



NMBS

NMBS AVG vereisten voor Derden & Leveranciers

NMBS Data Protection Office



Inhoudsopgave

Documentcontrole/Historiek van de wijzigingen	2
Document Referenced	2
Reviewlijst	2
1 Inleiding	3
2 Gegevensbescherming	4
3 Vereisten inzake Gegevensbescherming & Vertrouwelijkheid	4
4 Vereisten inzake gegevensbewaring	6
5 Vereisten inzake applicatie-ontwikkeling	8
6 Vereisten inzake Authenticatie & Identiteitsbeheer	8
7 Vereisten inzake Incident Response	8
8 Vereisten inzake Audit & Inspectie	8
9 Onderzoek	8
10 Vereisten inzake Beschikbaarheid	8
11 Encryptievereisten	8
Bijlage A	9
Checklist Vereisten Gegevensbescherming	9
Checklist gegevensbewaring	13
Bijlage B	13

Documentcontrole/Historiek van de wijzigingen

Versie	Datum	Titel	Status
V1.0	12.5.2020	NMBS AVG vereisten voor Derden & Leveranciers	Final

Document Referenced

Ref	Titel
DR1.1	NMBS Minimale Beveiligingsvereisten voor Derden & Leveranciers
DR1.2	Beleid inzake cyber- en informatiebeveiliging

Reviewlijst

Naam	Datum	Versie
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 NMBS Tim Verdickt	7.5.2020	0.9
NMBS Legal Anaïs Kempeners Gerout Eevers	7.5.2020	0.9

1 Inleiding

Dit document bevat de Minimale algemene vereisten voor gegevensbescherming om “Derde partijen” of “Leveranciers” te helpen bij het identificeren van en voldoen aan de vermelde AVG-vereisten, indien van toepassing, voor het presteren of leveren van professionele diensten, producten of oplossingen aan NMBS of aan NMBS gelieerde ondernemingen.

In dit document wordt onder "NMBS" verstaan: NMBS en aan NMBS gelieerde ondernemingen. Dit document is een addendum dat een integraal onderdeel is van de RFP waaraan alle leveranciers moeten voldoen afgezien van alle andere MUST HAVES (technische & functionele vereisten).

Door middel van dit document wil NMBS haar huidige niveau van AVG-naleving handhaven, schendingen van de naleving voorkomen en het risicolandschap beheersen, terwijl tegelijkertijd de Leverancier gestimuleerd wordt om succesvol te presteren op basis van de prijsstelling, de operationele parameters die hierin worden uiteengezet, de onderhandelingen tussen de partijen en een formele schriftelijke overeenkomst waarin de relatie tussen de partijen wordt vastgelegd.

Doel

Het doel van dit document is het definiëren van de minimale algemene vereisten voor gegevensbescherming voor leveranciers die professionele diensten, producten, oplossingen of ondersteuning aan NMBS willen leveren. Alle leveranciers die een contract hebben gesloten voor het leveren van dergelijke diensten **MOETEN** voldoen aan de minimumvereisten voor gegevensbescherming die in dit document vermeld staan. Naar eigen goedgevoelen kan NMBS van de leverancier verlangen dat deze een of meer van de in dit document vermelde vereisten uitvoert, naleeft en/of aantoont.

De informatie in deze RFP vormt de meest nauwkeurigste en kwantificeerbare data waarover NMBS momenteel beschikt en wordt uitsluitend verstrekt om de Leverancier bij het indienen van een voorstel te helpen. Bovendien is alle informatie in deze RFP vertrouwelijk, eigendom van NMBS en:

- 1) mag niet worden gebruikt voor andere doeleinden dan bij het opstellen van uw voorstel ;
- 2) mag alleen worden bekendgemaakt aan de directeuren, managers en werknemers van uw bedrijf op een need-to-know basis direct gerelateerd aan het leveranciersvoorstel, en pas nadat zij op de hoogte zijn gesteld van en akkoord zijn gegaan met de vertrouwelijke aard en beperkingen van de informatie ;
- 3) mag niet worden bekendgemaakt aan derden om een andere reden dan hetgeen hierin is bepaald of zoals vooraf schriftelijk door NMBS is goedgekeurd.

2 Gegevensbescherming

NMBS erkent de waarde van persoonsgegevens en doet al het mogelijke om deze te beschermen. NMBS is wettelijk verplicht haar klanten, werknemers en leveranciers te informeren over de persoonlijke gegevens die ze heeft verzameld, waarvoor ze deze gegevens gebruikt en op welke basis, met welke partijen NMBS deze deelt en hoe lang deze gegevens zullen worden verwerkt. NMBS kan persoonsgegevens alleen op een wettige basis en voor een specifiek doel verwerken. Alle verwerkingsactiviteiten moeten worden gedocumenteerd in het gegevensverwerkingsregister. NMBS moet de betrokkenen ook op de hoogte stellen van hun rechten met betrekking tot hun persoonsgegevens: betrokkenen hebben onder andere het recht te weten welke informatie NMBS over hen heeft, een kopie ervan te ontvangen, onjuiste gegevens te wijzigen of gegevens te laten verwijderen.

NMBS neemt gegevensbescherming serieus en zorgt ervoor dat de persoonsgegevens van haar klanten, werknemers en leveranciers veilig worden gehouden en worden gebruikt in overeenstemming met de toepasselijke regelgeving.

Leveranciers MOETEN aantonen dat ze in staat zijn om de AVG en hun lokale regels voor gegevensbescherming na te leven en moeten aantonen hoe ze hun plicht om samen te werken met NMBS, of haar vertegenwoordigers, zullen vervullen zodat NMBS de AVG kan blijven naleven, inclusief de plicht om data-inbreuken binnen de wettelijke termijnen te melden, zowel aan de autoriteit als aan de betrokkenen, indien nodig.

3 Vereisten inzake Gegevensbescherming & Vertrouwelijkheid

- (a) De leverancier MOET een beleid voeren waarin alle regels en verantwoordelijkheden van zijn personeel en werknemers, leveranciers en aannemers zijn vastgelegd om naleving van de AVG en de lokale regels voor gegevensbescherming te bereiken en te handhaven.
- (b) De leverancier zou moeten aantonen hoe het beleid inzake gegevensbescherming in de praktijk wordt gebracht, bijvoorbeeld door middel van interne richtlijnen en procedures.
- (c) De leverancier MOET aantonen dat hij zijn personeel en werknemers voldoende heeft opgeleid om het beleid inzake gegevensbescherming te kunnen naleven.
- (d) De leverancier MOET zorgen voor:
 - a. één aanspreekpunt voor NMBS om zaken met betrekking tot gegevensbescherming te bespreken, bij voorkeur een DPO ;
 - b. een SPOC en contactprocedures voor het melden (24/7) van incidenten die betrekking hebben op de persoonsgegevens van medewerkers, klanten of leveranciers van NMBS ;

- c. een exit scenario waarin wordt beschreven hoe NMBS alle persoonsgegevens zal recupereren en hoe en wanneer de leverancier alle persoonsgegevens achteraf zal vernietigen.

(e) De leverancier MOET procedures volgen waarin wordt aangegeven hoe:

- a. data-inbreuken binnen de wettelijke termijnen moeten worden afgehandeld, met inbegrip van de vereiste kennisgeving aan NMBS krachtens de DPA, aan de Gegevensbeschermingsautoriteit en de betrokkenen, indien nodig ;
- b. een gegevensverwerkingsregister moet worden bijgehouden in overeenstemming met de AVG ;
- c. zijn incidentregister moet worden bijgewerkt ;
- d. DPIA's binnen zijn organisatie moeten worden uitgevoerd ;
- e. de toegang tot persoonsgegevens moet worden beheerd en geregistreerd. Groepsaccounts of vooraf gedefinieerde toepassingsaccounts mogen niet worden gebruikt voor toegang tot persoonsgegevens. Alleen persoonlijke accounts mogen toegang hebben tot persoonsgegevens.
- f. persoonlijke gegevens altijd up-to-date worden gehouden ;
- g. de integriteit van de persoonsgegevens wordt gegarandeerd ;
- h. voor de beschikbaarheid van de persoonsgegevens wordt gezorgd ;
- i. de verwerking van persoonsgegevens wordt beperkt ;
- j. aan de geldende bewaartermijnen voor persoonsgegevens wordt gehouden ;
- k. de rechten van de betrokkene (toegang, wijziging, verwijdering) worden gegarandeerd ;
- l. de eigen naleving van de AVG en die van alle leveranciers en contractanten, die persoonsgegevens op basis van de AVG verwerken, worden gecontroleerd en beoordeeld ;
- m. de naleving van alle NMBS-vereisten met betrekking tot gegevensbescherming wordt gegarandeerd ;
- n. achtergrondcontroles worden uitgevoerd voor medewerkers die toegang hebben tot specifieke categorieën van persoonsgegevens.

De leverancier MOET kunnen aantonen dat deze beleidslijnen of procedures bestaan, up-to-date worden gehouden en bekend zijn bij zijn personeel en werknemers.

(f) De leverancier MOET ondersteuning bieden aan NMBS in geval van:

- a. een inbreuk in verband met persoonsgegevens ;
- b. een vereiste op grond van de AGV om een DPIA in te vullen voor de verwerkingsactiviteiten die de leverancier uitvoert namens NMBS.
- c. iedere audit die NMBS zal uitvoeren om te controleren of de leverancier voldoet aan de AVG en deze vereisten.

(g) De leverancier MOET in zijn beleid de datum van de meest recente herziening aangeven.

(h) De Leverancier MOET ervoor te zorgen dat de SPOC die hij onder (d) levert voldoende kennis heeft en voldoende training krijgt om de SPOC in staat te stellen zijn taak te vervullen.

- (i) De Leverancier **MOET** vertrouwelijke informatie van NMBS strikt vertrouwelijk houden en mag deze niet aan derden bekendmaken, noch gebruikmaken van dergelijke gegevens voor eigen voordeel of ten behoeve van een ander, of voor enig ander gebruik dan het overeengekomen doel.
- (j) De Leverancier zal alle redelijke inspanningen ondernemen om een hostingsysteem in verband met vertrouwelijke informatie van NMBS te beveiligen en te verdedigen tegen derden die de beveiliging ervan trachten te schenden, met inbegrip van, maar niet beperkt tot, inbreuken door onbevoegde toegang of het aanbrengen van onbevoegde wijzigingen aan dit systeem.
- (k) De Leverancier zal alle vertrouwelijke informatie van NMBS in transit (verzameld, gekopieerd en verplaatst) en in rust (opgeslagen op de fysieke servers) beschermen en beveiligen, inclusief tijdens elektronische datatransmissie of elektronische of fysieke mediaoverdracht.
- (l) De Leverancier zal alle kopieën of reproducties van vertrouwelijke informatie van NMBS met dezelfde beveiliging bewaren als de originele gegevens. Op het moment dat vertrouwelijke informatie van NMBS niet langer nuttig is voor de primaire of bewaardoelinden, zoals gespecificeerd door NMBS, **MOET** de Leverancier dergelijke gegevens vernietigen waardoor deze data onbruikbaar en niet meer terug te halen zijn. NMBS behoudt zich het recht voor om een verzoek in te dienen voor de methode van gegevensopschoning of vernietiging van hardware.
- (m) Voor alle toepassingschermen, voorpagina's van rapporten en landingspagina's van webtoepassingen die vertrouwelijke informatie bevatten, **MOET** de leverancier op elke pagina duidelijke vertrouwelijkheidsmeldingen in leesbaar lettertype opnemen (bijvoorbeeld een duidelijk bericht dat de informatie op een dergelijk scherm of rapport vertrouwelijk is onder aan een webpagina of onder aan een rapportpagina).
- (n) De ontwikkel-, test- en QA-omgevingen van de leverancier mogen geen echte vertrouwelijke informatie van NMBS gebruiken en mogen nooit op productiesystemen draaien.
- (o) De provider **MOET** ervoor zorgen dat de door hem geïmplementeerde beleidslijnen en processen ten minste aan de hierboven uiteengezette eisen kunnen voldoen. Indien de Leverancier om welke reden dan ook dit niet kan bevestigen (het beleid van de Leverancier richt zich bijvoorbeeld niet op een hierboven genoemd element) op het moment dat hij op de RFP reageert, **MOET** de Leverancier NMBS over deze tekortkoming informeren in zijn voorstel/reactie op de RFP.

4 Vereisten inzake gegevensbewaring

- (a) De Leverancier **MOET** een procedure en de vereiste processen handhaven om te voldoen aan de bewaarregels met betrekking tot vertrouwelijke informatie, inclusief persoonsgegevens, die ervoor zorgen dat deze informatie automatisch wordt gewist na de vooraf ingestelde bewaarperiode.
- (b) Bewaarvereisten voor NMBS-gegevens kunnen in de RFP worden gespecificeerd of naderhand door NMBS worden gewijzigd, afhankelijk van gewijzigde wetgeving of andere criteria. Indien van toepassing **MOET** de Leverancier in zijn voorstel tot de RFP erkennen dat hij aan de vereisten kan voldoen en, op verzoek van NMBS aantonen dat de bewaarvereisten worden geïmplementeerd.
- (c) Systemen voor het bewaren van documenten **MOETEN** voldoen aan alle beveiligings- en gegevensbeschermingscontroles die in dit document worden beschreven.
- (d) De leverancier zal bewijzen leveren over procedures voor het vernietigen van opslagmedia die aan het einde van de levensduur zijn gekomen. Gegevens zullen worden gewist volgens door NMBS aanvaarde procedures.

5 Vereisten inzake applicatie-ontwikkeling

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

6 Vereisten inzake Authenticatie & Identiteitsbeheer

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

7 Vereisten inzake Incident Response

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

8 Vereisten inzake Audit & Inspectie

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

9 Onderzoek

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

10 Vereisten inzake Beschikbaarheid

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

11 Encryptievereisten

Voor deze vereisten verwijst NMBS naar haar document:
Minimale Beveiligingsvereisten voor Derden & Leveranciers

Bijlage A

Checklist Vereisten Gegevensbescherming

Vereiste Nee	Vereisten	Controle	Conform	
PC-01	De leverancier MOET een beleid hebben waarin alle regels zijn vastgelegd om ervoor te zorgen dat de leverancier de AVG en de lokale wetgeving inzake gegevensbescherming naleeft.	VERPLICHT	JA	NEE
PC-02	De leverancier zou moeten bewijzen dat er processen zijn en worden gebruikt die de leverancier in staat stellen om de naleving van de AVG te realiseren en te handhaven.	AANGERADEN	JA	NEE
PC-03	De leverancier zou bewijzen moeten leveren van AVG-bewustmakingscampagnes voor alle medewerkers, inclusief ondersteunend personeel en personeel van de leverancier.	AANGERADEN	JA	NEE
PC-04	De leverancier MOET zorgen voor: (a) bewijzen van AVG-training voor zijn personeelsleden, inclusief ondersteunend personeel en toeleveranciers die toegang hebben tot persoonsgegevens ; (b) één aanspreekpunt voor NMBS voor het bespreken en verkrijgen van alle vereiste informatie wat betreft de naleving door de leverancier van de regels en voorschriften inzake gegevensbescherming, bij voorkeur een DPO ; (c) een SPOC en contactprocedures voor het melden (24/7) van data-inbreuken ; (d) een exit scenario waarin wordt beschreven hoe NMBS alle persoonsgegevens zal recupereren en hoe en wanneer de leverancier alle persoonsgegevens achteraf zal vernietigen.	VERPLICHT	JA	NEE
PC-05	De leverancier MOET procedures volgen waarin wordt aangegeven hoe: (a) data-inbreuken binnen de wettelijke termijnen moeten worden afgehandeld, met inbegrip van de vereiste kennisgeving aan NMBS krachtens de DPA, aan de Gegevensbeschermingsautoriteit en de betrokkenen, indien nodig ;	VERPLICHT	JA	NEE

	<p>(b) de gegevensverwerkingsregister moet worden bijgehouden in overeenstemming met de AVG ;</p> <p>(c) zijn incidentregister moet worden bijgewerkt ;</p> <p>(d) DPIA's binnen zijn organisatie moeten worden uitgevoerd ;</p> <p>(e) de toegang tot persoonsgegevens moet worden beheerd en geregistreerd. Groepsaccounts of vooraf gedefinieerde toepassingsaccounts mogen niet worden gebruikt voor toegang tot persoonsgegevens. Alleen persoonlijke accounts mogen toegang hebben tot persoonsgegevens ;</p> <p>(f) persoonlijke gegevens altijd up-to-date worden gehouden ;</p> <p>(g) de integriteit van de persoonsgegevens worden gewaarborgd ;</p> <p>(h) voor de beschikbaarheid van de persoonsgegevens wordt gezorgd ;</p> <p>(i) de verwerking van persoonsgegevens wordt beperkt ;</p> <p>(j) aan de geldende bewaartermijnen voor persoonsgegevens wordt gehouden ;</p> <p>(k) de rechten van de betrokkene (toegang, wijziging, verwijdering) worden gegarandeerd ;</p> <p>(l) de eigen naleving van de AVG en die van alle leveranciers en contractanten, die persoonsgegevens op basis van de AVG verwerken, worden gecontroleerd en beoordeeld ;</p> <p>(m) de naleving van alle NMBS-vereisten met betrekking tot gegevensbescherming wordt gegarandeerd ;</p> <p>(n) achtergrondcontroles worden uitgevoerd voor medewerkers die toegang hebben tot specifieke categorieën van persoonsgegevens</p> <p>De leverancier MOET kunnen aantonen dat deze beleidslijnen of procedures bestaan, up-to-date worden gehouden en bekend zijn bij zijn personeel en werknemers.</p>			
<p>PC-06</p>	<p>De leverancier MOET ondersteuning bieden aan NMBS in geval van:</p> <p>(a) een inbreuk in verband met persoonsgegevens ;</p> <p>(b) een vereiste op grond van de AGV om een DPIA in te vullen voor de verwerkingsactiviteiten die de leverancier uitvoert namens NMBS.</p>	<p>VERPLICHT</p>	<p>JA</p>	<p>NEE</p>


	(c) iedere audit die NMBS zal uitvoeren om te controleren of de leverancier voldoet aan de AVG en deze vereisten.			
PC-07	De leverancier MOET in zijn beleid de datum van de meest recente herziening aangeven.	VERPLICHT	JA	NEE
PC-08	De Leverancier MOET ervoor te zorgen dat de SPOC die hij onder (d) levert voldoende kennis heeft en voldoende training krijgt om de SPOC in staat te stellen zijn taak te vervullen.	VERPLICHT	JA	NEE
PC-09	De Leverancier MOET vertrouwelijke informatie van NMBS strikt vertrouwelijk houden en mag deze niet aan derden bekendmaken, noch gebruikmaken van dergelijke gegevens voor eigen voordeel of ten behoeve van een ander, of voor enig ander gebruik dan het overeengekomen doel.	VERPLICHT	JA	NEE
PC-10	De Leverancier zal alle redelijke inspanningen ondernemen om een hostingsysteem in verband met vertrouwelijke informatie van NMBS te beveiligen en te verdedigen tegen derden die de beveiliging ervan trachten te schenden, met inbegrip van, maar niet beperkt tot, inbreuken door onbevoegde toegang of het aanbrengen van onbevoegde wijzigingen aan dit systeem.	VERPLICHT	JA	NEE
PC-11	De Leverancier zal alle vertrouwelijke informatie van NMBS in transit (verzameld, gekopieerd en verplaatst) en in rust (opgeslagen op de fysieke servers) beschermen en beveiligen, inclusief tijdens elektronische datatransmissie of elektronische of fysieke mediaoverdracht.	VERPLICHT	JA	NEE
PC-12	De Leverancier zal alle kopieën of reproducties van vertrouwelijke informatie van NMBS met dezelfde beveiliging bewaren als de originele gegevens. Op het moment dat vertrouwelijke informatie van NMBS niet langer nuttig is voor de primaire of bewaardoelinden, zoals gespecificeerd door NMBS, MOET de Leverancier dergelijke gegevens vernietigen waardoor deze data onbruikbaar en niet meer terug te halen zijn. NMBS behoudt zich het recht voor om een verzoek in te dienen voor de methode van gegevensopschoning of vernietiging van hardware.	VERPLICHT	JA	NEE
PC-13	De Leverancier dient met NMBS de standaard NMBS-overeenkomst aan te gaan waarin alle toepasselijke regels voor de verwerking van gegevens namens NMBS	VERPLICHT	JA	NEE

	zijn vastgelegd of indien de Leverancier optreedt als afzonderlijke verwerkingsverantwoordelijke voor het ontvangen van gegevens van NMBS en het verwerken van gegevens uit eigen naam.			
PC-14	Voor alle toepassingschermen, voorpagina's van rapporten en landingspagina's van webtoepassingen die vertrouwelijke informatie bevatten, MOET de leverancier op elke pagina duidelijke vertrouwelijkheidsmeldingen in leesbaar lettertype opnemen (bijvoorbeeld een duidelijk bericht dat de informatie op een dergelijk scherm of rapport vertrouwelijk is onder aan een webpagina of onder aan een rapportpagina).	VERPLICHT	JA	NEE
PC-15	De ontwikkel-, test- en QA-omgevingen van de leverancier mogen geen echte vertrouwelijke informatie van NMBS gebruiken en mogen nooit op productiesystemen draaien.	VERPLICHT	JA	NEE

Checklist gegevensbewaring

Vereiste Nee	Vereisten	Controle	Conform	
DR-01	De leverancier kan worden verplicht om het bewaren van vertrouwelijke informatie te ondersteunen.	VERPLICHT	JA	NEE
DR-02	Bewaarvereisten voor NMBS-gegevens kunnen in de RFP worden gespecificeerd. Indien van toepassing MOET de Leverancier in zijn voorstel tot de RFP erkennen dat hij aan de vereisten kan voldoen en, op verzoek van NMBS, of haar verantwoordelijken, aantonen dat de bewaarvereisten worden geïmplementeerd.	VERPLICHT	JA	NEE
DR-03	Systemen voor het bewaren van documenten MOETEN voldoen aan alle beveiligings- en privacycontroles die in dit document worden beschreven.	VERPLICHT	JA	NEE

Bijlage B

Documentnaam	Kopie
Minimale Beveiligingsvereisten voor Derden & Leveranciers	 <p>SNCB Minimum Security Requirements for 3rd Parties Suppliers v1.0.pdf</p>