Annex 3: Emergency procedures and exclusions

1. Introduction

Annex 3 is an appendix to the Certified Pick up Terms and Conditions and describes (i) the (i) manner in which a Container may lawfully be delivered in the absence of the CPu Service through the emergency procedures, as well as the (ii) exclusions to the obligation to use the CPu Service for delivering Containers.

An emergency procedure means the actions to be taken by NxtPort and the User(s) (in addition to the mitigation measures described in Annex 2) (the '**Emergency Procedures**'):

a) complete unavailability of the CPu Solution
b) specific connections to Users are exceptionally unavailable
c) on the instruction of the authorities
d) if a User is unable to provide all the Mandatory Data with respect to a specific Container

Exclusions include the procedures to be followed in the event that a Container is excluded from the Certified Pick up obligation, but is already registered in the CPu Solution:

a) Transshipment Containers that need to leave the Terminal for reasons of scanning / physical verification / inspection
b) Export containers to be collected back

2. Emergency procedures

If the CPu solution is not available, the NxtPort Terminal Operator may allow the activation of a certain Fallback mechanism.

The following Fallback mechanisms are currently recognised and accepted:

1) Terminal Operator uses the Alfapass or name of Planner shared by CPu with Terminal Operator when creating PickUpRight
2) SCR as a Third Party Application
3) Terminal operator specific portal

Annex 4: IT Security Policy

1.1 Management guidelines for information security

- NxtPort has implemented appropriate information security policies and is ISO 27001-certified. NxtPort's management requires employees and external consultants with access to Data to be bound by written, confidentiality and privacy responsibilities with respect to that Data. These responsibilities remain in effect after termination or alteration of employment or appointment.

1.2 Personnel

- NxtPort provides information and training (*awareness*) on information security to employees and relevant external consultants.
- Employees are required to comply with policies and regulations on information security, Personal Data Protection and handling of Data.

1.3. Access control

User access management

- NxtPort implements access control policies to support the creation, modification and deletion of user accounts for systems or applications that access or provide access to Data.
- NxtPort implements a *user account and access provisioning* process to assign and revoke access rights to systems and applications.
- The use of 'generic' or 'shared' accounts is prohibited without system controls enabled to track specific user access and prevent shared passwords.
- Mandatory strong authentication (two-factor authentication) for admin accounts is implemented.
- NxtPort controls and restricts access to utilities capable of bypassing system or application security controls.
- User access to systems and applications that store or access Data is controlled by a secure login procedure.

Physical access management – Facility security

- Physical access to facilities where Data is stored or processed is protected in accordance with *good industry practices* (Tier 4 data centres).
- policies and procedures are in place for maintaining a safe and secure working environment in offices, rooms, facilities and secure areas
- physical security perimeters (fences, walls, barriers, guards, gates, electronic surveillance, physical authentication mechanisms, reception desks and security patrols) are implemented
- a complete inventory is maintained of all critical assets
- two-factor authentication for data centre access is mandatory
- Fire protection is in place: fire alarm system, early fire detection system, appropriate fire extinguishers, regular fire drills.
- The infrastructure is robust and provides adequate resistance to damage from the elements and unauthorised access
- Redundant data centres that are at least so far apart that a manageable damage event does not simultaneously affect the data centre originally used and the data centre with the backup capacity

1.4 Security of communications

Network and server security

- NxtPort logically separates User Data within a shared environment.
- NxtPort secures network segments of remote access points where User Data can be accessed.
- External network perimeters are secured and configured so as to prevent unauthorised traffic.
- Inbound and outbound points are protected by firewalls and intrusion detection systems (IDS).
- Ports and protocols are restricted to those with a specific purpose.
- NxtPort synchronises system clocks on network servers with a universal time source (e.g. UTC) or network time protocol (NTP).
- Anti-spam systems have been implemented
- 0-Day Malware protection is available

- Security measures to prevent *network-based attacks* are in place
- IDP / IDS systems have been implemented
- DDoS protection has been implemented
- Network segmentation has been implemented.
- Direct access from the Internet is limited to a segregated DMZ.
- Responsibility for the necessary DMZ infrastructure is clearly defined
- Network zones are separated with a firewall that allows only necessary network traffic
- Application-level Firewalls are in place
- Remote management takes place securely
- Remote management takes place via a secure communication channel (e.g. SSH, TLS/SSL, IPSec, VPN)
- Remote login takes place with strong authentication
- Network redundancy has been implemented

Cryptographic measures
- Data, including personal data, is *encrypted at rest*.

Cloud measures
- NxtPort encrypts Data during transmission between each application layer and between interfacing applications.

1.5 Application and Data Security

Application security
- NxtPort logically separates User Data within a shared service environment.
- NxtPort secures network segments of remote access points where User Data can be accessed.

1.6 Operational security

Service management
- NxtPort has implemented formal SOPs for system processes that affect User Data. Notifications can occur through generic change logs. Procedures are to track author, revision date and version number, and are to be approved by management.
- NxtPort monitors service availability.

Management of vulnerabilities
- NxtPort conducts annual penetration tests for systems and applications that store User Data or provide access to User Data, including Personal Data. Problems identified should be remediated within a reasonable time.
- NxtPort has implemented a patch and vulnerability management process to identify, report and remediate vulnerabilities by:
    a) Implementing patches or fixes from vendors.
    b) Developing a recovery plan for critical vulnerabilities.
- NxtPort has implemented measures to detect and prevent malware, malicious code and unauthorised execution of code. Control measures are to be regularly updated with the latest available technology (e.g. implementing the latest *signatures* and definitions).

Logging and monitoring
- NxtPort generates administrator and event logs for systems and applications that store User Data or allow access to User Data.
- NxtPort periodically monitors system logs to identify system failures, errors or potential security incidents affecting User Data.

1.7 Management of suppliers

- NxtPort has contractual agreements with third parties who handle User Information and these agreements include appropriate information security, confidentiality and data protection requirements, as detailed in the Agreement. Agreements with such parties are reviewed periodically to validate that information security and data protection requirements remain appropriate.

- NxtPort periodically reviews its suppliers' information security policies and validates that these measures remain appropriate according to the risks represented by the supplier's handling of User Information, taking into account any *state-of-the-art* technology and the cost of implementation.
- NxtPort limits third-party access to User Data, including Personal Data, to that required for the provider's service provision.
- At the User's request, NxtPort will provide the User with a list of third parties with required access to Data, including Personal Data.
- NxtPort allows access to User Data, including Personal Data, only to the extent necessary to perform the services that the third party has contractually agreed to provide.
- NxtPort provides exit provisions with defined file formats and retention of all logical relationships.
- Cloud service providers regularly notify NxtPort of security measures, IT security management system changes, security incidents, *Information Security* assessment results and penetration tests.
- Continuity of service provision is monitored with upstream providers in the event of provider outages.

1.8 Resilience

- NxtPort conducts business continuity risk assessment activities to determine relevant risks, threats, impacts, likelihood and required controls and procedures. Restoration will be performed at acceptable levels based on criteria established by NxtPort in accordance with reasonable time frames.
- Based on the results of the risk assessment, NxtPort annually documents, implements, tests and reviews its Business Continuity and Disaster Recovery (BC/DR) plans to validate its ability to restore the availability of and access to User Data in a timely manner, in the event of a physical or technical incident that results in loss or corruption of User Data.
- The User is able to monitor, upon request, measurable parameters as agreed upon in the SLA.

1.9 Transparency

- NxtPort's locations (country, region) where User Data will be stored and processed are disclosed and are located solely within the EEA.
- NxtPort's subcontractors vital to the delivery of cloud services are disclosed. Transparency about what interventions NxtPort or third parties are permitted as to the User's data and processes is provided
- Information on changes is provided on a regular basis (e.g. new or terminated positions, new subcontractors, other SLA-related issues)
- Transparency is provided as to what software NxtPort will install on the systems and the security requirements / risks that may result for a User from this.
- Transparency as to government intervention or inspection rights, as to any legally definable rights of third parties to view data, and as to any obligations that NxtPort has to verify stored data at a potential location is provided.

1.10 Audit and Compliance

- NxtPort periodically assesses whether its systems and equipment that store User Data or provide access to User Data, including Personal Data, comply with legal and regulatory requirements and contractual obligations owed to the User.
- NxtPort maintains current independent verification of the effectiveness of its technical and organisational security measures (e.g. ISO certification). The independent information security assessment shall be conducted at least annually.
- NxtPort performs independent security audits on a regular basis (and at least once a year).

Annex 5: Processing of Personal Data

1 Data controller

The data controller for this processing is NxtPort BV, registered under company number (LER Antwerp) 0429.672.881 with registered office at Sint-Pietersvliet 7, B-2000 Antwerp.

In its capacity as data controller, NxtPort shall take all appropriate technical and organisational measures to protect Personal Data against accidental or unauthorised destruction, accidental loss, and any unauthorised processing of Personal Data.

NxtPort will continue to ensure that Personal Data is processed in a lawful, proper and transparent manner; that Personal Data is collected for specific, expressly defined and justified purposes and that they are not subsequently processed in any manner incompatible with those purposes; that Personal Data is sufficient, relevant and limited to what is necessary for the purposes mentioned; that the Personal Data is correct and, if necessary, updated; that Personal Data is not kept longer than necessary for the purposes mentioned.

NxtPort guarantees that no transfer to third countries for data processing or storage shall take place without taking the necessary measures to comply with the protection requirements of the European privacy regulations.

2 Data subjects

Data subjects are natural persons whose data is processed in the context of handling Containers through Certified Pick up.

3 Personal data being processed

NxtPort collects and processes the following Data:

Contact details of Users and appointees of Users (name, e-mail address, telephone number).

4 Source of the Personal Data

The Personal Data is provided by a User.

5 Data processing purposes

The Personal Data will be processed purely for the imposed CPu Service as also further described in the CPu Terms and Conditions, including for the following purposes:

- The collection of Containers;
- Securing the port and the handling of Containers

In the context of this processing, the Personal Data will be passed on to third parties within the EU, namely to bodies to which NxtPort is legally obliged to pass on certain information, such as the (Maritime) police and various Federal Government Services. Certain Personal Data will also be transferred to external companies that provide technical support for certain applications. NxtPort shall make the necessary arrangements with each third party to whom the Personal Data are passed on and, if necessary, conclude a processing agreement with these third parties. NxtPort selects only those processors that offer the necessary guarantees with regard to data processing and data protection.

6 Legal basis for processing

For the processing of the Personal Data, NxtPort cites:

(i) The performance of its obligations under the CPu Terms and Conditions;

(ii) The performance of the concession agreement concluded with the Port Authority in implementation of art. 5.6 "Certified Pick up" of the Port Police Regulations

7 Retention period

NxtPort shall retain the Personal Data for as long as is necessary for the purposes set out in this statement. After that time, the Personal Data shall be deleted.

For more information: privacy@nxtport.com

8 The rights of the data subject

The data subject retains the right to object at any time to the processing of the Personal Data concerned for reasons relating to the specific situation if NxtPort bases its decision upon legitimate interests or the public interest / public authority. The data subject should make their case as to the specific reasons for doing so. NxtPort will then cease the processing unless it invokes compelling legitimate grounds for processing that outweigh the interests, rights, and freedoms of the data subject or that are related to the institution, exercise or substantiation of a legal claim.

The data subject is entitled to obtain a definitive answer from NxtPort as to whether or not the Personal Data concerned is being processed and, where relevant, to obtain insight into that Personal Data. When responding to this request, NxtPort will also include the details of the processing. NxtPort will send the data subject a copy of the Personal Data that is being processed.

The data subject is entitled to immediate rectification by NxtPort of the incorrect Personal Data concerned. The data subject can also have incomplete Personal Data completed. In some cases, the data subject themselves can correct or complete the Personal Data, through correction or addition in the CPu Service.

The data subject has the right to obtain without undue delay the erasure of the Personal Data concerned from NxtPort. NxtPort is obliged to erase the Personal Data concerned when it is no longer required for the purposes for which it was collected or otherwise processed, when there is no longer a legal basis to process the Personal Data, if the data subject objects to the processing and there are no prevailing, compelling, justified grounds for the operation, if the Personal Data is being unlawfully processed, when the data in accordance with Union law or law of the Member State should be cleared or if the Personal Data has been collected in connection with an offer of information society services.

Where NxtPort has disclosed the Personal Data and is required to delete the Personal Data, it shall take reasonable steps to inform other data controllers processing the Personal Data that the data subject has requested that NxtPort delete any link to, or copy or reproduction of, that Personal Data.

NxtPort cannot delete certain Personal Data, namely when the processing is necessary for the purpose of fulfilling a legal obligation or exercise of a task of general interest, for reasons of general interest in the field of public health, with a view to archiving in the public interest, scientific or historical research or statistical purposes, or for the establishment, exercise or underpinning of a legal action. The data subject will be notified of this after a request for deletion, if that is the case.

If (i) the correctness of the Personal Data is disputed by a data subject, (ii) the processing is unlawful and the data subject opposes the deletion of the Personal Data, (iii) NxtPort no longer needs the Personal Data for the processing purposes but the data subject does still needs it for the institution, exercising or substantiation of a legal claim, or (iv) the data subject has objected to the processing, then the data subject – pending any potential justified grounds presented by NxtPort or whilst it checks the correctness of the data – is entitled to obtain limitation of the processing.

In such an event, Personal Data is, barring the storage thereof, only processed with the consent of the data subject or for the institution, exercising or substantiation of a legal claim or to protect the rights of another natural person or legal person or on compelling grounds of general interest for the European Union or a Member State.

The data subject is entitled to obtain the relevant Personal Data that he or she supplied to NxtPort themselves in a structured, common and machine-legible manner, and the data subject is entitled to transfer the said data to another controller. This is possible when the processing is based on consent or an agreement to which the data subject is a party involved, or if the processing takes place through automated processes.

Finally, the data subject is also always entitled to submit a complaint to the supervisory authority, namely the Belgian Data Protection Authority.

Annex 6: Alfapass Terms and Conditions

See link: yet to be received from Alfapass.