Transportministeriet

Aftalt førtidigt ophør af Kontrakten og overdragelse af togmateriel

Bilag 1: Transition Service Agreement (TSA)

GoCollective

Transitional Services Agreement

Between

GoCollective Holding A/S

Skøjtevej 26

DK-2770 Kastrup

Denmark

Company registration number: 44 69 98 18

(Hereinafter referred to as "Service Provider")

and

Selskabet af den 13.01.2026 A/S

c/o DSB

Telegade 2, Høje Taastrup

2630 Taastrup

Denmark

Company registration number: 46180011

(Hereinafter referred to as the "Service Recipient")

(Each referred to as a "Party" and collectively the "Parties")

Appendices

The following appendixes are enclosed and form an integral part of this agreement:

Appendix 1: Transitional Services Schedules ("TSS") – *presumably 4 subschedules*

Appendix 2: How to invoice DSB

Appendix 3: Data Processing Agreement

Appendix 4: Audit report (ISAE 3402 type II assurance report)

Appendix 5: Information Security Requirements

Appendix 6: Governance Model

Appendix 7: Nexus Mobilization Cost

1. Condition Precedent

1.1. This TSA is conditional upon

i. addendum no. 20 to the agreement between the Danish Ministry of Transport and GoCollective being duly signed by the Danish Ministry of Transport and GoCollective, and;

ii. such addendum subsequently being approved by the Danish Financial Committee.

1.2. If addendum no. 20 becomes void due to it not being approved by the Danish Financial Committee, this TSA shall automatically become void as well, without any Party incurring any liability towards the other Party as a result thereof.

2. Preamble

2.1. Pursuant to the handover of GoCollective's rail operation to the Service Recipient under the ownership of DSB, the Service Recipient must be able to continue the rail operation as it was prior to the handover. In this context, handover is to be understood as the date on which, as decided by the Danish Ministry of Transport, DSB took over the obligation to provide rail services in Central and Western Jutland and on the Svendborg Line from GoCollective, hereinafter referred to as the "Commencement Date".

2.2. The Service Provider has agreed to provide or procure the provision of certain services which are used in respect to the business of the Service Recipient (the "Services") set forth in the transitional services schedules (the "TSS") attached in appendix 1 to this transitional services agreement (the "TSA"), to the Service Recipient, and the Service Recipient has agreed to accept and pay for such Services on the terms and conditions of this TSA.

2.3. In parallel with this TSA, the Parties undertake, subject to mutual alignment on the terms, to enter into a separate agreement pursuant to which the Service Provider shall establish a standalone IT setup (the "IT Setup") for the Service Recipient. Such separate agreement shall enter into force as soon as practicable after the execution of this TSA and, in any event, no later than the Commencement Date of this TSA. Pursuant to such separate agreement, the Service Provider shall establish the IT Setup within twelve (12) months from the effective date of that agreement. The IT Setup shall comprise the IT systems necessary to enable the continued rail operation substantially as carried out immediately prior to the Commencement Date. As part of such agreement, the Service Provider shall ensure that ownership of the IT Setup is gradually transferred to the Service Recipient and that any licenses and other IT agreements required for the Service Recipient to use the IT Setup are put in place. As from the date falling twelve (12) months after the effective date of the separate agreement for the IT Setup, the Service Recipient shall have full ownership of and be entitled to use the IT Setup for the rail operation. Notwithstanding the foregoing, the Service Provider shall remain responsible for operating the IT Setup and providing the Services under this TSA until this TSA is terminated in accordance with its terms.

2.4. The term "Service Recipient" shall be deemed to include DSB (company registration number 25050053), being the parent company of the Service Recipient, to the extent DSB performs or may perform certain tasks on behalf of the Service Recipient. Accordingly, the Services may be provided directly to DSB as if DSB were the Service Recipient.

3. Services

3.1. The Services included are provided in accordance with the specification of the Services in each TSS. Any services not explicitly mentioned in a TSS are considered Additional Services as further defined in section 5 and are only provided subjected to a pre-agreed price for time and material.

3.2. Certain assets are transferred from the Service Provider, including group companies, to the Service Recipient on the Commencement Date. The Parties acknowledge that some of these transferred assets may be branded with the "GoCollective" name, logo, trademarks or other GoCollective-related markings. From and after the Commencement Date, the Service Recipient shall be solely responsible for removing or permanently covering all such branding and markings at its own cost and risk. The Service Recipient warrants that such removal or covering shall be fully completed as soon as reasonably practicable and, in any event, no later than twelve (12) months after the Commencement Date.

3.3. Notwithstanding the foregoing, from the Commencement Date the Service Recipient shall ensure that key customer-facing communications and customer touchpoints, including website, newsletters, customer service communications, marketing materials and any other proactive communications with customers, clearly identify the Service Recipient and its brand as the new operator and contracting party. The transitional period set out above (section 3.2) applies solely to the practical replacement or removal of physical and operational branding elements and shall not entitle the Service Recipient to continue conducting customer-facing activities or communications under the GoCollective name or brand following the Commencement Date.

4. Quality of Services

4.1. The Service Provider shall ensure that the Services are provided, in any material respect, in a manner and with a scope substantially similar to the standard and manner in which they were provided, as the case may be, immediately prior to the Commencement Date (as this term is defined in section 5). Hereunder, the Service Provider undertakes to ensure that the provision of the Services is afforded a level of priority no less favorable than that applied prior to the Commencement Date, and that the Service Provider shall not prioritize the provision of services to any group companies or other affiliated entities in a manner that adversely affects the Service Recipient.

4.2. When providing the Services, the Service Provider must apply reasonable due skill, care and diligence. Furthermore, the Service Provider must ensure compliance with applicable Danish law, including, but not limited to, the bookkeeping act (in Danish "bogføringsloven").

4.3. The Service Recipient undertakes to collaborate closely with the Service Provider in order to ensure the good performance of the Services. Each Service Recipient shall provide the Service Provider with information in its possession that is considered reasonable and proportionate to ensure the good performance of the Services and shall answer any reasonable written request for such information made by the Service Provider. Each Service Recipient shall keep the Service Provider informed in writing of any event that might have a negative impact on the performance of the Services.

4.4. The Service Provider undertakes to ensure compliance with the agreed Information Security Requirement, cf. appendix 6, for NIS2-critical systems.

4.5. If a Service Recipient makes a request to the Service Provider regarding the provision of a Service of which the Service Provider is in charge, the latter hereby undertakes to attend a meeting or a conference call with the Service Recipient having made the request without undue delay, in order to discuss about such request.

4.6. In case of non-compliance - if the Services fail to comply with the requirements set out in this TSA - the Service Recipient shall promptly give notice to the Service Provider in writing, setting out a reasonably detailed description of the non-compliance. The Service Provider undertakes to promptly investigate the non-compliance claimed by the Service Recipient and to take any relevant measures to ensure that the Services are delivered in accordance with the TSA. Service Provider shall respond in accordance with the principle of "*fix first, settle later*" that being to resolve the non-compliance according to DSB's requirements.

5. Reimbursement of external costs re. establishment of systems

5.1. Subject to agreement with the Service Recipient, the Service Provider has engaged external consultants to assist in preparing the necessary changes in existing systems, hereunder the ERP solution, allowing the Service Provider to provide the Services to the Service Recipient from the Commencement Date.

5.2. The Service Recipient shall reimburse the Service Provider for the documented costs and any applicable VAT related to the consultancy work performed by such external consultants on behalf of the Service Provider in accordance with Clause 5.1. The documentation on costs (in the form of an invoice from the external consultant) must include a description prepared by the external consultant on the scope of work, explicitly stating the tasks performed. The payment terms described in Clause 9 apply. The currently expected costs to external consultants are shown in appendix 7.

5.3. Internal hours spent by the Service Provider prior to the Commencement Date shall be borne by the Service Provider and will not be charged to DSB.

6. Additional Services

6.1. At any time during the Service Term (as defined below), each Service Recipient may request to the Service Provider the provision of additional services (the "Additional Services") not included under Appendix 1 as of the Commencement Date (as defined below).

6.2. The Service Provider shall consider in good faith any such request and will cooperate in good faith with the Service Recipient concerned to determine the costs and other terms and conditions under which those Additional Services could be rendered by the Service Provider.

6.3. The Service Provider shall promptly within ten (10) days at the latest notify in writing the Service Recipient concerned if the Service Provider accepts (with or without modifications) or rejects the request for Additional Services, such acceptance and notification not being unreasonably withheld, conditioned or delayed. In case the request for Additional Services is rejected, the Service Provider shall duly justify such refusal in writing.

6.4. Any Additional Service to be rendered in accordance with this section 5 shall be rendered by the Service Provider as soon as reasonably practicable as of the date on which the Parties agreed on the terms and conditions of such Additional Services.

7. Term and Termination

7.1. The TSA shall be in full force and effect as from the "Commencement Date" and shall not expire until it is terminated for convenience by either party by giving not less than six (6) months' prior written notice to the other Party, such notice to expire at the end of a calendar month.

7.2. Notwithstanding section 7.1 above, the TSA cannot be terminated during the first eighteen (18) months from Commencement Date. Hence, the earliest time the TSA can expiry due to a termination for convenience is eighteen (18) months after the Commencement Date subject to a termination notice has been sent at the latest twelve (12) months after the Commencement Date.

7.3. The TSA may be terminated in whole or in part with respect to one or more Services (TSS). For the avoidance of doubt, the termination of the Services under one or more TSS shall not result in the termination between the Service Recipient and the Service Provider of the TSA, which shall remain in full force and effect as long as any other Service is still being provided by the Service Provider. Services within each TSS cannot be terminated partially, unless subject to an agreement between the Parties.

7.4. Each Party may, without limiting its other rights and remedies, terminate this TSA or the Services, by giving a written notice thereof to the other Parties, if one of the other Parties commits a material breach of its obligations under this TSA which is not remedied within thirty (30) calendar days after serving written notice requiring such breach to be remedied.

7.5. Upon expiry or termination of this TSA, in accordance with its terms, at the Service Recipient's request, the Service Provider shall return to the Service Recipient - or alternatively delete/destroy - all documents which are deemed Confidential Information received for the purpose of or in connection with the implementation of the TSA, unless the Service Provider is required by law, regulation or similar to maintain the information.

8. Standalone Infrastructure

8.1. Subject to the intention of the Parties to enter into a separate agreement re. assistance in the establishment of an independent IT-setup at the Service Recipient, it shall be the sole responsibility of the Service Recipient, upon and after expiry or early termination of a Service, to ensure that adequate procedures are in place so that such Service may be provided from that time either by themself or by any of their affiliates or by a successor operator, or no longer be required. No Service Term in respect of a given Service shall under any circumstances be construed as any kind of guarantee or undertaking by the Service Provider that such term shall be sufficient to allow the Service Recipient to implement their business and activities on a standalone basis as from the end of such Service Term.

8.2. Upon termination of any Service under any of the TSS, the Service Provider shall provide the Service Recipient with such information and assistance, including transfer of relevant

knowledge, on-the-job training of personnel, etc., as is reasonably necessary to complete an orderly transfer of the relevant Service or Services from the Service Provider to the successor operator (which may be the Service Recipient themselves, any of its affiliates or a third-party) and shall assist in providing to such successor operator the Service Recipient' data in their possession in its then current format in a readable format compatible with Excel and SAP. Any assistance related to the orderly transfer of a relevant service exceeding 8 hours of work will be considered as outside the scope of a "reasonable effort". Such will instead be considered an additional service and shall be treated in accordance with section 5 in this TSA.

8.3. Once the Service Provider has provided the Service Recipient' data, the Service Provider shall delete or destroy any copy of such data in its possession, unless it would be required to maintain a copy of such data pursuant to any applicable Law.

9. Price and Payment

9.1. The Service Recipient shall pay to the Service Provider, in respect of each Service, the price for such Service as specified in the relevant TSS (the "Charges").

9.2. In excess of the Charges, the Service Provider must pay a fixed compliance fee of DKK 141.667,00,- per month excl. of VAT (the "Compliance Fee") as long as the TSA is applicable, irrespective of the number of applicable TSSs. A contribution margin of 5 % will be added to the cost excl. VAT.

9.3. The monthly fee for the services must be paid no later than on the third (3) last business day of that month subject to the Service Recipient having received an invoice from the Service Provider at the latest thirty (30) days in advance. The Service Provider shall invoice the Charges electronically in accordance with the invoicing requirements stipulated in **Appendix 2**.

9.4. All invoices/credit notes shall identify the Charges included using: (i) the delivery/Part ID number used in Appendix 1, (relevant subschedule/TSS) a description of the Services charged and time of delivery; and (ii) purchase order number as well as the receiving company's EAN-number. Any failure to directly link these items can result in a rejection of the invoice.

9.5. Additional Services will be provided subject to an hourly fee of 850,00 DKK excl. VAT. Any third-party costs or other costs incurred to provide the additional services will be passed on as-is, however subject to an addition of 5 % as administrative fee by the Service Provider.

9.6. All prices will be indexed yearly based on the increase in the SBLON1, sector C, Industry-index from October (K3) till October (K3). The first indexation will take place January 1, 2027, based on the increase of the index from October 2025 till October 2026.

9.7. All invoices submitted by the Service Provider in accordance with this TSA shall be paid by the Service Recipient in cleared funds to the bank account or accounts designated by the Service Provider to the Service Recipient 30 days after the Service Recipient has received the correct electronic invoice in accordance with **Appendix 2**. Payment is deemed to have been made, when the amount is debited from the Service Recipient's bank account.

9.8. All prices or rates specified in or deriving from this TSA do not include any applicable value added tax or other similar duties and taxes (if any) ("VAT"). Where VAT is chargeable on a

supply of Services pursuant to this TSA, the Service Recipient will pay to the Service Provider an amount equal to such VAT in addition to the agreed price or rate payable in consideration for the supplied Services.

9.9. If any taxes or duties are required to be deducted or withheld from any payments made by the Service Recipient to the Service Provider hereunder, then the Service Recipient shall (i) withhold or deduct the required amount and promptly pay such taxes or duties to the relevant tax authority and (ii) pay additional amounts to the Service Provider so that the net amount actually received by the Service Provider after such withholding or deduction of tax or duty be equal to the amount that the Service Provider would have received had no such withholding or deduction been required or tax or duty been imposed.

9.10. All sums payable hereunder which are not paid in a timely manner shall bear interest at a rate equal to the rate determined by the Danish act on interest ("renteloven") from the date payment was due through and including the date on which payment is made.

9.11. In addition to the above, if a payment is not made to the Service Provider although due in accordance with this section 8, the Service Provider shall have the right, exercisable upon fifteen (15) days' advance written notice, without any liability arising therefrom for the Service Provider, to cease providing the Service(s) for which payment has not been made until payment in full is made, provided that the demand for payment is undisputed or the disputation of a payment is not objectively reasonable.

9.12. Each Party will be solely responsible for the employment and remuneration of its employees and subcontractors and any claims with respect thereto, and will be solely responsible for the payment of all taxes and social charges applicable to it, or such employees and subcontractors. Each Party acknowledges that, as an independent contractor, neither it nor any of its employees or subcontractors will be eligible for any employee benefits of the other Party, including, but not limited, to vacation, medical, dental, or pension benefits.

10. Audit Reports

10.1. Subject to DSB's written request, each year, by mid-January the latest, the Service Provider must provide audit reports (ISAE 3402) prepared by an auditor of high reputation and in accordance with international standards or allow other audits as required by DSB. The requirements for audits and audit reports appear from **Appendix 4.**

10.2. The Service Provider is entitled to invoice the Service Recipient for the costs associated to obtain the audit report in accordance with Clause 9.5 regarding additional services.

11. Liability

11.1. Subject to the mandatory rules of applicable law, the liability of the Service Provider shall not exceed the amount of the fees paid by the Service Recipient under the TSA within the last twelve (12) months, or – if the TSA is terminated prior to twelve (12) months from the Commencement Date – the calculated fee for a twelve (12) months period based on the average monthly fee paid since the Commencement Date.

11.2. Notwithstanding any provision of this TSA to the contrary, each Party shall not be liable to the other Party (i) for any loss of opportunity and any indirect damages of any kind incurred by

the other Party resulting from, or arising out of or in connection with, this TSA, and (ii) for any expenses other than reasonable expenses incurred in connection with defending or asserting any third party claim exclusively and directly related to a matter indemnified under the TSA (such reasonable expenses, excluding, for the avoidance of doubt, any management time and similar costs).

11.3. The limitation of liability set out in this Clause shall not apply to the extent that a loss or damage is caused by the Service Provider's willful misconduct or gross negligence or if an authority issues a fine, enforcement notice or similar directly to the Service Provider – eg. as a sanction for a GDPR-breach. Furthermore, the limitation of liability shall not apply with regard to any third party claims concerning breach of intellectual property rights.

12. Confidentiality

12.1. During the term of this TSA and three (3) years thereafter, the Parties shall maintain in confidence and not disclose the other Parties' Confidential Information (as defined below), using the same degree of care, but no less than reasonable care, as it uses to protect its own confidential information of like nature. The Service Provider may use Confidential Information only for the purposes of providing the Services to the Service Recipient and fulfilling its obligations under this TSA (the "Permitted Purpose"). The recipient of any Confidential Information may disclose such Confidential Information only to its Affiliates and their respective employees or contractors who have a need to know such information for the Permitted Purpose. Confidential Information may not be reproduced, except as required for the Permitted Purpose.

12.2. At request of the disclosing Party, upon expiry or termination of this TSA, the recipient of any Confidential Information agrees promptly to return or destroy, at the disclosing Party's option, all materials owned or communicated by the other Party that disclose or embody Confidential Information.

12.3. For the purpose of this section 10, "Confidential Information" means any information of a confidential nature relating to the business of either Party or its Affiliates which is disclosed to the other Party in connection with the provision of the Services, excluding any information that the recipient can demonstrate: (a) was publicly known at the time of disclosure to it, or becomes publicly known through no act of the recipient, (b) was rightfully received from a third party without a duty of confidentiality; or (c) is required to be disclosed pursuant to any applicable law or regulation or any decision or request from any court, governmental authority, including the Danish Ministry of Transportation, or regulatory body, in which case the recipient of the Confidential Information shall promptly notify the disclosing Party and take reasonable steps to assist in contesting such order or in protecting, to the permitted extent, the disclosing Party's right prior to disclosure.

12.4. The Parties have entered into a separate NDA covering the confidential material shared prior to and during the handover.

13. No Agency, Joint Venture or Partnership

13.1. Except as otherwise provided herein, no Party will have any right, power or authority to create any obligation, express or implied, on behalf of any other Party nor shall either Party act or

represent or hold itself out as having authority to act as an agent or partner of the other Party, or in any way bind or commit the other Party to any obligations. Nothing in this TSA is intended to create or constitute a joint venture, partnership, agency, or other association of any kind between the Parties, and each Party shall be responsible only for its respective obligations as set forth in this TSA.

14. Force Majeure

14.1. The obligations of a Party shall be suspended during the period and to the extent that such Party is prevented from complying therewith by an event of force majeure as defined by Danish law and Danish case law (including, for avoidance of doubt, any circumstances beyond its reasonable control such as civil disturbances, accidents, pandemics, strikes, acts of terrorism, act of war or conditions arising out of or attributable to war whether declared or undeclared) (a "Force Majeure Event").

14.2. In such event, the Party affected by a Force Majeure Event shall give notice of suspension as soon as possible to the other Party stating, if possible, the date and extent of such suspension, the cause thereof and, to the extent possible, the projected duration of such Force Majeure Event, and the Party affected by the Force Majeure Event shall resume the performance of such obligations as soon as possible after the removal of the cause of such suspension. A Party shall not be liable for any loss suffered by the other Party as a result of or in relation to a Force Majeure Event.

15. Intellectual Property – Limited License

15.1. The Service Recipient is granted by the Service Provider a non-exclusive, non-transferable, non-sub licensable right to use any intellectual property rights required to receive and use the Services, in particular on the software and documentation mentioned in the TSS, solely to the extent needed to receive and use the Services and in any event strictly subject to the confidentiality obligations contained in section 9 hereof.

15.2. Any license granted hereunder shall terminate ipso facto upon expiry or early termination of the TSS relating to the relevant Service or, with respect to licenses relating to IT systems, upon the gradual transfer of such IT systems to the Service Recipient as part of the establishment of the IT Setup pursuant to the separate agreement intended to be concluded between the Parties.

16. Intellectual Property – Documentation

16.1. For the duration of the TSA, the Service Recipient grants the Service Provider a non-exclusive, non-transferable and not sub-licensable license to use, copy, modify and enhance the Service Recipient's documents and data during the Service Term, however only for the purposes of allowing the Service Provider to perform its obligations under this TSA.

16.2. In case of the Service Provider's changes of data and documents, or addition of new data and documents, belonging to the Service Recipient, all rights including intellectual property rights to such changes or new data shall belong to the Service Recipient.

17. Service Provider's Employees

17.1. The employees of the Service Provider who carry out the Services shall remain under the authority and the exclusive subordination of the Service Provider which, as a consequence, is the only entity that may, in particular, determine the working conditions for these employees and exercise disciplinary authority over them. In this respect, each Service Recipient undertakes not to give any orders or instructions to the employees of the Service Provider carrying out the Services.

17.2. As a result, no provision of this TSA intends to create or may lead to an employment relationship being created between the Service Recipient and the Service Provider or any of its employees, representatives or subcontractors.

17.3. The Service Provider undertakes that it will comply with any applicable tax, social security and labour rules to which it may be subject in connection with the employment of its employees carrying out the Services as well as with DSB's Ethical Guidelines.

17.4. The employees of the Service Provider carrying out the Services will however be required to comply with all the provisions of the internal rules and health and safety rules which apply to them when they work in the Service Recipient' premises.

18. Governance

18.1. With the purpose of ensuring a close, agile and trustful cooperation between the Parties for the term of this TSA, the Parties have agreed to implement and work by the governance model described in **Appendix 6**.

During the term of this TSA, and in respect of each of the TSS, each Party will appoint one of its employees who will have overall responsibility for managing and coordinating the delivery or receipt of the Services under each of the TSS. During the term of this TSA and upon providing notice to the other Party, each Party may, at its discretion, select other individuals in replacement of the then current Chief Representative

18.2. The appointed representatives shall meet whenever required and if no other agreement is made bi-weekly during the first three (3) months to review the services provided, agreed KPIs and the cooperation in general. After the first three (3) months, or if the appointed representatives agree earlier, the meeting interval shall be changed to a monthly meeting.

18.3. In the event of a dispute between the Parties in connection with this TSA, the Parties shall seek to enter into negotiations with a view to resolving the dispute with a positive, cooperative and responsible attitude. If necessary, after discussion between the Parties, efforts shall be made to raise the negotiations to a higher level in the organizations of the Parties.

18.4. In case of any conflict or inconsistency between the terms and conditions of this TSA and the terms of any TSS, the provisions of the TSA shall prevail.

19. Successors and Assigns

19.1. Neither Party may assign any of its rights or delegate any of its duties or obligations under this TSA without the express written consent of the other Party, such consent not to be unreasonably withheld. The Service Recipient shall be entitled to request sufficient

documentation for an equivalent level of credit worthiness to the extent that the Service Provider wishes to assign any of its duties or obligations (i) to any of the Affiliates of the Service Provider or of its permitted successive assignees or transferees; or (2) in connection with a merger, demerger, reorganization, sale of business or similar transaction involving the Service Provider or its permitted successive assignees or transferees.

20. Subcontracting

20.1. The Service Provider is authorized to subcontract the Services in whole or in part.

20.2. The Service Provider shall remain responsible for its obligations under this TSA performed by any subcontractors to the same extent as if such obligations had been performed directly by the Service Provider.

21. Entire Agreement and Amendments

21.1. This TSA and all TSS set forth the entire understanding of the Parties hereto with respect to the subject matter hereof and supersede all prior contracts, agreements, arrangements, communications, discussions, representations and warranties, whether oral or written, between the Parties.

21.2. This TSA may be amended only by a written agreement executed by the authorized representatives of the Parties.

22. Place of jurisdiction & applicable law

22.1. Any dispute arising out of or relating to this TSA, or the breach thereof, shall, unless otherwise agreed, be settled by the Danish courts in accordance with Danish Law. Danish private international law, which refers to foreign law, as well as the United Nations Convention on Contracts for the International Sale of Goods (CISG), shall not apply.

Signatures

For GoCollective

Signed by:
0A3C4EB1556943F...
Name: Henrik La Cour
Title: CEO

Signed by:
F58BFEFD3ACE43A...
Name: Markus Honner
Title: CFO

For Selskabet af 13.01.2026 A/S

DocuSigned by:
Pernille Damm Nielsen
C2D41CB3A6B14DC...
Name: Pernille Damm Nielsen
Title: CEO

Signed by:
Flemming Jensen
B1552943F30C4FF...
Name: Jens Flemming Jensen
Title: Chairman of the board

GoCollective

Appendix 1: Transition Service Schedule (TSS)
IT

Services Provider	GoCollective Holding A/S
Services Recipient	Selskabet af den 13.01.2026 A/S
Description of provided services	The services are provided, in any material respect, in a manner and with a scope substantially similar to the standard and manner in which they were provided, as the case may be, immediately prior to the commencement date of this TSS. There will be no guaranteed response time on solving services issues (Tickets), all services will be delivered as a best effort. The services provided include: • Services in general that are a prerequisite for the Service Recipient's IT-infrastructure to operate. • Operation, maintenance and 1st level remote support of systems (see list below) • Data and reporting through existing integrations • Operation, maintenance and support of IT Infrastructure and network • IT security through security systems, access controls, endpoint protection, awareness training and threat monitoring • General IT operation and support, including helpdesk-function, IT development (internal systems only) and change management. • Supporting Annual Salary Adjustment process (compensation module) and Performance & Goals process (performance and goals module) in SuccessFactors, conditioned upon the process is run at the same time as GoCollective runs it. • GoCollective assigns the licenses needed for the Service Recipient's employees to conduct their tasks. Notwithstanding the above, the services provided do <u>not</u> include: • 2nd and 3rd level support of third-party systems. Such may be subject to a fee. • Significant development tasks (more than 10 hours) in internal systems. These are limited to minor development tasks. Anything beyond will be subject to a change request and subject to a fee as further described in the TSA. • Any compliance, regulatory, governance, or audit obligations applicable to the Service Recipient. The Service Provider's responsibilities are strictly limited to technical operation of the agreed IT systems and platforms and do not extend to ensuring or documenting compliance with applicable laws, regulations, or internal policies of the Service Recipient. • Local on-site support • Any service regarding carve out, this is handled as projects and are invoices apart from this agreement.
Systems/assets involved	<u>Operating Systems & End-User Software</u> M365 environment Configuration and support for servers, systems and databases in datacenter Configuration and support for servers, systems and databases in MS Azure Azure Tenant License management within PCs tablets, mobile phones and printers

GoCollective

Appendix 1: Transition Service Schedule (TSS)
IT

	ERP (SAP / xSuite / Prometheus) Arkyn SuccessFactors Azets Perspektiv (Payroll system) incl. MIT Perspektiv (module for the payroll system) Omnia / SLS Sitra / Supeo CompuLogic (SMS provider) Integrations (SnapLogic / SFTP) AWS platform IT Infrastructure & Networking Configuration of Network (routers, switches, access points) MPLS IT Security Microsoft defender (EDR) Rapid7 Firewalls,	
Duration of services	According to TSA	
Cost of Services	FTE cost per months: DKK 354.166,67 excl. VAT External cost of systems per months: Re-invoicing of the actual cost *A contribution margin of 5 % will be added to the joint cost of FTE and external systems excl. VAT.* As described in Clause 1.3 of the TSA, the Parties intend to enter into a separate agreement regarding the Service Provider's establishment of a stand-alone IT environment (the "IT Setup") for the Service Recipient. Ownership of the IT Setup, and the rights to use the related IT systems and licenses, shall be transferred to the Service Recipient on a gradual basis. Accordingly, the external costs of systems covered by this TSS shall be reduced during the term of the TSS to reflect the Service Recipient's gradual assumption of ownership and license rights. For the avoidance of doubt, the transfer of ownership shall have no impact on the services to be rendered by the Service Provider to the Service Recipient during the term of this TSS.	
Other particulars (if any)	None.	
Contact information	For the Service Provider Henrik C. Andersen IT Director henrik.c.andersen@gocollective.dk +45 2324 9507	For the Service Recipient

GoCollective

Appendix 1: Transition Service Schedule (TSS)
BI

Services Provider	GoCollective Holding A/S	
Services Recipient	Selskabet af den 13.01.2026 A/S	
Description of provided services	The services are provided, in any material respect, in a manner and with a scope substantially similar to the standard and manner in which they were provided, as the case may be, immediately prior to the commencement date of this TSS. The services provided include: • Operation, maintenance and troubleshooting of data pipelines and integrations • Maintenance of data models, schemas and database structures, and ensuring correct propagation of SAP-driven hierarchy changes (also including MUX hierarchy updates) into BI reporting. BI ensures correctness from hierarchy onwards to reporting • Maintenance and operational support of reports and dashboards. • Ensuring continued availability and functioning of dashboards and reports (no design changes). • Support related to business rules, transformations and KPI logic – without modification • Forecast and KPI integration • Data quality and governance • Providing operational support for the use of BI insights and enabling decision-making by maintaining access to BI insights modelling • Ensuring continued access to the BI platform, including credentials, permissions and environments as they are constituted at commencement of the TSS. Notwithstanding the above, the services provided do <u>not</u> include: • The services do not include onboarding or integration of new data sources beyond those already in use. • The services do not include development or expansion of new data models beyond the existing BI setup. • The services do not include creation or design of new reporting solutions outside the current reporting landscape. • The services do not include enhancements or functional changes to existing data pipelines, transformations or KPI structures.	
Systems involved	DataHub Reporting – AWS (BI)	
Duration of services	According to TSA	
Cost of Services	FTE cost per months: DKK 70.833,00 excl. VAT External cost of systems per months (re-invoicing): None (external costs are covered by the IT-TSS) *A contribution margin of 5 % will be added to the total cost excl. VAT.*	
Other particulars (if any)	None.	
Contact information	<u>For the Service Provider</u>	<u>For the Service Recipient</u>

Appendix 1: Transition Service Schedule (TSS)
BI

	Tristan David Willacy Head of BI tristan.willacy@gocollective.dk +45 2465 3178	

GoCollective

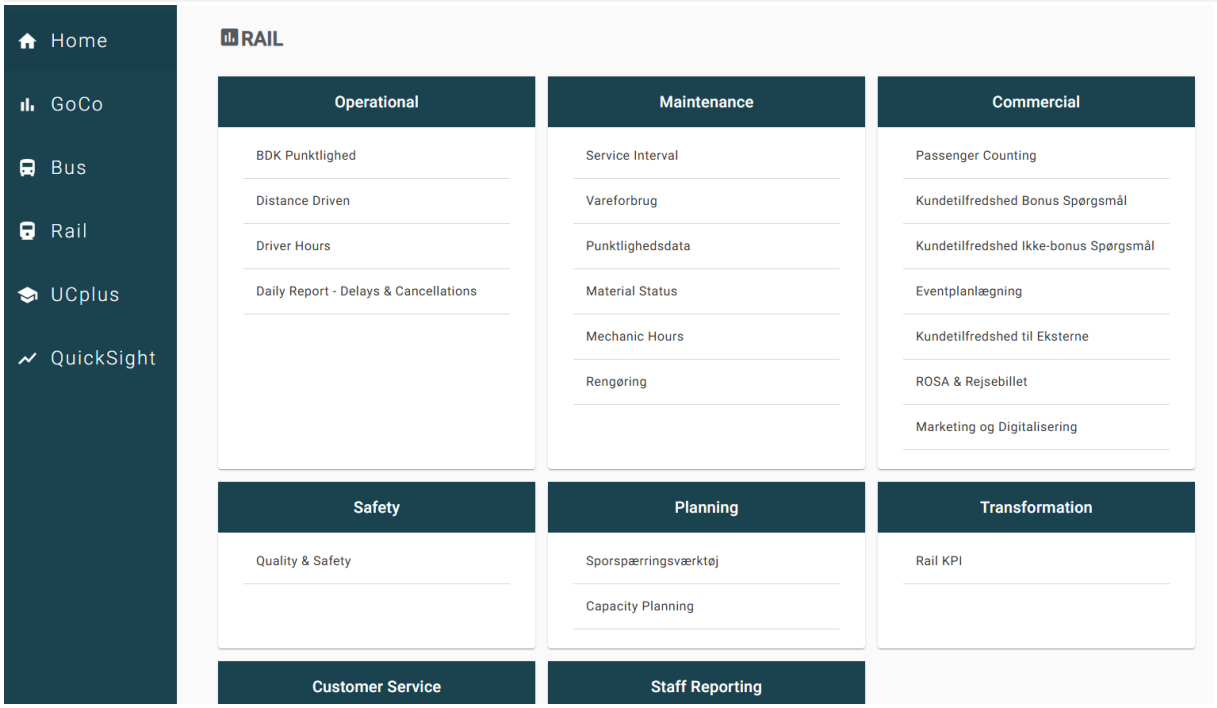
Appendix 1: Transition Service Schedule (TSS)
BI

Annex 1

GoCollectives – Power BI rapport

- GoCollective's rapporteringssystem er baseret på "Datahub" med data træk fra følgende forskellige Sources:
- *Adibus, Admire, BDK, Chekc-ind, DSB (Rosa), Figree, Excelupload, Mainsupply, KMD, Metacompliance, Multiple, Rejsebillet, Rejsekort, SAP, Succesfactor, Supeo og Trapeze.*

GoCollective's rapporteringssystem (bu



GoCollective

Appendix 1: Transition Service Schedule (TSS)
Finance and Accounting

Services Provider	GoCollective Holding A/S
Services Recipient	Selskabet af den 13.01.2026 A/S
Description of provided services	The services are provided, in any material respect, in a manner and with a scope substantially similar to the standard and manner in which they were provided, as the case may be, immediately prior to the commencement date of this TSS. The services provided include: • Accounts payable management (entire P2P process) • Invoice handling (w/PO and wo/PO, invoice approval, Master Data maintenance Business Partner, vendor payments (when and covering period?), closing operations, vendor communication and reconciling vendor statements, internal and external queries, GR/IR • Accounts receivable management (entire O2C process) • Invoice/credit note handling, Master Data maintenance for customers – Business Partner, bad debt administration quarterly, incoming payments, dunning, internal and external queries, maintenance WBS elements (capex, revenue) • Fixed assets (investments/IFRS16/reconciliations) • Master Data maintenance, posting asset transactions, depreciation run, closing operations and monthly reconciliations. Accounting for IFRS16 leasing if relevant • Intercompany transactions and reconciliations • Bank transactions (Danske Bank), including securing sufficient cash balances (cashpool process). Includes T&E, SAP CoA maintenance, maintenance SAP Autobank set-up • Reporting VAT Denmark, foreign VAT and taxes • Monthly reporting to DSB and Financial Statement preparation in Caseware • Relevant GL reconciliations for above areas including handling of audit documentation and questions • System maintenance for systems mentioned in “Systems Involved” • Create/change profit centers and cost centers incl. hierarchies • Fuel Price Updates in SAP: Weekly update of contracted fuel prices in SAP. • SAP Support, training and documentation including onboarding of new users • SAP MM support incl. tickets and data maintenance and Commercial support to improve efficiency • Maintain reporting templates and visuals (Group Controlling) • Maintain planning & forecast templates (Group Controlling) Notwithstanding the above, the services provided do <u>not</u> include: • Cash Flow / Treasury Management • VAT advises • Tax advises • German VAT • Transfer Pricing • Insurance and claims handling • Audit administration (all dialog with auditors about materials related to above mentioned areas are handled by GC)

Appendix 1: Transition Service Schedule (TSS)
Finance and Accounting

	• Potential future compliance matters or extra work connected to new accounting standards/requirements (time and material)	
Systems involved	SAP xSuite Oillink Fuel Management System (FMS) Sproom DataHub	
Duration of services	According to TSA	
Cost of Services	FTE cost per months: DKK 318.750,00 excl. VAT External cost of systems per months: Re-invoicing of the actual cost *A contribution margin of 5 % will be added to the joint cost of FTE and external systems excl. VAT.*	
Other particulars (if any)	None.	
Contact information	For the Service Provider Pia Haugsted Head of Financial Controlling & Accounting pia.haugsted@gocollective.dk +45 2276 1710	For the Service Recipient

GoCollective

Appendix 1: Transition Service Schedule (TSS)
Payroll

Services Provider	GoCollective Holding A/S
Services Recipient	Selskabet af den 13.01.2026 A/S
Description of provided services	The services are provided, in any material respect, in a manner and with a scope substantially similar to the standard and manner in which they were provided, as the case may be, immediately prior to the commencement date of this TSS. The services provided includes but are not limited to: • In-house payroll processing from A–Z. Payroll processing in the payroll system, including accruals and ongoing settlement of vacation, and monthly posting of payroll in SAP. Monthly comments to Business Controlling. Further includes handling of mileage and allowances refunds. • Data processing, mapping and integration between SuccessFactors, and the payroll system. Integration between Trapeze and the payroll system, including handling of absence and payroll in the payroll system. • Statutory reporting, includes monthly reporting to Danmarks Statistik, DI membership fees and funds (barsel etc), and tax reporting to SKAT. • Pension administration, includescontact with Danica regarding updates of white-collar employees (entries and exits), PensionDanmark, and HTS. • Reconciliations (S73, GL-accounts), including monthly GL account reconciliations for all payroll-related balance sheet accounts and quarterly true-ups. Invoice handling for payroll related expenses (Azets, TMN, ATP, DI, etc.).Reimbursement applications (sickness, maternity, flex) • Reimbursement applications related to courses and training, including AMU and VEU. These applications are handled by UCplus. • General system maintenance of minor updates for Azets Perspektiv, Mit Perspektiv and SuccessFactors • First line system support and system maintenance for Trapeze, CrewWeb and CrewApp2. • Update rates for local and collective agreements. Simple adjustments to below mentioned systems Notwithstanding the above, the services provided do <u>not</u> include: • System maintenance: Implementation of new system features and renegotiated Local agreements and collective agreements (This will be a payable service). • Maintenance of employee and organisational master data in SuccessFactors and Trapeze.
Systems involved	Azets Perspektiv (Payroll System) Mit Perspektiv (Payroll System) SuccessFactors Trapeze CrewWeb (Trapeze) CrewApp2 (Trapeze)
Duration of services	According to TSA
Cost of Services	FTE cost per months: DKK 162.916,67 excl. VAT External cost of systems per months: Re-invoicing of the actual cost

Appendix 1: Transition Service Schedule (TSS)
Payroll

	A contribution margin of 5 % will be added to the total cost excl. VAT.	
Other particulars (if any)	None.	
Contact information	For the Service Provider Pia Haugsted Head of Financial Controlling & Accounting pia.haugsted@gocollective.dk +45 2276 1710	For the Service Recipient [X]

How to invoice DSB

To facilitate the handling of invoices in DSB's "vendor invoice management system" and ensuring timely payment, the Supplier must make sure that the following information is included in each invoice submitted to DSB for payment:

1. Identification of the purchase order number received from DSB (PO no.) or the requisitioner's e-mail address. The purchase order number starts with the numbers 42, 45, 48 or 58 and consists of 10 digits. (A sample purchase order from DSB can be found below)

2. The EAN-location number of the relevant DSB company, which the Supplier are invoicing. (The EAN location numbers are listed below).

3. Non-Danish Suppliers may submit their invoices as pdf-files to: faktura@dsb.dk. (An automatic reply will appear in Danish. Please disregard any advice that invoices by email will not be accepted as this only applies to companies with a Danish business address).

4. The Supplier's account information for transfer of money and if available the Supplier's VAT.

DSB
Group Procurement

January 2026

DSB
Telegade 2
2630 Taastrup
Denmark

Phone 0045 33 53 44 44
indkob@dsb.dk
www.dsb.dk

EAN-location numbers:

Navn	**EAN-nummer**	**CVR-nummer**
DSB	DSB 5798009883698	25050053
	DSB Division Vedligehold 5790001963613	
DSB Service & Retail A/S	5790001704742	10882230
DSB Ejendomsudvikling A/S	5790001775018	31631238
Selskabet af 23.05.2017 46DD A/S	5790002425172	38630830
Selskabet af 28.08.2017 67DD A/S	5790002430411	38874675
Selskabet af 04.09.2020 EB A/S	5790002597114	41120347
Selskabet af den 04.01.2021 EB A/S	5790002610226	42010944
Selskabet af 03.01.2022 EB A/S	5790002644566	42948535
Fladsågårdsvej 2 ApS	5790002828065	44854902
Rosbjergvej 100 ApS	5790002828089	44854929
Carsten Niebuhrs Gade 48 ApS	5790002828072	44854899
DSB EU Jernbanebyen 1 ApS	5790002711664	43726137

EC2025	5790002845000	45460398
DSB EU Vingelodden P/S	5790002851841	45935469

A sample purchase order from DSB:

Purchase order

Doc: 4800017813

Supplier address

Date 02.12.2015

EAN. 5798000893474

SE-nr. DK15013907
CVR. 25050053

Reference: Central Shared Service
Phone: 33534444
Email: indkob@dsb.dk
Questions concerning payment: kreditor@dsb.dk

Currency USD
Terms of delivery: DDP dsb (Frit Leveret)

Invoice address:
DSB
Kreditorbogholderiet
Telegade 2
2630 Taastrup
EAN-nr: 5798000893474

Delivery address:
DSB Koncern
IT-Udvikling & Vedligehold
Telegade 2
2630 Taastrup
att. Marianne Stub-Holm

Ite.	Par no (supplier)	Delivery	Quantity Unit	Net price
10	Quote 20035437 Details		1 PC	10.605,06

Total net value excl. tax: USD 10.605,06

Changelog

CHANGE	VERSION
1.1.	Clauses 9.2. and 10.4., *(Corrected cross-references).*
1.2	Clause 7.6 (*now made optional and amended wording*)

Standard Contractual Clauses

For the purposes of Article 28(3) of Regulation 2016/679 (the GDPR)

between

Selskabet af den 13.01.2026 A/S
CVR 46180011
Telegade 2, Høje Taastrup
2630 Taastrup
Denmark

(the data controller)

and

GoCollective Holding A/S
CVR 44699818
Skøjtevej 26
2770 Kastrup
Denmark

(the data processor)

each a ‘party’; together ‘the parties’

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to meet the requirements of the GDPR and to ensure the protection of the rights of the data subject.

1. Table of Contents

2. Preamble

1. These Contractual Clauses (the Clauses) set out the rights and obligations of the data controller and the data processor, when processing personal data on behalf of the data controller.

2. The Clauses have been designed to ensure the parties' compliance with Article 28(3) of Regulation 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data and repealing Directive 95/46/EC (General Data Protection Regulation).

3. In the context of the provision of transitional services within IT, finance, BI and payroll, the data processor will process personal data on behalf of the data controller in accordance with the Clauses.

4. The Clauses shall take priority over any similar provisions contained in other agreements between the parties.

5. Four appendices are attached to the Clauses and form an integral part of the Clauses.

6. Appendix A contains details about the processing of personal data, including the purpose and nature of the processing, type of personal data, categories of data subject and duration of the processing.

7. Appendix B contains the data controller's conditions for the data processor's use of sub-processors and a list of sub-processors authorised by the data controller.

8. Appendix C contains the data controller's instructions with regards to the processing of personal data, the minimum security measures to be implemented by the data processor and how audits of the data processor and any sub-processors are to be performed.

9. Appendix D contains provisions for other activities which are not covered by the Clauses.

10. The Clauses along with appendices shall be retained in writing, including electronically, by both parties.

11. The Clauses shall not exempt the data processor from obligations to which the data processor is subject pursuant to the General Data Protection Regulation (the GDPR) or other legislation.

3. The rights and obligations of the data controller

1. The data controller is responsible for ensuring that the processing of personal data takes place in compliance with the GDPR (see Article 24 GDPR), the applicable EU or Member State[1] data protection provisions and the Clauses.

[1] References to "Member States" made throughout the Clauses shall be understood as references to "EEA Member States".

2. The data controller has the right and obligation to make decisions about the purposes and means of the processing of personal data.

3. The data controller shall be responsible, among other, for ensuring that the processing of personal data, which the data processor is instructed to perform, has a legal basis.

4. The data processor acts according to instructions

1. The data processor shall process personal data only on documented instructions from the data controller, unless required to do so by Union or Member State law to which the processor is subject. Such instructions shall be specified in appendices A and C. Subsequent instructions can also be given by the data controller throughout the duration of the processing of personal data, but such instructions shall always be documented and kept in writing, including electronically, in connection with the Clauses.

2. The data processor shall immediately inform the data controller if instructions given by the data controller, in the opinion of the data processor, contravene the GDPR or the applicable EU or Member State data protection provisions.

5. Confidentiality

1. The data processor shall only grant access to the personal data being processed on behalf of the data controller to persons under the data processor's authority who have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality and only on a need to know basis. The list of persons to whom access has been granted shall be kept under periodic review. On the basis of this review, such access to personal data can be withdrawn, if access is no longer necessary, and personal data shall consequently not be accessible anymore to those persons.

2. The data processor shall at the request of the data controller demonstrate that the concerned persons under the data processor's authority are subject to the abovementioned confidentiality.

6. Security of processing

1. Article 32 GDPR stipulates that, taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the data controller and data processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

   The data controller shall evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. Depending on their relevance, the measures may include the following:
   a. Pseudonymisation and encryption of personal data;

   b. the ability to ensure ongoing confidentiality, integrity, availability and resilience of processing systems and services;

   c. the ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

d. a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

2. According to Article 32 GDPR, the data processor shall also – independently from the data controller – evaluate the risks to the rights and freedoms of natural persons inherent in the processing and implement measures to mitigate those risks. To this effect, the data controller shall provide the data processor with all information necessary to identify and evaluate such risks.

3. Furthermore, the data processor shall assist the data controller in ensuring compliance with the data controller's obligations pursuant to Articles 32 GDPR, by *inter alia* providing the data controller with information concerning the technical and organisational measures already implemented by the data processor pursuant to Article 32 GDPR along with all other information necessary for the data controller to comply with the data controller's obligation under Article 32 GDPR.

   If subsequently – in the assessment of the data controller – mitigation of the identified risks require further measures to be implemented by the data processor, than those already implemented by the data processor pursuant to Article 32 GDPR, the data controller shall specify these additional measures to be implemented in Appendix C.

7. Use of sub-processors

1. The data processor shall meet the requirements specified in Article 28(2) and (4) GDPR in order to engage another processor (a sub-processor).

2. The data processor shall therefore not engage another processor (sub-processor) for the fulfilment of the Clauses without the prior general written authorisation of the data controller.

3. The data processor has the data controller's general authorisation for the engagement of sub-processors. The data processor shall inform in writing the data controller of any intended changes concerning the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data controller the opportunity to object to such changes prior to the engagement of the concerned sub-processor(s). Longer time periods of prior notice for specific sub-processing services can be provided in Appendix B. The list of sub-processors already authorised by the data controller can be found in Appendix B.

4. Where the data processor engages a sub-processor for carrying out specific processing activities on behalf of the data controller, the same data protection obligations as set out in the Clauses shall be imposed on that sub-processor by way of a contract or other legal act under EU or Member State law, in particular providing sufficient guarantees to implement appropriate technical and organisational measures in such a manner that the processing will meet the requirements of the Clauses and the GDPR.

   The data processor shall therefore be responsible for requiring that the sub-processor at least complies with the obligations to which the data processor is subject pursuant to the Clauses and the GDPR.

5. A copy of such a sub-processor agreement and subsequent amendments shall – at the data controller's request – be submitted to the data controller, thereby giving the data controller the opportunity to ensure that the same data protection obligations as set out in the Clauses are imposed on the sub-processor. Clauses on business related issues that do not affect the legal data protection content of the sub-processor agreement, shall not require submission to the data controller.

6. If the sub-processor does not fulfil his data protection obligations, the data processor shall remain fully liable to the data controller as regards the fulfilment of the obligations of the sub-processor. This does not affect the rights of the data subjects under the GDPR – in particular those foreseen in Articles 79 and 82 GDPR – against the data controller and the data processor, including the sub-processor.

8. Transfer of data to third countries or international organisations

1. Any transfer of personal data to third countries or international organisations by the data processor shall only occur on the basis of documented instructions from the data controller and shall always take place in compliance with Chapter V GDPR.

2. In case transfers to third countries or international organisations, which the data processor has not been instructed to perform by the data controller, is required under EU or Member State law to which the data processor is subject, the data processor shall inform the data controller of that legal requirement prior to processing unless that law prohibits such information on important grounds of public interest.

3. Without documented instructions from the data controller, the data processor therefore cannot within the framework of the Clauses:

    a. transfer personal data to a data controller or a data processor in a third country or in an international organization

    b. transfer the processing of personal data to a sub-processor in a third country

    c. have the personal data processed in by the data processor in a third country

4. The data controller's instructions regarding the transfer of personal data to a third country including, if applicable, the transfer tool under Chapter V GDPR on which they are based, shall be set out in Appendix C.6.

5. The Clauses shall not be confused with standard data protection clauses within the meaning of Article 46(2)(c) and (d) GDPR, and the Clauses cannot be relied upon by the parties as a transfer tool under Chapter V GDPR.

9. Assistance to the data controller

1. Taking into account the nature of the processing, the data processor shall assist the data controller by appropriate technical and organisational measures, insofar as this is possible, in the fulfilment of the data controller's obligations to respond to requests for exercising the data subject's rights laid down in Chapter III GDPR.

    This entails that the data processor shall, insofar as this is possible, assist the data controller in the data controller's compliance with:

a. the right to be informed when collecting personal data from the data subject
b. the right to be informed when personal data have not been obtained from the data subject
c. the right of access by the data subject
d. the right to rectification
e. the right to erasure ('the right to be forgotten')
f. the right to restriction of processing
g. notification obligation regarding rectification or erasure of personal data or restriction of processing
h. the right to data portability
i. the right to object
j. the right not to be subject to a decision based solely on automated processing, including profiling

2. In addition to the data processor's obligation to assist the data controller pursuant to Clause 6.3., the data processor shall furthermore, taking into account the nature of the processing and the information available to the data processor, assist the data controller in ensuring compliance with:

    a. The data controller's obligation to without undue delay and, where feasible, not later than 72 hours after having become aware of it, notify the personal data breach to the competent supervisory authority, the Danish Data Protection Authority ("Datatilsynet"), unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons;

    b. the data controller's obligation to without undue delay communicate the personal data breach to the data subject, when the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons;

    c. the data controller's obligation to carry out an assessment of the impact of the envisaged processing operations on the protection of personal data (a data protection impact assessment);

    d. the data controller's obligation to consult the competent supervisory authority, the Danish Data Protection Authority ("Datatilsynet"), prior to processing where a data protection impact assessment indicates that the processing would result in a high risk in the absence of measures taken by the data controller to mitigate the risk.

3. The parties shall define in Appendix C the appropriate technical and organisational measures by which the data processor is required to assist the data controller as well as the scope and the extent of the assistance required. This applies to the obligations foreseen in Clause 9.1. and 9.2.

10. Notification of personal data breach

1. In case of any personal data breach, the data processor shall, without undue delay after having become aware of it, notify the data controller of the personal data breach.

2. The data processor's notification to the data controller shall, if possible, take place within 36 hours after the data processor has become aware of the personal data breach to enable the data controller to comply with the data controller's obligation to

notify the personal data breach to the competent supervisory authority, cf. Article 33 GDPR.

3. In accordance with Clause 9(2)(a), the data processor shall assist the data controller in notifying the personal data breach to the competent supervisory authority, meaning that the data processor is required to assist in obtaining the information listed below which, pursuant to Article 33(3)GDPR, shall be stated in the data controller's notification to the competent supervisory authority:

    a. The nature of the personal data breach including where possible, the categories and approximate number of data subjects concerned and the categories and approximate number of personal data records concerned;

    b. the likely consequences of the personal data breach;

    c. the measures taken or proposed to be taken by the controller to address the personal data breach, including, where appropriate, measures to mitigate its possible adverse effects.

4. The parties shall define in Appendix C all the elements to be provided by the data processor when assisting the data controller in the notification of a personal data breach to the competent supervisory authority.

11. Erasure and return of data

1. On termination of the provision of personal data processing services, the data processor shall be under obligation to delete all personal data processed on behalf of the data controller and certify to the data controller that it has done so unless Union or Member State law requires storage of the personal data.

12. Audit and inspection

1. The data processor shall make available to the data controller all information necessary to demonstrate compliance with the obligations laid down in Article 28 and the Clauses and allow for and contribute to audits, including inspections, conducted by the data controller or another auditor mandated by the data controller.

2. Procedures applicable to the data controller's audits, including inspections, of the data processor and sub-processors are specified in appendices C.7. and C.8.

3. The data processor shall be required to provide the supervisory authorities, which pursuant to applicable legislation have access to the data controller's and data processor's facilities, or representatives acting on behalf of such supervisory authorities, with access to the data processor's physical facilities on presentation of appropriate identification.

13. The parties' agreement on other terms

1. The parties may agree other clauses concerning the provision of the personal data processing service specifying e.g. liability, as long as they do not contradict directly or indirectly the Clauses or prejudice the fundamental rights or freedoms of the data subject and the protection afforded by the GDPR.

14. Commencement and termination

1. The Clauses shall become effective on the date of both parties' signature.

2. Both parties shall be entitled to require the Clauses renegotiated if changes to the law or inexpediency of the Clauses should give rise to such renegotiation.

3. The Clauses shall apply for the duration of the provision of personal data processing services. For the duration of the provision of personal data processing services, the Clauses cannot be terminated unless other Clauses governing the provision of personal data processing services have been agreed between the parties.

4. If the provision of personal data processing services is terminated, and the personal data is deleted or returned to the data controller pursuant to Clause 11.1. and Appendix C.4., the Clauses may be terminated by written notice by either party.

5. Signature

   On behalf of the data controller

Name	[NAME]
Position	[POSITION]
Date	[DATE]
Signature	[SIGNATURE]

   On behalf of the data processor

Name	Henrik la Cour	Markus Honner
Position	CEO	CFO
Date		
Signature		

15. Data controller and data processor contacts/contact points

1. The parties may contact each other using the following contacts/contact points:

2. The parties shall be under obligation continuously to inform each other of changes to contacts/contact points.

Name	[NAME]
Position	[POSITION]
Telephone	[TELEPHONE]
E-mail	[E-MAIL]

Name	Martin Rømer Johannesen
Position	Head of Legal & Compliance
Telephone	+45 4076 4669
E-mail	dataprotection@gocollective.dk / Martin.johannesen@gocollective.dk

Appendix A Information about the processing

A.1. The purpose of the data processor's processing of personal data on behalf of the data controller is:

The purpose of the processing is to enable the data processor to provide transitional services to the data controller within IT, finance, business intelligence and payroll following the handover of the data processor's rail business to the data controller. The processing is necessary to support the continued operation, administration and orderly transition of the transferred business, including access to and use of relevant systems, data, reporting, payroll administration, finance processes, user support and related transitional assistance.

The processing shall be limited to what is necessary for the provision of the transitional services described in the TSA between the parties and any related documented instructions from the data controller.

A.2. The data processor's processing of personal data on behalf of the data controller shall mainly pertain to (the nature of the processing):

The processing mainly consists of hosting, accessing, using, maintaining, supporting, transferring, extracting, structuring, storing, disclosing and otherwise processing personal data in connection with the provision of transitional IT, finance, business intelligence and payroll services.

This includes processing personal data in order to provide system access and user administration, technical support, payroll administration, financial administration, reporting, data extraction, data migration, reconciliation, troubleshooting, business intelligence analysis and other related transition assistance necessary to ensure continuity and orderly handover of the relevant business processes.

A.3. The processing includes the following types of personal data about data subjects:

The processing includes both ordinary personal data and special categories of personal data to the extent necessary for the provision of transitional services within IT, finance, BI and payroll.

Ordinary personal data may include name, employee number, job title, organisational affiliation, work location, contact details, employment information, payroll and remuneration information, tax information, bank account details, pension and benefit information, time registration, absence and leave information, user IDs, access rights, system logs and other data contained in or generated through the relevant IT, finance, BI and payroll systems.

Special categories of personal data may include health information, including sickness absence information, medical certificates or other health-related documentation, information relevant to social security (including the social security number) or employment law obligations, and information concerning trade union membership where such information is processed in connection with payroll, benefits, collective agreements or employment administration.

To the extent such information is included in the systems or records made available to the data processor, the processing may also include national identification numbers and other confidential information necessary for payroll, HR, finance, reporting, access administration, support and statutory compliance purposes.

A.4. Processing includes the following categories of data subject:

Current and former employees, consultants and other staff members of the data controller, including individuals transferred to or otherwise associated with the data controller in connection with the handover of the rail business.

Customer representatives, passengers and other individuals whose personal data may be contained in or processed through the r

elevant IT, finance, BI or operational reporting systems.

Supplier, vendor, partner and other business contact persons, including contact persons at public authorities, advisors and other external stakeholders.

A.5. The data processor's processing of personal data on behalf of the data controller may be performed when the Clauses commence. Processing has the following duration:

The processing may be performed for the duration of the TSA and shall continue only for as long as necessary for the data processor to provide the transitional services under the TSA and to complete any related assistance, handover, reconciliation, deletion or return of personal data in accordance with the Clauses and the data controller's documented instructions.

Appendix B Authorised sub-processors

B.1. Approved sub-processors

On commencement of the Clauses, the data controller authorises the engagement of the following sub-processors:

NAME	CVR	ADDRESS	DESCRIPTION OF PROCESSING

The data controller shall on the commencement of the Clauses authorise the use of the above-mentioned sub-processors for the processing described for that party. The data processor shall not be entitled – without the data controller's explicit written authorisation – to engage a sub-processor for a 'different' processing than the one which has been agreed upon or have another sub-processor perform the described processing.

B.2. Prior notice for the authorisation of sub-processors

Changes to the authorized sub-processors shall be notified latest thirty (30) days in advance.

Appendix C Instruction pertaining to the use of personal data

C.1. The subject of/instruction for the processing

The data processor's processing of personal data on behalf of the data controller shall be carried out by the data processor performing the following:

The data processor is instructed to process personal data solely for the purpose of providing the transitional services described in the TSA and Appendix A, including IT support and system access, finance administration, business intelligence reporting, payroll administration, data extraction, data migration, reconciliation, troubleshooting, handover assistance and related support. The data processor may only process personal data on documented instructions from the data controller and only to the extent necessary for the performance of those services.

C.2. Security of processing

The level of security shall take into account:

The processing concerns employment, payroll, finance, IT, business intelligence and operational data and may include ordinary personal data, confidential information, national identification numbers and special categories of personal data, including health information and trade union membership where relevant. The level of security shall therefore be appropriate to a medium to high risk processing environment and shall ensure the ongoing confidentiality, integrity, availability and resilience of the systems and services used for the processing.

The data processor shall determine the specific technical and organisational measures required to achieve this level of security, taking into account the nature, scope, context and purposes of the processing and the risks to the rights and freedoms of the data subjects.

Personal data shall be protected by appropriate encryption in transit and, where technically feasible and proportionate, at rest. Pseudonymisation, masking or segregation shall be applied where appropriate, including for reporting, testing, troubleshooting or business intelligence activities where direct identification of data subjects is not necessary.

The data processor shall maintain appropriate access controls, role-based access rights, authentication measures, confidentiality obligations, segregation of duties, malware protection, patch management, vulnerability management, change management and incident management processes to ensure the ongoing confidentiality, integrity, availability and resilience of the processing systems and services.

The data processor shall maintain backup, disaster recovery and business continuity arrangements designed to restore availability and access to personal data in a timely manner in the event of a physical or technical incident. Backup and recovery procedures shall be tested at appropriate intervals.

The data processor shall regularly test, assess and evaluate the effectiveness of its technical and organisational measures, including through internal controls, security reviews, vulnerability assessments, audit activities or equivalent measures appropriate to the relevant systems and services.

Access to personal data shall be limited to authorised personnel with a documented need to know. User access shall be granted, reviewed and revoked in accordance with access management procedures, and privileged access shall be restricted and subject to appropriate controls.

Personal data transmitted electronically shall be protected against unauthorised access, alteration and disclosure by appropriate technical measures, including secure transmission channels, encryption, access restrictions and secure file transfer methods where relevant.

Personal data stored in systems, databases, file shares, applications, backup media or other storage locations shall be protected by appropriate logical and physical security measures, including access controls, segregation, backup protection and secure disposal procedures.

Physical locations where personal data are processed shall be protected by appropriate physical security measures, including controlled access to offices, server rooms and other restricted areas, visitor management and measures to prevent unauthorised access to devices, media and documents.

Remote working shall be permitted only where appropriate security measures are in place, including secure devices, secure network access, authentication controls, confidentiality safeguards and procedures to prevent unauthorised viewing, copying, printing, storage or disclosure of personal data.

Relevant access, administrative and security events shall be logged to the extent technically feasible and proportionate. Logs shall be protected against unauthorised access and alteration and shall be retained for a period appropriate to the purpose of monitoring, investigation, audit and security incident handling.

C.3. Assistance to the data controller

The data processor shall insofar as this is possible – within the scope and the extent of the assistance specified below – assist the data controller in accordance with Clause 9.1. and 9.2. by implementing the following technical and organisational measures:

The data processor shall assist the data controller, taking into account the nature of the processing and the information available to the data processor, with the handling of data subject requests, personal data breaches, data protection impact assessments, prior consultations with supervisory authorities and other compliance obligations relating to the processing under the Clauses.

Such assistance shall include, where relevant, providing information about the processing, locating, extracting, correcting, restricting, deleting or returning personal data, supporting investigations of suspected or confirmed personal data breaches, providing available logs and technical information, assisting with assessment of risks and mitigation measures, and implementing reasonable technical or organisational measures requested by the data controller.

C.4. Storage period/erasure procedures

Personal data shall be processed and stored only for as long as necessary to provide the transitional services under the TSA and to complete any related handover, reconciliation, assistance, deletion or return activities. The data processor shall not retain personal data for

longer than necessary for the documented purposes of the processing, unless retention is required by Union or Member State law.
Upon termination or expiry of the transitional services, the data processor shall, at the choice and documented instruction of the data controller, delete or return all personal data processed on behalf of the data controller and delete existing copies, unless continued storage is required by Union or Member State law. The data processor shall provide confirmation of deletion or return upon request.

C.5. Processing location

Processing of the personal data under the Clauses cannot be performed at other locations than the following without the data controller's prior written authorisation:

Processing may take place at the data processor's premises at Skøjtevej 26, 2770 Kastrup, Denmark, at other premises controlled by the data processor within the EU/EEA, through secure remote access from locations within the EU/EEA, and at the premises or hosting locations of authorised sub-processors listed in Appendix B, provided that such processing complies with the Clauses and the data controller's documented instructions.

C.6. Instruction on the transfer of personal data to third countries

The data processor is not authorised to transfer personal data to a third country or an international organisation, or to permit personal data to be processed from a third country, unless the data controller has provided prior documented instructions and an appropriate transfer mechanism under Chapter V GDPR is in place.

If the data controller instructs a transfer to a third country or international organisation, the transfer shall be based on an adequacy decision, standard contractual clauses, binding corporate rules, an approved code of conduct or certification mechanism, or another valid transfer basis under Chapter V GDPR, as documented by the data controller.
If the data controller does not in the Clauses or subsequently provide documented instructions pertaining to the transfer of personal data to a third country, the data processor shall not be entitled within the framework of the Clauses to perform such transfer.

C.7. Procedures for the data controller's audits, including inspections, of the processing of personal data being performed by the data processor

The data controller may audit the data processor's compliance with the Clauses, including through review of documentation, security policies, access controls, incident records, audit reports, certifications, technical descriptions and other relevant materials. The data processor shall make available information necessary to demonstrate compliance and shall reasonably cooperate with the data controller's audit activities.
Audits shall, as far as reasonably possible, be conducted on the basis of existing documentation and written responses. On-site inspections may be carried out where the data controller reasonably deems this necessary, subject to reasonable prior notice, during normal business hours and in a manner that does not unreasonably disrupt the data processor's business operations or compromise security, confidentiality or the rights of other customers or third parties. Each party shall bear its own internal costs in connection with ordinary audit activities. If an audit identifies material non-compliance attributable to the data processor, the data processor shall without undue delay prepare and implement an appropriate remediation plan and keep the data controller informed of progress.

C.8. [IF APPLICABLE] Procedures for audits, including inspections, of the processing of personal data being performed by sub-processors

The data processor shall ensure that each authorised sub-processor is subject to contractual obligations that allow the data processor to monitor and verify the sub-processor's compliance with applicable data protection obligations and the requirements of the Clauses. The data processor shall remain fully liable to the data controller for the performance of the sub-processor's obligations.

Upon request, the data processor shall provide the data controller with relevant information available to the data processor regarding the sub-processor's compliance, including audit reports, certifications, security documentation or summaries thereof, subject to applicable confidentiality, security and contractual restrictions.

If the data controller reasonably requires further assurance regarding a sub-processor, the data processor shall use reasonable efforts to facilitate additional information, written responses or audit measures through the sub-processor. Any direct inspection of a sub-processor shall be subject to the sub-processor's security, confidentiality and operational requirements and shall be coordinated through the data processor.

Appendix D The parties' terms of agreement on other subjects

Not applicable.

1. AUDIT

1.1 General audit report

1.1.1 Annually in December, Supplier shall present a general ISAE 3402 type 2 (or successor or equivalent) report on the security maintained by Supplier, including system security, data security and operational security, from an auditor of high reputation and in accordance with international standards.

1.1.2 Prior to the Take-Over Date, Supplier shall on DSB's request present the general audit report on the security maintained by Supplier, including system security, data security and operational security from the previous year.

1.2 Special audit reports

1.2.1 Annually in December, Supplier shall present the following DSB specific audit reports/statements covering the period 1. December previous year to 30. November present year.

a) ISAE 3402 type 2 Assurance Report, covering the security related to systems used for financial reporting and maintained in respect of the IT Infrastructure, at the Service Locations and/or in respect of remote access to IT Infrastructure and the DSB Environment, including systems' security, data security and operational security.

1.2.2 The detailed scope of the reports stated in [insert reference] shall be further defined and agreed between the Parties after the Effective Date and the detailed contents in all DSB specific reports shall be evaluated and adjusted annually in March by the Parties, if necessary. Changes to the scope of the reports shall be handled under the Contract Change Procedure.

1.2.3 The DSB specific audit reports shall be prepared (i) in accordance with international standards ISA 402, ISAE 3402 type 2, ISAE 3000 with reasonable assurance, or ISRS 4400 Agreed Upon Procedures, or any other reasonably relevant auditing standard as required below, with specific reference to this Agreement, and (ii) in accordance with DSB's specified control objectives for the specific audit reports, which have been disclosed in the Data Room and will be delivered to Supplier after the Effective Date.

1.2.4 The ISAE 3402 type 2 report shall be prepared in accordance with the following procedure:

a) The scope of the specific audit report shall be determined in March between all relevant parties, including Supplier, Supplier's auditor, DSB internal and external auditors and DSB IT management. Supplier shall take the initiative to ensure that the scope is determined by the parties.

b) An interim audit of the DSB specific ISAE 3402, type 2 shall be carried out in the period from March to July.

c) The interim audit shall result in an interim report on findings by medio August, including a follow-up on previous findings, new findings, preliminary conclusions and recommendations, suggested actions required and deadlines for actions. The interim report shall be discussed by end of August between relevant parties, including Supplier, Suppliers auditor, DSB internal and external auditors and DSB IT management.

d) Upon any findings being made during the audit requiring Supplier to remedy or make changes, Supplier shall initiate the actions required in accordance with [insert reference].

e) In December, the Supplier shall issue the final report covering the audit period 1. December to 30. November and the final list of findings. Supplier shall submit the final auditor statement to DSB within medio December.

f) In January, the Supplier shall present a Bridge letter from Management stating that no material changes to the control environment have occurred in December and that controls covered in the final report are still in place and operating effectively, to cover the calendar year. Supplier shall submit the Bridge letter to DSB within medio January.

1.2.5 Within fifteen (15) Days, of the Supplier's receipt of the final audit statement, stating or indicating that remedial actions or changes are required due to findings made, Supplier shall submit a written plan to DSB, for DSB's approval, on Supplier's remedy or changes required, including a binding time schedule. DSB may not unreasonably withhold its approval thereto. If the findings are priority 1 findings and a plan is not submitted within the said period, this shall be considered a material breach. For all other findings non-submission of the plan within thirty (30) Days of receipt of the report, shall be considered a breach. The dates within which priority 1 findings are to be remedied under the plan shall be considered Critical Milestones.

1.3 Obligation to co-operate and use of auditor

1.3.1 Supplier acknowledges that DSB is subject to be audited by DSB internal audit and external audit and Supplier undertakes to fully cooperate in relation to any auditing of the Services, IT Infrastructure and Supplier's compliance with this Agreement, including coordinating all relevant matters with DSB.

1.3.2 If Supplier is not delivering or following the procedures for audits and audit reports under [insert reference] (Special audits reports), DSB shall have the right to use an alternative auditor selected by DSB, to prepare the specific audits and such audit reports and Supplier shall reimburse DSB for all DSB's documented reasonable costs incurred in the course of the audits.

1.4 Other auditing

1.4.1 DSB shall be entitled to perform additional audits by forwarding a Task CSR regarding Supplier's assistance for:

a) Verifying the accuracy of Supplier's Charges and invoices (in light of agreed formulas), including with respect to any Service Credits and proposed or actual variations to Charges in accordance with this Agreement.
b) Examining Supplier's performance of the Services including verification of compliance with the relevant Service Levels.

c) Verifying compliance with the terms of this Agreement and applicable Law.

d) Reviewing the measurement and monitoring tools and procedures used by Supplier under this Agreement (for inspection and verification purposes).

e) Reviewing Supplier's data processing activities under the Agreement.

f) Any other subjects reasonably required by DSB.

1.4.2 Supplier shall provide DSB's external auditor with access to Supplier's Service Locations, the IT Infrastructure and any other relevant systems or documents, and Supplier shall further provide assistance as agreed under the Task CSR.

1.4.3 Upon request and against payment of costs to be agreed under a Task CSR, Supplier shall provide DSB with a certification from a well-reputed independent third party to be approved by DSB (such approval not to be unreasonably withheld) that Supplier complies with [insert reference] (on reports and documentation) and [insert reference] (on retention of relevant records) in any and all respects.

1.4.4 If the audit under this [insert reference] identifies a Default by Supplier which is not immaterial, Supplier shall reimburse DSB for all DSB's documented reasonable costs incurred in the course of the audit including Charges paid to Supplier under the applicable Task CSR. In addition, if the audit identifies any overpayment of charges to Supplier, Supplier shall promptly reimburse the full amount of any overpayment, together with interest on that amount accruing daily from the date of overpayment until the date of repayment in full to DSB at the rate of the lending rate of the Danish National Bank plus 2 % (two per cent).

1.4.5 Supplier shall on demand provide DSB with all reasonable co-operation and assistance in relation to each audit, including all information requested by DSB within the scope of the audit, reasonable access to any Service Location and to any equipment used (whether exclusively or non-exclusively) in the performance of the Services, and access to Supplier Personnel.

1.4.6 Supplier shall on Supplier’s premises provide to DSB's external auditor space, office furnishings, utilities and office-related equipment and duplicating services as the auditor may reasonably require to perform the audit.

1.4.7 The performance of an audit in relation to any matter shall not be deemed to be acceptance or approval of that matter.

New Rail Information Security Requirements

Contents

1. General

This clause is based on ISO 27001:2022 and NIS2,[1] articles 20(1) AND 21(1).

The Supplier shall in connection with the fulfilment of the TSA establish, implement, maintain, and continually improve an information security management system (ISMS) based on the recent versions of ISO/IEC 27001 or similarly (nationally or internationally) recognized standards, based on risk assessments, cf. clause 2.

The Supplier shall take appropriate and proportionate technical, operational, and organizational security measures to manage the risks posed to the security of the network and information systems which the Supplier uses for their operations or for the provision of their IT Services in relation to the TSA, and to prevent or minimize the impact of incidents on Selskabet af den 13.01.2026 A/S ("New Rail").

Taking into account the state-of-the-art and, where applicable, relevant European and international standards, as well as the cost of implementation, the Supplier's measures referred to above shall ensure a level of security of the network and information systems which the Supplier uses for their operations or in connection with the IT Services in relation to the TSA appropriate to the risks posed, cf. clause 2.

The Supplier's security measures shall be based on an all-hazards approach that aims to protect network and information systems which the Supplier uses for their operations or for the provision of their IT Services in relation to the TSA and the physical environment of those systems from incidents.

The Supplier shall ensure that the management body of the Supplier approves the cybersecurity risk-management measures taken by the Supplier in relation to the TSA and oversees its implementation.

The Supplier shall ensure that the Supplier's ISMS fulfils at least the specific requirements below, cf. clause 3 to clause 6. The specific requirements below must be met regardless of the implications of the Supplier's ISMS and risk assessment in general.

The Supplier shall in connection with the fulfilment of the TSA, as part of its ISMS, fulfil the requirements set out below in clauses 3-6.

[1] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union, amending Regulation (EU) No 910/2014 and Directive (EU) 2018/1972, and repealing Directive (EU) 2016/1148

2. Risk assessments concerning information security

This clause is based on ISO 27001:2022 Clause 6.1.2 Information security risk assessment, and NIS2, article 21(1).

The Supplier shall in relation to the fulfilment of the TSA, as part of its ISMS, define, apply, and maintain an information security risk assessment process to identify, assess and control information security risks related to the IT Services, in accordance with a recognized standard.

The Supplier shall retain documented information about the information security risk assessment process and all risk assessments shall be documented and updated at least yearly or when changes that may impact security occurs.

The Supplier shall in relation to the fulfilment of the TSA, upon request, include a specific threat in a risk assessment, including but not limited to results of changes in New Rail's own risk assessments, threat landscapes, or national or international legislation.

The Supplier shall as part of the Supplier's risk assessment take due account of the degree of New Rail's exposure to risks, New Rail's size, and the likelihood of occurrence of incidents and their severity, including their societal and economic impact.

The Supplier shall in relation to the fulfilment of the TSA, without undue delay, provide its risk assessments in relation to the TSA to New Rail, upon request.

3. Organisational controls

3.1. Policies for information security

This clause is based on ISO 27001:2022 Annex A 5.1 and NIS2, article 21(2)(a) and (f))

The Supplier shall define an information security policy and topic-specific policies for information security, which shall be approved by the Supplier's management body, published, communicated to, and acknowledged by the Supplier's employees, any subcontractors, and to New Rail, and which shall be included in the Supplier's ISMS and support the current risk assessment.

The Supplier's policies shall be reviewed at planned intervals, at least once (1) a year, and in case of substantial changes, including changes to the Supplier's current risk assessments, to ensure the continued suitability, adequacy, and performance-related effectiveness of the policies.

The Supplier shall as an integral part of the requirements in this clause 3.1 establish policies on risk analysis and information system security.

The Supplier shall as an integral part of the requirements in this clause 3.1 establish policies and procedures to assess the effectiveness of cybersecurity risk-management measures.

3.2. Information security roles and responsibilities

This clause is based on ISO 27001:2022 Annex A 5.2

The Supplier shall define and allocate information security roles and responsibilities.

3.3. Segregation of duties

This clause is based on ISO 27001:2022 Annex A 5.3

The Supplier shall ensure that conflicting duties and areas of responsibility are segregated proportionally considering the Supplier's organization, risk, etc.

The Supplier must – if considered necessary and proportional by the Supplier - ensure segregation of duties in the following areas:

- Development, test, and production environments
- Request, approval, and allocation of access rights
- Design, implementation, and review of code
- Initiating, approving, and executing changes

3.4. Contact with authorities

This clause is based on ISO 27001:2022 Annex A 5.5

The Supplier shall establish and maintain contact with authorities relevant to the services provided by the Supplier.

3.5. Threat intelligence

This clause is based on ISO 27001:2022 Annex A 5.7

The Supplier shall collect and analyse information relating to information security threats relevant for the IT Services in order to produce threat intelligence.

Threat intelligence must be collected and reported subject to requests for use in the two following levels:

1. Strategic threat intelligence, including high-level information on the threat landscape and changes in the landscape.
2. Tactical and operational threat intelligence, including information on e.g. attacker methodologies, tools and technologies, technical indicators etc.

The strategic threat intelligence must be shared with New Rail, where relevant or otherwise per request. The tactic and operational threat intelligence must be shared with New Rail, enabling New Rail to adjust relevant preventive and detective controls.

3.6. Inventory of information and other associated assets

This clause is based on ISO 27001:2022 Annex A 5.9 and NIS2, article 21(2)(i)

The Supplier shall develop and maintain an inventory of information and other associated assets, including owners, which are necessary for the IT Services.

The Supplier shall as an integral part of the requirements in this clause 3.6 establish measures on asset management.

3.7. Acceptable use of information and other associated assets

This clause is based on ISO 27001:2022 Annex A 5.10

The Supplier shall identify, document, and implement rules for the acceptable use and procedures for handling information and other associated assets.

3.8. Return of assets

This clause is based on ISO 27001:2022 Annex A 5.11

The Supplier shall ensure that all the Supplier’s employees and other interested parties return all assets in their possession in relation to the IT Services, upon termination of their employment, TSA, or agreement.

3.9. Classification of information

This clause is based on ISO 27001:2022 Annex A 5.12

The Supplier shall in the relation to fulfilment of the TSA process and handle information based on a documented classification schemetaking into consideration confidentiality, integrity, and availability.
For clarity: This requirement does not imply labelling of information.

3.10. Information transfer

This clause is based on ISO 27001:2022 Annex A 5.14 and NIS2, article 21(2)(j)

The Supplier shall adopt an information transfer policy, and ensure that rules, procedures, or agreements are in place for all types of transfer facilities within the Supplier's organization and between the Supplier and other parties.

The policy, procedures and measures shall be designed to protect transferred information from interception, eavesdropping, copying, modification, misrouting and destruction.

Where the transfer of New Rail information from the Supplier to third parties, including public authorities, partners or other suppliers of New Rail, is necessary in connection with the IT Services, such transfer may solely take place on basis of written agreements between New Rail and the Supplier.

The Supplier shall as an integral part of the requirements in this clause 3.10 apply multi-factor authentication solutions, secured voice, video and text communications and secured emergency communication systems, where appropriate.

3.11. Access control

This clause is based on ISO 27001:2022 Annex A 5.15 and NIS2, article 21(2)(i)

If the IT Services are integrated with one of New Rail's Identity and Access Management Systems (presently Active Directory (AD), Entra ID, and New Rail's Sailpoint Identity and Access Management (IAM) solution), the requirements in sections 3.11 – 3.19 must be fulfilled for users with access to the Supplier's operating systems, database systems and other systems that are relevant for the provision of services to New Rail.

If the IT Servicesare not integrated with one of New Rail's Identity and Access Management Systems, the requirements in sections 3.11 – 3.19 must be fulfilled for all users of the services and users with access to the operating systems, database systems and other systems relevant for the provision of services to New Rail.

The Supplier shall establish and implement rules to control physical and logical access to information or other associated assets based on New Rail's business and information security requirements.

The Supplier shall ensure that the requirements in this clause are fulfilled for all users with access to the operating systems, database systems and other systems in connection with the IT Services.

The Supplier shall as an integral part of the requirements in this clause 3.11 establish access control policies.

3.12. Identity management

This clause is based on ISO 27001:2022 Annex A 5.16

The Supplier shall ensure that the full life cycle of identities is managed for relevant systems.

The Supplier shall apply a consistent identity and access management process that is providing effective user identification and administration in accordance with best practice.

The Supplier shall when relevant and proportional ensure that the processes used in the context of identity management in connection with the IT Services ensures that:

a) for identities assigned to persons, a specific identity is only linked to a single person to be able to hold the person accountable for actions performed with this specific identity

b) identities assigned to multiple persons (e.g. shared identities) are only permitted where they are necessary for business or operational reasons and are subject to dedicated approval, documentation and monitoring
c) identities assigned to non-human entities are subject to appropriately segregated approval and independent ongoing oversight
d) identities are disabled or removed in a timely fashion if they are no longer required or considered compromised (e.g. if their associated entities are deleted or no longer used, or if the person linked to an identity has left the Supplier's organization or changed the role)
e) in a specific domain, a single identity is mapped to a single entity, i.e. mapping of multiple identities to the same entity within the same context (duplicate identities) is avoided
f) records of all significant events concerning the use and management of user identities and of authentication information are kept.

3.13. Authentication information

This clause is based on ISO 27001:2022 Annex A 5.17

The Supplier shall ensure that allocation and management of authentication information is controlled by a management process, including advising personnel on the appropriate handling of authentication information.

The Supplier shall apply documented procedures for creating and administrating passwords in accordance with best practice.

The Supplier shall ensure that the processes used in the context of allocation of authentication information in connection with the IT Services ensure that records of significant events concerning allocation and management of authentication information are kept and their confidentiality is granted, and that the record-keeping method is approved (e.g. by using an approved password vault tool).

The Supplier shall ensure that any person having access to or using authentication in connection with the IT Services is advised to ensure that secret authentication information such as passwords are kept confidential and secret authentication information used in the context of identities linked to multiple users or linked to non-personal accounts are solely shared with authorized persons.

The Supplier shall, when passwords are used as authentication information, ensure that the password management system in connection with the IT Services enforces strong passwords according to best practice recommendations and enforces password changes as necessary, for example after an information security incident, or upon termination or change of employment when a user has known passwords for identities that remain active (e.g. shared identities).

3.14. Access rights

This clause is based on ISO 27001:2022 Annex A 5.18

The Supplier shall provision, review, modify and remove access rights in accordance with the Supplier's topic-specific policy on and rules for access control.

3.15. Privileged access rights

This clause is based on ISO 27001:2022 Annex A 8.2

The Supplier shall restrict and manage the allocation and use of privileged access rights.

When assigning privileged access rights to relevant systems, the Suppler must, conditioned upon the risk involved, ensure the following:

- The purpose of the privileged access right is described
- The privileged access cannot be used for business activities
- Assignment of privileged access rights are approved by an authorized person/body
- Privileged access rights to a system can only be assigned by a person different from approver and user
- The use of privileged access rights – where possible – is limited to the period of time where there is an actual work-related need
- Logging and review of the use of privileged access right take place at regular intervals
- The assignment of privileged access rights must follow the 'principle of least privilege' to the extent possible

3.16. Information access restriction

This clause is based on ISO 27001:2022 Annex A 8.3

The Supplier shall restrict access to information and associated assets in accordance with the established topic-specific policy on access control and the defined roles.

3.17. Access to source code

This clause is based on ISO 27001:2022 Annex A 8.4

The Supplier shall appropriately manage read and write access to source code, development tools and software libraries.

3.18. Information security in supplier relationships

This clause is based on ISO 27001:2022 Annex A 5.19 and NIS2, article 21(2)(d)

The Supplier shall define and implement processes and procedures to manage the information security risks associated with the use of sub-suppliers' products or services.

Based on the risk associated with each relevant direct sub-supplier, The Supplier shall perform commercially reasonable efforts to ensure that the information security requirements to each direct sub-supplier provide at least a level of security of New Rail information adequate to the level of security agreed between New Rail and the Supplier.

3.19. Addressing information security within supplier agreements

This clause is based on ISO 27001:2022 Annex A 5.20 and NIS2, article 21(2)(d)

The Supplier shall establish and agree relevant information security requirements with each direct sub-supplier based on the type of supplier relationship.

3.20. Managing information security in the ICT supply chain

This clause is based on ISO 27001:2022 Annex A 5.21 and NIS2, article 21(2)(d)

The Supplier shall, based on the risk associated with each relevant direct sub-supplier, perform commercially reasonable efforts to define and implement processes and procedures to manage the information security risks associated with the ICT (information and communications technologies) products and services supply chain.

The Supplier shall as an integral part of the requirements in clause 3.20 perform commercially reasonable efforts to establish measures on supply chain security, including security-related aspects concerning the relationships between the Supplier and its direct suppliers or service providers.

3.21. Monitoring, review and change management of supplier services

This clause is based on ISO 27001:2022 Annex A 5.22 and NIS2, article 21(2)(d)

Monitoring, review and change management of supplier services is considered part of requirement 3.20 Managing information security in the ICT supply chain.

3.22. Information security for use of cloud services

This clause is based on ISO 27001:2022 Annex A 5.23 and NIS2, article 21(2)(d)

The Supplier shall establish processes for acquisition, use, and management of cloud services in accordance with New Rail's information security requirements.
For clarity: New Rail's information security requirements are stated in this document.

3.23. Information Security Incident Management and Preparation

This clause is based on ISO 27001:2022 Annex A 5.24 and NIS2, article 21(2)(b)

The Supplier shall plan and prepare for managing information security incidents by defining, establishing, and communicating an information security incident management process, including roles, and responsibilities.

The Supplier shall as an integral part of the requirements in this clause 3.23 establish measures on information security incident handling.

3.24. Assessment and decision on information security events

This clause is based on ISO 27001:2022 Annex A 5.25 and NIS2, article 23(1)

The Supplier shall assess information security events and decide if they are to be categorized as information security events.

The Supplier shall ensure that major information security events are identified, analysed, handled and reported.

The Supplier shall, when realising that an information security event should be reassigned to New Rail or a third-party supplier, provide a swift handover of the information security event to the relevant party to support quick restoration of service operation.

The Supplier shall resolve information security events in a consistent and effective manner that focuses on minimising the business impact.

Information security incidents affecting the services provided to New Rail must be reported to New Rail without undue delay in order for New Rail to comply with its obligations to report such information security incident to the Danish Civil Aviation and Railway Authority and/or other relevant parties.

Where appropriate, the Supplier shall ensure that New Rail receives any information on significant information security incident that are likely to adversely affect the provision of New Rail's services, including information required to determine any cross-border impact of the incident.

[See Appendix XX for a description of the procedure.]

3.25. Response to information security incidents

This clause is based on ISO 27001:2022 Annex A 5.26

The Supplier shall respond to information security incidents in accordance with the information security incident management process.

The Supplier shall ensure full alignment with New Rail's Service Desk services for all relevant processes.

3.26. Learning from information security incidents

This clause is based on ISO 27001:2022 Annex A 5.27

The Suppler shall use the knowledge gained from information security incidents to strengthen and improve information security measures and take all necessary actions to reduce the risk of similar incidents occurring again.

3.27. Collection of evidence

This clause is based on ISO 27001:2022 Annex A 5.28

The Supplier shall establish and implement procedures for the identification, collection, acquisition, and preservation of evidence related to information security incidents.

3.28. Information security during disruption

This clause is based on ISO 27001:2022 Annex A 5.29, and NIS2, article 21(2)(c)

The Supplier shall plan how to maintain information security at an appropriate level during disruption.

The Supplier shall ensure that business continuity aspects, including information security incidents, response, and recovery for the IT Services, are considered and documented.

The Supplier shall perform and document a review of business continuity aspects, including information security incidents, response and recovery for the IT Services.

The Supplier shall ensure that a disaster recovery plan is maintained. The recovery plan should provide for recovery of systems, infrastructure, and applications relevant for the IT Services within an agreed period of time.

The Supplier shall maintain a procedure for updates and maintenance of the disaster recovery plan. The disaster recovery plan shall be reviewed and approved by the Supplier's management body, at least annually.

The Supplier shall ensure that the disaster recovery plan is reviewed and, if considered necessary, tested, at least, annually, based on updated threat scenarios and the defined purpose of the disaster recovery test.

The Supplier shall as an integral part of the requirements in this clause 3.28 establish measures on business continuity and crisis management.

3.29. ICT readiness for business continuity

This clause is based on ISO 27001:2022 Annex A 5.30

The Supplier shall plan, implement, maintain, and, if considered necessary, test ICT readiness based on business continuity objectives and New Rail's ICT continuity requirements.

3.30. Legal, statutory, regulatory, and TSAual requirements

3.30.1. General

This clause is based on ISO 27001:2022 Annex A 5.31

The Supplier shall identify, document, and update legal, statutory, regulatory, and TSAual requirements relevant to information security and the Supplier's approach to meet these requirements.

3.30.2. NIS2 - Supervision and enforcement

This clause is based on NIS2, articles 32(2), 32(4), 32(5), 33(2) and 33(4)

The Supplier shall assist New Rail in complying with the obligations concerning supervision and enforcement in NIS2, including at least assistance to New Rail and/or competent authorities with:

a) on-site inspections and off-site supervision, including random checks conducted by trained professionals,
b) regular and targeted security audits carried out by an independent body or a competent authority,
c) ad hoc audits, including where justified on the ground of a significant incident or an infringement of mandatory provisions by either New Rail or the Supplier,
d) security scans based on objective, non-discriminatory, fair, and transparent risk assessment criteria,
e) requests for information necessary to assess the cybersecurity risk-management measures adopted by New Rail, including documented cybersecurity policies, as well as compliance with the obligation to submit information to the competent authorities pursuant to NIS2, Article 27,
f) requests to access data, documents, and information necessary for competent authorities to carry out their supervisory tasks, requests for evidence of implementation of cybersecurity policies, such as the results of security audits carried out by a qualified auditor and the respective underlying evidence.

The Supplier is obligated to comply with and assist New Rail in relation to enforcement measures concerning NIS2 enacted by competent authorities, including at least:

a) warnings about infringements of NIS2 by either New Rail or the Supplier,
b) binding instructions, including measures necessary to prevent or remedy an incident, as well as time-limits for the implementation of such measures and for reporting on their implementation, or an order requiring New Rail or the Supplier to remedy the deficiencies identified or the infringements of NIS2,

c) orders to New Rail or the Supplier to cease conduct that infringes NIS2 and desist from repeating that conduct,
d) orders to New Rail or the Supplier to ensure that the cybersecurity risk-management measures comply with NIS2, Article 21 or to fulfil the reporting obligations laid down in Article 23, in a specified manner and within a specified period,
e) orders to New Rail or the Supplier to inform the natural or legal persons with regard to which the New Rail provide services or carry out activities which are potentially affected by a significant cyber threat of the nature of the threat, as well as of any possible protective or remedial measures which can be taken by those natural or legal persons in response to that threat,
f) orders to New Rail or the Supplier to implement the recommendations provided as a result of a security audit within a reasonable deadline.

The Supplier shall, if competent authorities establish a deadline by which New Rail is requested to take action to remedy deficiencies or to comply with requirements, use its best efforts at all times, and at all times loyally and conscientiously perform all of the obligations in relation to the TSA to remedy such deficiencies and comply with requirements in a spirit of cooperation and fairness with New Rail.

3.31. Intellectual Property Rights

This clause is based on ISO 27001:2022 Annex A 5.32

The Supplier shall implement and apply appropriate procedures and/or measures to ensure that intellectual property rights are respected, including in connection with the use of third-party software.

3.32. Protection of Records

This clause is based on ISO 27001:2022 Annex A 5.33

The Supplier shall, in relation to the fulfilment of the TSA, implement appropriate measures to ensure that records are protected from loss, destruction, falsification, unauthorized access and unauthorized release.

3.33. Privacy and protection of PII

This clause is based on ISO 27001:2022 Annex A 5.34

[See clause xx of the TSA, if applicable].

3.34. Independent review of information security

This clause is based on ISO 27001:2022 Annex A 5.35

[See clause xx of the TSA, if applicable].

3.35. Documented operating procedures

This clause is based on ISO 27001:2022 Annex A 5.37

The Supplier shall document operating procedures for information processing facilities and make them available to personnel who need them.

4. People controls

4.1. Screening

This clause is based on ISO 27001:2022 Annex A 6.1

The Supplier shall apply a process to ensure that personnel possessing risk-positions relevant to the Services are eligible and suitable for the roles for which they are considered and remain eligible and suitable during their employment.

The Supplier shall carry out background verification checks on all candidates for employment to perform work related to the provision of IT Services prior to joining the organization and on an ongoing basis taking into consideration applicable laws, regulations and ethics and be proportional to New Rail's requirements, the classification of the information to be accessed and the perceived risks.

4.2. Terms and conditions of employment

This clause is based on ISO 27001:2022 Annex A 6.2

The Supplier shall ensure that the employment TSAual agreements for all employees and external consultants who are involved in the IT Services state the personnel's and the Supplier's responsibilities for information security.

4.3. Information security awareness, education and training

This clause is based on ISO 27001:2022 Annex A 6.3 and NIS2, article 21(2)(g) and (i)

The Supplier shall ensure that the Supplier's personnel and relevant interested parties receive appropriate information security awareness, education and training and regular updates of the Supplier's information security policy, topic-specific policies and procedures, as relevant for their job function. The awareness programme shall be evaluated and updated at least yearly to ensure relevance.

The Supplier shall include at least the following topics, when designing the awareness program:

- creation and protection of passwords
- protection and sharing of data
- protection and update of equipment, including how to act when equipment is used off-premises

The Supplier shall as an integral part of the requirements in this clause 4.3 establish cybersecurity training for all employees who are involved in the IT Services.

The Supplier shall as an integral part of the requirements in this clause 4.3 establish measures on human resources security.

4.4. Disciplinary process

This clause is based on ISO 27001:2022 Annex A 6.4

The Supplier shall formalise and communicate a disciplinary process to take actions against personnel and other relevant interested parties who have committed an information security policy violation.

4.5. Responsibilities after termination or change of employment

This clause is based on ISO 27001:2022 Annex A 6.5

The Supplier shall define, enforce, and communicate information security responsibilities and duties that remain valid after termination or change of employment to relevant personnel and other interested parties.

4.6. Remote working

This clause is based on ISO 27001:2022 Annex A 6.7

The Supplier shall adopt a policy for, and implement security measures in order to protect, information accessed, processed or stored by the Supplier's personnel outside the Supplier's premises.

The Supplier shall apply a documented procedure for access to computers or other electronic devices that are not at the Supplier's premises with the purpose of ensuring that the security obligations are also extended to the processing at such devices.

The Supplier shall ensure that relevant measures, such as multi-factor authentication and rules for storage of data, are included in the procedure.

4.7. Information security event reporting

This clause is based on ISO 27001:2022 Annex A 6.8 and NIS2, article 23
The Supplier shall provide a mechanism for the Supplier's personnel to report observed or suspected information security events through appropriate channels in a timely manner.

The Supplier shall ensure timely, consistent, and effective reporting of information security events, cf. clause 3.24.

5. Physical controls

5.1. Physical security perimeters

This clause is based on ISO 27001:2022 Annex A 7.1

The Supplier shall define and use security perimeters to protect areas that contain information and other associated assets. The measures shall be based on an all-hazards approach that aims to protect network and information systems and the physical environment of those systems from incidents.

5.2. Physical entry

This clause is based on ISO 27001:2022 Annex A 7.2

The Supplier shall ensure that secure areas are protected by appropriate entry controls and access points and that only authorized personnel have access to the secure areas.

The Supplier shall ensure appropriate authentication mechanisms based on use of access cards, or by biometrics or two-factor authentication, such as an access card or key, and a secret pin code.

A log trail of access and access attempts must be kept.

The Supplier shall ensure that identities of visitors in connection with the IT Services are authenticated, that date and time of entry and departure is recorded, and that visitors are always supervised while on premises.

The Supplier shall ensure that delivery and loading areas are designed so that deliveries can be loaded and unloaded without delivery personnel gaining unauthorized access to other parts of the premises.

5.3. Physical security monitoring

This clause is based on ISO 27001:2022 Annex A 7.4

The Supplier shall continuously monitor premises for unauthorized physical access and apply procedures for periodic control and follow-up on physical security. The procedures must define intervals for control and follow-up.

5.4. Protecting against physical and environmental threats

This clause is based on ISO 27001:2022 Annex A 7.5

The Supplier shall design and implement protection against physical and environmental threats, such as natural disasters and other intentional or unintentional physical threats to infrastructure.

The Supplier shall identify relevant physical and environmental threats and consider appropriate measures, based on risk assessment results, in the contexts of fire, flooding, electrical surges etc.

5.5. Equipment siting and protection

This clause is based on ISO 27001:2022 Annex A 7.8

The Supplier shall ensure that equipment used in connection with the IT Services is sited securely and protected.

5.6. Security of assets off-premises

This clause is based on ISO 27001:2022 Annex A 7.9

The Supplier shall protect off-site assets which stores or processes information in connection with the IT Services.

5.7. Storage media

This clause is based on ISO 27001:2022 Annex A 7.10

The Supplier shall ensure that storage media used in connection with the IT Services is managed through its life cycle of acquisition, use, transportation, and disposal in accordance with the Supplier's classification scheme and handling requirements.

The Supplier shall ensure that secure deletion of data or formatting of storage media is performed where storage media containing confidential information need to be reused within the organization (see clause 5.11).

5.8. Supporting utilities

This clause is based on ISO 27001:2022 Annex A 7.11

The Supplier shall protect information processing facilities from power failures and other disruptions caused by failures in supporting utilities.

5.9. Cabling security

This clause is based on ISO 27001:2022 Annex A 7.12

The Supplier shall ensure that cables carrying power, data or supporting information services in connection with the IT Services are protected from interception, interference, or damage.

5.10. Equipment maintenance

This clause is based on ISO 27001:2022 Annex A 7.13

The Supplier shall maintain equipment correctly to ensure, availability, integrity and confidentiality of information.

5.11. Secure disposal or re-use of equipment

This clause is based on ISO 27001:2022 Annex A 7.14

The Supplier shall ensure that items of equipment containing storage media should be verified to ensure that any New Rail data, licensed software etc. has been removed or securely overwritten prior to disposal or re-use.

6. Technological controls

6.1. Basic cyber hygiene

This clause is based on NIS2, article 21(2)(g)

The Supplier shall establish and maintain basic cyber hygiene practices.

6.2. User endpoint devices

This clause is based on ISO 27001:2022 Annex A 8.1

The Supplier shall implement, apply, and maintain procedures and/or measures to protect information stored on, processed by or accessible via user endpoint devices.

6.3. Secure authentication

This clause is based on ISO 27001:2022 Annex A 8.5 and NIS2, article 21(2)(j)

The Supplier shall implement secure authentication technologies and procedures based on information access restrictions and the topic-specific policy on access control.

The Supplier shall ensure that user accounts are locked, and an alarm is sent, after a predefined amount of identification failures.

The Supplier shall apply a procedure that prevents browser-based autofill of password when a username is entered, and forces logoff after a configurable idle time.

The Supplier shall as an integral part of the requirements in this clause 6.3 establish and make use of multi-factor authentication or continuous authentication solutions, where appropriate.

6.4. Capacity management

This clause is based on ISO 27001:2022 Annex A 8.6

The Supplier shall monitor and adjust the use of resources in line with current and expected capacity requirements and apply documented operational procedures for capacity management. The procedures must be based on the criticality of the services provided and include:

a) Deletion of obsolete data
b) Decommissioning or scaling of applications, systems, databases or environments
c) Optimising batch processes and schedules
d) Optimising application logic or database inquiries
e) Rejecting or restricting bandwidth for resource-demanding services that are not business critical
f) Capacity monitoring

The Supplier shall dispose and remove components in the IT Services securely, as they become obsolete.

6.5. Protection against malware

This clause is based on ISO 27001:2022 Annex A 8.7

The Supplier shall implement protection against malware, supported by appropriate user awareness. The

Supplier shall apply documented procedures and measures for protection against virus and malware on all equipment that is connected to its network and relevant for the IT Services.

6.6. Management of technical vulnerabilities

This clause is based on ISO 27001:2022 Annex A 8.8

The Supplier shall maintain procedures for vulnerability management, which ensure that information about technical vulnerabilities is obtained, exposure to such vulnerabilities is evaluated and appropriate measures are taken to mitigate the associated risk through security patches or mitigations.

The Supplier shall assess all implemented security components based on test integration results, penetration tests and vulnerability scans.

The Supplier shall without undue delay implement countermeasures in the form of security patches or mitigations, rectifying any significant security findings from performed penetration tests and vulnerability scans.

6.7. Configuration management

This clause is based on ISO 27001:2022 Annex A 8.9

The Supplier shall establish, document, implement, monitor, and review configurations, including security configurations, of hardware, software, services and networks used in connection with the IT Services.

6.8. Information deletion

This clause is based on ISO 27001:2022 Annex A 8.10

The Supplier shall delete information stored in IT systems, devices or in any other storage media, when the information is no longer required in connection with the IT Services.

6.9. Data masking

This clause is based on ISO 27001:2022 Annex A 8.11

The Supplier shall ensure data masking to prevent the exposure of data and to comply with legal, statutory, regulatory, and TSAual requirements, and New Rail's requirements, if applicable.

6.10. Data leakage prevention

This clause is based on ISO 27001:2022 Annex A 8.12

The Supplier shall apply data leakage prevention measures to systems, networks and any other devices that process, store, or transmit sensitive information in connection with the IT Services.

6.11. Information backup

This clause is based on ISO 27001:2022 Annex A 8.13

The Supplier shall maintain and regularly test backup copies of information, software and systems that are relevant for the IT Services, in accordance with a topic-specific policy on backup and based on agreement with New Rail in relation to New Rail information.

6.12. Redundancy of information processing facilities

This clause is based on ISO 27001:2022 Annex A 8.14

The Supplier shall ensure that information processing facilities are implemented with redundancy sufficient to meet New Rail's availability requirements.

6.13. Logging

This clause is based on ISO 27001:2022 Annex A 8.15

The Supplier shall produce, store, protect and analyse logs that record activities, exceptions, faults, and other relevant events. The Supplier shall ensure traceability of New Rail related activities in the Supplier's operating systems, database systems and other systems by which access to New Rail data is possible.

The Supplier shall ensure that the clocks of information processing systems used by the Supplier in connection with the IT Services are synchronized to approved time sources.

The Supplier shall implement and maintain measures to protect against unauthorized changes to log information and operational problems with the logging facility in connection with the IT Services.

The Supplier shall ensure that New Rail has access to or may request log data, reports and statistics. In addition – where relevant – the Supplier shall provide for the export of log information in a recognized format, such as syslog.

The Supplier shall ensure that the IT system architecture ensures that diagnostic data (logs, events, etc.) on the performance of the IT systems and network is available in real time and using an open format.

The Supplier shall ensure that all test and condition monitoring software and equipment required to send, receive, process, configure, print, interpret system and test data, enable fault diagnosis and repair of the Supplier's IT services are available.

6.14. Monitoring activities

This clause is based on ISO 27001:2022 Annex A 8.16

The Supplier shall in relation to the fulfilment of the TSA monitor networks, systems and applications for anomalous behaviour and appropriate actions shall be taken to evaluate potential information security incidents.

6.15. Installation of software on operational systems

This clause is based on ISO 27001:2022 Annex A 8.19

The Supplier shall implement procedures and measures to securely manage the software installation on operational systems.

The Supplier shall apply a documented procedure for patch management to ensure that security patches on operational software are applied.

The Supplier shall ensure that applicable security patches on operational software are tested and applied no later than thirty (30) working days after release unless otherwise is agreed with New Rail. Security patches categorised as emergency critical or similar by the software manufacturer shall be applied without undue delay unless otherwise is agreed with New Rail.

6.16. Networks security

This clause is based on ISO 27001:2022 Annex A 8.20

The Supplier shall secure, manage, and control networks and network devices to protect information in systems and applications.

The Supplier shall implement and maintain measures to ensure the security of information in networks and to protect connected services from unauthorized access.

6.17. Security of network services

This clause is based on ISO 27001:2022 Annex A 8.21

The Supplier shall identify, implement and monitor security mechanisms, service levels and service requirements of network services.

The Supplier shall ensure that security measures are implemented by either internal or external network service providers.

The Supplier shall ensure that rules on the use of networks and network services are formulated and implemented.

The Supplier shall consider at least the following security features:

a) technology applied for security of network services, such as authentication, encryption and network connection measures
b) technical parameters required for secured connection with the network services in accordance with the security and network connection rules
c) caching (e.g. in a content delivery network) and its parameters that allow users to choose the use of caching in accordance with performance, availability and confidentiality requirements
d) procedures for the network service usage to restrict access to network services or applications, where necessary.

6.18. Segregation of networks

This clause is based on ISO 27001:2022 Annex A 8.22

The Supplier shall ensure that groups of information services, users and information systems are segregated in the Supplier's networks, at a minimum between services provided over the internet (e.g. DMZ, DMP, Purdue network model) and internal networks.

6.19. Web filtering

This clause is based on ISO 27001:2022 Annex A 8.23

The Supplier shall manage access to external websites to reduce exposure to malicious content.

6.20. Use of cryptography

This clause is based on ISO 27001:2022 Annex A 8.24 and NIS2, article 21(2)(h)

The Supplier shall define and implement rules for the effective use of cryptography, including cryptographic key management.

The Supplier shall apply a policy for use, protection, and life cycle of cryptographic keys.

6.21. Secure development life cycle

This clause is based on ISO 27001:2022 Annex A 8.25 and NIS2, article 21(2)(e)

The Supplier shall establish and apply rules for the secure development of software. The Supplier shall ensure that all employees contributing to the analysis, design and implementation of software used in connection with the IT Services are trained in secure development and that the development of software takes place using safe and recognized methods.

The Supplier shall as an integral part of the requirements in this clause 6.21 establish measures on security in network and information systems acquisition, development, and maintenance, including vulnerability handling and disclosure.

6.22. Application security requirements

This clause is based on ISO 27001:2022 Annex A 8.26

The Supplier shall identify, specify, and approve information security requirements when developing or acquiring applications.

The Supplier shall provide a release and deployment management process that takes an end-to-end view of a change to a service and that verifies that both technical and non-technical aspects of a software release are considered together.

The Supplier shall establish software control and distribution procedures, including the management of the configuration items pertaining to Software under the responsibility of the Supplier.

6.23. Secure system architecture and engineering principles

This clause is based on ISO 27001:2022 Annex A 8.27 and NIS2, article 21(2)(e)

The Supplier shall establish, document, maintain and apply principles for engineering secure systems to any information system development activities.

The Supplier shall ensure that the design process prioritizes preventing potential conflicts between security functionality and the defined business/functional architecture.

6.24. Secure coding

This clause is based on ISO 27001:2022 Annex A 8.28

Where relevant, the Supplier shall in relation to the fulfilment of the TSA apply secure coding principles to software development in connection with the IT Services.

6.25. Security testing in development and acceptance

This clause is based on ISO 27001:2022 Annex A 8.29

Where relevant, the Supplier shall define and implement security testing in the development life cycle.

Where relevant, the Supplier shall define and maintain an updated list of validation and verification activities for requirements and activities related to configuration and security functionality.

Where relevant, the Supplier shall define and maintain an updated list of validation and verification activities for requirements and activities related to organizational and security related application conditions.

Where relevant, the Supplier shall perform a security handover to all relevant stakeholders according to the agreed roles and responsibilities. This handover should take place leading up to solution delivery.

6.26. Outsourced development

This clause is based on ISO 27001:2022 Annex A 8.30

The Supplier shall direct, monitor and review the activities related to outsourced system development in connection with the IT Services.

6.27. Separation of development, test and production environments

This clause is based on ISO 27001:2022 Annex A 8.31

The Supplier shall in relation to the fulfilment of the TSA separate and secure development, testing and production environments to the extent that this is required due to business needs (including legislation) and relevant for the IT Services.

The Supplier shall in relation to the fulfilment of the TSA identify and implement the level of separation necessary to prevent problems in connection with the IT Services.

The Supplier shall in relation to the fulfilment of the TSA ensure that development and testing environments in connection with the IT Services are protected considering:

a) patching and updating of all the development, integration and testing tools (including builders, integrators, compilers, configuration systems and libraries)
b) secure configuration of systems and software
c) control of access to the environments
d) monitoring of change to the environment and code stored therein
e) secure monitoring of the environments
f) taking backups of the environments.

6.28. Change management

This clause is based on ISO 27001:2022 Annex A 8.32

The Supplier shall ensure that changes to information processing facilities and information systems, operational changes, and changes to business processes are subject to change management procedures. The change management procedures in connection with the IT Services shall include at least:

a) planning and assessing the potential impact of changes considering all dependencies
b) authorization of changes
c) communicating changes to relevant interested parties
d) tests and acceptance of tests for the changes (see clause 6.25)

e) implementation of changes including deployment plans
f) emergency and contingency considerations including fall-back procedures
g) maintaining records of changes that include all of the above
h) ensuring that operating documentation (see clause 3.35) and user procedures are changed as necessary to remain appropriate
i) ensuring that ICT continuity plans and response and recovery procedures (see clause 3.29) are changed as necessary to remain appropriate.

6.29. Test information

This clause is based on ISO 27001:2022 Annex A 8.33

Where relevant, the Supplier shall ensure that test information is appropriately selected, protected and managed in accordance with best practices. Where testing activities require the use of personal data of which New Rail is the data controller, the use of such personal data may only take place upon prior agreement with New Rail.

Where relevant, the Supplier shall in relation to the fulfilment of the TSA ensure that any access control procedures, which apply to operational application systems, also apply to test application systems.

Where relevant, the Supplier shall in relation to the fulfilment of the TSA ensure that operational information is erased from a test environment when it is no longer required for the testing purpose.

6.30. Protection of information systems during audit testing

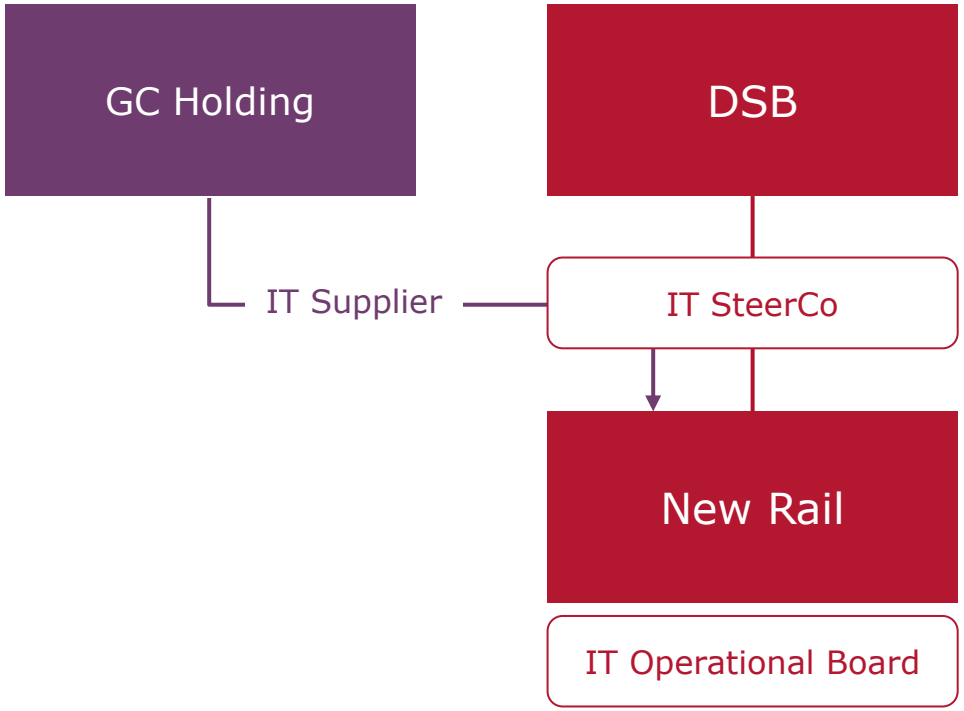
This clause is based on ISO 27001:2022 Annex A 8.34

Where relevant, the Supplier shall plan and agree audit tests and other assurance activities involving assessment of operational systems between the tester and appropriate management.

PROJECT NEXUS

TSA Governance Model

The IT governance Model with representation from GoCollective, New Rail and DSB based on IT management & delivery roles



IT SteerCo	
SteerCo Chairman	Michael Moesgaard (DSB)
Senior Supplier	Henrik Andersen (GoCo Holding)
Senior User	Steen Thyregod (New Rail)
IT Delivery Manager	Ida Steman-Johannesen (GoCo Holding)
IT Business Partner	Lene Reimer (DSB)

IT Operational Board	
Lead	Steen Thyregod (New Rail)
Senior User (Non-SAP)	Grethe Jørgensen (New Rail)
Senior User (SAP)	René Zimmer Jakholm (New Rail)
IT Coordinator	Henrik Hansen (New Rail)
IT Business Partner	Lene Reimer (DSB)

The two-tier IT governance model will ensure a balanced demand for IT services, and an ongoing follow-up on IT supplier performance

IT STEERCO

Purpose

- Follow-up on supplier agreement (TSA/MSA) and IT service delivery performance
- Follow-up on demand for additional IT services
- *SteerCo* for New Rail Carve-Out IT project (TSA build)

Membership

- SteerCo Chairman (DSB)
- Senior Supplier (GoCollective)
- Senior User (New Rail)
- IT Delivery Manager (GoCollective)
- IT Business Partner (DSB, facilitator)

Meeting frequency

- First 3 months from cutover: Bi-weekly
- Hereafter: Monthly

IT OPERATIONAL BOARD

Purpose

- Status on IT services from IT vendor
- Status on IT services from New Rail internal
- Process & prioritize new demand
- *SteerCo* for NIS2 project

Membership

- Lead (New Rail)
- Senior User, non-SAP (New Rail)
- Senior User, SAP (New Rail)
- IT Coordinator (New Rail)
- IT Business Partner (DSB, facilitator)

Meeting frequency: One week before SteerCo

- First 3 months from cutover: Bi-weekly
- Hereafter: Monthly

BI

MÅNEDSMØDE

Agenda:

- Status på driften og igangværende og leverede sager
- Udviklingsønsker og prioritering

Deltagere:

- New Rail: Steen Thyregod (Spoc) + relevante deltagere fra New Rail og evt. DSB
- GoCollective: Tristan Willacy + relevante fra BI

- Frekvens og format kan justeres efter behov

Payroll

MÅNEDSMØDE

Agenda:

- Status på lønkørsler, refusioner og bogføring af lønnen
- Udviklingsønsker og prioritering

Deltagere:

- New Rail: Steen Thyregod (Spoc) + relevante deltagere fra New Rail og evt. DSB
- GoCollective: Pia Haugsted og relevante fra Lønkontoret

- Frekvens og format kan justeres efter behov

Finans og controlling og procurement masterdata

MÅNEDSMØDER

1) Analysemøde på ”arbejdsdag 4” med gennemgang af udvikling i faktiske tal mod budget

2) Regnskabsmøde med GC Holding:

Agenda:

- Status på performance indenfor hvert område
  - Debitor
  - Kreditor
  - Finans
  - Anlæg
  - Finansiel controlling
  - Andet, rapportering
- Udviklingsønsker og prioritering

Deltagere:

- New Rail: Steen Thyregod (Spoc) + relevante deltagere fra New Rail (møde 1+2)
- GoCollective: Pia Haugsted og relevante fra Finans (møde 2)
- DSB: Repræsentanter fra DSB Regnskab (møde 1+2) og repræsentanter fra Koncernøkonomi (møde 1)
- Frekvens og format kan justeres efter behov

Finans og controlling og procurement masterdata

ÅRLIGT

Et eller flere møder i forbindelse med:

- Årsregnskabsprocessen, som omfatter klargøring af dokumentation af processer og kontroller herunder it, løbende revision, hardclose og statusrevision – både i relation til det finansielle regnskab og bæredygtighedsrapportering
- Revision af DSB's koncernregnskab og datterselskaber, som omfatter procesrevision, løbende revision, hardclose og statusrevision– både i relation til det finansielle regnskab og bæredygtighedsrapportering
- Selvangivelsen
- Dokumentation af transaktionsdokumentation og revision heraf, jf. Regnskabsreglementet for DSB ("Transfer pricing for DSB")
- New Rails regnskabsaflæggelse og revision bliver en del af DSBs proces og DSB har lead på processen og inddragelse af GoCollective for New Rail

Deltagere:

- DSB Finans
- New Rail: Steen Thyregod (Spoc) + relevante deltagere fra New Rail
- GoCollective: Pia Haugsted og relevante fra Finans

Nexus Project			Spent until end May DKK	Projected costs (expected) DKK	Total spent + projected (expected) DKK	Paid
New Rail Mobilization	Internal	All workstreams	3.412.000	1.000.000	4.412.000	
		Total GoCo internal Mobilization	3.412.000	1.000.000	4.412.000	No reimbursement by DSB to GoCollective for internal costs
	External	**IT**				
		Consolut (Muxtec)	-	2.330.000	2.330.000	
		XSuite	150.000	23.000	173.000	
		Arkyn	70.000	190.000	260.000	
		Prometheus	-	-	-	
		MMS	-	550.000	550.000	
		ITM8	-	100.000	100.000	
		Kronborg IT (ex. Consultant)	210.000	330.000	540.000	
		Hastus	-	-	-	
		HR			-	
		TMN consult (ex.consultant)	75.000	200.000	275.000	
					-	
					-	
		Total external Mobilization	505.000	3.723.000	4.228.000	The final actual external cost will be reimbursed by DSB to GoCollective

Transportministeriet
Frederiksholms Kanal 27F
1220 Copenhagen K

Telephone 41 71 27 00
trm@trm.dk
www.trm.dk