Annexes

Versie 1

Annex 1 : CPu Oplossing

1. ALGEMENE BESCHRIJVING

Door de introductie van CPu zal de huidige manier van afhaling van containers via pincodes in de Haven Van Antwerpen worden vervangen door een volledige digitale oplossing.

Het betreft hier een digitaal systeem 1) waarop alle betrokken partijen moeten zijn op aangesloten en 2) dat gevoed wordt door gegevens doorgestuurd door bepaalde Gebruikers of ingebracht wordt door de diverse Gebruikers (de Organisator van het zeetransport, de Terminal, de Eerste gemachtigde, de Transportorganisator en elke Gebruiker die zich tussen de Eerste gemachtigde en de Transportorganisator bevindt). Hierdoor ontstaat een digitale ketting waarbij het Releaserecht, en uiteindelijk het Pickuprecht, digitaal kan worden overgemaakt aan de volgende Gebruiker in de logistieke keten. Uiteindelijk verleent CPu een Finaal Pickuprecht zodat een container de terminal mag verlaten. De autoriteiten krijgen te allen tijde een zicht op deze digitale ketting.

2. CPU OPLOSSING EN UITGEBREIDE CPU OPLOSSING

De CPu Oplossing bestaat uit volgende componenten:

1. CPU Core
2. Asynchronous APIs
3. Notifications
4. CPoint integratie
5. AlfaPass Validation Service integratie
6. Basis GUI

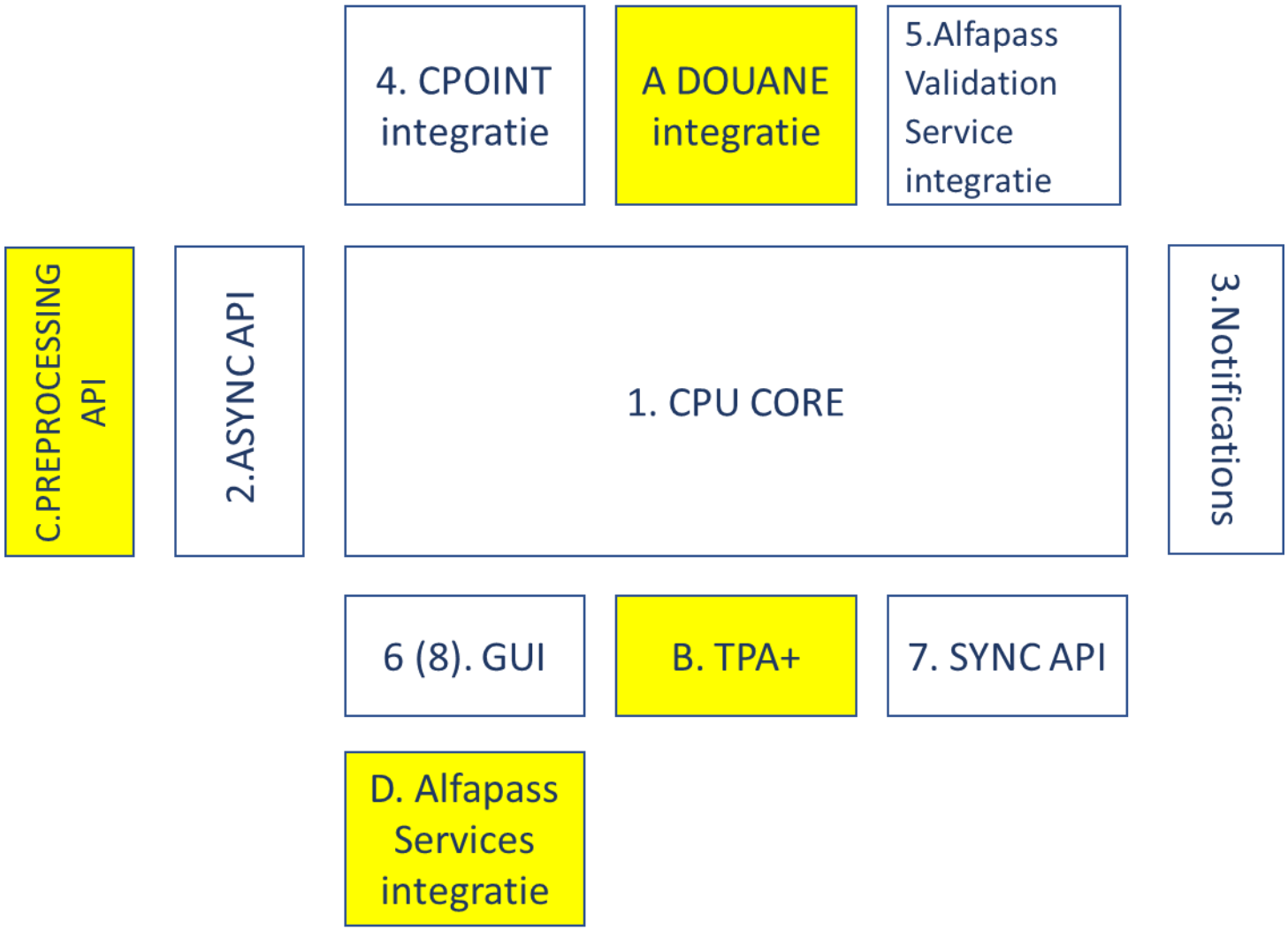
De CPu Oplossing is uitgebreid met volgende componenten:

7. Synchronous APIs
8. GUI+

Daarnaast worden volgende Add-On oplossingen aangeboden, die samen met de CPu Oplossing de Uitgebreide CPU Oplossing vormen:

A. Douane integratie
B. TPA specifieke APIs
C. Preprocesssing APIs
D. Alfapass Services integratie

Overzicht:



Beschrijving van de componenten van de CPu Oplossing

1. CPU Core

- Ondersteunen van het creëren van een commercial release recht dat finaal kan omgezet worden in een Finaal Pickuprecht.
- Ondersteunen van terminal bewegingen (gate in/discharge en gate out/load) en Terminal Vrijgave.

2. Asynchronous APIs

- Het creëren en updaten van een commercial release. Zie Documentatie voor verdere toelichting
- Het accepteren, weigeren, doorzetten en intrekken van een commercial release
- Het delen van terminal bewegingen incl status van commercial release.

3. Notifications

- Terugkoppelen van requests zoals onder 2. Asynchronous API opgenomen
- Delen van events gerelateerd aan een commercial release, Pickuprecht, terminal beweging of terminal release status

4. CPoint integratie

CPu maakt gebruikt van CPOINT als repository van actieve bedrijven en actieve gebruikers. CPOINT zelf is geen onderdeel van de CPU Oplossing, enkel de integratie.

5. Alfapass Validation Service integratie

CPu maakt gebruikt van de AlfaPass Validation Service om de geldigheid van een Pickuprecht bij afhaling per truck te valideren. Hiertoe heeft NxtPort een integratie API met Alfapass Validation Services ontwikkelt. De Alfapass Validation Service is geen onderdeel van de CPU Oplossing, enkel de Alfapass Validation Service integratie

6. GUI

Een User-interface die de Gebruikers in de mogelijkheid stelt om bepaalde Gegevens uit te wisselen en een beperkt aantal CPu functionaliteiten uit te voeren.

7. Synchronous APIs

Ten behoeve van de validatie van het Pickuprecht zijn additionele synchrone APIs ter beschikking gesteld.

Ten behoeve van verwerking van de commercial release is voor de terminals een additionele API ter beschikking gesteld om details op te vragen.

8. GUI+

Additionele schermen zijn ter beschikking gesteld voor verschillende rollen om in bulk de status van commercial releases te consulteren en bepaalde acties te triggeren.

Beschrijving van de Add-on componenten van de Uitgebreide CPU oplossing:

A. Douane integratie

Douane verstuurt verschillende berichten rechtstreeks of onrechtstreeks naar CPU via verschillende transport protocols. Beschikbare berichten worden (gedeeltelijk) verwerkt door de Uitgebreide CPU basisoplossing zoals beschreven in de Documentatie. CPu is niet verantwoordelijk voor het niet-beschikbaar zijn van douane gegevens, noch voor de kwaliteit van de gegevens.

De douane applicaties en (tussenliggende) communicatie infrastructuur maken geen deel uit van de Uitgebreide CPU oplossing.

B. Preprocesssing APIs

Een beperkt aantal EDIFACT berichttypes zullen tijdelijk ondersteund worden voor aanlevering van de Gegevens. De lijst van ondersteunde EDIFACT types is opgenomen in Documentatie. Validatie van berichten is vereist in UAT omgeving om van support te kunnen genieten buiten kantooruren. Hiertoe dient de procedure zoals op de website beschreven staat, gevolgd te worden.

C. TPA-specifieke APIs

Ten behoeve van Aanlevering van Gegevens via Derde Applicatie zijn er specifieke APIs ontwikkeld.

De Derde Applicatie is geen onderdeel van de Uitgebreide CPu oplosssing

D. Alfapass Services integratie

Om bepaalde handelingen te bevestigen, wordt gebruik gemaakt van de Alfapass Services, een verzameling van services aangeboden door AlfaPass om de identiteit van een Gebruiker te verifiëren op basis van een Alfapass identiteit.

(i) Dit omvat Alfapass API's zoals
   a. the Alfapass Validation Service,
   b. the MyAlfapass API,
   c. the Alfapass Customer Group Verification API.

(ii) Het gebruik van Alfapass authentication tokens, zoals
- Gebruik van Alfapass Smartcard op verschillende manieren
- Gebruik van MyAlfapass

(iii) the Alfapass Customer Group Verification Service in combinatie met de Alfapass Customer Group Verification API.

Om de Alfapass Services te kunnen gebruiken heeft CPu specifieke API's ontwikkeld.

De Alfapass Services zijn geen onderdeel van de Uitgebreide CPu oplossing, enkel de integratie met de Alfapass Services.

Specifieke voorwaarden zijn van toepassing op de Alfapass Services zoals door Alfapass opgesteld. Ter informatie is een link opgenomen naar deze voorwaarden: link

3. FUNCTIONALITEIT

3.1 BASISFUNCTIONALITEIT CPU

De scheepsagent creëert een commercial release in CPU.

De scheepsagent transfereert een commercial release naar een volgende partij. Deze partij zal het commercial release recht accepteren of weigeren en vervolgens doorzetten naar de volgende partij. Zo gaat het commercial release recht van de ene naar de andere partij tot deze is aangekomen bij de Transportorganisator en er een Pickuprecht gecreëerd wordt. CPu zal vervolgens een Finaal Pickuprecht creëren zodat een container van terminal kan afgehaald of gestripped worden op terminal.

De scheepsagent kan op elk moment het Releaserecht "updaten" en "revoken".

Een scheepsagent kan een Releaserecht "deleten" indien de scheepsagent houder is van dit recht.

Belanghebbenden kunnen via notifications van bepaalde gebeurtenissen geïnformeerd worden.

Een terminal moet CPU bevragen voor afhaling per truck op het moment dat een container wordt afgehaald en CPU zal terugkoppelen of de Transporteur effectief het Finaal pickuprecht bezit en de container aldus mag afhalen. Het Finaal pickuprecht en de Status zal door CPu aan de terminal geretourneerd worden als notificatie op een asynchrone API voor afhaling per truck (zie link OBJ) of als response op een synchrone API (voor truck zie link OBJ).

Een terminal moet CPU bevragen voor afhaling per rail of barge op het moment dat een container de Tweede Barge and Rail Cut Off (2BRCO) bereikt en CPu zal terugkoppelen of de Planner effectief het Finaal pickuprecht bezit en de container aldus mag afhalen. Het Finaal pickuprecht en de Status zal door CPu aan de terminal geretourneerd worden als response op een synchrone API (zie link).

3.2 Additionele functionaliteit van CPU

3.2.1 *Introductie van douane licht*

De CPU oplossing is uitgebreid met volgende logica om de Douane Vrijgave te faciliteren.

- Verwerking van CCRM berichten om te bepalen of een container de terminal mag verlaten vanuit douane standpunt.
- Inclusie van douane status bij opvragen van de Status.
- Verwerking van additionele douane berichten om controles en de (gedeeltelijke) afschrijving van vrachtlijsten te visualiseren
- Specifieke logica voor identificatie van port equalisatie en het triggeren van een oranje douane licht.
- Verwerking van CUSCAR berichten voor betere koppeling douane berichten

3.2.2 *Preprocessing APIs*

Een beperkt aantal EDIFACT berichttypes zullen tijdelijk ondersteund worden voor aanlevering van de Gegevens.

Stopzetting van deze ondersteuning zal met Community Vertegenwoordiging bersproken worden.

De lijst van ondersteunde EDIFACT types is opgenomen op de NxtPort Website. Validatie van berichten is vereist in UAT omgeving om van support te kunnen genieten buiten kantooruren. Hiertoe dient de procedure zoals op de website beschreven staat, gevolgd te worden.

Ondersteuning van volgende type EDI berichten kan aangevraagd worden en kan eventueel door NxtPort overwogen worden mits het eventueel in rekening brengen van de specifieke kosten:

- COREOR
- CODECO (original ‘0’ and delete ’9’ are supported as codes)
- COARRI

Het gebruik van Preprocessing APIs ontheft de partijen niet om alle Verplichte Gegevens aan te leveren. Ontbrekende gegevens kunnen mogelijkerwijs ook via de GUI aangeleverd worden.

3.2.3 *TPA specifieke APIs*

Ten behoeve van TPAs kunnen specieke APIs ter beschikking gesteld worden en deze kunnen op aanvraag ter beschikking gesteld worden. De specifieke kosten kunnen in rekening gebracht worden indien dit wordt beslist door de Community vertegenwoordigingCommunity vertegenwoordiging.

4. STATUSINFORMATIE

De Status van de CPu Oplossing wordt bijgehouden in volgende lichten:

- Commercial Release
- Terminal Ready
- Pickup Light
- Terminal Operation
- Gate Operation

Volgende lichten maken deel uit van de Uitgebreide CPu Oplossing:

- Customs
- Customs Progress

5. DOCUMENTATIE

5.1 Proces documentatie

- Link naar CPU website: link

5.2 Technische documentatie

5.2.1 *Terminals*

- Algemene informatie mbt APIs: link
- Specifieke informatie mbt APIs: link. Dit bevat onder meer:
    - Lossingsbericht
    - Terminal vrijgave
    - Gate-out bericht.

- Specifieke informatie mbt Notificaties: link

- Best practises: zie link

5.2.2 *Sheepsagent*

- Algemene informatie mbt APIs : link
- Specifieke informatie mbt APIs: link. Dit bevat onder meer:
    - Commerciële vrijgave: zie link
- Specifieke informatie mbt Notificaties: link
- Best practises: link

5.2.3 *Release Parties*

- Algemene informatie mbt APIs : link
- Specifieke informatie mbt APIs: link. Dit bevat onder meer:
    - Transfer Release Right bericht : zie link
- Specifieke informatie mbt Notificaties: link
- Best practises: zie link

5.2.4 *Transport operators*

- Algemene informatie mbt APIs : link
- Specifieke informatie mbt APIs: link. Dit bevat onder meer:
    - Generate Pick-up Right: zie link
- Specifieke informatie mbt Notificaties: link
- Best practises: zie link

5.3 TPA

De getekende TPA's of Third Party Agreements maken integraal deel uit van de Documentatie. Deze zijn gekend tussen NxtPort en Aanbieder(s) van een Derde Applicatie en kunnen door Gebruiker opgevraagd worden. Dit kan niet door NxtPort geweigerd worden zonder gegronde redenen.

Annex 2 : SLA

1. Inleiding

Deze Service Level Agreement (hierna de "**SLA**") is een bijlage bij de Certified Pick Up Voorwaarden en beschrijft het niveau van opgelegde taak dat de Gebruiker van NxtPort in het kader van de Certified Pick Up Oplossing zal verkrijgen.

De SLA kan, overeenkomstig art. 15.2 aangepast worden door NxtPort om de Service Levels aan te passen aan de CPu Oplossing die op dat ogenblik wordt aangeboden.

2. Definities

De in deze SLA gebruikte termen met een hoofdletter hebben de betekenis zoals hierin beschreven. Termen met een hoofdletter die niet in deze sectie worden gedefinieerd hebben de respectieve betekenissen die in de CPu Voorwaarden worden toegekend.

Beschikbaarheid	betekent een percentage van de totale tijd, berekend zoals beschreven in art. 5 van deze Annex 2, wanneer de CPU Oplossing beschikbaar is voor een bepaalde Gebruiker
Beschikbaarheidsniveau	betekent de streefniveaus van Beschikbaarheid zoals bepaald in deze SLA.
Downtime	betekent de tijd dat de Gebruiker de CPu Oplossing niet kan gebruiken omwille van P1 en P2 incidenten. Downtime begint wanneer de onbeschikbaarheid zich voordoet en eindigt wanneer de Beschikbaarheid van de CPu Oplossing is hersteld of een alternatieve (tijdelijke) oplossing en/of alternatieve werkwijze wordt aangeboden en is exclusief Gepland Onderhoud en Geplande hotfixes
Gepland Onderhoud	Betekent gepland onderhoud zoals beschreven in art. 5.3. van deze Annex2
Hersteltijd	Betekent de verstreken tijd tussen (i) de ontvangst van de melding van het Incident, in overeenstemming met deze SLA of het ontdekken van een Incident door NxtPort en (ii) de oplossing van het Incident en/of alternatieve werkwijze wordt

	aangeboden waarbij de klok wordt stilgezet als er een vervolgactie is bij de Gebruiker
Incident management	Betekent het antwoord op, het behandelen en het escaleren van een Incident zoals beschreven in art. 6.
Incident	Betekent een ongeplande onderbreking van de CPu Oplossing waarbij de CPu Oplossing niet, slecht of gedeeltelijk werkt of functioneert en dit ten aanzien van één Gebruiker, een beperkte set Gebruikers of alle Gebruikers.
Reactietijd	Betekent de verstreken tijd tussen ontvangst van een melding van een Incident of de vaststelling door Nxtport van een Incident, in overeenstemming met deze SLA, en ontvangstbevestiging of melding van een Incident uitgestuurd door NxtPort.
Service Levels	Betekent de gegarandeerde niveaus van opgelegde taak zoals beschreven in deze SLA.
Service Level Default	Betekent een situatie waarbij NxtPort er niet in slaagt een Service Level te halen of overschrijden zoals uiteengezet in art. 5 of 6.van deze Annex 2
Werkdagen	Een dag waarop de banken in Brussel, België, open zijn.

3. Doel

Deze SLA beschrijft de gegarandeerde opgelegde taak door NxtPort met betrekking tot de CPu Oplossing door middel van:

- Gegarandeerde Beschikbaarheidsniveaus (art. 5);
- Incident management waarbij Herstel en Reactietijden nagestreefd worden (art. 6);

4. Duurtijd

Deze SLA vormt een intrinsiek deel van de CPu Voorwaarden en heeft dezelfde duurtijd.

5. Beschikbaarheid

5.1. Beschikbaarheidsniveau

NxtPort zal zich er zich toe inspannen de CPu Oplossing te allen tijde probleemloos beschikbaar te stellen. Indien een Incident de Beschikbaarheid substantieel vermindert, streeft NxtPort ernaar dit Incident binnen de in de SLA opgenomen termijnen op te lossen.

NxtPort verbindt er zich toe dat er een Beschikbaarheid van de CPu Oplossing van 99,9% per maand, waarbij de Beschikbaarheid wordt berekend als volgt:$(1 - \frac{aantal\ minuten\ Downtime}{totaal\ aantal\ minuten\ per\ maand}) \times 100\ \%$

5.2. Meting

De Beschikbaarheid wordt gemeten door gebruik te maken van de geautomatiseerde systemen van NxtPort, gedurende elke kalendermaand. Het wordt tot op de minuut nauwkeurig berekend, op basis van het aantal minuten in de betreffende maand. Maandelijks kan dit gedeeld worden met Community Vertegenwoordiger.

5.3. Gepland Onderhoud

Bij het onderhoud en de ontwikkeling van de CPu Oplossing kan het voorkomen dat NxtPort de CPu Oplossing tijdelijk offline moet halen om onderhoudsdiensten te leveren. Periodiek onderhoud wordt ingepland na overleg met Community Vertegenwoordiging.

NxtPort streeft ernaar om Downtime ten gevolge van Gepland Onderhoud te beperken tot acht (8) uur per kalendermaand met een maximum van zes (6) uur per onderhoudsinterventie en per weekend tijdens een zaterdag of zondag, en zal de Gebruikers ten minste één (1) week voorafgaand aan het Gepland Onderhoud op de hoogte te stellen van het Geplande Onderhoud indien onderhoudsinterventie langer dan negentig (90) minuten is gepland.

5.4 Geplande Hotfixes

2x per maand van max 1uur downtime buiten kantooruren waarbij deze op voorhand zullen aangekondigd worden na overleg met Community Vertegenwoordiging

6. Incident management

6.1. Melding Incident

Incidenten dienen door de Gebruikers gemeld te worden aan NxtPort door gebruik te maken via volgende kanaal:

- Webform: https://nxtport.atlassian.net/servicedesk/customer/portal/9
- Voor terminals: telefoon nr voor P1 incidenten

Indien Incidenten op een andere wijze aan NxtPort worden gemeld kan een correcte afhandeling niet worden gegarandeerd. De Gebruiker verbindt er zich toe naar best vermogen alle relevante informatie aan NxtPort te verschaffen die kan helpen bij het verhelpen van een Incident alsook het tijdig verschaffen van alle gevraagde additionele informatie, bijvoorbeeld reproductie op de acceptatieomgeving indien vereist. Bij gebreke van juiste of volledige info zal een stop de klok mechanisme toegepast worden om de Hersteltijd te meten.

6.2. Reactie- en hersteltijden

Incidenten worden bij melding/vaststellen door NxtPort onderverdeeld in verschillende prioriteitsniveaus als volgt:

Prioriteit	Voorwaarden	Reactietijd	Hersteltijd
P1 **Fatal**	Volgende voorwaarden zijn vervuld: 1. Kritische bedrijfsprocessen van de CPU Oplossing zijn niet beschikbaar 2. Alle of de meeste Gebruikers (binnen één bepaalde groep van Gebruikers (bijv. Terminaloperators)) zijn geïmpacteerd **3.** Geen Workaround of fallback mogelijk	**NxtPort: <15 min** **(Uitgebreide Kantooruren)**	**NxtPort: <2 uur** **(Uitgebreide Kantooruren)**

P2 Severe	Volgende voorwaarden zijn vervuld: 1) Kritische of belangrijke bedrijfsprocessen van de CPU Oplossing worden negatief geimpacteerd zijnde - Kritische bedrijfsprocessen van de CPU Oplossing zijn onbeschikbaar voor een beperkt aantal Gebruikers binnen één bepaalde groep van Gebruikers of - Belangrijke bedrijfsprocessen van de CPU Oplossing zijn onbeschikbaar voor een beperkt aantal Gebruikers binnen één bepaalde groep van Gebruikers 2) Geen Workarounds of fallback mogelijk	**NxtPort: <30 min (Uitgebreide Kantooruren)**	**NxtPort: <4 uur (tijdens Kantooruren)** **NxtPort: <6 uur (tijdens Uitgebreide Kantooruren)**
P3 Medium	1 van volgende voorwaarden zijn vervuld: 1) Kritische of belangrijke bedrijfsprocessen van de CPU Oplossing worden negatief geimpacteerd of zijn onbeschikbaar 2) Kritische of belangrijke bedrijfsprocessen van de Uitgebreide CPU Oplossing worden negatief geimpacteerd of zijn onbeschikbaar 3) Datakwaliteit gerelateerde issues	**NxtPort: < 2 uur (tijdens Kantooruren)**	**NxtPort: best effort bij hoogdringendheid of opgenomen in release kalender**
P4 Minor	Minder belangrijke functionaliteiten: - *Kleine degradatie van functionaliteiten of prestaties* - *Beperkt aantal betrokken Gebruikers*	**NxtPort: <1 week**	**NxtPort: wordt opgenomen in release kalender**
PX	Klantspecifieke functionaliteiten die enkel ter beschikking gesteld worden aan individuele of	**NxtPort: best effort tijdens Kantooruren**	**NxtPort: best effort (individuele**

	beperkt aantal Gebruikers binnen een groep van Gebruikers (bv terminal operators)	**(individuele overeenkomsten kunnen opgesteld worden)**	**overeenkomsten kunnen opgesteld worden)**

Bovenstaande reactietijden en hersteltijden kunnen bijgesteld worden na overleg met de Community Vertegenwoordiger.

6.3. Meting van de Reactie- en Hersteltijden

Reactietijden worden gemeten vanaf het moment dat de Gebruiker een Incident meldt tot het moment dat NxtPort op deze melding reageert.

Het is van vitaal belang dat de Gebruiker elk Incident meldt zoals uiteengezet in art. 6.1. Als een Incident niet op de juiste manier wordt ingediend via de online service desk, is de Reactie- en Hersteltijd niet van toepassing op dat Incident.

6.4. Kantooruren – Uitgebreide Kantooruren

Incidentmanagement wordt door NxtPort als volgt aangeboden:

1. Kantooruren
    - Maandag tem vrijdag 09u tot 17u
2. Uitgebreide Kantooruren: Kantooruren uitgebreid met:
    - Maandag tem vrijdag 06u tot 09u / 17u tot 22u
    - Zaterdag 8 tem 12u

Incident management zal enkel gebruikt worden voor het indienen van incidenten.

Deze dekking wordt aangeboden voor de CPu Oplossing en waarbij de tijden na overleg met de Community Vertegenwoordiger kunnen aangepast worden.

6.5. Proactieve support

De status van de CPu Oplossing wordt gemonitord en worden intern gemeld aan het NxtPort supportteam. Zo worden onder meer sterke schommelingen in ingestion van Gegevens of gebruik door de Gebruikers opgemerkt, gemeld en geëscaleerd.

Incidenten die door NxtPort zelf worden vastgesteld (en dus niet ingevolge een melding van een gebruiker overeenkomstig art. 6.1), zullen door NxtPort hersteld worden binnen de hersteltijden zoals uiteengezet in art. 6.2. en gedeeld worden met de Community Vertegenwoordiger.

6.6. Cyber Incident management

Indien Nxtport kennis krijgt van of een vermoeden heeft van (i) een "**Cyber Incident**" (actie ondernomen door het gebruik van computernetwerken die resulteren in een feitelijk of potentieel nadelig effect op het informatiesysteem van Nxtport en / of van de Gebruiker(s) en / of op de Gegevens) ; of van (ii) elke andere ongeoorloofde toegang tot de CPu Oplossing of elk gebruik, misbruik, beschadiging of vernietiging van Gegevens door een derde partij ("**Ander Incident**"), zal Nxtport :

(i) de geïmpacteerde Gebruiker(s) onmiddellijk schriftelijk op de hoogte stellen (en niet langer dan 36 uur nadat ze kennis hebben genomen van het Cyberincident of Ander Incident);
(ii) alle richtlijnen naleven die door de sector als redelijk worden beschouwd inclusief met betrekking tot:
  - het verkrijgen van bewijsmateriaal over hoe, wanneer en door wie het informatiesysteem van de Gebruiker en / of de Gegevens zijn of kunnen zijn gecompromitteerd, en dit op verzoek van de Gebruiker aan hem verstrekken en dat bewijs bewaren en beschermen voor een periode van 12 maanden;

(iii) zo snel mogelijk de audittrail en eventlogging aanleveren om aan de kant van de Gebruiker incident response te kunnen doen;
(iv) zo snel mogelijk mitigatiestrategieën implementeren om de impact van het Cyberincident of Ander Incident of de waarschijnlijkheid of impact van een toekomstig vergelijkbaar incident te verminderen; en
(v) de Gegevens bewaren en beschermen (inclusief, indien nodig, terugkeren naar een back-up of alternatieve site of andere actie ondernemen om Gegevens te herstellen).

NxtPort houdt zich het recht voor om pro-actief of reactief de Beschikbaarheid van de CPu Oplossing te verminderen omwille van security redenen waarbij deze onbeschikbaarheid niet zal meegeteld worden in de formule van Beschikbaarheidsniveau.

6.7. Opvolging - audit

Maandelijks wordt er een meeting opgezet met de Community vertegenwoordiger om volgende topics te bespreken:

- Algemeen overzicht van Incidenten
- Nadere toelichting van P1 en P2 Incidenten
- Bespreking Reactie en Hersteltijden
- Root cause analyses
- Beschikbaarheidsniveau (incl onbeschikbaarheid omwille van security redenen)
- Mitigerende acties

Na een melding van een Incident door een Gebruiker, zal NxtPort op eenvoudig verzoek van de Gebruiker een eventlogging aanleveren om aan de kant van de Gebruiker Incident response te kunnen doen. Op verzoek van de betrokken Gebruikers zal een opvolgingsgesprek worden ingepland.

7. Toepassing en uitsluitingen

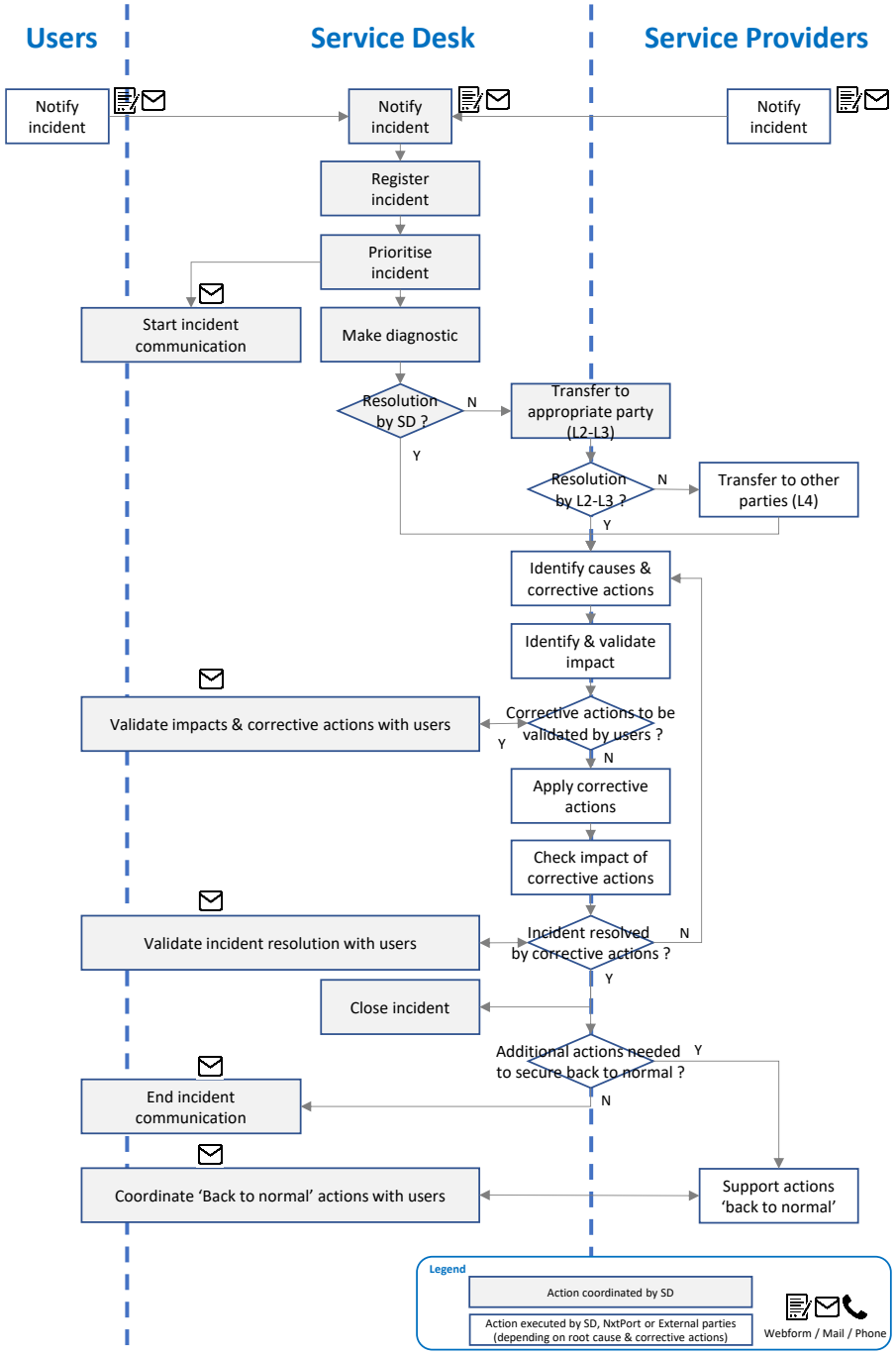
Deze SLA is van toepassing op de CPu Oplossing. Deze SLA is niet van toepassing op software, hardware of diensten die niet worden aangeboden door en/of worden beheerd door NxtPort of een van haar onderaannemers, met inbegrip van, maar niet beperkt tot, Incidenten die het gevolg zijn van onvoldoende bandbreedte bij de Gebruiker of die verband houden met software of diensten van derden (met inbegrip van de Derde Applicatie) die niet zijn aangeschaft via en/of worden beheerd door NxtPort of een van haar onderaannemers.

Add-on componenten van de Uitgebreide CPu Oplossing kunnen onder de SLA van de CPu oplossing opgenomen worden als er een betrouwbare connectie is met de CPu Oplossing en als de integratie van de actuele versie van de achterliggende integratie component (bv Derde Applicatie) met de actuele majeure versie van de CPu Oplossing is getest door aanbieder van de achterliggende integratie component, inclusief testverslag, in samenspraak met NxtPort en de Community Vertegenwoordiger.

Bovendien is deze SLA niet van toepassing:

- in het geval dat een Incident wordt veroorzaakt door het gebruik van apparatuur, software of service(s) op een manier die niet wordt ondersteund of niet in overeenstemming is met de Documentatie
- op Incidenten die het gevolg zijn van het gebruik van CPu Oplossing op een manier die niet in overeenstemming is met de Documentatie (bijvoorbeeld pogingen om handelingen uit te voeren die niet worden ondersteund);
- in gevallen van een security incident veroorzaakt zonder nalatigheid van NxtPort;
- in gevallen van Force Majeure.

Annex 2.A : Incident Management


Users
Service Desk
Service Providers
Notify incident
Notify incident
Notify incident
Register incident
Prioritise incident
Start incident communication
Make diagnostic
Resolution by SD ?
N
Y
Transfer to appropriate party (L2-L3)
Resolution by L2-L3 ?
N
Y
Transfer to other parties (L4)
Identify causes & corrective actions
Identify & validate impact
Validate impacts & corrective actions with users
Corrective actions to be validated by users ?
Y
N
Apply corrective actions
Check impact of corrective actions
Validate incident resolution with users
Incident resolved by corrective actions ?
N
Y
Close incident
Additional actions needed to secure back to normal ?
Y
N
End incident communication
Coordinate 'Back to normal' actions with users
Support actions 'back to normal'
Legend
Action coordinated by SD
Action executed by SD, NxtPort or External parties (depending on root cause & corrective actions)
Webform / Mail / Phone

Annex 3 : Noodprocedures en uitsluitingen

1. Inleiding

Deze annex 3 is een bijlage bij de Certified Pick Up Voorwaarden en beschrijft (i) de (i) wijze waarop een Container bij gebrek aan de CPu Dienst via de noodprocedures rechtmatig kan afgeleverd worden alsook de en (ii) uitsluitingen op de verplichting tot het gebruiken van de CPu Dienst voor de aflevering van Containers.

Onder een noodprocedure verstaan we de handelingen die door NxtPort en de Gebruiker(s) zullen dienen gesteld te worden (en dit bijkomend aan de mitigerende maatregelen beschreven in Annex 2) (de "**Noodprocedures**"):

a) volledige onbeschikbaarheid van de CPu Oplossing
b) specifieke connecties met Gebruikers zijn uitzonderlijk onbeschikbaar
c) bij instructie van overheidswege
d) indien een Gebruiker in de onmogelijkheid verkeert om alle Verplichte Gegevens ten aanzien van een specifieke Container aan te leveren

Onder uitsluitingen worden de procedures begrepen die dienen worden te volgen in het geval een Container uitgesloten is van de verplichting tot Certified Pick up, maar wel reeds aangemeld is in de CPu Oplossing:

a) Transhipment Containers die om redenen van scanning /fysieke verificatie/keuring de Terminal dienen te verlaten
b) Exportcontainers die terug dienen afgehaald te worden

2. Noodprocedures

Indien de CPu oplossing niet beschikbaar is, kan NxtPort Terminaloperator toelaten om een bepaald Fallback mechanisme te activeren.

Volgende Fallback mechanismes zijn momenteel onderkend en aanvaard:

1) Terminaloperator gebruikt de AlfaPass of naam van Planner die door CPu gedeeld werd met Terminaloperator bij creatie van PickUpRecht
2) SCR als Derde Applicatie
3) Terminaloperator specifieke portal

Annex 4: IT Security Policy

Bijlage 5 : IT-beveiligingsbeleid

1.1 Managementrichtlijnen voor informatiebeveiliging

- NxtPort heeft een passend informatiebeveiligingsbeleid geïmplementeerd en is ISO 27001 gecertificeerd. Het management van NxtPort vereist van werknemers en externe consultatns met toegang tot Gegevens dat zij gebonden zijn door schriftelijke, vertrouwelijkheids- en privacyverantwoordelijkheden met betrekking tot die Gegevens. Deze verantwoordelijkheden blijven van kracht na beëindiging of verandering van dienstverband of aanstelling.

1.2 Personeel

- NxtPort verschaft informatie en opleiding (*awareness)* over informatiebeveiliging aan werknemers en relevante externe consultants.
- Medewerkers zijn verplicht zich te houden aan de policies en regelgeving op het gebied van informatiebeveiliging, Persoonsgegevensbescherming en omgang met Gegevens.

1.3 Toegangscontrole

Beheer van gebruikerstoegang

- NxtPort implementeert beleid voor toegangscontrole ter ondersteuning van het aanmaken, wijzigen en verwijderen van gebruikersaccounts voor systemen of applicaties die toegang hebben of geven tot Gegevens.
- NxtPort implementeert een *user account and access provisioning* proces om toegangsrechten tot systemen en applicaties toe te wijzen en in te trekken.
- Het gebruik van "generieke" of "gedeelde" accounts is verboden zonder systeemcontroles die zijn ingeschakeld om specifieke gebruikerstoegang te traceren en gedeelde wachtwoorden te voorkomen.
- Verplichte sterke authenticatie (tweefactorauthenticatie) voor de admin accounts wordt geïmplementeerd.
- NxtPort controleert en beperkt de toegang tot hulpprogramma's die in staat zijn om systeem- of toepassingsbeveiligingscontroles te omzeilen.
- Gebruikerstoegang tot systemen en applicaties die Gegevens opslaan of toegankelijk maken, wordt gecontroleerd door een veilige aanmeldingsprocedure.

Beheer van fysieke toegang - Beveiliging van faciliteiten

- De fysieke toegang tot faciliteiten waar Gegevens wordt opgeslagen of verwerkt, wordt beschermd in overeenstemming met *good industry practices* (Tier 4-datacenters).
- er zijn beleidsregels en procedures vastgesteld voor de handhaving van een veilige en beveiligde werkomgeving in kantoren, ruimten, faciliteiten en beveiligde zones
- er worden fysieke veiligheidsperimeters (omheiningen, muren, barrières, bewakers, poorten, elektronische bewaking, fysieke authenticatiemechanismen, receptiebalies en veiligheidspatrouilles) geïmplementeerd
- er wordt een volledige inventaris bijgehouden van alle kritische activa
- tweefactorauthenticatie voor toegang tot het datacenter is verplicht
- Er is brandbeveiliging aanwezig: brandalarmsysteem, systeem voor vroegtijdige branddetectie, geschikte brandblussers, regelmatige brandoefeningen.
- De infrastructuur is robuust en biedt voldoende weerstand tegen beschadiging door de elementen en tegen toegang door onbevoegden
- Redundante datacenters die ten minste zo ver van elkaar verwijderd zijn dat een beheersbare schadegebeurtenis niet tegelijkertijd het oorspronkelijk gebruikte datacenter en het datacenter met de backupcapaciteit treft

1.4 Beveiliging van communicatie

Beveiliging van netwerken en servers

- NxtPort scheidt Gebruikergegevens logisch binnen een gedeelde omgeving.
- NxtPort beveiligt netwerksegmenten van externe toegangspunten waar Gebruikergegevens toegankelijk zijn.
- Externe netwerk perimeters zijn beveiligd en geconfigureerd om ongeautoriseerd verkeer te voorkomen.
- Inkomende en uitgaande punten worden beschermd door firewalls en intrusion detection systems (IDS).
- Poorten en protocollen worden beperkt tot die met een specifiek doel.

- NxtPort synchroniseert systeemklokken op netwerkservers met een universele tijdbron (bijv. UTC) of netwerktijdprotocol (NTP).
- Anti-spam systemen zijn geïmplementeerd
- 0-Day Malware bescherming is beschikbaar
- Er zijn beveiligingsmaatregelen ter voorkoming van *netwerk base attachks* aanwezig
- IDP / IDS-systemen zijn geïmplementeerd
- Bescherming tegen DDoS is geïmplementeerd
- Netwerksegmentatie is geïmplementeerd.
- Rechtstreekse toegang vanaf Internet is beperkt tot een afgescheiden DMZ.
- De verantwoordelijkheid voor de noodzakelijke DMZ-infrastructuur is duidelijk gedefinieerd
- Netwerkzones zijn gescheiden met een firewall die alleen het noodzakelijke netwerkverkeer toelaat
- Er zijn Firewalls op applicatieniveau aanwezig
- Beheer op afstand gebeurt op een veilige manier
- Beheer op afstand vindt plaats via een beveiligd communicatiekanaal (bijv. SSH, TLS/SSL, IPSec, VPN)
- Inloggen op afstand gebeurt met sterke authenticatie
- Netwerkredundantie is geïmplementeerd

Cryptografische maatregelen
- Gegevens, met inbegrip van persoonlijksgegevens, worden in rust versleuteld (*encrypted at rest*).

Cloud maatregelen
- NxtPort versleutelt Gegevens tijdens transmissie tussen elke applicatielaag en tussen interfacing applicaties.

1.5 Applicatie- en Gegevensbeveiliging

Beveiliging van applicaties
- NxtPort scheidt Gebruikergegevens logisch binnen een gedeelde serviceomgeving.
- NxtPort beveiligt netwerksegmenten van externe toegangspunten waar Gebruikergegevens toegankelijk zijn.

1.6 Operationele beveiliging

Servicebeheer
- NxtPort heeft formele SOPs geïmplementeerd voor systeemprocessen die van invloed zijn op Gebruikergegevens. Notificaties kunnen plaatsvinden door middel van generieke change logs. Procedures moeten auteur, revisiedatum en versienummer bijhouden, en moeten worden goedgekeurd door het management.
- NxtPort monitort de beschikbaarheid van de service.

Beheer van vulnerabilities
- NxtPort voert jaarlijks penetratietesten uit voor systemen en applicaties die Gebruikergegevens opslaan of toegang verlenen tot Gebruikergegevens, inclusief Persoonsgegevens. Geïdentificeerde problemen dienen binnen een redelijke termijn te worden verholpen.
- NxtPort heeft een patch- en kwetsbaarheidsbeheerproces geïmplementeerd om kwetsbaarheden te identificeren, te rapporteren en te verhelpen door:
    a) Patches of fixes van leveranciers te implementeren.
    b) Een herstelplan te ontwikkelen voor kritieke kwetsbaarheden.
- NxtPort heeft maatregelen geïmplementeerd om malware, kwaadaardige code en ongeautoriseerde uitvoering van code te detecteren en te voorkomen. Controlemaatregelen moeten regelmatig worden bijgewerkt met de nieuwste beschikbare technologie (bijv. het implementeren van de nieuwste *signatures* en definities).

Logging en monitoring
- NxtPort genereert beheerders- en eventlogs voor systemen en applicaties die Gebruikergegevens opslaan of toegang tot Gebruikergegevens toestaan.
- NxtPort controleert systeemlogs periodiek om systeemstoringen, fouten of potentiële beveiligingsincidenten te identificeren die van invloed zijn op Gebruikergegevens.

1.7 Beheer van leveranciers

- NxtPort heeft contractuele overeenkomsten met derden die omgaan met Gebruikerinformatie en deze overeenkomsten bevatten passende informatiebeveiligings-, vertrouwelijkheids- en gegevensbeschermingsvereisten, zoals gedetailleerd in de Overeenkomst. Overeenkomsten met dergelijke partijen worden periodiek herzien om te valideren dat de vereisten voor informatiebeveiliging en gegevensbescherming passend blijven.
- NxtPort beoordeelt periodiek de informatiebeveiligingspolicies van haar leveranciers en valideert dat deze maatregelen passend blijven volgens de risico's die de behandeling van Gebruikerinformatie door de leverancier vertegenwoordigt, rekening houdend met eventuele *state-of-the-art* technologie en de kosten van implementatie.
- NxtPort beperkt toegang van derde partijen tot Gebruikergegevens, inclusief Persoonsgegevens, tot hetgeen vereist voor de dienstverlening van de leverancier.
- Op verzoek van de Gebuiker verstrekt NxtPort de Gebruiker een lijst van derden met de vereiste toegang tot Gegevens, waaronder Persoonsgegevens.
- NxtPort staat toegang tot Gebruikergevens, inclusief Persoonsgegevens, alleen toe voor zover noodzakelijk voor het uitvoeren van de diensten die de derde contractueel is overeengekomen te leveren.
- NxtPort voorziet in exit-bepalingen met vastgelegde bestandsformaten en retentie van alle logische relaties.
- Cloud service providers stellen NxtPort regelmatig op de hoogte van beveiligingsmaatregelen, wijzigingen in het IT-beveiligingsbeheersysteem, beveiligingsincidenten, de resultaten van *Information security*-beoordelingen en penetratietests.
- De continuïteit van de dienstverlening wordt bewaakt met upstream providers in het geval van uitval van de provider.

1.8 Resilience

- NxtPort voert risicobeoordelingsactiviteiten voor bedrijfscontinuïteit uit om relevante risico's, bedreigingen, impacts, waarschijnlijkheid en vereiste controles en procedures te bepalen. Herstel wordt uitgevoerd op aanvaardbare niveaus gebaseerd op door NxtPort vastgestelde criteria in overeenstemming met redelijke termijnen.
- Op basis van de resultaten van de risicobeoordeling documenteert, implementeert, test en beoordeelt NxtPort jaarlijks haar Business Continuity and Disaster Recovery (BC/DR) plannen om het vermogen te valideren om de beschikbaarheid van en toegang tot Gebruikergegevens tijdig te herstellen, in het geval van een fysiek of technisch incident dat resulteert in verlies of corruptie van Gebruikergegevens.
- De Gebruiker is in staat om, op verzoek, meetbare parameters te monitoren zoals overeengekomen in de SLA.

1.9 Transparantie

- De locaties van NxtPort (land, regio) waar de Gebruikergegevens zullen worden opgeslagen en verwerkt, worden bekendgemaakt en bevinden zich enkel binnen de EER.
- De onderaannemers van NxtPort die van vitaal belang zijn voor het leveren van de clouddiensten worden openbaar gemaakt. Transparantie over welke interventies NxtPort of derde partijen zijn toegestaan in de gegevens en processen van de Gebruiker wordt gegeven
- Op regelmatige basis wordt informatie over wijzigingen verstrekt (bijv. nieuwe of beëindigde functies, nieuwe onderaannemers, andere SLA gerelateerde zaken)
- Transparantie wordt verschaft over welke software NxtPort zal installeren op de systemen en de beveiligingseisen / risico's die hieruit kunnen voortvloeien voor een Gebruiker.
- Transparantie over overheidsinterventie of inzagerechten, over eventuele wettelijk definieerbare rechten van derden om gegevens in te zien en over eventuele verplichtingen die NxtPort heeft om opgeslagen gegevens op een mogelijke locatie te controleren wordt verstrekt.

1.10 Audit en Naleving

- NxtPort beoordeelt periodiek of haar systemen en apparatuur die Gebruikergegevens opslaan of toegang geven tot Gebruikergegevens, inclusief Persoonsgegevens, voldoen aan de wettelijke en regelgevende vereisten en contractuele verplichtingen die aan de Gebruiker verschuldigd zijn.
- NxtPort onderhoudt actuele onafhankelijke verificatie van de effectiviteit van haar technische en organisatorische beveiligingsmaatregelen (bijv. ISO-certificering). De onafhankelijke informatiebeveiligingsbeoordeling wordt ten minste jaarlijks uitgevoerd.
- NxtPort voert regelmatig (en dit minstens éénmaal per jaar) onafhankelijke security audits uit.

Annex 5 : Verwerking Persoonsgegevens

1 Verantwoordelijke voor de verwerking

De verantwoordelijke voor deze verwerking is NxtPort BV, geregistreerd onder ondernemingsnummer (RPR Antwerpen) 0429.672.881 met maatschappelijke zetel te Sint-Pietersvliet 7, 2000 Antwerpen.

NxtPort zal als verantwoordelijke voor de verwerking alle passende technische en organisatorische maatregelen nemen ter bescherming van Persoonsgegevens tegen toevallige of ongeoorloofde vernietiging, tegen toevallig verlies en iedere niet toegelaten verwerking van Persoonsgegevens.

NxtPort zal er verder op toezien dat Persoonsgegevens verwerkt worden op een rechtmatige, behoorlijke en transparante wijze; dat Persoonsgegevens verzameld worden voor welbepaalde, uitdrukkelijk omschreven en gerechtvaardigde doeleinden en dat deze vervolgens niet verder op een met die doeleinden onverenigbare wijze worden verwerkt; dat de Persoonsgegevens toereikend zijn, ter zake dienend en beperkt tot wat noodzakelijk is voor de genoemde doeleinden; dat de Persoonsgegevens juist zijn en zo nodig worden geactualiseerd; dat Persoonsgegevens niet langer worden bewaard dan nodig voor de genoemde doeleinden.

NxtPort garandeert dat er geen overdracht naar derde landen voor gegevensverwerking of -opslag plaatsvindt zonder de nodige maatregelen te nemen om te voldoen aan de beschermingsvereisten uit de Europese privacyregelgeving.

2 De betrokkenen

De betrokkenen zijn natuurlijke personen waarvan de gegevens verwerkt wordt in het kader van de afhandeling van Containers door Certified Pick up.

3 De Persoonsgegevens die worden verwerkt

NxtPort verzamelt en verwerkt volgende Gegevens:

Contactgegevens van Gebruikers en aangestelden van Gebrukers (naam, emailadres, telefoonnummer).

4 Bron van de Persoonsgegevens

De Persoonsgegevens worden aangeleverd door een Gebruiker.

5 Doeleinden voor gegevensverwerking

De Persoonsgegevens zullen louter verwerkt worden voor de opgelegde CPu Dienst zoals verder ook beschreven in de Cpu Voorwaarden, met onder andere volgende doelstellingen:

- De afhaling van Containers;
- Het beveiligen van de haven en de afhandeling van Containers

De Persoonsgegevens zullen in het kader van deze verwerking doorgegeven worden aan derden binnen de EU, namelijk aan de instanties waaraan NxtPort wettelijk verplicht is bepaalde informatie mede te delen, zoals de (Scheepvaart)politie, verschillende Federale Overheidsdiensten. Tevens zullen bepaalde Persoonsgegevens worden doorgegeven aan externe bedrijven die zorgen voor de technische ondersteuning van bepaalde applicaties. NxtPort maakt met elke derde aan wie de Persoonsgegevens doorgegeven worden de nodige afspraken en sluit met deze derden, indien nodig, een verwerkersovereenkomst. NxtPort kiest enkel verwerkers die de nodige garanties bieden m.b.t. gegevensverwerking en -bescherming.

6 Rechtgrond voor de verwerking

Voor de verwerking van de Persoonsgegevens baseert NxtPort zich op:

(i) De uitvoering van haar verplichtingen onder de CPu Voorwaarden;
(ii) De uitvoering van de concessieovereenkomst afgesloten met het Havenbedrijf in uitvoering van art. 5.6 "Certified Pick Up" van de Havenpolitieverordening

7 Bewaartermijn

NxtPort zal de Persoonsgegevens bewaren zolang dit nodig is voor het bereiken van de deze verklaring genoemde doeleinden. Daarna zullen de Persoonsgegevens verwijderd worden.

Voor meer informatie: privacy@nxtport.com

8 De rechten van de betrokkene

De betrokkene heeft te allen tijde het recht om vanwege met de specifieke situatie verband houdende redenen bezwaar te maken tegen de verwerking van de betreffende Persoonsgegevens wanneer NxtPort zich baseert op gerechtvaardigde belangen of het algemeen belang/openbaar gezag.De betrokkene dient hierbij de specifieke redenen te beargumenteren. NxtPort zal vervolgens de verwerking staken tenzij zij dwingende gerechtvaardigde gronden voor de verwerking aanvoert die zwaarder wegen dan de belangen, rechten en vrijheden van de betrokkene als de betrokkene of die verband houden met de instelling, uitoefening of onderbouwing van een rechtsvordering.

De betrokkene heeftt het recht om van NxtPort uitsluitsel te verkrijgen over het al dan niet verwerken van de betreffende Persoonsgegevens en, wanneer dat het geval is, om inzage te verkrijgen van die Persoonsgegevens. NxtPort zal bij het beantwoorden van dit verzoek ook de details van de verwerking meegeven. NxtPort zal de betrokkene een kopie verzenden van de Persoonsgegevens die worden verwerkt.

De betrokkene heeft het recht om van de NxtPort onverwijld rectificatie van de betreffende onjuiste Persoonsgegevens te verkrijgen. De betrokkene kan ook onvolledige Persoonsgegevens laten vervolledigen. In sommige gevallen kan de betrokkene zelf de Persoonsgegevens corrigeren of aanvullen, door correctie of aanvulling in de CPu Dienst.

De betrokkene heeft het recht van NxtPort zonder onredelijke vertraging wissing van de betreffende Persoonsgegevens te verkrijgen. NxtPort is verplicht de betreffende Persoonsgegevens te wissen wanneer ze niet langer nodig zijn voor de doeleinden waarvoor zij zijn verzameld of anderszins verwerkt, wanneer er niet langer een rechtsgrond is om de Persoonsgegevens te verwerken, als de betrokkene bezwaar maakt tegen de verwerking en er geen prevalerende dwingende fgerechtvaardigde gronden zijn voor de werking, wanneer de Persoonsgegevens onrechtmatig verwerkt zijn, wanneer de gegevens conform het Unierecht of het lidstatelijke recht gewist dienen te worden of als de Persoonsgegevens zijn verzameld in verband met een aanbod van diensten van de informatiemaatschappij.

Wanneer NxtPort de Persoonsgegevens openbaar gemaakt zou hebben en zij verplicht is de Persoonsgegevens te wissen, neemt zij redelijke maatregelen om andere verwerkingsverantwoordelijken die de Persoonsgegevens verwerken, ervan op de hoogte te stellen

dat de betrokkene de NxtPort hebt verzocht om iedere koppeling naar, of kopie of reproductie van die Persoonsgegevens te wissen.

NxtPort kan bepaalde Persoonsgegevens niet wissen, nl. wanneer de verwerking nodig is voor het nakomen van een wettelijke verplichting of uitoefening van een taak van algemeen belang, om redenen van algemeen belang op het gebied van volksgezondheid, m.o.o. archivering in het algemeen belang, wetenschappelijk of historisch onderzoek of statistische doeleinden of voor de instelling, uitoefening of onderbouwing van een rechtsvordering. De betrokkene zal hiervan na een vraag tot wissing op de hoogte worden gebracht, wanneer dat het geval is.

Wanneer (i) de juistheid van de Persoonsgegevens door een betrokkene wordt betwist, (ii) de verwerking onrechtmatig is en de betrokkene zich verzet tegen wissing van de Persoonsgegevens, (iii) de NxtPort de Persoonsgegevens niet meer nodig heeft voor de verwerkingsdoeleinden maar de betrokkene ze nog nodig hebt voor de instelling, uitoefening of onderbouwing van een rechtsvordering of (iv) de betrokkene bezwaar gemaakt hebt tegen de verwerking, heeft de betrokkene – in afwachting van eventuele gerechtvaardigde gronden die de NxtPort aanvoert of terwijl zij de juistheid van de gegevens nakijkt – het recht om beperking van de verwerking te verkrijgen.

In zo'n geval worden Persoonsgegevens, met uitzondering van de opslag ervan, slechts verwerkt met toestemming van de betrokkene of voor de instelling, uitoefening of onderbouwing van een rechtsvordering of ter bescherming van de rechten van een andere natuurlijke persoon of rechtspersoon of om gewichtige redenen van algemeen belang voor de Europese Unie of voor een lidstaat.

De betrokkene heeft het recht de relevant Persoonsgegevens, die hij of zij zelf aan de NxtPort heeft verstrekt, in een gestructureerde, gangbare en machineleesbare vorm te verkrijgen, en de betrokkene heeft het recht die gegevens aan een andere verwerkingsverantwoordelijke over te dragen. Dit kan wanneer de verwerking berust op toestemming of op een overeenkomst waarbij de betrokkene als de betrokkene partij bent, of wanneer de verwerking via geautomatiseerde procedés wordt verricht.

De betrokkene heeft tenslotte ook steeds het recht om klacht in te dienen bij de toezichthoudende autoriteit, namelijk de Gegevensbeschermingsautoriteit.

Annex 6: Terms and Conditons Alfapass

Zie link: nog te ontvangen van Alfapass.