage des données ou de destruction du matériel.

(m) Pour l'ensemble des écrans d'application, des premières pages de rapports, ainsi que des pages d'arrivée d'applications web qui contiennent des informations confidentielles, le fournisseur DOIT inclure sur chaque page des notifications de confidentialité placées en évidence dans une police de caractères lisible (par exemple, une notification bien visible au bas d'un écran web ou d'une page de rapport indiquant que les informations figurant sur cet écran ou dans ce rapport sont confidentielles).

(n) Les environnements de développement, de test et d'assurance qualité des fournisseurs n'utiliseront pas de véritables informations confidentielles de la SNCB et ne tourneront jamais sur des systèmes de production.

(o) Le fournisseur DOIT s'assurer que les politiques et processus qu'il met en place peuvent au moins garantir le respect des exigences définies ci-dessus. S'il n'est pas en mesure d'apporter cette garantie pour quelque raison que ce soit (par exemple, ses politiques ne reprennent pas un élément énuméré ci-dessus) au moment où il répond à l'appel d'offres, le fournisseur DOIT le notifier à la SNCB dans sa proposition/réponse à l'appel d'offres.

4 Exigences en matière de conservation des données

(a) Les fournisseurs DOIVENT maintenir une procédure ainsi que les processus requis pour se conformer aux règles sur la conservation des données confidentielles, y compris des données à caractère personnel, qui garantissent l'effacement automatique de ces informations après la période de conservation prédéfinie.

(b) Les exigences en matière de conservation des données de la SNCB peuvent être spécifiées dans l'appel d'offres ou modifiées après coup par la SNCB, en fonction d'un changement dans la législation ou d'autres critères. Le cas échéant, le fournisseur DOIT reconnaître dans sa proposition de réponse à l'appel d'offres qu'il est en mesure de satisfaire aux exigences et démontrer, sur simple demande de la SNCB, que les exigences en matière de conservation des données sont mises en œuvre.

(c) Les systèmes de conservation de dossiers DOIVENT se conformer à tous les contrôles de sécurité et de protection des données énoncés dans le présent document.

(d) Le fournisseur apportera une preuve de la mise en place de procédures de destruction des supports de stockage en fin de vie. Les données seront effacées conformément aux procédures approuvées par la SNCB.

5 Exigences en matière de développement d'applications

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

6 Exigences en matière d'authentification et de gestion des identités

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

7 Exigences en matière de réaction aux incidents

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

8 Exigences en matière d'audits et d'inspections

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

9 Enquête

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

10 Exigences en matière de disponibilité

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

11 Exigences en matière de chiffrement

Pour ces exigences, la SNCB renvoie à son document :
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs

Annexe A

Liste de vérification des exigences en matière de protection des données

Exigence N°	Exigences	Contrôle	Conforme	
PC-01	Le fournisseur DOIT disposer d'une politique fixant l'ensemble des règles à suivre pour garantir sa conformité au RGPD, ainsi qu'aux lois applicables à l'échelon local sur la protection des données.	**INDISPENSABLE**	OUI	NON
PC-02	Le fournisseur devrait fournir la preuve de la mise en place et de l'utilisation de processus lui permettant d'atteindre et de maintenir sa conformité au RGPD.	**CONSEILLÉ**	OUI	NON
PC-03	Le fournisseur devrait fournir la preuve qu'il met sur pied des campagnes de sensibilisation au RGPD pour l'ensemble de son personnel, y compris le personnel de soutien et le personnel de ses fournisseurs.	**CONSEILLÉ**	OUI	NON
PC-04	Le fournisseur DOIT prévoir : (a) la preuve qu'il dispense des formations sur la protection des données au regard du RGPD auprès de son personnel, y compris le personnel de soutien et les sous-traitants qui ont accès aux données à caractère personnel ; (b) un point de contact unique (SPOC), de préférence un DPO, pour permettre à la SNCB d'examiner et d'obtenir toutes les informations requises concernant la conformité du fournisseur avec les règles et réglementations sur la protection des données ; (c) un SPOC et des procédures de contact pour signaler (24 heures sur 24 et 7 jours sur 7) les fuites de données ; (d) un scénario de sortie décrivant comment la SNCB récupérera toutes les données à caractère personnel ainsi que comment et quand le fournisseur détruira toutes les informations à caractère personnel après coup.	**INDISPENSABLE**	OUI	NON
PC-05	Le fournisseur DOIT maintenir des procédures fixant la manière de :	**INDISPENSABLE**	OUI	NON

	(a) gérer les fuites de données dans les délais légaux, y compris les notifications requises à la SNCB en vertu du DPA, à l'autorité de protection des données et aux personnes concernées le cas échéant ; (b) tenir et conserver un registre de traitement des données conformément au RGPD ; (c) mettre à jour son registre d'incidents ; (d) réaliser les analyses d'impact (DPIA) au sein de son organisation ; (e) contrôler et enregistrer l'accès aux données à caractère personnel. Les comptes de groupe ou les comptes prédéfinis dans des applications ne doivent pas être utilisés pour accéder à des données à caractère personnel, seuls les comptes personnels sont autorisés à y accéder. (f) veiller à mettre à jour en permanence les données à caractère personnel ; (g) garantir l'intégrité des données à caractère personnel ; (h) assurer la disponibilité des données à caractère personnel ; (i) limiter le traitement des données à caractère personnel ; (j) respecter les périodes de conservation en vigueur pour les données à caractère personnel ; (k) garantir les droits des personnes concernées (accès, rectification, effacement, etc.) ; (l) contrôler et évaluer sa propre conformité au RGPD et celle de l'ensemble des fournisseurs et sous-traitants qui traitent des données à caractère personnel en son nom ; (m) garantir la conformité avec toutes les exigences de la SNCB en matière de protection des données ; (n) vérifier les antécédents du personnel qui aura accès à des catégories spécifiques de données à caractère personnel. Le fournisseur DOIT être en mesure de prouver à l'aide d'éléments tangibles que ces politiques ou procédures sont mises à jour et connues de son personnel et de ses collaborateurs.			

PC-06	Le fournisseur DOIT apporter son aide à la SNCB dans les cas suivants : (a) une fuite de données à caractère personnel ; (b) une obligation en vertu du RGPD de remplir un DPIA pour les activités de traitement que le fournisseur effectue pour le compte de la SNCB ; (c) tout audit réalisé par la SNCB pour vérifier le respect par le fournisseur du RGPD et de ces exigences.	**INDISPENSABLE**	OUI	NON
PC-07	Le fournisseur DOIT indiquer dans ses politiques la date de la dernière révision.	**INDISPENSABLE**	OUI	NON
PC-08	Le fournisseur DOIT s'assurer que le SPOC qu'il fournit en vertu du point (d) possède des connaissances suffisantes et bénéficie d'une formation suffisante pour lui permettre d'accomplir sa mission.	**INDISPENSABLE**	OUI	NON
PC-09	Le fournisseur DOIT respecter la stricte confidentialité des informations confidentielles de la SNCB et ne pas les divulguer à des tiers, ni les utiliser pour son propre intérêt ou l'intérêt d'autrui ou pour tout autre usage que celui qui a été convenu.	**INDISPENSABLE**	OUI	NON
PC-10	Le fournisseur consentira tous les efforts raisonnables pour sécuriser et protéger tout système hébergeant des informations confidentielles de la SNCB contre des tiers qui pourraient tenter d'en violer la sécurité, y compris, mais sans s'y limiter, les violations par accès non autorisé ou les modifications non autorisées apportées audit système.	**INDISPENSABLE**	OUI	NON
PC-11	Le fournisseur protégera et sécurisera toutes les informations confidentielles de la SNCB qui sont en transit (recueillies, copiées et déplacées) et au repos (stockées sur des serveurs physiques), y compris lors de toute transmission électronique de données ou de tout transfert de support électronique ou physique.	**INDISPENSABLE**	OUI	NON
PC-12	Le fournisseur conservera toutes les copies ou reproductions des informations confidentielles de la SNCB en appliquant le même degré de sécurité que pour les originaux. Au moment où les informations confidentielles de la SNCB n'auront plus d'utilité pour leur but premier ou leur conservation, le	**INDISPENSABLE**	OUI	NON

	fournisseur **DOIT**, comme spécifié par la SNCB, détruire ces données en les rendant inutilisables ou irrécupérables. La SNCB se réserve le droit de s'enquérir de la méthode de nettoyage des données ou de destruction du matériel.			
PC-13	Le fournisseur doit conclure avec la SNCB l'accord type fixant toutes les règles applicables concernant le traitement de données pour le compte de la SNCB ou dans le cas où le fournisseur agit en tant que responsable du traitement distinct pour la réception de données de la SNCB et le traitement de données en son propre nom.	**INDISPENSABLE**	OUI	NON
PC-14	Pour l'ensemble des écrans d'application, des premières pages de rapports, ainsi que des pages d'arrivée d'applications web qui contiennent des informations confidentielles, le fournisseur DOIT inclure sur chaque page des notifications de confidentialité placées en évidence dans une police de caractères lisible (par exemple, une notification bien visible au bas d'un écran web ou d'une page de rapport indiquant que les informations figurant sur cet écran ou dans ce rapport sont confidentielles).	**INDISPENSABLE**	OUI	NON
PC-15	Les environnements de développement, de test et d'assurance qualité des fournisseurs n'utiliseront pas de véritables informations confidentielles de la SNCB et ne tourneront jamais sur des systèmes de production.	**INDISPENSABLE**	OUI	NON

Liste de vérification des exigences en matière de conservation des données

Exigence N°	Exigences	Contrôle	Conforme	
DR-01	Le fournisseur peut être sollicité pour permettre la conservation des informations confidentielles.	**INDISPENSABLE**	OUI	NON
DR-02	Les exigences en matière de conservation des données de la SNCB peuvent être spécifiées dans l'appel d'offres. Le cas échéant, le fournisseur DOIT reconnaître dans sa proposition de réponse à l'appel d'offres qu'il est en mesure de satisfaire aux exigences et de démontrer, sur simple demande de la SNCB, ou de ses représentants, que les exigences en matière de conservation des données sont mises en œuvre.	**INDISPENSABLE**	OUI	NON
DR-03	Les systèmes de conservation de dossiers DOIVENT être conformes à tous les contrôles de sécurité et de protection de la vie privée énoncés dans le présent document.	**INDISPENSABLE**	OUI	NON

Annexe B

Nom du document	Copie
Exigences minimales de la SNCB en matière de sécurité pour les tiers et fournisseurs	SNCB Minimum Security Requirements for 3rd Parties Suppliers v1.0.pdf