Richtlinie zur koordinierten Offenlegung von Schwachstellen

Dieses Dokument beschreibt die koordinierte Richtlinie zur Offenlegung von Schwachstellen („Richtlinie“) der Société Nationale des Chemins de Fer Belges (mit Sitz in der Frankrijkstraat 56, 1060 Brüssel, und der Unternehmensnummer 0203.430.576) und ihrer verbundenen Unternehmen („**SNCB**“). Jede Person, die Schwachstellen im Netz und in den Informationssystemen der SNCB aufdeckt, untersucht und/oder offenlegt (entweder selbst oder durch Dritte) („**Teilnehmer**“), muss dieses streng in Übereinstimmung mit dieser Richtlinie tun. Im Falle von Widersprüchen zwischen der vorliegenden Richtlinie und anderen von der SNCB abgeschlossenen Vereinbarungen, haben die Bestimmungen der vorliegenden Richtlinie Vorrang (es sei denn, die SNCB hat ausdrücklich und schriftlich zugestimmt, von einem Teil der vorliegenden Richtlinie abzuweichen).

1. Geltungsbereich der Richtlinie

1.1 Die SNCB hat diese Richtlinie eingeführt, um die Leistungsfähigkeit und die Sicherheit der Netz- und Informationssysteme der SNCB und/oder der für die SNCB genutzten Systeme („Systeme“) zu verbessern. So können Teilnehmer mit guten Absichten potenzielle Schwachstellen in den Systemen der SNCB aufspüren und identifizieren und SNCB-Informationen über Schwachstellen liefern. Es handelt sich um Sicherheitsschwachstellen, die von Dritten missbraucht werden könnten oder die das reibungslose Funktionieren der Produkte, Dienstleistungen oder Systeme der SNCB stören könnten.

1.2 Die SNCB gewährt nur dann Zugang zu den Systemen und erlaubt den Teilnehmern nur dann, Daten in die Systeme einzugeben (oder dies zu versuchen), wenn es darum geht, die Sicherheit der SNCB zu verbessern und die SNCB über bestehende Schwachstellen zu informieren, und zwar unter strikter Einhaltung der Bestimmungen der vorliegenden Richtlinie.

1.3 Folgende Systeme der SNCB fallen in den Geltungsbereich dieser Richtlinie:

(a) Öffentlich zugängliche Websites;

(b) Öffentlich zugängliche (mobile) Anwendungen.

1.4 Alle Systeme der SNCB, die in Artikel 1.3 nicht ausdrücklich genannt werden, fallen nicht in den Geltungsbereich dieser Richtlinie.

1.5 Darüber hinaus fallen Systeme, die sich auf Dritte stützen, ebenfalls nicht in den Geltungsbereich dieser Richtlinie, es sei denn, diese Dritten stimmen dieser Richtlinie im Voraus ausdrücklich zu, oder der Teilnehmer hält sich an die geltenden Richtlinien dieser Dritten.

1.6 Jede Untersuchung in Bezug auf (Teile von) Systeme(n), die in Artikel 1.3 nicht ausdrücklich genannt sind, und jeder andere Verstoß gegen diese Richtlinie, kann eine vertragliche, außervertragliche und/oder strafrechtliche Haftung und/oder eine strafrechtliche Verfolgung des betreffenden Teilnehmers nach geltendem Recht nach sich ziehen. Die vorliegende Richtlinie schränkt in keiner Weise das Recht der SNCB ein, dringende, einstweilige oder sichernde Maßnahmen bei einem zuständigen Gericht zu beantragen. Der Teilnehmer verpflichtet sich, die SNCB von allen Ansprüchen und Schäden im weitesten Sinne

freizustellen, die sich aus, infolge, oder im Zusammenhang mit einem Verstoß gegen diese Richtlinie ergeben.

1.7 Diese Richtlinie ist gemäß den Artikeln 8, 22, 23 und 30 Absatz 3 Nummer 11 des Gesetzes vom 26. April 2024 zur Schaffung eines Rahmens für die Cybersicherheit von Netz- und Informationssystemen von allgemeinem öffentlichem Sicherheitsinteresse (NIS-2-Gesetz) auszulegen.

2. Gegenseitige Verpflichtungen der Parteien

2.1. Der Teilnehmer handelt in gutem Glauben und im Sinne dieser Richtlinie. Dem Teilnehmer ist es untersagt, Systeme zu untersuchen und Schwachstellen in Systemen auf der Grundlage vertraulicher Informationen von der, oder über, die SNCB aufzuspüren, die der Teilnehmer oder ein Dritter im Rahmen seiner Beschäftigung bei der SNCB, oder der Erbringung von Dienstleistungen für die SNCB, unrechtmäßig oder rechtmäßig erlangt hat.

2.2. Der Teilnehmer verpflichtet sich, bei allen seinen Tätigkeiten den Grundsatz der Verhältnismäßigkeit strikt einzuhalten. Dazu gehört, dass der Teilnehmer die Verfügbarkeit der von den Systemen bereitgestellten Diensten nicht stören darf, und dass er die Schwachstelle nicht über das zum Nachweis des Sicherheitsproblems unbedingt erforderliche Maß hinaus ausnutzen darf. Das Vorgehen des Teilnehmers sollte verhältnismäßig bleiben: Wenn sich das Problem nachweislich als geringfügig erweist, darf der Teilnehmer keine weiteren Maßnahmen ergreifen.

2.3. Diese Richtlinie gewährt dem Teilnehmer in keinster Weise das Recht, den Inhalt Informationstechnologie-, Kommunikations- oder personenbezogener Daten der SNCB absichtlich abzufangen, zu beobachten, zu inspizieren, zu lesen, aufzuzeichnen, zu speichern oder anderweitig zu verarbeiten.

2.4. Der Teilnehmer darf die folgenden Handlungen nicht vornehmen: (i) das Kopieren oder Ändern von Daten aus den Systemen oder das Löschen von Daten aus den Systemen; (ii) das Ändern der Parameter der Systeme; (iii) das Installieren von Malware (d. h.: Viren, Würmer, Trojaner, ...) oder ähnlicher Software, die die Funktionalität der Systeme der SNCB außer Kraft setzt; (iv) das Durchführen von Denial-of-Service-Angriffen (Distributed Denial of Service − DDOS); (v) das Durchführen von Social-Engineering-Angriffen; (vi) das Durchführen von Phishing-Angriffen; (vii) das Durchführen von Junk-Mail-Angriffen (Spamming); (viii) das Durchführen von Passwortdiebstahl oder Brute-Force-Angriffen; (ix) das Anwenden anderer destruktiver Methoden bei der Suche nach Schwachstellen; (x) das Installieren eines Geräts, das das Abfangen, Speichern oder die Kenntnisnahme von nicht öffentlich zugänglicher Kommunikation oder elektronischer Kommunikation ermöglicht; (xi) das absichtliche Abfangen, Abhören oder Speichern von nicht öffentlich zugänglicher Kommunikation oder elektronischer Kommunikation; (xii) das absichtliche Nutzen, Speichern, Übermitteln oder Verbreiten des Inhalts von nicht öffentlich zugänglicher Kommunikation oder Daten aus einem System, von denen der Teilnehmer vernünftigerweise hätte wissen müssen, dass sie illegal erlangt wurden.

2.5. Wird der Teilnehmer bei der Durchführung seiner Untersuchung von einem Dritten unterstützt, so muss er dafür sorgen und sicherstellen, dass der Dritte diese Richtlinie zur Kenntnis genommen hat und sich bereit erklärt, diese Bestimmungen im Rahmen der Unterstützung des Teilnehmers einzuhalten.

2.6. Der Teilnehmer darf unter keinen Umständen Informationen, die im Rahmen dieser Richtlinie erhoben wurden, an Dritte weitergeben, es sei denn, er hat dieses ausdrücklich

schriftlich mit der SNCB vereinbart und gegebenenfalls in Übereinstimmung mit Artikel 5.5 (*Öffentliche Bekanntmachung*).

2.7. Dem Teilnehmer ist es nicht gestattet, Informationstechnologie-, Kommunikations- oder personenbezogene Daten an Dritte zu übermitteln oder zu verbreiten.

2.8. Wenn die Schwachstelle vernünftigerweise andere Organisationen in Belgien betreffen könnte, kann die SNCB sie dem Zentrum für Cybersicherheit Belgien („ZCB“) (vulnerabilityreport@cert.be) gemäß Artikel 5.5(d) melden. Wenn der Teilnehmer selbst beschließt, eine solche Meldung vorzunehmen, muss er die SNCB darüber informieren.

2.9. Auf Seiten des Teilnehmers selbst darf keine betrügerische Absicht, Schädigungsabsicht oder der Wille zur Nutzung oder Beschädigung des besuchten Systems oder seiner Daten bestehen. Dies gilt auch für Systeme von Dritten in Belgien oder im Ausland.

2.10. Im Falle von Zweifeln über bestimmte Bestimmungen dieser Richtlinie muss der Teilnehmer die SNCB vorab per E-Mail an die Adresse disclose@belgiantrain.be kontaktieren und eine schriftliche Genehmigung einholen, bevor er handelt.

3. Verarbeitung von personenbezogenen Daten

3.1. Diese Richtlinie soll nicht zu einer Verarbeitung personenbezogener Daten führen. Es ist jedoch möglich, dass der Teilnehmer im Rahmen seiner Untersuchung von Schwachstellen personenbezogene Daten verarbeiten muss, auch wenn dies zufällig geschieht. Sollte das der Fall sein, so verarbeiten die Teilnehmer diese personenbezogenen Daten gemäß den nachstehenden Bestimmungen.

3.2. Die folgenden Begriffsbestimmungen sind zu beachten:

(a) **„Datenschutzgesetzgebung“** bezeichnet jede gesetzliche Regelung der Europäischen Union und/oder ihrer Mitgliedstaaten, einschließlich, aber nicht beschränkt auf Gesetze, Richtlinien und Verordnungen zum Schutz personenbezogener Daten, insbesondere die DSGVO.

(b) **„DSGVO“** bezeichnet die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung).

3.3. Die Begriffe **„betroffene Person“**, **„personenbezogene Daten“, „Verletzung des Schutzes personenbezogener Daten“** und **„Verarbeitung(en)“** haben die gleiche Bedeutung wie in der Datenschutzgesetzgebung.

3.4. Im Rahmen dieser Richtlinie kann die Verarbeitung durch den Teilnehmer und/oder seine verbundenen Unternehmen und Mitarbeiter Identifizierungsdaten, technische Daten, Daten über persönliche Merkmale und Daten über die Beziehung und den Beruf der betroffenen Personen sowie jede andere Art von (sensiblen) Daten umfassen, mit denen der Teilnehmer entsprechend der Art der Tätigkeiten, die Gegenstand dieser Richtlinie sind, und zum Zweck der Durchführung dieser Tätigkeiten in Kontakt kommen kann. Grundsätzlich sind die von dieser Richtlinie betroffenen Personen (i) die Mitarbeiter oder Beauftragten der SNCB, die die Dienste nutzen, und (ii) die Kunden oder Lieferanten der SNCB und deren Mitarbeiter oder Beauftragte. Der Teilnehmer kann daher personenbezogene Daten in begrenztem Umfang und fortlaufend für die Dauer der vom Teilnehmer gemäß dieser Richtlinie erbrachten

Dienstleistungen verarbeiten, und der Teilnehmer bewahrt diese Daten nur so lange auf, wie es für die Erfüllung des Zwecks der oben beschriebenen Dienstleistungen erforderlich ist. Bei der Verarbeitung dieser Daten verpflichtet sich der Teilnehmer, die gesetzlichen Verpflichtungen zum Schutz personenbezogener Daten sowie die Bestimmungen dieser Richtlinie einzuhalten, insbesondere:

(a) darf der Teilnehmer personenbezogene Daten nur gemäß den Anweisungen der SNCB, die in dieser Richtlinie dargelegt sind, und nur zum Zweck der Aufdeckung von Schwachstellen in den Systemen verarbeiten. Jegliche Verarbeitung personenbezogener Daten zu anderen Zwecken ist ausgeschlossen, auch im Zusammenhang mit der Übermittlung personenbezogener Daten an ein Drittland oder einer internationale Organisation, es sei denn, dies ist gesetzlich vorgeschrieben; in einem solchen Fall muss der Teilnehmer die SNCB vor der Verarbeitung über diese gesetzliche Verpflichtung informieren, es sei denn, das Gesetz verbietet eine solche Information aus Gründen des öffentlichen Interesses;

(b) verpflichtet sich der Teilnehmer, die Verarbeitung personenbezogener Daten auf das zur Aufdeckung von Schwachstellen unbedingt erforderliche Maß zu beschränken;

(c) stellt der Teilnehmer sicher, dass die zur Verarbeitung personenbezogener Daten befugten Personen zur Vertraulichkeit verpflichtet sind, oder einer angemessenen gesetzlichen Geheimhaltungspflicht unterliegen;

(d) verpflichtet sich der Teilnehmer, bei der Beauftragung eines anderen Auftragsverarbeiters die in dieser Richtlinie und insbesondere in Artikel 3.5 dargelegten Bedingungen einzuhalten;

(e) ergreift der Teilnehmer geeignete technische und organisatorische Maßnahmen zur Gewährleistung eines dem Risiko angemessenen Sicherheitsniveaus (wie z. B. Verschlüsselung) gemäß Artikel 32 der DSGVO. Dazu gehören gegebenenfalls (i) die Pseudonymisierung und Verschlüsselung personenbezogener Daten, (ii) die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Verarbeitungssystemen und -diensten dauerhaft zu gewährleisten, (iii) die Fähigkeit, die Verfügbarkeit personenbezogener Daten und den Zugang zu ihnen im Falle eines physischen oder technischen Zwischenfalls rechtzeitig wiederherzustellen, und (iv) ein Verfahren zur regelmäßigen Prüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung;

(f) erklärt der Teilnehmer, dass er sich der Risiken bewusst ist, die mit der Umsetzung dieser Richtlinie verbunden sind, und dass er über die erforderlichen Fachkenntnisse und Erfahrungen verfügt, um die Systeme auf sichere und rechtskonforme Weise zu testen;

(g) verpflichtet sich der Teilnehmer, die SNCB im Rahmen des Möglichen und unter Berücksichtigung der Art der Verarbeitung und der ihm zur Verfügung stehenden Informationen bei der Erfüllung ihrer Pflichten in Bezug auf die Ausübung der Rechte der betroffenen Personen, die Sicherheit der Verarbeitung und eine eventuelle Folgenanalyse zu unterstützen;

(h) verpflichtet sich der Teilnehmer, die SNCB so schnell wie möglich nach Bekanntwerden eines möglichen Verstoßes im Zusammenhang mit personenbezogenen Daten unter der Adresse dataprotectionofficer@belgiantrain.be zu informieren.

(i) darf der Teilnehmer personenbezogene Daten nicht länger als nötig aufbewahren. Während dieses Zeitraums muss der Teilnehmer ein dem Risiko angemessenes Sicherheitsniveau gewährleisten (vorzugsweise verschlüsselt). Bei Beendigung der Teilnahme an dieser Richtlinie sind diese personenbezogenen Daten unverzüglich zu löschen, es sei denn, der Teilnehmer ist nach geltendem Unionsrecht oder nationalem Recht verpflichtet, sie aufzubewahren;

(j) verpflichtet sich der Teilnehmer, ein Verzeichnis der Verarbeitungsvorgänge zu führen, die er im Auftrag der SNCB durchgeführt hat. Dieses Verzeichnis enthält eine Beschreibung der vom Teilnehmer getroffenen Sicherheitsmaßnahmen gemäß Artikel 30 Absatz 2 der DSGVO;

(k) stellt der Teilnehmer der SNCB alle Informationen zur Verfügung, die erforderlich sind, um die Einhaltung der Verpflichtungen aus Artikel 3 nachzuweisen, und kooperiert bei Prüfungen, einschließlich Inspektionen, die von der SNCB, einem anderen von der SNCB beauftragten Prüfer und/oder einer zuständigen Behörde durchgeführt werden.

3.5. Der Teilnehmer kann sich bei seiner Untersuchung auf Dritte stützen. In diesem Fall muss der Teilnehmer sicherstellen, dass der Dritte von dieser Richtlinie Kenntnis hat und sich verpflichtet, bei der Hilfeleistung die Bestimmungen dieser Richtlinie einzuhalten, einschließlich der Vertraulichkeit, der Durchführung geeigneter Sicherheitsmaßnahmen und der in Artikel 3.3 genannten Grundsätze in Bezug auf Umfang, Art und Dauer der Verarbeitung. Der Teilnehmer erkennt an, dass er gegenüber der SNCB in vollem Umfang haftet, wenn der Dritte, auf den er sich verlässt, seinen Datenschutzpflichten nicht nachkommt.

3.6. Wenn der Teilnehmer personenbezogene Daten, die von der SNCB gespeichert und/oder anderweitig verarbeitet werden, in einer Weise verarbeitet, die dieser Richtlinie zuwiderläuft, oder zu anderen Zwecken als der Erkennung potenzieller Schwachstellen in den Systemen, erkennt der Teilnehmer an, dass er, als der für die Verarbeitung Verantwortliche angesehen wird und in vollem Umfang für die von ihm in diesem Zusammenhang durchgeführte Verarbeitung haftet. Der Teilnehmer hält die SNCB schadlos und entschädigt die SNCB in vollem Umfang für alle Ansprüche einer betroffenen Person oder eines Dritten sowie für alle damit zusammenhängenden Schäden, die der SNCB im Zusammenhang mit einem Verstoß des Teilnehmers (oder eines Dritten, für den der Teilnehmer bürgt) gegen seine Verpflichtungen in Bezug auf die Verarbeitung personenbezogener Daten entstehen.

4. Vergütungen

4.1. Die SNCB verpflichtet sich, dem Teilnehmer unter den folgenden Bedingungen eine Vergütung zu gewähren:

(a) die Schwachstelle ist bei der SNCB noch nicht bekannt;

(b) die Schwachstelle wurde zuvor nicht von einer anderen Person als dem Teilnehmer gemeldet; und

(c) die Meldung steht im Einklang mit dieser Richtlinie und ist vollständig.

4.2. Die SNCB behält sich das Recht vor, die Form dieser Vergütung nach eigenem Ermessen festzulegen.

4.3. Jede Forderung nach einer Vergütung außerhalb dieser Bedingungen wird als illegaler Erpressungsversuch gewertet.

5. Vorgehen

5.1. Entdeckung

Stellt der Teilnehmer Informationen über eine Schwachstelle fest, so führt er, soweit dies vernünftigerweise möglich ist, Vorabprüfungen durch, um das Vorhandensein der Schwachstelle zu bestätigen und etwaige Risiken zu ermitteln. Nach dieser ersten Einschätzung des inhärenten Risikos dieser Schwachstellen setzt sich der Teilnehmer gemäß Artikel 5.2. so bald wie möglich mit der SNCB in Verbindung.

5.2. Meldung

(a) Der Teilnehmer sendet alle Informationen über festgestellte Schwachstellen an die SNCB unter disclose@belgiantrain.be.

(b) Der Teilnehmer beachtet bei der Übermittlung von Informationen die folgenden Leitlinien:

(i) Der Teilnehmer kommuniziert auf Niederländisch, Französisch oder Englisch.

(ii) Der Teilnehmer verwendet das in 0 (Bericht über die Schwachstellen) enthaltene Formular und stellt alle darin geforderten Informationen, über die er verfügt, zur Verfügung. Die identifizierten Schwachstellen werden vollständig und detailliert beschrieben, einschließlich IP-Adressen, Logs, Screenshots, betroffene URLs usw. Es ist wichtig, dass die SNCB die Schwachstelle genau nachvollziehen kann, um diese zu beheben.

(iii) Der Teilnehmer bestätigt ausdrücklich, dass keine vertraulichen Informationen (direkt oder indirekt, rechtmäßig oder unrechtmäßig) erlangt von, oder über die SNCB, bei der Aufdeckung oder Bestimmung der Schwachstelle verwendet wurden.

(iv) Der Teilnehmer stellt bei Bedarf die entsprechenden Kontaktinformationen zur Verfügung, damit die SNCB die Meldung mit dem Teilnehmer weiterverfolgen kann.

(c) Die SNCB verpflichtet sich, dem Teilnehmer beim Erhalt einer Meldung so schnell wie möglich eine Empfangsbestätigung und die nächsten Schritte des Verfahrens zu übermitteln.

5.3. Kommunikation

(a) Die Parteien verpflichten sich, alle Anstrengungen zu unternehmen, um eine kontinuierliche und wirksame Kommunikation zu gewährleisten, um die festgestellte und gemeldete Schwachstelle zu ermitteln und zu beheben.

(b) Wenn nach einer angemessenen Frist keine Rückmeldung einer der Parteien vorliegt, können sich die Parteien an das Zentrum für Cybersicherheit Belgien (ZCB) (vulnerabilityreport@cert.be) als (Standard-)Koordinator wenden.

5.4. Untersuchung und Ziel

(a) In der Untersuchungsphase wird die SNCB die Umgebung und das festgestellte Verhalten des Teilnehmers reproduzieren, um die angegebenen Informationen zu überprüfen.
(b) Die SNCB wird den Teilnehmer regelmäßig über die Ergebnisse dieser Untersuchung und die aufgrund dieser Informationen getroffenen Maßnahmen informieren.
(c) Während dieses Prozesses berücksichtigen die Parteien ähnliche oder verwandte Berichte, bewerten das Risiko und den Schweregrad der festgestellten Schwachstelle und ermitteln alle etwaigen anderen betroffenen Produkte oder Systeme.
(d) Diese Richtlinie soll die Entwicklung einer Lösung zur Behebung von Systemschwachstellen ermöglichen, bevor (weitere) Schäden entstehen.

5.5. Öffentliche Bekanntmachung

(a) Die SNCB entscheidet nach Anhörung des Teilnehmers, wie das Vorhandensein einer Schwachstelle bekannt gegeben wird.

(b) Unter keinen Umständen wird eine Offenlegung erfolgen, bevor eine Lösung implementiert wurde und ein Sicherheitshinweis an die betroffenen Nutzer versendet werden kann.

(c) Eine öffentliche Bekanntmachung ist ohne die ausdrückliche schriftliche Zustimmung der SNCB nicht gestattet.

(d) Wenn eine Schwachstelle auch andere Organisationen betrifft, benachrichtigt die SNCB das ZCB (vulnerabilityreport@cert.be).

6. Geltendes Recht

6.1. Diese Richtlinie unterliegt dem belgischen Recht und ist nach diesem auszulegen. Alle Streitigkeiten in Bezug auf Gültigkeit, Auslegung oder Umsetzung der vorliegenden Richtlinie werden von den zuständigen Gerichten in Brüssel endgültig entschieden.

6.2. Das ZCB (vulnerabilityreport@cert.be) kann als Vermittler zwischen der SNCB und dem Teilnehmer bei Streitigkeiten im Zusammenhang mit der Anwendung der vorliegenden Richtlinie auftreten.

7. Dauer

7.1. Die vorliegende Richtlinie gilt ab dem 02.04.2026 und bleibt gültig, bis die SNCB eine Änderung gemäß Artikel 7.2 bekannt gibt.

7.2. Die SNCB kann diese Richtlinie ändern oder aufheben. Die SNCB wird wesentliche Änderungen an dieser Richtlinie durch Veröffentlichung auf der Website der SNCB bekannt geben. Sofern die SNCB nicht ausdrücklich etwas anderes bestimmt, treten Änderungen der vorliegenden Richtlinie dreißig (30) Tage nach ihrer Offenlegung in Kraft.

Anlage 1: Bericht über die Schwachstellen

Name: Vorname:	
(Anschrift/Land):	
E-Mail-Adresse: Telefonnummer:	
Beschreibung der Schwachstelle:	
Art der Schwachstelle:	
Details zur Konfiguration:	
Betriebssystem:	
Durchgeführte Vorgänge (Logs):	
Verwendete Werkzeuge:	
Daten und Zeiten der Prüfungen:	
IP-Adresse oder URL des betroffenen Systems:	
Wenn personenbezogene Daten verarbeitet werden:	• Arten von personenbezogenen Daten, auf die zugegriffen wird bzw. die verarbeitet werden: • Kategorien von betroffenen Personen (Kunde, Mitarbeiter, Lieferant): • Übermittlung von Daten an ein Land außerhalb der Europäischen Union oder des Europäischen Wirtschaftsraums bzw. Zugang zu einem solchen Land? Wenn ja: - geben Sie das/die betreffende(n) Land/Länder an: - senden Sie den ausgefüllten und unterzeichneten Anhang II zurück
Alle anderen relevanten Informationen:	
Anhänge (Bildschirmfotos).	
Dem ZCB gemeldet	Wenn die Schwachstelle auch dem ZCB gemeldet wurde, geben Sie bitte das Datum der Meldung an.
Mit der Übermittlung dieser Informationen bestätige ich als Teilnehmer an der Richtlinie der SNCB für die koordinierte Offenlegung von Schwachstellen ausdrücklich, dass meine Untersuchung und die oben genannten Informationen, die ich als Ergebnis meiner Untersuchung erhalten habe, in keiner Weise direkt oder indirekt auf vertraulichen Informationen von der oder über die SNCB beruhen oder aus diesen resultieren.	

Anlage 2: Übermittlung personenbezogener Daten außerhalb der EU und des EWR (modale vertragliche Klauseln)

Wenn der Teilnehmer von der SNCB ermächtigt wird, personenbezogene Daten von der SNCB an den Teilnehmer oder ein verbundenes Unternehmen des Teilnehmers zu übermitteln (oder jede weitere Übermittlung), in jedem Fall, wenn eine solche Übermittlung nach der Verordnung (EU) 2016/679 ohne den Schutz der übermittelten personenbezogenen Daten durch die Standardvertragsklauseln gemäß dem Durchführungsbeschluss (EU) 2021/914 der Kommission vom 4. Juni 2021 über Standardvertragsklauseln für die Übermittlung personenbezogener Daten an Drittländer gemäß der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates verboten wäre, in der jeweils von den zuständigen Behörden gemäß den im EWR geltenden Datenschutzgesetzen und -vorschriften geänderten oder ersetzten Fassung („EWR-Standardvertragsklauseln"), wird hiermit ausdrücklich zwischen der SNCB („Datenexporteur") und dem Teilnehmer oder einem der verbundenen Unternehmen des Teilnehmers (jeweils als „Datenimporteur") vereinbart, dass das anwendbare Modul 2 der EWR-Standardvertragsklauseln („EWR-Standardvertragsklauseln für Übermittlungen von Verantwortlichen an Auftragsverarbeiter"), das hiermit durch Verweis einbezogen wird, ab dem Beginn der betreffenden Übermittlung gilt, und sowohl die SNCB als auch der Teilnehmer bestätigen, dass:

- Klausel 7 (Kopplung) der Standardvertragsbestimmungen gilt;
- Klausel 9 (Einsatz von Unterauftragsverarbeitern) Anwendung findet, und die „Frist" einen (1) Monat beträgt;
- in Klausel 11 Buchstabe a (Rechtsbehelf) der fakultative Text nicht anwendbar ist;
- in Klausel 13 Buchstabe a (Aufsicht) folgender Text gewählt wird: „*Die Aufsichtsbehörde, die dafür verantwortlich ist, sicherzustellen, dass der Datenexporteur bei Datenübermittlungen die Verordnung (EU) 2016/679 einhält, fungiert als zuständige Aufsichtsbehörde (entsprechend der Angabe in Anhang I.C).*";
- „Option 1" in Klausel 17 (Anwendbares Recht) Anwendung findet und der „Mitgliedstaat" Belgien ist;
- in Klausel 18 (Gerichtsstand und Zuständigkeit) der Mitgliedsstaat Belgien ist;
- Anhang 1 von Modul 2 gilt als mit den relevanten Informationen des Artikels 3.3 dieser Richtlinie vorausgefüllt, die Parteien sind der Datenexporteur und der/die Datenimporteur(e), die Aufsichtsbehörde ist die belgische *Datenschutzbehörde* und die Verarbeitungen gelten als in dieser Richtlinie beschrieben; und
- Anhang 2 von Modul 2 gilt als bereits mit den relevanten Informationen aus den Artikeln (e) und (f) dieser Richtlinie ausgefüllt.