Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden

Dit document beschrijft het beleid voor de gecoördineerde bekendmaking van kwetsbaarheden ("beleid") van de Nationale Maatschappij der Belgische Spoorwegen (met maatschappelijke zetel te Frankrijkstraat 56, 1060 Brussel, en ondernemingsnummer 0203.430.576) en haar verbonden ondernemingen (**"NMBS"**). Elke persoon die (zelf of via een derde partij) kwetsbaarheden in de netwerk- en informatiesystemen van NBMS opspoort, onderzoekt en/of bekendmaakt (**"Deelnemer"**) dient dit strikt conform dit Beleid te doen. Indien dit Beleid conflicteert met andere overeenkomsten afgesloten door NMBS, hebben de bepalingen van dit Beleid voorrang (tenzij NMBS uitdrukkelijk schriftelijk is overeengekomen dat van een onderdeel van dit Beleid kan worden afgeweken).

1.Toepassingsgebied van dit Beleid

1.1. NMBS heeft dit Beleid ingevoerd vanuit de bekommernis om het prestatievermogen en de beveiliging van de netwerk- en informatiesystemen van en/of aangewend ten behoeve van NMBS ("Systemen") te verbeteren. Zo kunnen Deelnemers met goede bedoelingen mogelijke kwetsbaarheden in NMBS' systemen opsporen en identificeren, en informatie over kwetsbaarheden bezorgen aan NMBS. Dit betreft beveiligingskwetsbaarheden die door derden kunnen worden misbruikt of die de goede werking van NMBS' producten, diensten of systemen kunnen verstoren.

1.2. NMBS verleent enkel toegang tot de systemen en laat Deelnemers enkel toe om gegevens in te voeren (of te proberen in te voeren) in de systemen met het doel om de beveiliging van NMBS te verbeteren en NMBS te informeren over bestaande kwetsbaarheden, en in strikte overeenstemming met de voorwaarden van dit Beleid.

1.3. Enkel de volgende systemen van NMBS vallen onder het toepassingsgebied van dit Beleid:

(a) Publiek toegankelijke websites;
(b) Publiek toegankelijke (mobiele) applicaties.

1.4. Alle NMBS-systemen die niet uitdrukkelijk zijn geïdentificeerd in artikel 1.3 vallen níet onder het toepassingsgebied van dit Beleid.

1.5. Daarnaast vallen systemen die afhankelijk zijn van derden ook buiten het toepassingsgebied van dit Beleid, tenzij die derden vooraf uitdrukkelijk instemmen met dit Beleid of de Deelnemer voldoet aan het toepasselijke beleid van deze derden.

1.6. Elk onderzoek met betrekking tot (delen van) systemen die niet uitdrukkelijk zijn geïdentificeerd in artikel 1.3, en elke andere inbreuk op dit Beleid kan resulteren in contractuele, buitencontractuele en/of strafrechtelijke aansprakelijkheid en/of vervolging van de betrokken Deelnemer krachtens de toepasselijke wetgeving. Niets in dit Beleid beperkt het recht van NMBS om bij een bevoegde rechter spoedeisende, voorlopige of bewarende maatregelen te vorderen. De Deelnemer vrijwaart NMBS en stelt NMBS schadeloos voor elke vordering en alle schade in de ruimste zin van het woord, voortvloeiend uit, als gevolg van of in verband met enige schending van dit Beleid.

1.7. Dit Beleid wordt geïnterpreteerd in overeenstemming met de artikelen 8, 22, 23 en 30 §3, 11° van de wet van 26 april 2024 tot vaststelling van een kader voor de cyberbeveiliging

van netwerk- en informatiesystemen van algemeen belang voor de openbare veiligheid (NIS2-Wet).

2. Wederzijdse verplichtingen van de partijen

2.1. De Deelnemer handelt te goeder trouw en binnen het doel van dit Beleid. Het is de Deelnemer niet toegelaten om systemen te onderzoeken en kwetsbaarheden in systemen op te sporen op basis van vertrouwelijke informatie van of over NMBS die op onrechtmatige wijze werd verkregen of rechtmatig werd verkregen door de Deelnemer of enige derde ingevolge enige tewerkstelling bij of dienstverlening aan NMBS.

2.2. De Deelnemer verbindt zich ertoe om bij al zijn activiteiten het evenredigheidsbeginsel nauwgezet na te leven. Dit houdt onder meer in dat de Deelnemer de beschikbaarheid van de diensten geleverd door de systemen niet mag verstoren en dat de Deelnemer geen gebruik mag maken van de kwetsbaarheid buiten wat strikt noodzakelijk is voor het aantonen van het beveiligingsprobleem. De houding van de Deelnemer moet evenredig blijven: indien het probleem op kleine schaal is aangetoond, mag de Deelnemer geen verdere actie ondernemen.

2.3. Dit Beleid verleent de Deelnemer op geen enkele wijze het recht om opzettelijk de inhoud van NMBS' informatietechnologie-, communicatie- of persoonsgegevens te onderscheppen, observeren, inspecteren, lezen, registreren, opslaan of anderszins te verwerken.

2.4. Het is de Deelnemer niet toegestaan de volgende handelingen te verrichten: (i) het kopiëren of wijzigen van gegevens van de systemen of het verwijderen van gegevens van de systemen; (ii) het wijzigen van de parameters van de systemen; (iii) het installeren van malware (d.w.z.: virussen, wormen, trojaanse paarden, ...) of vergelijkbare software die de functionaliteit van de NMBS systemen uitschakelt; (iv) "denial of service"-aanvallen (Distributed Denial Of Service - DDOS) uit te voeren; (v) "social engineering"-aanvallen uit te voeren; (vi) phishing-aanvallen uit te voeren; (vii) junkmail-aanvallen (spamming) uit te voeren; (viii) wachtwoorddiefstal of "brute force"-aanvallen uit te voeren; (ix) een andere destructieve methode te gebruiken bij het zoeken naar kwetsbaarheden; (x) een apparaat te installeren dat het mogelijk maakt om niet-publiekelijk beschikbare communicatie of elektronische communicatie te onderscheppen, op te slaan of er kennis van te nemen; (xi) het opzettelijk opvangen, onderscheppen of opslaan van niet publiekelijk beschikbare communicatie of elektronische communicatie; (xii) het opzettelijk gebruiken, opslaan, communiceren of verspreiden van de inhoud van communicatie die niet publiekelijk beschikbaar is of van gegevens van een systeem waarvan de Deelnemer redelijkerwijs had moeten weten dat ze illegaal verkregen waren.

2.5. Als de Deelnemer bij de uitvoering van zijn onderzoek wordt bijgestaan door een derde partij, moet hij ervoor zorgen dat en maakt hij zich sterk dat de derde partij vooraf kennis heeft genomen van dit Beleid en ermee instemt deze voorwaarden na te leven wanneer hij de Deelnemer bijstaat.

2.6. De Deelnemer zal in geen enkel geval informatie die in het kader van dit Beleid werd verzameld, delen met of verspreiden onder derden, behalve wanneer dit uitdrukkelijk schriftelijk is overeengekomen met NMBS en, indien relevant, in overeenstemming met artikel 5.5 (openbare aankondiging).

2.7. Het is de Deelnemer niet toegestaan informatietechnologie-, communicatie- of persoonsgegevens aan derden door te geven of te verspreiden.

2.8. Indien de kwetsbaarheid redelijkerwijs andere organisaties in België kan treffen, kan NMBS deze melden aan het Centrum voor Cyberbeveiliging België ("CCB") (vulnerabilityreport@cert.be), overeenkomstig artikel 5.5(d). Indien de Deelnemer zelf beslist om dergelijke melding uit te voeren, informeert de Deelnemer NMBS hierover.

2.9. In hoofde van de Deelnemer zelf mag er geen sprake zijn van bedrieglijk opzet, het oogmerk om te schaden, of de wil om gebruik te maken van of schade te veroorzaken aan het bezochte systeem of aan de gegevens ervan. Dit geldt ook voor systemen van derden in België of in het buitenland.

2.10. In geval van twijfel over bepaalde voorwaarden van dit Beleid zal de Deelnemer vooraf contact opnemen met NMBS via mail naar het adres disclose@belgiantrain.be en schriftelijke toestemming verkrijgen alvorens te handelen.

3. Verwerking van Persoonsgegevens

3.1. Dit Beleid heeft niet tot doel om te resulteren in enige Verwerking van Persoonsgegevens. Het is echter wel mogelijk dat de Deelnemer, zelfs toevallig, Persoonsgegevens moet Verwerken in het kader van zijn onderzoek naar kwetsbaarheden. Indien dit het geval is, Verwerken Deelnemers dergelijke Persoonsgegevens in overeenstemming met wat hieronder is uiteengezet.

3.2. De volgende definities moeten in acht worden genomen:

(a) **"Gegevensbeschermingswetgeving"** betekent elke wettelijke regeling van de Europese Unie en/of haar Lidstaten, met inbegrip van, maar niet beperkt tot wetten, Richtlijnen en Verordeningen, voor de bescherming van Persoonsgegevens, in het bijzonder de GDPR.

(b) **"GDPR"** betekent de Verordening (EU) 2016/679 van het Europees Parlement en de Raad van 27 april 2016 betreffende de bescherming van natuurlijke personen in verband met de verwerking van persoonsgegevens en betreffende het vrije verkeer van die gegevens en tot intrekking van Richtlijn 95/46/EG (Algemene Verordening Gegevensbescherming).

3.3. De termen **"Betrokkene", "Persoonsgegevens", "Inbreuk op Persoonsgegevens"** en **"Verwerking(en)"** hebben dezelfde betekenis als in de Gegevensbeschermingswetgeving.

3.4. In de context van dit Beleid kan de Verwerking door de Deelnemer en/of zijn verbonden ondernemingen en werknemers, identificatiegegevens, technische gegevens, gegevens over persoonlijke kenmerken en gegevens met betrekking tot de relatie en het beroep van de Betrokkenen omvatten, evenals elk ander type (gevoelige) gegevens waarmee de Deelnemer in aanraking kan komen in overeenstemming met de aard van de activiteiten die het onderwerp zijn van dit Beleid en ten behoeve van het verrichten van deze activiteiten. In principe zijn de Betrokkenen waarop dit Beleid betrekking heeft (i) NMBS' werknemers of aangestelden die gebruik maken van de diensten en (ii) klanten of leveranciers van NMBS en hun werknemers of aangestelden. De Deelnemer mag derhalve Persoonsgegevens op beperkte wijze en doorlopend verwerken voor de duur van de dienstverlening door de Deelnemer in overeenstemming met dit Beleid en de Deelnemer zal deze gegevens slechts zolang bewaren

als nodig is om te voldoen aan het doel van de hierboven beschreven diensten. Bij het Verwerken van dergelijke gegevens verbindt de Deelnemer zich ertoe de wettelijke verplichtingen inzake de bescherming van Persoonsgegevens na te leven, evenals de bepalingen van dit Beleid, in het bijzonder:

(a) De Deelnemer zal Persoonsgegevens enkel Verwerken in overeenstemming met de instructies van NMBS die in dit Beleid zijn bepaald, en alleen met het doel om kwetsbaarheden op te sporen in de systemen. Elke Verwerking van Persoonsgegevens voor enig ander doel is uitgesloten, ook met betrekking tot de overdracht van Persoonsgegevens aan een derde land of een internationale organisatie, tenzij de toepasselijke wetgeving dit vereist; in een dergelijk geval zal de Deelnemer NMBS vóór de Verwerking op de hoogte stellen van deze wettelijke verplichting, tenzij deze wetgeving dergelijke informatie verbiedt op grond van redenen van algemeen belang.

(b) De Deelnemer verbindt zich ertoe de Verwerking van Persoonsgegevens te beperken tot hetgeen strikt noodzakelijk is voor het detecteren van kwetsbaarheden.

(c) De Deelnemer draagt er zorg voor dat diegenen die bevoegd zijn Persoonsgegevens te Verwerken, zich verplicht hebben tot geheimhouding of gebonden zijn aan een passende wettelijke geheimhoudingsplicht.

(d) De Deelnemer verbindt zich ertoe de voorwaarden die in dit Beleid en in het bijzonder in artikel 3.5 zijn opgenomen, na te leven bij het inschakelen van een andere verwerker.

(e) De Deelnemer neemt passende technische en organisatorische maatregelen om een beveiligingsniveau te waarborgen dat afgestemd is op het risico (zoals bijvoorbeeld versleuteling), in overeenstemming met artikel 32 van de GDPR. Dit omvat onder meer, indien toepasselijk (i) de pseudonimisering en versleuteling van Persoonsgegevens, (ii) het vermogen om de permanente vertrouwelijkheid, integriteit, beschikbaarheid en veerkracht van verwerkingssystemen en -diensten te waarborgen, (iii) het vermogen om de beschikbaarheid van en toegang tot Persoonsgegevens tijdig te herstellen in geval van een fysiek of technisch incident en (iv) een proces voor het regelmatig testen, beoordelen en evalueren van de effectiviteit van technische en organisatorische maatregelen om de beveiliging van de Verwerking te waarborgen.

(f) De Deelnemer verklaart dat hij de risico's begrijpt die gepaard gaan met de implementatie van dit Beleid en over de nodige expertise en ervaring te beschikken om de systemen op een veilige en wettelijk conforme wijze te testen.

(g) De Deelnemer verbindt zich ertoe, in de mate van het mogelijke en rekening houdend met de aard van de Verwerking en de informatie waarover hij beschikt, NMBS bij te staan bij de uitvoering van haar verplichtingen inzake de uitoefening van de rechten van de Betrokkenen, de beveiliging van de Verwerking en de eventuele impactanalyse.

(h) De Deelnemer verbindt zich ertoe NMBS zo snel mogelijk na kennisname van een mogelijke inbreuk in verband met Persoonsgegevens te informeren op het adres dataprotectionofficer@belgiantrain.be.

(i) De Deelnemer mag Persoonsgegevens niet langer bewaren dan noodzakelijk. Gedurende deze periode moet de Deelnemer zorgen voor een beveiligingsniveau dat in verhouding staat tot het risico (bij voorkeur

versleuteld). Bij beëindiging van de deelname aan dit Beleid moeten deze Persoonsgegevens onmiddellijk worden gewist, tenzij de Deelnemer op grond van toepasselijk Unierecht of nationaal recht verplicht is deze te bewaren.

(j) De Deelnemer verbindt zich ertoe een register bij te houden van de Verwerkingsactiviteiten die hij in opdracht van NMBS heeft uitgevoerd. Dit register bevat een beschrijving van de beveiligingsmaatregelen die de Deelnemer heeft genomen, in overeenstemming met artikel 30 §2 van de GDPR.

(k) De Deelnemer stelt aan NMBS alle informatie ter beschikking die nodig is om de naleving van de verplichtingen van dit artikel 3 aan te tonen en verleent zijn medewerking aan audits, inclusief inspecties, uitgevoerd door NMBS, een andere auditor in opdracht van NMBS en/of enige bevoegde autoriteit.

3.5. De Deelnemer kan voor zijn onderzoek een beroep doen op derden. De Deelnemer dient er in dat geval voor te zorgen dat deze derde vooraf op de hoogte is van dit Beleid en stemt ermee in om bij het verlenen van assistentie de voorwaarden van het beleid na te leven, met inbegrip van vertrouwelijkheid, de implementatie van passende beveiligingsmaatregelen en de principes die zijn vastgelegd in artikel 3.4 met betrekking tot de omvang, aard en duur van de Verwerking. De Deelnemer erkent dat hij volledig aansprakelijk blijft ten opzichte van NMBS indien de derde waarop hij vertrouwt zijn verplichtingen inzake gegevensbescherming niet nakomt.

3.6. Indien de Deelnemer door NMBS opgeslagen en/of anderszins Verwerkte Persoonsgegevens Verwerkt op een wijze die in strijd is met dit Beleid of voor andere doeleinden dan het opsporen van mogelijke kwetsbaarheden in de systemen, erkent de Deelnemer dat hij als verantwoordelijke voor de Verwerking zal worden beschouwd en volledig aansprakelijk zal zijn voor de door hem in dat kader uitgevoerde Verwerking. De Deelnemer vrijwaart NMBS en stelt NMBS volledig schadeloos voor enige vordering van een Betrokkene of andere derde en alle daarmee verband houdende schade opgelopen door NMBS met betrekking tot enige inbreuk door de Deelnemer (of enige derde waarvoor de Deelnemer instaat) op zijn verplichtingen op vlak van Verwerking van Persoonsgegevens.

4. Beloningen

4.1. NMBS verbindt zich ertoe een beloning toe te kennen aan de Deelnemer onder de volgende voorwaarden:

(a) De kwetsbaarheid is nog niet gekend binnen NMBS;
(b) De kwetsbaarheid werd niet eerder door een andere persoon dan de Deelnemer gemeld; en
(c) De melding is conform dit Beleid en compleet.

4.2. NMBS behoudt zich het recht voor om naar eigen inzicht te bepalen welke vorm dergelijke beloning krijgt.

4.3. Elk verzoek om een beloning buiten deze voorwaarden, zal worden gelijkgesteld aan een illegale poging tot afpersing.

5. Procedure

5.1. Ontdekking

Wanneer de Deelnemer informatie over een kwetsbaarheid ontdekt, voert hij, voor zover dit redelijkerwijs mogelijk is, vooraf controles uit om het bestaan van de kwetsbaarheid te bevestigen en eventuele risico's te identificeren. Na deze eerste beoordeling van het inherente risico van deze kwetsbaarheden neemt de Deelnemer zo snel als redelijkerwijs mogelijk is, contact op met NMBS overeenkomstig artikel 5.2.

5.2. Melding

(a) De Deelnemer stuurt elke informatie over geïdentificeerde kwetsbaarheden naar NMBS op het adres disclose@belgiantrain.be.

(b) De Deelnemer zal volgende richtlijnen volgen bij het doorsturen van informatie:
   (i) De Deelnemer communiceert in het Nederlands, Frans of Engels.
   (ii) De Deelnemer gebruikt het formulier opgenomen in Bijlage 1 (Kwetsbaarheidsrapport) en bezorgt alle daarin gevraagde informatie waarover hij beschikt. De geïdentificeerde kwetsbaarheden worden volledig en in detail beschreven, inclusief IP-adressen, logs, screenshots, betrokken URL's, enz. Het is belangrijk dat NMBS de kwetsbaarheid zelf kan terugvinden om ze weg te werken.
   (iii) De Deelnemer bevestigt uitdrukkelijk dat geen (rechtstreeks dan wel onrechtstreeks, rechtmatig dan wel onrechtmatig verkregen) vertrouwelijke informatie van of over NMBS werd gebruikt bij het opsporen of vaststellen van de kwetsbaarheid.
   (iv) De Deelnemer zal indien gewenst relevante contactinformatie verstrekken zodat NMBS de melding verder met de Deelnemer kan opvolgen.

(c) NMBS verbindt zich ertoe om, wanneer ze een melding ontvangt, de Deelnemer zo snel mogelijk een bericht van ontvangst te sturen en de volgende stappen van de procedure.

5.3. Communicatie

(a) De partijen verbinden zich ertoe alles in het werk te stellen om een voortdurende en doeltreffende communicatie te verzekeren met als doel de geïdentificeerde en gemelde kwetsbaarheid te identificeren en op te lossen.

(b) Indien na een redelijke termijn een reactie van een van de partijen uitblijft, kunnen de partijen een beroep doen op het Centrum voor Cybersecurity België (CCB) (vulnerabilityreport@cert.be) als (standaard-) coördinator.

5.4. Onderzoek en doelstelling

(a) Tijdens de onderzoeksfase zal NMBS de omgeving en het geïdentificeerde gedrag van de Deelnemer reproduceren om de verstrekte informatie te verifiëren.

(b) NMBS zal de Deelnemer regelmatig op de hoogte houden van de resultaten van dit onderzoek en de acties die naar aanleiding van deze informatie worden ondernomen.

(c) Tijdens dit proces houden de partijen rekening met gelijkaardige of gerelateerde rapporten, beoordelen ze het risico en de ernst van de geïdentificeerde kwetsbaarheid en identificeren ze eventuele andere getroffen producten of systemen.
(d) Dit Beleid heeft als doel de ontwikkeling van een oplossing mogelijk te maken om de kwetsbaarheid van het systeem op te lossen voordat er (verdere) schade wordt aangericht.

5.5. Openbare aankondiging

(a) NMBS beslist, na de Deelnemer gehoord te hebben, hoe het bestaan van de eventuele kwetsbaarheid bekend wordt gemaakt.
(b) In geen geval zal een openbare bekendmaking plaatsvinden voordat een oplossing is geïmplementeerd en een beveiligingsbericht kan worden verspreid onder de betrokken gebruikers.
(c) Geen enkele openbaarmaking is toegestaan zonder de uitdrukkelijke schriftelijke toestemming van NMBS.
(d) Als een kwetsbaarheid ook andere organisaties treft, meldt NMBS dit aan het CCB (vulnerabilityreport@cert.be).

6. Toepasselijk recht

6.1. Dit Beleid wordt beheerst door en geïnterpreteerd volgens Belgisch recht. Alle geschillen met betrekking tot de geldigheid, interpretatie of uitvoering van dit Beleid zullen definitief worden beslecht door de bevoegde rechtbanken van Brussel.

6.2. Het CCB (vulnerabilityreport@cert.be) kan optreden als bemiddelaar tussen NMBS en de Deelnemer voor geschillen met betrekking tot de toepassing van dit Beleid.

7. Duur

7.1. Dit Beleid is van toepassing vanaf 02/04/2026 en blijft van toepassing totdat NMBS een wijziging aankondigt conform artikel 7.2.

7.2. NMBS kan dit Beleid wijzigen of beëindigen. NMBS zal materiële wijzigingen van dit Beleid aankondigen door publicatie op de website van NMBS. Tenzij uitdrukkelijk anders vermeld door NMBS, worden wijzigingen van dit Beleid dertig (30) dagen na bekendmaking van kracht.

Bijlage 1: Kwetsbaarheidsrapport

Naam: Voornaam:	
(Adres/Land):	
E-mailadres: Telefoonnummer:	
Beschrijving van de kwetsbaarheid:	
Soort kwetsbaarheid:	
Configuratiedetails:	
Besturingssysteem:	
Uitgevoerde bewerkingen (logs):	
Gebruikte tools:	
Data en tijdstippen van de tests:	
IP-adres of URL van het getroffen systeem:	
Indien Persoonsgegevens worden verwerkt:	• Soorten geraadpleegde/verwerkte Persoonsgegevens: • Categorieën van Betrokkenen (klant, werknemer, leverancier): • Doorgifte van gegevens aan/toegang vanuit een land buiten de Europese Unie of de Europese Economische Ruimte? Zo ja: - vermeld het (de) betrokken land(en): - stuur de ingevulde en ondertekende bijlage II terug.
Iedere andere relevante informatie:	
Bijlagen (screenshots).	
Gemeld aan het CCB	Indien de kwetsbaarheid eveneens gemeld is aan het CCB, graag de datum van melding vermelden.
Door het overmaken van deze informatie, bevestig ik als Deelnemer aan het NMBS Beleid voor de gecoördineerde bekendmaking van kwetsbaarheden, uitdrukkelijk dat mijn onderzoek en bovenvermelde informatie verkregen ingevolge mijn onderzoek, op geen enkele wijze rechtstreeks of onrechtstreeks gebaseerd is op of het gevolg is van vertrouwelijke informatie van of over NMBS.	

Bijlage 2: Doorgifte van Persoonsgegevens buiten de EU en EER (Modale contractuele bepalingen)

Wanneer de Deelnemer toestemming krijgt van NMBS om Persoonsgegevens door te geven van NMBS naar de Deelnemer of een aan de Deelnemer gelieerde onderneming (of een verdere doorgifte), in elk geval, wanneer een dergelijke doorgifte verboden zou zijn door Verordening (EU) 2016/679 zonder de bescherming voor de doorgegeven Persoonsgegevens die wordt geboden door de standaardcontractbepalingen die zijn opgenomen in het Uitvoeringsbesluit (EU) 2021/914 van de Commissie van 4 juni 2021 betreffende standaardcontractbepalingen voor de doorgifte van Persoonsgegevens naar derde landen overeenkomstig Verordening (EU) 2016/679 van het Europees Parlement en de Raad, zoals van tijd tot tijd gewijzigd of vervangen door een bevoegde autoriteit krachtens de toepasselijke wet- en regelgeving inzake gegevensbescherming in de EER ("EER-standaardcontractbepalingen"), wordt hierbij uitdrukkelijk overeengekomen tussen NMBS ("gegevensexporteur") en de Deelnemer of een van de gelieerde ondernemingen van de Deelnemer (elk als "gegevensimporteur") dat de toepasselijke module 2 van de EER-standaardcontractbepalingen ("EER-standaardcontractbepalingen voor doorgifte tussen Verwerkingsverantwoordelijke en Verwerker"), die hierbij door middel van verwijzing worden opgenomen, van toepassing zal zijn vanaf het begin van de desbetreffende doorgifte, en zowel NMBS als de Deelnemer bevestigen dat:

- Bepaling 7 (Docking) van de standaardcontractbepalingen van toepassing is;
- Bepaling 9 (Gebruik van subverwerkers) van toepassing is en de "termijn" 1 maand is;
- Bij bepaling 11(a) (Verhaal) de optionele tekst niet van toepassing is;
- Bij bepaling 13(a) (Toezicht) wordt volgende tekst geselecteerd: *"De toezichthoudende autoriteit die erop toeziet dat de gegevensexporteur Verordening (EU) 2016/679 naleeft met betrekking tot de gegevensdoorgifte, zoals aangegeven in bijlage I.C, treedt op als de bevoegde toezichthoudende autoriteit";*
- "Optie 1" bij bepaling 17 (Toepasselijk recht) van toepassing is en de "Lidstaat" België is;
- Bij bepaling 18 (Forum en jurisdictiekeuze) de lidstaat België is;
- Bijlage 1 van module 2 wordt geacht vooraf te zijn ingevuld met de relevante informatie van artikel 3.4 van dit Beleid, de partijen zijn de gegevensexporteur en de gegevensimporteur(s), de toezichthoudende autoriteit is de Belgische Gegevensbeschermingsautoriteit en de Verwerkingen worden geacht te zijn beschreven in dit Beleid; en
- Bijlage 2 van module 2 wordt geacht vooraf te zijn ingevuld met de relevante informatie uit artikels 3.4(e) en 3.4(f) van dit Beleid.