

Appendix E.4.3 – Agreement on data sharing and confidentiality in the context of marshalling services

This agreement is concluded between:

_____ (name of railway undertaking), _____ (legal form) with registered office at _____ and with company number _____, represented by _____

hereinafter referred to as "The Railway Undertaking"

_____ (name of user-operator), _____ (legal form) with registered office at _____ and with company number _____, represented by _____

hereinafter referred to as "The User-Operator".

INFRABEL, limited company under public law, with registered office at 1060 Brussels, Marcel Broodthaersplein 2 and with company number 0869.763.267, represented by Mrs Ann Billiau, in her capacity of Chief Client Officer.

Hereinafter referred to as "Infrabel"

PORT OF ANTWERP-BRUGES, limited company under public law, with registered office at 2030 Antwerpen, Zaha Hadidplein 1, and with company number 0248.399.380, represented by Danny Van Dessel, digital & analytics manager.

Hereinafter referred to as "PoAB"

RAILPORT ANTWERP, limited company under public law, with registered office at 2030 Antwerp, Zaha Hadidplein 1, and with company number 0538.888.250, represented by Mr Nils van Vliet, CEO

Hereinafter referred to as "Railport"

Hereinafter also referred to individually as "a Party" or collectively as "the Parties".

Context

In the context of the marshalling services, as stipulated in the "General conditions of use for the Antwerp-North marshalling facility for the provision of marshalling services to third parties" (hereinafter: "General Terms and Conditions"), the Parties are required to exchange certain data. This exchange between the Parties is necessary to enable efficient planning and execution of the marshalling services.

Because the data exchanged in some cases consists of business-sensitive information, and to ensure a level playing field between railway companies, the exchange of the data is subject to confidentiality obligations and use restrictions.

In this agreement, the Party required to disclose its information is referred to as the "Disclosing Party" and the Parties to whom the information is to be disclosed are referred to as "Receiving Parties".

Article 1 – Confidential Data to be communicated:

In the context of the marshalling services, the Parties shall provide each other with the Confidential Data as provided under the **Appendix** of this Agreement (this list is non-exhaustive and may be amended during the course of the Agreement, subject to the agreement of the Parties).

The following are not considered Confidential Data:

- a. Information already in the possession of a Receiving Party before being obtained from the Disclosing Party;
- b. Information that is or becomes public knowledge other than as a result of the breach of the agreement;
- c. Information disclosed by a Receiving Party pursuant to a law or regulation, or at the request of a competent court or competent government agency, provided (cumulatively):
 - that, in such circumstances, the Receiving Party informs the Disclosing Party as soon as possible, to give the Disclosing Party the opportunity to defend or protect itself against such dissemination or disclosure, or to limit it to the extent reasonably possible;
 - that the Receiving Party will disclose only the part of the Confidential Data that is required to be disclosed.
- d. Information disclosed to a third party pursuant to prior written authorisation from the Disclosing Party;
- e. Information legally obtained from a third party, without a similar confidentiality obligation.

Article 2 – Obligations of the Disclosing Parties

The Disclosing Parties:

- a. Ensure timely communication of the Confidential Data to be provided to the Receiving Parties. The requirement of communication to Receiving Parties shall be deemed to be fulfilled if the data is entered into a platform set up by a Receiving Party for that purpose, provided that the other Receiving Parties also have access to such data;
- b. Monitor the accuracy of the Confidential Data communicated, to the extent reasonably possible.

Article 3 – Obligations of the Receiving Parties

The Receiving Parties shall:

- a. Ensure to keep the Confidential Data strictly secret and confidential and not disclose it, in whole or in part, directly or indirectly, to any person, entity, organisation or administration (including any Representative thereof) without the prior written and specific consent of the Disclosing Party. The requirement of prior specific and written consent does not apply if the data is disclosed in the context of the operation of the Audit Committee as stipulated in Article 6 of the General Terms and Conditions;
- b. Limit access to the Confidential Data to their own staff, provided, however, that (i) these employees participate in the marshalling services, (ii) access to the Confidential Data is strictly necessary in the context of the marshalling services, and (iii) the employees are also bound by a similar confidentiality obligation;

- c. Protect the Disclosing Party's Confidential Data by paying the same amount of attention to it as to its own confidential data;
- d. Undertake to implement and respect the appropriate, technical and organisational security measures necessary to protect the Confidential Data, against, inter alia, destruction, loss, alteration, unauthorised disclosure or unauthorised access, without prejudice to the provisions of Article 6;
- e. Ensure that Confidential Data originating from third parties are only exchanged by the Parties if the third parties concerned have given their prior written consent.

The following shall not be considered a prohibited disclosure: informing other railway companies that a particular marshalling track or train path is already reserved or occupied, as well as the expected duration of such occupation, provided that this information is given without disclosing the identity of the Disclosing Party.

Article 4 – Permitted uses

Unless otherwise provided in this agreement, the Receiving Parties shall not use the Confidential Data disclosed to them for any purpose other than for the marshalling services.

The User-Operator is only allowed to use the Confidential Data for the performance of its duties as stipulated in the General Terms and Conditions. The User-Operator shall take appropriate organisational measures to limit the use of these data to what is permitted in this agreement.

Infrabel is authorised to use the Confidential Data in the framework of its duties as provided for in Article 199 of the Law of 21 March 1991 on the reform of some public companies, for internal statistics or data analysis. Any communication of the statistical data and analyses with stakeholders other than the Parties should always be anonymous so that no information of the third parties and their operations is disclosed.

Infrabel, PoAB and Railport are authorised to use the Confidential Data within the framework of an IT platform to be set up, which will aim to organise and optimise freight traffic for the entire port.

The RID data will only be used by the Receiving Parties for safety, security or disaster response measures.

Article 5 – Duration of obligations

The obligations set out in this agreement shall commence from the time the Disclosing Party has indicated its intention to use the marshalling services. They will remain in force for a period of 5 years or, if appropriate, whichever is longer, as long as the Confidential Data has not entered the public domain or lost its confidential nature, unless this is due to a breach of this agreement by the Receiving Party and/or its employees.

Article 6 – Fate of the Confidential Data after the termination of the marshalling services

Unless otherwise regulated in a future agreement to be concluded, the User-Operator undertakes to delete the Confidential Data in its possession as soon as possible and to the extent possible, and to destroy any copy or reproduction thereof.

Article 7 – Breach of obligations in this agreement

Failure, incompleteness, or delay in the communication of the Confidential Data by the Disclosing Parties shall constitute a breach of this agreement. Any damages arising from the failure, incompleteness, or delay in providing the Confidential Data to be communicated by the Disclosing Party shall not be recoverable from the Receiving Parties.

In the event of any unauthorised disclosure, access, or use of the Confidential Data, the Receiving Party undertakes to immediately notify the Disclosing Party in writing by providing full details of the breach and (ii) use its best efforts, at its expense, to remedy the breach and/or prevent further breach and remedy the consequences thereof.

Except in cases of wilful misconduct or gross negligence, in the event of an unauthorised disclosure, access or use of Confidential Data, the contractual and extra-contractual liability of the Party at fault shall be limited to a maximum amount of EUR 25,000 during the entire term of this Agreement.

Article 8 – Protection of personal data

The Parties will always comply with the applicable laws and regulations on data protection and the processing of personal data, and will deal appropriately and lawfully with any personal data processed in the scope of the marshalling services. They shall ensure that each data subject is properly informed, that a register of processing operations is kept and that appropriate technical and organisational measures are taken to protect the personal data they process. They will only process personal data in a manner consistent with the processing principles in the GDPR and only on a legitimate legal basis.

The Port of Antwerp-Bruges processes personal data in accordance with the statement found under the following link: <https://www.portofantwerpbruges.com/en/privacy-statement-notification-agreements>.

The parties shall ensure to provide the statement under the link to all persons whose personal data are processed by the Port of Antwerp-Bruges, in the context of the agreement and to treat these personal data, in accordance with the applicable laws and regulations on data protection and processing of personal data.

Agreement drawn up in Brussels in 5 originals, of which each Party declares to have received one copy. If the agreement is signed digitally, the requirement of multiple originals is deemed to be fulfilled under Art. 8.20 of the Civil Code.

For the **Railway Undertaking**,

Name:

Place and date:

Signature:

For **The User-Operator**,

Name:

Place and date:

Signature:

For **Port of Antwerp-Bruges**,

Name:

Place and date:

Signature:

For **Railport**,

Name:

Place and date:

Signature:

For **Infrabel**,

Name:

Place and date:

Signature:

APPENDIX: List of data exchanged

This list is non-exhaustive and may be modified during the course of the agreement subject to the agreement of all Parties.

- Planning data:
 - o By the User-Operator:
 - Connection plan (link between arriving and departing trains including scheduled wagons on arrival and departure)
 - o By the Railway Undertaking:
 - Train composition on arrival and departure
 - Marshalling orders with wagon details
 - Wagon data (wagon number, type of wagon, weight, length, special characteristics, RID info)
 - Train arrival/departure data (Characteristic/Date, Train number, Arrival/Departure time, Traction, Maximum length, Maximum tonnage, Braking regime, Origin/Destination)
- Real-time data:
 - o By Infrabel:
 - ETA arriving trains
 - o By the Railway Undertaking:
 - Train composition on arrival and departure
 - Real-time marshalling orders with wagon details
 - Wagon data (wagon number, wagon type, weight, length, special characteristics, RID (yes or no) + RID info)
 - o By the User-Operator
 - Location (track number) of the wagons in the Marshalling Facility
 - Duration of track occupation in yards C2 and B2