DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

APPENDIX 1 – SERVICE DESCRIPTION/PLANNING

Table des matières

1 Service Description 2
1.1 Main Services 2
1.2 Project implementation Services 2
1.2.1 Expense Project 2
1.2.2 Travel Project 4
1.3 Transversal Services Description 5
1.3.1 Governance Services 5
1.3.2 Tracking of support and maintenance services 6
1.4 Support and Maintenance Services 6
1.4.1 Corrective maintenance 6
1.4.2 Active Production Monitoring 7
2 Perimeter 8
3 Profile Description 8
4 Service Provider Organization 10
5 Planning 10

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Preamble

The purpose of this Annex is to define and describe the Services expected by the Customer and concluded with the Service Provider under the Contract.

1 Service Description

1.1 Main Services

Service Provider provides :

- Project implementation Services
- Transversal Services
- Support and Maintenance Services

Transversal Services and Specific Services are together referred to as the « Services ».

1.2 Project implementation Services

1.2.1 Expense Project

Goals
Deliver Notilus Expense project to production.
Deliverables
• Kick-off meeting report • Project planning • functional analysis material • preparatory document for the functional analysis • Functional analysis • Interface specifications • Acceptance report (one per interface) • Notilus platform with the production database • Standard Notilus BI cube • Notilus configuration with the production database • Standard user guides

Implementation Plan Notilus Expense core platform (France)		**RACI**			
		NOTILUS			**CUSTOMER**
	Decision-making representative	Project Manager	Functional Consultant	Technical Consultant	
Project management team	R	R	I	I	A, C
Design					
Functional analysis/Detailed functional specifications (DFS)					

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Workshop on the functional analysis for Notilus EXPENSE	I	I	R	I	A, C
Writing of the detailed functional specifications	I	I	R	I	A, C
NOTILUS Installation					
Technical installation of the Notilus platform (production environment) & test platform (with interface)	I	I	I	R	A, C
Installation of Notilus DECISION (Analysis) Provision of the standard Notilus BI cube	I	I	I	R	A, C
Solution Implementation					
Training to the functional setup of Notilus EXPENSE (EDM and MOBILITY)	I	I	R	I	A, C
Solution Integration					
- Input interfaces					
STANDARD input interface: => **HR** (branches, departments, people, users, signatories, line manager) with success factor => **INTERNAL CODE** (projects or customers or products - excluding Files 2 and 3, excluding allocation), => **EXCHANGE RATES** (file from SAP).	I	I	I	R	A, C
BNP BUSINESS CARDS interface	I	I	I	R	A, C
- Output interfaces					
STANDARD output interface toward **SAP**: => **EXPENSE REPORTS** (accounting entries relating to expense reports: expense account, VAT, consideration), => **ADVANCES** (accounting entries relating to advances: consideration, bank)	I	I	I	R	A, C
Qualification / Validation / Production start					
Putting in Running Order - Validation - Operational Acceptance Test => Pre-production database					
Training of the Notilus EXPENSE validation group (8 people maximum trained by session)	I	I	R	I	A, C
Functional and technical validation	I	I	C/A	C	R
Support to the functional and technical validation (1/2 day/week remotely, during 2 weeks) Processing of the open tickets on our support tool (projet in Validation) and update calls	I	I	R	C	A, C
Minutes of the Operational Acceptance Test	I	I	R	I	A, C
Production start					
Switching into production	I	I	I	R	A, C
Skills transfer & Change management					

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Training of the key users (8 people maximum trained by session of half a day)	I	I	R	I	A, C
DECISION training (Analysis)	I	I	I	R	A, C

1.2.2 Travel Project

Goals
Deliver Notilus Travel project to production.
Deliverables
• Kick-off meeting report • Forecast schedule • Project plan • functional analysis material • preparatory document for the functional analysis • Functional analysis • Notilus configuration with the production database • Standard user guides

Implementation Plan Notilus Travel core platform France		**RACI**			
		NOTILUS			**CUSTOMER**
	Decision-making	Project Manager	Functional Consultant	Technical Consultant	
Project management team	R	R	I	I	A/C
Project start up					
Notilus TRAVEL kick-off meeting & Report: - introduction of stakeholders and presentation of their roles, - project presentation (stakes and risks), scope validation and demonstration of NOTILUS, - methodology presentation: validation of the schedule, milestones, phases, deliverables, and exchange mode and frequency, - anticipate the subjects to study, the documents to provide, and the files to enrich.	C	R	I	I	A/C
Design					
Functional analysis/Detailed functional specifications (DFS)					
Workshop on the functional analysis for Notilus TRAVEL	I	I	R	I	A/C
Writing of the detailed functional specifications	I	I	R	I	A/C
NOTILUS Installation					

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Technical installation of the Notilus Travelhub platform	I	I	I	R	A/C
Solution Implementation					
ON LINE : Setting and test of the connection NOTILUS/EGENCIA	I	I	R	I	A/C
Training to the functional setup of Notilus TRAVEL	I	I	R	I	A/C
OFF LINE: setting and test of the connection NOTILUS/TMC	I	I	R	I	A/C
Validation of the technical setup NOTILUS/AGENCE/Egencia	I	I	R	I	A/C
Qualification / Validation / Production start					
Putting in Running Order - Validation - Operational Acceptance Test => Pre-production database					
Training of the Notilus TRAVEL validation group (8 people maximum trained by session)	I	I	R	I	A/C
Functional and technical validation	I	I	C/A	C	R
Support to the functional and technical validation (1/2 day/week remotely, during 2 weeks) Processing of the open tickets on our support tool (projet in Validation) and update calls	I	I	R	C	A/C
Minutes of the Operational Acceptance Test	I	I	R	I	A/C
Production start					
Switching into production	I	I	I	R	A/C
Skills transfer & Change management					
Creation of userguides (create and control of a travel request, reservations management)	I	I	R	I	A/C
"Internal Support Team" training (8 persons trained during 1 day) for administration	I	I	R	I	A/C

1.3 Transversal Services Description

1.3.1 Governance Services

Code : GOV	Governance Services
Goals	
Manage and Monitor the Services and ensure that contractual commitments and Services Levels are met.	
Prerequisites	**Deliverables**
• Roadmap • Contractual Commitments • Services Levels	• Operational reports which provide the status of activities • Support and minutes of regular meetings to ensure multi-level reporting (operational to strategic) • Action plans when necessary

Main Activities	**Customer**	**Provider**
Ensure contractual commitment compliance	I	A, R

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Monitor workload of Service Provider collaborators	I	A,R
Adjust the sizing of the Service Provider's teams with regard to contractual commitments	I	A,R
Proactively propose solutions to optimize the Services	C	A, R
Monitor the delivery	I	A, R
Ensure a level of skills & knowledge in line with contractual commitments	C	A, R
Manage Service Provider's requests for authorization to the Customer's Information System	A, R	C
Produce required dashboards to monitor the Services	I	A, R
Prepare and lead the Governance on Service Provider side	C	A, R
Maintain Services' agreed documentation	I	A, R
Ensure Service Continuity	I	A, R
Periodically conduct Quality Assurance Reviews on products, processes & deliverables	C	A, R

1.3.2 Tracking of support and maintenance services

Code : TRK	Name : Tracking of support and maintenance services	
Goals		
To communicate to the Customer all analytics related to the requests arisen to the Service Provider, along with the associated KPIs (as per defined in the Master Service Agreement) Those KPIs will relate to the solving performances, qualifications and to the workflows associated to the requests.		
Prerequisites	**Deliverables**	
	• Monthly reports on requests submitted and associated KPIs (as per defined in the Master Service Agreement)	
Main Activities	**Customer**	**Provider**
Send monthly report on requests tracking with standard SLA metrics	I	A,R
Organize & prepare requests tracking upon demand of the Customer or the Service Provider	C, I	A, R

1.4 Support and Maintenance Services

1.4.1 Corrective maintenance

Code : COR	Name : Corrective maintenance
Goals	

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

To solve :

1. Bugs and transactional incidents that will arise in the course of the application use by the Customer.
2. Anomalies related to optimization performances of the application at iso-functionality / constant perimeter of work. (On application pre-defined KPIs)

These incidents will be submitted to the Service Provider through requests.
This will be with or without source code modifications.
All corrective activities requested should be addressed with no limitation on number of activities/incidents.

Depending on the type of request, it may be handled or requalified to be sent to another support level;

Prerequisites	Deliverables
• Request received through Service Provider ticketing applicationDetailed description of the issue, with information for Service Provider to be able to replicate it	• Correction impact analysis (in case of workaround) • Application change made, delivery of the necessary elements: sources owned by the Customer, package, technical and functional documentation (if applicable) • Workaround (if applicable) • Delivery plan • Release documentation (in case of updates)

Main Activities	Customer	Provider
Qualify / Prioritize request with relevant criticality level and detailed description of the issue	A,R	C
Acknowledge reception & first analysis of the request	I	A,R
Carry out the diagnosis / analysis of the request	C	A,R
Communicate a proposed solution associated with provisional delivery date (Definitive fix or workaround, according to SLA / according to agreement with Customer)	C	A, R
Correction impact analysis (in case of workaround)	C	A,R
Develop agreed solution	I	A,R
Perform Unit Tests, Non-regression Tests and Function Integration Test (on Service Provider test environment)	I	A,R
Deliver fix to Customer Pre Prod environment	I	A,R
Update, if necessary, the functional documentation	I	A,R
Test fix on Pre Prod environment (for production readiness)	A,R	C,I
Provide the Acceptance	A, R	C, I
Define release date of the fix for production	A,R	C,I
Relase fix on Production environment	I	A,R
Ensure the follow-up of the request in ticketing application	I	A,R
Issue a proposal for evolutive maintenance (in the event of a necessary software evolution)	I,C	A,R

1.4.2 Active Production Monitoring

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Code : PRM	Name : Production Monitoring
Goals	
To periodically monitor the operation of an Applicative System in production. Frequency has to be defined and can be different depending on the project phase. This service will be started following agreement between Parties of the project.	
Prerequisites	**Deliverables**
• Request from the Customer • OR : Detect early warning signals of potential optimization/data issues	• Production monitoring report • Preventive maintenance propositions (actions or developments to be carried out to prevent a recurring issue), if applicable

Main Activities	**Customer**	**Provider**
Implement an Applicative System production monitoring	I	A R
Execute the Applicative System production monitoring procedure	I	A,R
Write the production monitoring report	C	A R
Deliver, if necessary, preventive maintenance propositions	C	A R

2 Perimeter

The perimeter of the Notilus SAAS contract is to define the conditions under which the Supplier provides the Customer with hosting services, remote provision of data and functions of the Software Package for a defined number of Users, maintenance and data back-up, and, where applicable, the related telecommunications costs.

In order to provide these services to its Customer, the Supplier has operating contracts with industrial partners (hosting companies, manufacturers, telecommunication operators, software publishers) enabling it to provide the Customer with a global offer and to remain its sole interlocutor.

The Supplier provides the following services for the Customer:

- Project implementation and delivery.

- Hosting of the Software Package: meaning specifically the provision to the Customer of the functionality of the Software Package by remote access.

- Customer Support.

See document “Notilus Charte TnE SaaS- V2.6_en-EN.pdf” for more details.

3 Profile Description

Profile	DESCRIPTION

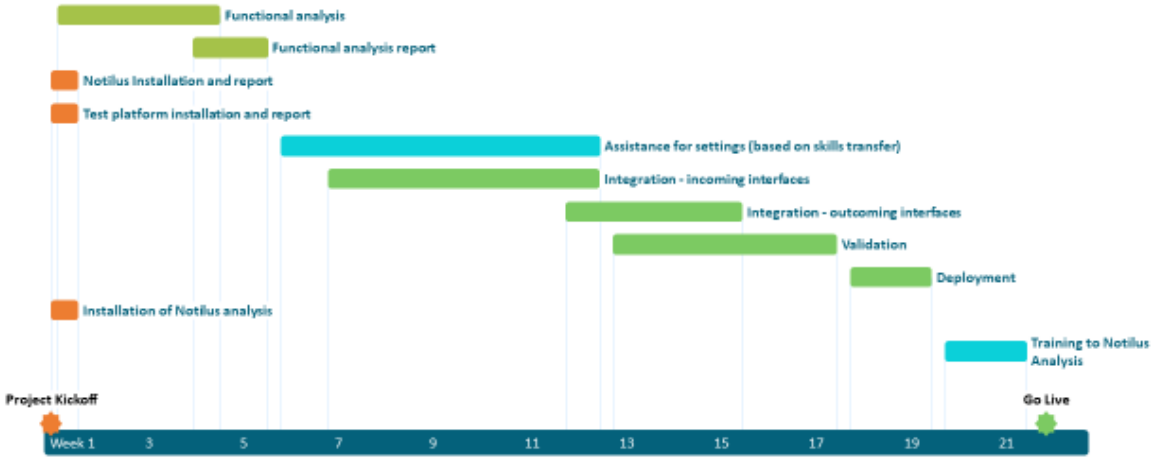
DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

4 Service Provider Organization

Notilus (www.notilus.com) is a privately owned company, part of Cegid (www.cegid.com).

5 Planning



APPENDIX 2: FINANCIAL CONDITIONS

1. NAME OF SERVICES AND SOFTWARE PACKAGES

Services and Software Packages provided in SAAS mode	
Designations	**Suppliers**
Hosting of the NOTILUS application including the followingNOTIILUS T&E services: - NOTILUS T&E - NOTILUS TRAVEL CONNECT - NOTILUS INVOICE CONNECT - NOTILUS ANALYSIS - NOTILUS T&E ARCHIVAGE VALEUR PROBANTE	NOTILUS

Date of first Invoice: from the date of availability of the solution on our servers.

2. SUBSCRIPTION AMOUNT

The price includes a subscription covering both the provision of the Software Package and services rendered and detailed in Appendix 2 by the SUPPLIER in the framework of data hosting as defined hereinafter:

Subscription amount				
Duration	**Number of Active Profiles**	**AP UP excl. tax**	**Monthly cost excl. tax**	**Annual cost excl. tax**
36 months	800	3,75 €	3000 €	36 000 €

The SUPPLIER's subscription also includes:

- Standard archiving of documents until the end of the Contract (maximum 48 months);
- Use of the EDM service and corresponding maintenance. Documents entered into the EDM may not exceed the size limit of 3 MB per document;

=> It is not possible to collect a document beyond the standard 48-month contractual storage period or beyond the end of the Contract.
The invoicing of licenses will be staggered as follows to accompany the Pilot deployment from : Fixed Unit price for 800 AP valid from 1st country implementation

Country deployment	License range	License fees	Year or quarter
France	300 AP	8 910 €	Q3 & Q4 2022
Asia + Americas (without US) + France	700 AP	41 580 €	2023
WW (without US)	800 AP	47 520 €	2024

Additional Electronic Signature service and Evidentiary Value Archiving				
Duration	**Number of Active Profiles**	**AP UP excl. tax**	**Monthly cost excl. tax**	**Annual cost excl. tax**

36 months	800	1,20 €	960 €	11 520 €

The SUPPLIER will put in place an Evidentiary Value Archiving process in compliance with the Decree of 23 May 2019 establishing the conditions for digitalising documents drawn up or received on paper in application of Article L. 243-16 of the French Social Security Code.

The integrity of the receipts is guaranteed by an RGS 2* server certificate issued by a trusted third party. Evidentiary Value Archiving is provided for a period of Ten (10) years by our partner ARKHINEO.

The price is flat-rate and includes a shared volume on a basis of 24 Mb per AP per year.

If this volume is exceeded an adjustment will be made one (1) time a year on a basis of €1.60 excl. tax/2Mb range. The

CLIENT's Notilus administrator can view the Evidentiary Value Archiving service consumption at any time. The Service

provider will notify the Client before any additional cost with a prior written notice.

Invoicing will be established as soon as the Evidentiary Value Archiving services is opened.
The consultation of the consumption of the Probative Value Archiving service is accessible at any time by the CLIENT's Notilus administrator.

In case of termination of the Contract, the Client has several options:
1. The CLIENT wishes to retain simple access to Notilus to allow consultation of the receipts archived at ARKHINEO, The SUPPLIER will maintain restricted access (administrator profile) to the Notilus database at a monthly rate of €1.50 excl. tax x the number of existing APs, for a period of twelve (12) months, renewable => Benefit: consultation of the history of the Data via Notilus.
2. The Client wishes to retrieve all the documents archived at ARKHINEO. Client will be able to retrieve its documents archived at ARKHINEO, together with the sealing data, from its Notilus platform, until the termination date. The Supplier draws the Client's attention to the fact that once the documents are retrieved from the ARKHINEO "safe", they will lose their Probative Value. For those documents that are still valid for auditing, the Client should plan to store them with another trusted third party.
3. The Client wishes to continue to access his archived credentials at ARKHINEO after the termination date of his Notilus platform. The Client will contact ARKHINEO to find out the access and financial terms and conditions. The latter will depend on the Client's volume.

3. INVOICING FREQUENCY

The SUPPLIER issues annual invoices, payable in advance, on the last business day of the previous period.

4. METHOD AND CONDITIONS FOR INVOICING AND PAYMENT

Payment must be made by bank transfer.
Payment conditions are net 45 days from the date of invoice.
A service charge of €250 (except for any other entity/division joining the contract) excluding taxes per invoice is normally billed for any request for re-invoicing to another entity other than the one stipulated in the contract. Notilus authorize Plastic Omnium to list to this contract the entities which will be charged for the project. Notilus will grant a twice year changes for a re-invoicing request (new entities added to the scope wont' be concerned by the service charge).

5. CONDITIONS FOR REVISING THE SUBSCRIPTIONS

Once the global deployment is reached and in the case of an increase in the number of users, and/or the provisioning of additional services, a true-up invoice is issued at the end of the billing period.
Invoicing is based on billing period.
The SUPPLIER will tolerate an overrun of the number of active profiles for 2 months during one year of Product use. In the event of overrun during a third month in the same year, a true-up invoice for one quarter will be sent to the user. The subscription willautomatically move up to the next highest price range for the rates in force for the number of Active Profiles.

Once the global deployment is reached as described in the appendix 1, in order to establish a flexible monitoring of the number of active profiles and the associated billing, the Supplier and the Client will set up a half year monitoring committee.
This monitoring committee will allow us to analyze together the actual consumption of the year N-1 and to determine the appropriate billing band for the following period.
Upon signature of the contract, the Parties agree on applying the unit costs related to 800 APs.
If the actual consumption is below the forecast, then we will adjust the active profile bracket for the coming period.
In case of a downward adjustment, this would be within a maximum of -20% of the initial 800 APs. The activated license key will be the license key closest to the number of profiles then calculated (i.e. the 700 profile range for the first decrease).

Notilus licenses schedule agreed upon by the parties to the contract:

			36 months	36 months	36 months	36 months	36 months	36 months
Notilus rent in SaaS mode(*)			**150 AP**	**300 AP**	**350 AP**	**400 AP**	**450 AP**	**500 AP**
OFFER		**Content**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
Rent Hosting Maintenance Updates Support	**Licenses & Technical infrastructure**	**Notilus Expense** **Notilus Decision** **Notilus Travel** *Notilus Expense* *Notilus App* *Scan of receipts from Notilus app* *Technical infrastructure* *Credti card integration* *HTTPS* *Travel order / OnLine & OffLine booking* *Invoice Management* *Reporting*	7,30 €	5,51 €	5,22 €	4,88 €	4,54 €	4,53 €
Access to new version, corrective maintenance and support are included in the rent hereabove								
POG will benefit. New conditions will apply upon CES full scope deployment								
(**) : An active user is a person who submit at least one expense report per month.								

Monthly costs (without legal archiving)	1 095,00 €	1 653,00 €	1 827,00 €	1 952,00 €	2 043,00 €	2 265,00 €
Sales discount Notilus client	**22%**	**22%**	**22%**	**22%**	**22%**	**22%**
New cost per active profile	**5,69 €**	**4,30 €**	**4,07 €**	**3,81 €**	**3,54 €**	**3,53 €**
New monthly costs (without legal archiving)	**854,10 €**	**1 289,34 €**	**1 425,06 €**	**1 522,56 €**	**1 593,54 €**	**1 766,70 €**

Notilus options		**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
Notilus Invoice	**Invoice management import in Notilus (Airplus or other suppliers)**	1,50 €/active profile	1,22 €/active profile	1,16 €/active profile	1,10 €/active profile	1,04 €/active profile	1,00 €/active profile
Monthly costs		**225,00 €**	**366,00 €**	**406,00 €**	**440,00 €**	**468,00 €**	**500,00 €**
Legal archiving	**Hosting with Arkhineo (legal archiving over 10 years with consultation of all receipts in Notilus). This option has to be defined according to the countries authorized to digitalize receipts**	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile

5 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months
600 AP	700 AP	800 AP	900 AP	1000 AP	1200 AP	1500 AP	2000 AP	2500 AP	3000 AP	3500 AP
Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month
4,18 €	3,96 €	3,77 €	3,59 €	3,47 €	3,33 €	3,26 €	3,16 €	3,13 €	3,08 €	3,02 €

2 508,00 €	2 772,00 €	2 262,00 €	3 231,00 €	3 470,00 €	3 996,00 €	4 890,00 €	4 740,00 €	4 695,00 €	4 620,00 €	4 530,00 €
22%	22%	22%	22%	22%	22%	22%	22%	22%	22%	22%
3,26 €	3,09 €	2,94 €	2,80 €	2,71 €	2,60 €	2,54 €	2,46 €	2,44 €	2,40 €	2,36 €
1 956,24 €	2 162,16 €	2 352,48 €	2 520,18 €	2 706,60 €	3 116,88 €	3 814,20 €	4 929,60 €	6 103,50 €	7 207,20 €	8 244,60 €

Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month	Price per active users (**) per month
0,94 €/active profile	0,85 €/active profile	0,81 €/active profile	0,78 €/active profile	0,75 €/active profile	0,71 €/active profile	0,69 €/active profile	0,67 €/active profile	0,65 €/active profile	0,63 €/active profile	0,62 €/active profile
564,00 €	658,00 €	648,00 €	702,00 €	750,00 €	852,00 €	1 035,00 €	1 380,00 €	1 725,00 €	2 070,00 €	2 415,00 €
1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile

Rates listed in this document are prices in euros exclusive of taxes, net and without discount.
The price for providing the application will be reviewed once per new contract period on 1 January based on the Syntec Index for information services from the month of July preceding the renewal . Price review can take place earliest after 1st contract period (36 month after signature). It was decided that after the expiration of the contract, the parties can agree on a further contract period in which the prices are fixed.

6. LATE INTEREST

Payment default for all or part of the amount due by the CLIENT at the exact deadline will lead ipso jure and without prior official notice to:
- The invoicing of late fees based on three times the legal interest rate pursuant to article L 441-6 of the French Commercial Code, and the payment of all remaining sums due. Additionally, and in compliance with article 121-II of Law No 20102-387 dated 22 March 2012, a flat-rate indemnity of €40 will be due by the CLIENT for any payment delay.
- The right of the SUPPLIER to suspend services without notice.

Without prejudice to the SUPPLIER's right to proceed with terminating the contract with a 6 month notice period.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

7. SPECIAL SERVICE CONDITIONS

Travel expenses billed at actual cost based on second class prices for train journeys and economy class prices for plane journey of less than 3 hours. Meal and accommodation costs are billed at actual cost (2nd class train, eco for flight (booking in advance > 14 days) and rental car, hotel price gap incl. breakfast- 100 €- all travel costs prior confirmed by PO).

7.1 - Purpose

The CLIENT shall attend the days ordered herein within a period of 130 calendar days after signature of this registration sheet. Beyond this period, the services will be regarded as being completed and therefore billed to the CLIENT.

7.2 - Registration

Registration will be definitive upon receipt of this dated and signed document bearing the company seal.

7.3 - Session cancellation

Cancellation/rescheduling conditions starting from final booking:
. 50% of the daily price of the session remains due for any cancellation received less than ten business days before the scheduled date;
. For any cancellation received less than five business days before the date of the service, the price of the session days remains due to the SUPPLIER.
Only written and faxed cancellations are taken into account.

7.4 – Implementation payment plan

Notilus project services listed in Appendix 2 of this contract will be invoiced on a lump sum basis according to milestones defined as follows:
- 30% after the analysis workshop
- 30% at the beginning of the technical acceptance
- 40% at the go live

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Notilus

MOVING PEOPLE FURTHER

Governance

Description & operation

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Table of contents

I. Description **2**

II. Operation **2**

1. Project Director's role 2

2. Management committees 3

II.1.1 Strategic level 3

II.1.2 Tactical level 3

II.1.3 Operational level 4

II.1.4 Summary of the Committee members 4

3. Governance process 5

4. Governance operating methods 5

II.1.5 Scope management 5

II.1.6 Knowledge management 7

II.1.7 Skills management 7

II.1.8 Quality assurance and control 7

II.1.9 Risk management 9

II.1.10 Management of continuous improvement 10

II.1.11 Financial management 10

II.1.12 Communication management 11

III. Presentation of the key people involved **13**

IV. Management of the relationship with partners **14**

1. Relationships between service providers 15

2. Collaboration principle 15

3. Information to be 'structurally' shared 15

4. The mindset: a key factor of success 16

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

I. Description

Governance of the service provided is based on a model implementing the principles tried and tested by Notilus in various contexts and compared to the best practice frameworks ITIL and CMMI.

Governance of the service distinguishes between three levels of management which correspond to three approaches for analysing the service. Each level has its own actions and responsibilities, time aspect (short, medium and long-term actions), committees and communication method.
Strategic governance is a top-down approach to managing the contract and services produced as a whole. Led by the client's project management and the Notilus project director, it informs the client's strategic decisions and establishes a long trajectory that is then applied at operational level. It enables the necessary investment and contractual amendments to be made that ensure the continuity of operational services, while incorporating future movements and changes.
The strategic reflection is shaped by the results, successes and failures of the actions carried out in the field. For this to happen, it has strategic and operational indicators that are consolidated and supplied by the Notilus project manager.
Conversely, **operational governance** is a bottom-up approach to management. Led by the operational stakeholders, its aim is to analyse the actual outcomes of work performed and decide on the actions to trigger. It monitors all the service indicators and acts to improve the services, manage peaks in workload, anticipate medium-term needs, ensure adherence to schedules and carry out changes of organisation or scope.
Operational Management oversees everyday activity. It aims to carry out operational adjustments to the system and monitor the progress of works.

II. Operation

The governance process is the implementation of a management entity during the project build phase. It is entirely overseen by a Project Director and their operational project manager, who, at the end of the pre-sale phase, replace the sales team in the relationship with the client.
They are responsible throughout the project life cycle for the necessary support to the various transformations and give visibility over the progress of the actions undertaken.

1. Project Director's role

The Project Director, who is responsible for the development of **value**, provides a strategic overview in the medium term and guarantees:

- The completion of the project(s) under way,
- Adherence to the contractual commitments of the phase:
  - Writing the different plans (QAP, etc.),
  - Implementation of logistic resources,
  - Upskilling his resources,
  - Definition and implementation of the tools,
- That the resources ensure good communication with the service partners (TMCs, SBTs, banks, suppliers, etc.),
- Risk monitoring,
- The implementation of overall financial monitoring,

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

- The transition to 'Run' mode.

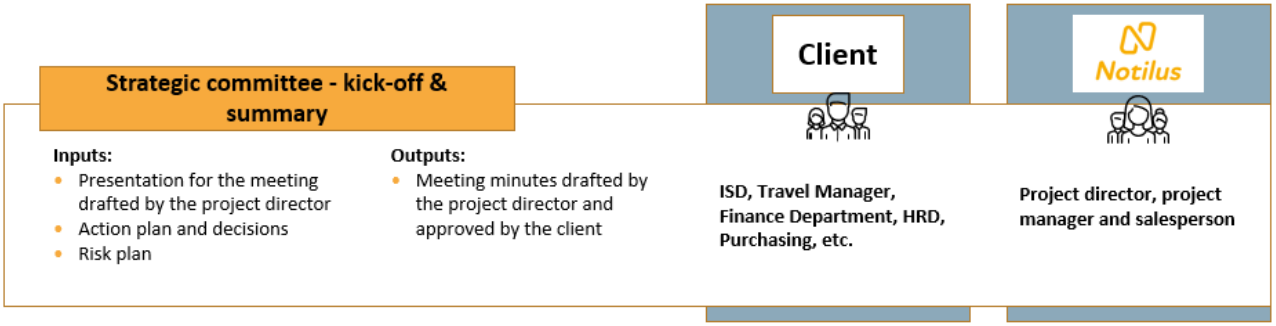
2. Management committees

Organisation of governance is based on three levels of management recommended by the ITIL standard. Each level has its own objectives, actions and responsibilities, time aspect (short, medium and long-term actions) and committees.
This paragraph specifies the members of these committees and how they are organised over time, in relation to one another and in light of the Notilus internal steering committees.

II.1.1 Strategic level

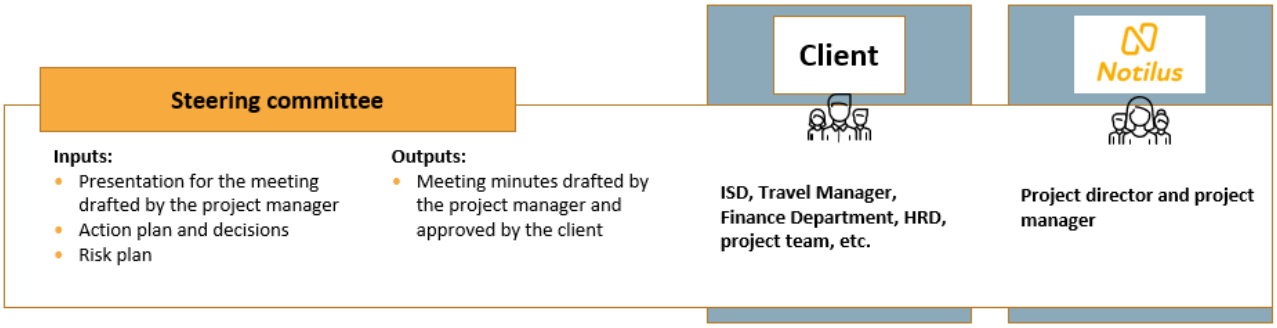
At strategic level, to guarantee the strategic committee's ability to take useful decisions, the participants are the sponsors, decision-making representatives and contract managers.
We distinguish between two strategic meetings:

- The launch meeting, which presents the project(s) and sets the objectives,
- A 'Summary and prospects' feedback session, planned after go-live, which establishes a project summary, reports on the inventory and recommendations deduced, and launches the second phase, the 'run' phase.



II.1.2 Tactical level

Tactical Governance is a Bottom-up approach to management. Led in priority by the Project Director and the Project Manager, the steering committee consolidates and analyses the actual results in the different fields and decides on the actions to trigger to observe the contract.

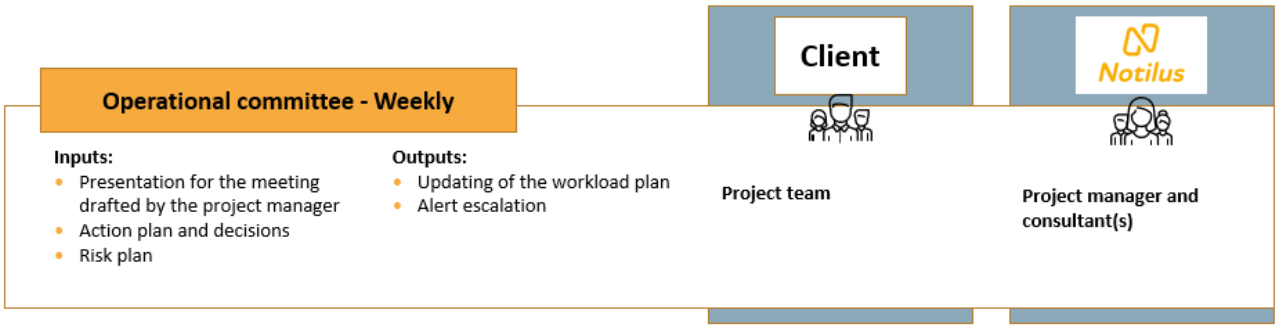


DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

II.1.3 Operational level

The project is monitored on a weekly basis by the project committee in a dedicated session. This committee's aim is to monitor the progress of the works. For this, focus is placed on:

- Work progress,
- Resource management,
- Identification of risks and difficulties,
- Monitoring the project committee's action plan,
- Various questions.



II.1.4 Summary of the Committee members

Client stakeholder	Challenges	Communication media	Frequency
Sponsor	Financial optimisation Quality of services Stakeholder satisfaction Value development	Kick-off meeting Steering committee Feedback	Unitary Every 3 weeks Unitary
Project manager	Task progress Upgrading of configuration Event management (incident, changes and requests) Meeting commitments	Kick-off meeting Steering committee Feedback	Unitary Every 3 weeks Unitary
Project team	Task progress Event management (incident, changes and requests) Quality of service User part satisfaction	Kick-off meeting Steering committee Feedback Operational committee	Unitary Every 3 weeks Unitary Weekly

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3. Governance process

In compliance with our project management methodology, governance is organised according to the following **processes**:

5

We pay particular attention to the following processes:

- **Knowledge management** - Beyond the implementation of a system to manage it, this involves sharing knowledge with all the stakeholders.
- **Communication management** – The multitude of stakeholders makes it necessary to achieve a good synergy between them – Notilus will therefore endeavour to facilitate the relationship between service providers in its practices.
- **Risk management** – The new contract is the theatre of new working methods between the client and the service provider. We must ensure that these changes take place guaranteeing secure service provision.

In the rest of this document, we describe the operating methods inherent to these processes.

4. Governance operating methods

II.1.5 Scope management

Process description

Scope management consists in defining the scope then managing the changes within it and their impacts.

Specifying the scope and the services

This phase enables the service provider to define the structural aspects of the scope precisely:

- **WHAT?** This means specifying:

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

  - The application scope covered within the framework of the contract,
  - The expected services and corresponding deliverables,
  - The service level agreements as well as key performance indicators,
- **HOW?** This concerns the processes for providing the services and governing them,
- **WHO?** We identify the different profiles of stakeholders involved within the framework of the contract and the structure of the team

This stage is key insofar as it translates the client's needs and the contract's terms into a framework describing how the service will be provided; the client's approval of the aspects reported secures execution of the contract.

Change management

Change management handles:

- **Operational type changes,** which concern change requests inherent to the provision of operational services.
- **Contractual type changes**, which correspond to events that call into question Notilus's commitments or the services provided (E.g. changing the levels of services expected, transfer of services to a third party, etc.).

In the service life cycle, several **major events** may take place, in particular a change of organisation or process requested by the client.

These events are escalated to Notilus governance via the committees managing the service with the client (Steering Committee, Strategic Committee, etc.) so that the latter can handle them to upgrade the system in place.

In this way, after a change request, Notilus measures **the operational and organisational impact** of these changes. This impact report is shared with the tactical, strategic and operational governance teams.

All this consultation enables us to apply the changes to be made to management, the quality plan and the service agreement on one hand as well as the organisation (team, reinforcement, reduction, upskilling, transfer, etc.) and the organisation of the operational service (adaptation of existing processes in-house, creation of new processes and withdrawal of certain processes).

During this whole phase, **the Project Director** monitors the organisational and operational transformation with his contacts to ensure that these changes are properly taken into account.

Conditions of execution

Scope management is under the Project Director's responsibility who delegates operational change management to the Project Manager.

These changes in scope and their impacts, entering within the framework of contractual type change, are monitored by the steering committee.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

II.1.6 Knowledge management

Process description

Knowledge management covers the whole life cycle of information necessary for our teams' work. The major challenge of this process is of course to enable those involved to **have all the information necessary** for their work within the framework of the contract in the most natural way possible.
But is must also enable real **knowledge sharing** between the other contract stakeholders (client, third-party service providers) and Notilus. In this respect, when defining the conditions of this process, we will endeavour to incorporate the different stakeholders' expectations, as well as their practices in terms of knowledge management, as soon as possible.
The information managed in this processed is grouped in a **documentary framework** and is as follows:

- Information relating to the services that we provide: operating methods, deliverables, etc.,
- Information relating to our contract and the conditions of joint work between the client and Notilus: QAP, service agreement, reversibility plan, autonomy plan, etc.,
- Information facilitating the client's understanding of the context: potential documentation from other service providers, contract documents, etc.

Conditions of execution

Knowledge management is a process that is under the Project Director's responsibility, who delegates its execution to the Project Manager.
In this respect, the latter is responsible for updating aspects of the documentary framework and their distribution to the contacts concerned; the Project Director will remain as change manager within their contractual framework.
The documentary framework is updated by the team members throughout the operational changes.

II.1.7 Skills management

Process description

Skills management aims to ensure that the team members **constantly** have the necessary and sufficient skills to provide the level of service expected.

Conditions of execution

Skills management is a process overseen by the Project Director who delegates its execution to the Project Manager for the operational service provision system

It is implemented when people enter or leave the Notilus team, as well as when changes take place that require the system's adaptation. These changes are managed on a weekly basis by the management team. Reporting is carried out at steering committee meetings.

II.1.8 Quality assurance and control

Process description

The purpose of quality assurance and control is to define and manage the measures taken by the

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

client and by Notilus to organise production and guarantee quality.

Conditions of execution

Quality assurance

The conditions of work and interaction with the client are documented in a **Quality Assurance Plan** drafted by the Project Director.
The QAP, a deliverable of this process, is:

- **A framework and work tool shared by all the stakeholders that gives a similar vision of the project;**
- **The quality specifications drafted in collaboration with the client and approved; each party must therefore observe them.**

It defines the procedures, processes and invariable or stable aspects over time. This is a document common to the different phases of the contract which can be supplemented throughout its life cycle.
The QAP is updated by the Project Director with the Notilus Quality Manager's assistance and this is monitored during the Steering Committee meetings.

Quality control

Quality control is performed regularly to detect non-conformities. It is carried out along 2 themes:

- **Quality control of products and services through the client acceptance process,**
- **Quality control of production and management processes via audits.**

Non-conformities in acceptance are those relating to operational work (development anomaly, application infrastructure incident, etc.). In this respect, they are handled at operational steering committee meetings.
The Project Manager is responsible for handling them and reports on them in an incident management table.
Non-conformities in audits are handled by the same committee. They are subject to an action plan to bring them into compliance monitored by the steering committee.
The Notilus Project Manager is responsible for handling them and reports on them in an action plan to bring them into compliance.

Client acceptance

The conditions of acceptance are specified again in the incoming transition phase, within the framework of QAP finalisation.
The aim is to provide a demonstration of the compliance of a deliverable (document, product or service) with the requirements stipulated in the contract, whether they concern the functional or technical aspects or the quality.

Audits

Audits are triggered by the client without justifying the reason. The contract holder is informed at the Steering Committee meeting, at least 10 working days before their resources are used.
They may target all the activities entrusted to the contract holder. The contract holder's contribution to these audits is limited to an average workload of 2 days a month.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

II.1.9 Risk management

Process description

We put in place a general risk management policy for each service.

Conditions of execution

This process is managed by the Project Director on 2 levels of oversight:

- **Operational through the Operational committees,**
- **Tactical through the Steering Committee.**

The risk management plan incorporated in the QAP and shared with the client improves the relationship between the service provider and the client by reassuring the latter about the resources implemented to guarantee the expected levels of service.
To this end, particular attention will be given:

- **To management of sensitive periods,**
- **To management of adherence with existing applications or those being developed by another service provider,**
- **To the quality of the assistance service given to other service providers,**
- **To cross-functional processes such as communication between stakeholders.**

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

II.1.10 Management of continuous improvement

Process description

Continuous improvement is a process managed throughout the deliverable's life cycle. This analysis document is initialised during audit and enhanced by analyses and recommendations given throughout service provision and its corresponding action plans are implemented iteratively so that they are constantly improving. This continuous improvement deliverable is then distributed to all the stakeholders for each of the areas for improvement concerned.

Definition

During the audit:
- Understanding the context
- Analysing what exists

Update & implementation

Enhancement of the content:
- Roll-out
- Innovation

Distribution

Distribution of the progress plan to all the partners

Conditions of execution

The Progress Plan, managed by the **Project Director**, is:

- **Monitored by the steering committee to follow up on the implementation of the progress plan,**
- **Shared in the operational committee to communicate the improvements to all the stakeholders.**

II.1.11 Financial management

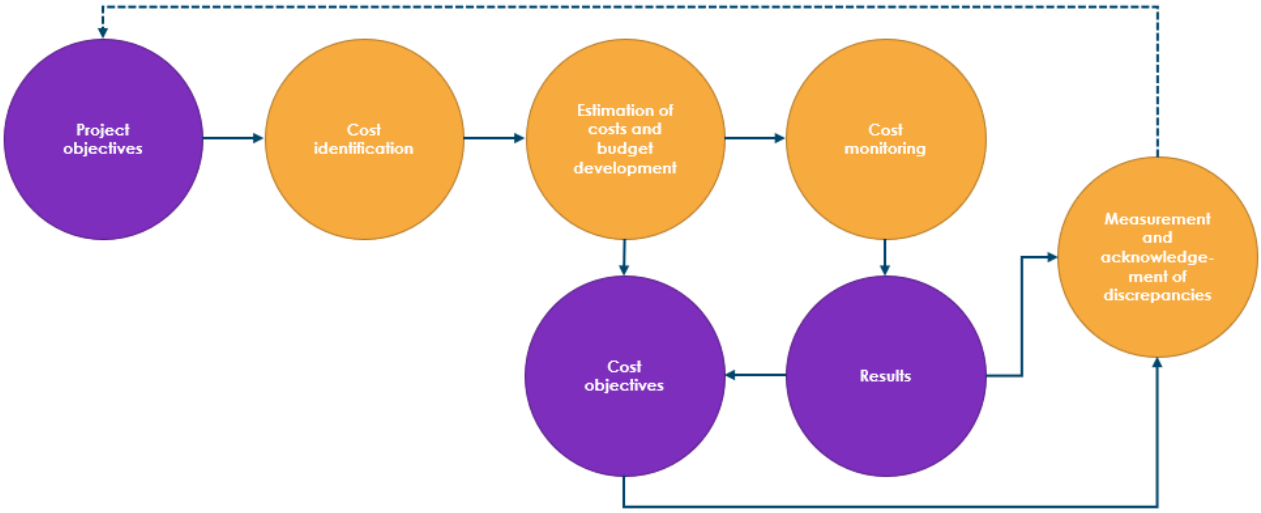
Process description

Budgetary and financial control, and more generally cost control, is a key aspect of project success. For this, the Project Director must build real monitoring to keep accurate control throughout the contract.

Cost control process in project management

- **Cost identification**
- **To achieve the project objectives.**
  - Estimation of costs and budget development
  - Taking into account direct and indirect costs related to the performance of work and therefore the project.
- **Cost monitoring**
  - Checking project progress, by comparing what has been accomplished with what was estimated and budgeted for.
  - Measurement and acknowledgement of discrepancies
  - Deciding on the actions to implement to correct any discrepancies.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B



Throughout the project life cycle

- **At the beginning of the projects:**
  - Through proper control and understanding of user needs,
  - By measuring the return on investment (ROI) of each requirement,
  - By estimating costs and planning upstream.
- **During projects:**
  - By qualitative and quantitative follow-up at the end of the project.
- **At the end of the project:**
  - By systematically drawing up a summary of projects in order to capitalise.

Communication and information-sharing is an essential condition for this cost control to be able to manage and therefore decide on action plans.

Continuous improvement: approach to make financial evaluations of projects reliable

Within the framework of implementing their project, the client implements new governance of their IT projects. This involves project arbitration by Business Departments, on the basis of project macro-costings as well as an analysis of their value.

Conditions of execution

This process is managed by the **Project Director** and translates into financial dashboards that are shared with the client at monthly steering committee meetings.

II.1.12 Communication management

It is essential to ensure **constant communication** between all the service stakeholders to guarantee a continuous and quality service.

Within the framework of governance, the client has already set up different committees whose primary aims are overseeing activities and sharing information.

We propose to supplement this system to provide even more value to the client with the implementation of a real relationship of trust between the different stakeholders.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Communication with the client's stakeholders

In the table below we present the media through which we will share information with the client's stakeholders, according to their challenges in respect of the contract.

Stakeholder	Challenges	Communication media	Frequency (by default)
Project operational manager	Project progress Upgrading of infrastructure Event management (incident, changes and requests) Quality of service Meeting commitments Stakeholder satisfaction Value development	Operational committee Steering committee Feedback Strategic committee	Weekly Monthly One-off Quarterly
Business manager	Project progress Upgrading of infrastructure Event management (incident, changes and requests) Quality of service Meeting commitments Stakeholder satisfaction Value development	Operational committee Steering committee Feedback Strategic committee	Weekly Monthly One-off Quarterly
Infrastructure manager (ISD)	Project progress Upgrading of infrastructure Event management (incident, changes and requests)	Operational committee Steering committee Feedback	Weekly Monthly One-off
Legal and administrative manager	Meeting commitments	Strategic committee	Quarterly
Business users	Project progress Incident resolution	Flash report on works under way (projects and tickets)	Monthly
Project director	Budgetary control Quality of services User satisfaction Alignment with strategic challenges	Strategic committee Flash report on works under way (projects and tickets)	Quarterly Monthly

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Communication with other service providers

Notilus is in contact with others service providers for the following reasons:

- **Collaboration within the framework of services such as the implementation of an upgrade to an existing application, or during the operational launch of a new application,**
- **Distribution of useful or necessary information. Examples: use of the technical base that Notilus maintains, visibility over projects under development...**

For all these reasons, we identify the following media:

Communication media	Frequency (by default)
Flash report on works under way (projects and tickets)	Monthly
Steering committee	Monthly
Service providers' committee	On request

Notilus teams' internal communication

Notilus teams' internal communications is governed by the following principles:

- **Organising regular management sessions which are generally held before those planned with the client:**
  - A daily coordination session if necessary,
  - A weekly management session bringing together Notilus stakeholders,
  - A monthly management session bringing together all Notilus stakeholders,
  - A monthly management session bringing together the project manager, director of supervision, account manager and quality structure.
- **Using the group's communication methods which are available in each service centre:**
  - A unique network, enabling all the tools to be shared (email, project management tools, development environments, etc.),
  - Collaborative tools: instant messaging, web conferencing, video conferencing, etc.

III. Presentation of the key people involved

The organisation proposed was structured to respond to the client's requirements:

- **Director of Supervision**

Within contract governance, the director of supervision oversees the running of the service and the suitability of its management for the contract's challenges. She is involved in internal management sessions as well as in strategic governance committees with the client. She has all the authority to take decisions involving Notilus and is one of the main stakeholders in the escalation and crisis management process.

- **Quality Manager**

He is independent from project management. In this respect, he monitors project quality and implements 'external' quality assurance for the project either by his own means or by delegating to other Notilus stakeholders. He audits the entire service based on observance of the Notilus methods quality standards.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

- **Project Director**

The project director, who is responsible for the development of value, provides a strategic overview in the medium-term and guarantees:

- Observance of contractual commitments towards the client,
- Good communication with the service partners,
- Monitoring of the service's tactical risks,
- Skills management within the framework of fluctuations in activity,
- Financial monitoring of all the service packages,
- Application of the Quality standards,
- Development of value and management of the improvement plan,
- Reversibility management.

- **Project manager**

The operational manager guarantees quality of service:

- Observance of quality of service for the client,
- Team management and optimisation
- Implementation and optimisation of the methods and tools of cross-functional activities: environments, configuration management, testing strategy, etc.
- The operational risk plan,
- Anticipation and monitoring of the workload plan,
- Anticipation and continuous updating of the reversibility strategy.

- **Consultant**

He is responsible for the upgrade support services. He directly refers to the project director and participates in operational committees. He guarantees:

- The application of configuration,
- Interface developments,
- The training of administrators.

IV. Management of the relationship with partners

In the service life cycle, several major events may take place, in particular a change of organisation required by the client.

These events are escalated to Notilus governance via the committees managing the service with the client (Steering Committee, Strategic Committee, etc.) so that the latter can handle them to upgrade the system in place.

In this way, after the client requests a change in organisation or processes, the Project Director measures the operational and organisational impacts of these changes and shares them with the rest of the governance team, having a more operational view.

All this consultation enables us to apply the changes to be made to management, the quality plan and the service agreement on one hand as well as the organisation (team, reinforcement, reduction, upskilling, transfer, etc.) and the organisation of the operational service (adaptation of existing processes in-house, creation of new processes and withdrawal of certain processes).

During this whole phase, the governance structure monitors the organisational and operational transformation to ensure that these changes required by the client are properly taken into account.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

1. Relationships between service providers

Each contract signed by the client has its own specific features, requirements and framework of execution. However, they all contribute to the same needs: to create an operational mobility management solution and keep it available to users (internal and external). It is therefore necessary to coordinate a certain number of actions and put in place 'cross-contract' collaborations on several topics:

- Maintenance **processes and procedures** are led by the use of the same tool shared by the different service providers. The rest must be pooled and compared to each party's commitments in order to offer a consistent, quality service to IS users,
- **Technological upgrades** (product and middleware versions, shared infrastructure, etc.) must be carried out in a coordinated manner between the stakeholders concerned: operator, architects and application maintainers at minimum;
- **Projects**: their impact on each of the applications and tools must be analysed from a 'software' and 'infrastructure' perspective. This is true irrespective of the application type, but it is even more important on applications that are strongly interfaced,
- **Schedules**: various stakeholders (contracting owners, operators, architects) are potentially concerned by operations carried out across several packages, within the framework of different contracts. So that they do not form 'bottlenecks', their actions must be seen in a consolidated manner,
- **Go-lives**: these require the potential participation of several project managers (simultaneous go-lives of several versions of applications whose upgrade is coordinated), that of the operator (who receives instructions from several project managers and must consolidate them) and that of the contracting owners' representatives (change management, information and training). It is essential that these actions are seen from a general perspective.

2. Collaboration principle

'Push' mode is the only mode that works overtime. For the 'owner' of information that (even 'potentially') affects several contracts, this involves systematically sending it to all the stakeholders (whether they are concerned or not). The communication methods implemented are as follows:

- The **Inter-services committee**, organised and coordinated by the client bringing together all the managers of the different contracts, must:
  - Identify the topics requiring coordination and/or cooperation
  - Level out any difficulties: scopes, responsibilities, etc.
- A **sharing and information ('news') space** in which we will provide a flash report on a monthly basis presenting the progress of work under way.

3. Information to be 'structurally' shared

In addition to the circumstantial discussions (relating to particular news), we must structurally share:

- The scope (applications, activities covered, length of the commitment, etc.) of each contract,
- The point(s) of contact (contract holder and client).

This sharing enables us to trigger more occasional coordination actions: information requests, joint

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

impact analysis and coordinated work proposal in the probationary phase and during the contract.

4. The mindset: a key factor of success

The best tool, the best committees and the best procedures will never replace 'willingness'. It is the responsibility of the various contracts' operational managers to get to know one another and **create and maintain a personal connection**, which is the guarantee of a successful collaboration for the client. In addition, it is the client's responsibility to promote this constructive mindset by **involving the different contracts' managers as far as possible in the actions undertaken within the client's company**: by creating this feeling of contributing to a common goal we can be sure of each party's collaboration.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Security Assurance Plan for SAAS and CLOUD services

"Name of the Service or of the Supplier"

Version	Creator	Approved by	Date
Version 1.0 FR	M. Ramtani Group CISO	F. Fromange Group IS Director	31 July 2014
Version 2.0	M. Ramtani Group CISO	P. Zembra Group IS Director	1 January 2018
Version 3.0	M. Ramtani Group CISO	P. Zembra Group IS Director	1 March 2019

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Contents

1. INTRODUCTION 3

1.1. *CONTEXT AND PURPOSE OF THE DOCUMENT* 3

1.2. *SCOPE* 3

1.3. *PERIMETER* 3

1.4. *AIMS AND RISKS* 4

2. GOVERNANCE AND ORGANISATION PRINCIPLES 4

2.1. *GOVERNANCE* 4

2.2. *OPERATIONAL PROCESSES* 5

3. PROTECTION RULES 7

3.1. *CONTINUITY OF SERVICE* 7

3.2. *COMPLIANCE WITH THE IT SYSTEM'S RULES OF USE* 8

3.3. *PARTNERSHIP THAT DOES NOT IMPLY THE USE OF THE PLASTIC OMNIUM IT SYSTEM PLASTIC OMNIUM* 8

3.4. *MANAGEMENT OF SECURITY INCIDENTS* 9

3.5. *CONFORMITY* 9

3.6. *DEVELOPMENT OF APPLICATIONS MADE AVAILABLE* 11

3.7. *MANAGEMENT OF RIGHTS AND ACCESS* 11

3.8. *DATA PROTECTION* 12

3.9. *MANAGEMENT OF TECHNICAL VULNERABILITIES* 13

3.10. *PROTECTION AGAINST MALICIOUS CODE* 13

3.11. *MONITORING AND CONTROL SYSTEM* 14

3.12. *MAINTENANCE AND UPDATING RULES* 14

3.13. *PHYSICAL SECURITY RULES* 16

3.14. *LOCATION OF DATA* 17

4. CONTROL RULES 17

6. GLOSSARY 19

6.1. *CLOUD COMPUTING* 19

6.2. *SAAS* 19

6.3. *IT HOSTING* 19

7. REVISION OF THE DOCUMENT 19

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

1. INTRODUCTION

1.1. *Context and purpose of the document*

The total or partial outsourcing of IT services serves to optimise the management of the IT system while responding to the expectations of the business lines, which require flexibility and responsiveness. Using external service providers also permits the management of hosting requirements to be delegated to experts who apply practices that could prove difficult to develop in-house.

The purpose of this document is to formalise the security clauses that have to be integrated into or associated with the following service subcontracting contracts:

- ✓ Cloud computing services (IAAS, SAAS, PAAS);
- ✓ The delegation of IT system services to a third party (partial outsourcing of the IT system);
- ✓ Basic hosting of IT infrastructure belonging to a Plastic Omnium Group entity or delegation of the operating of this infrastructure.

This Security Assurance Plan implementation policy is applicable in all Plastic Omnium Group entities. It may be supplemented, when necessary, particularly if:

- ✓ An entity faces IT system risk management challenges that are greater than expected or specific to its business line;
- ✓ Specific local legal or regulatory circumstances make adjustments necessary, particularly if specific rules on hosting data outside of the organisations' IT system have to be applied.

These security clauses must be applied by third parties (subcontractors, suppliers) to ensure the security of the Plastic Omnium Group's IT system.

1.2. *Scope*

- ✓ This document contains all of the security requirements of the Security Assurance Plan applicable to a mobility management service provision contract performed by the company, NOTILUS.

1.3. *Perimeter*

The perimeter concerns the service provided in hosted mode based on the solution, Notilus T&E.

This document lays down the security rules to be taken into account in the case of an outsourced IT service contract entered into with the company, NOTILUS.

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

1.4. *Aims and risks*

This Policy meets the following goals:

- ✓ Guaranteeing the consideration of security needs in facilities management or outsourcing contracts;
- ✓ Defining the respective roles and responsibilities of each person in light of these contracts;
- ✓ Making service providers and suppliers responsible for security requirements;
- ✓ Facilitating the identification and drafting of security clauses in contracts for project managers and the purchasing department.

2. GOVERNANCE AND ORGANISATION PRINCIPLES

2.1. *Governance*

EXT-G-01	Appointment of a security manager	Service provider / CISO
Plastic Omnium's service provider will appoint a Chief Information Security Officer (CISO) or, failing that, a security representative, for the services performed for or in cooperation with Plastic Omnium in order to guarantee the implementation of security measures that are applicable under the contract.		
Supplier's response: Notilus has named a CISO. You can contact our CISO who is also DPO at rgpd@dimosoftware.com. ***Measures implemented:***		

EXT-G-02	Appointment of a contract manager	Plastic Omnium
Plastic Omnium will appoint a manager for each outsourced IT system service provision contract. The contract manager acts as the interface between the service provider and the users of the service. Depending on the nature of the service, the contract manager may belong to the Information System division (hosting or delegation of infrastructure management) or to a business line division that uses the service (SaaS service).		
Supplier's response: Notilus will name an account manager to manage the relation between Notilus and Plastic Omnium. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-G-03	Use of subcontractors	Service provider
In the event the service provider were to use subcontractors to fulfil all or part of the service, the service provider shall remain responsible for the security of the entire service provided. Furthermore, all of the security rules applicable to the service provider also apply to its subcontractors. The service provider is therefore responsible for the activities and actions of its subcontractors.		
Supplier's response: Notilus is using providers to host the aplication (Visiativ mabaged services and Google cloud Platform) and for the long term legal archiving (arkhineo). Providers working with Notilus are certified ISO 27001 and respect the same security rules that apply to Notilus. ***Measures implemented:***		

2.2. *Operational processes*

EXT-O-01	Confidentiality of exchanges	Service provider
The service provider undertakes not to disclose any non-public information sent by Plastic Omnium, including when the relationship between the two parties is not yet or is no longer the subject of a contract. This requirement applies to all documents or information (technical, IT, commercial, financial, economic, social, etc.) as well as files, directories and E-mails. Use of this information for purposes other than the execution of the contract is forbidden.		
Supplier's response: All informations transmitted before, during and after the project are confidential. ***Measures implemented:***		

EXT-O-02	Encryption of exchanges	Technical teams / Service provider
Information is exchanged between Plastic Omnium and its service provider in accordance with a defined and formal method. The partner undertakes to respect the following procedures: ✓ Any sensitive data (considered to be confidential) exchanged must be encrypted regardless of the network used; ✓ This method is based on the use of cryptography tools that guarantee the confidentiality and integrity of the electronic messages exchanged in line with best practice in this area.		
Supplier's response: It's possible to use OpenPGP to sign and encrypt data exchanged. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-O-03	Monitoring of the service	CISO / Service provider
A committee will be created in order to monitor the service. This monitoring committee will be organised by the service manager within the Plastic Omnium Group. Security matters will be discussed on a regular basis by this committee. The partner will have to demonstrate, in particular, that the security measures are applied correctly by producing, for example, audit reports, balanced scorecards or action plans together with work schedules.		
Supplier's response: Security matters are reviewed during project meeting in the build phase and strategic meeting during the run phase. KPIs are produced for those commites including audit report or renewal certificate. ***Measures implemented:***		

EXT-O-04	End of contract and reversibility	Service provider
If all or part of the services or of the contract were to expire or be terminated, regardless of the reason, the service provider undertakes to: ✓ Avoid any interruption to or fall in quality of the services; ✓ Carry out operations that will give Plastic Omnium the control necessary to take back, or have a third party take back, the services (transfer of skills, explanatory documents, etc.) ; ✓ Securely return or, depending on the wishes of Plastic Omnium, destroy all of the equipment, documents or data that were entrusted to it during the period covered by the contract. More generally, the documents exchanged between the service provider and Plastic Omnium must be returned to their respective owners at the end of the contract.		
Supplier's response: Q.V. “Notilus - Réversibilité - v1.0_EN.pdf” ***Measures implemented:***		

EXT-O-05	Raising of awareness among employees	Service provider
The service provider ensures that the employees who are involved in the service provided for Plastic Omnium are informed of the IT systems’ security risks. The service provider shall take all measures necessary to ensure that the obligations mentioned in this document are respected by all those involved in the service.		
Supplier's response: All of Notilus employees are trained about security, training cycles and medium are managed by the CISO. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3. PROTECTION RULES

3.1. *Continuity of service*

EXT-I-01	Service commitments	Service provider
The service provider guarantees the availability of the service provided under the contract and the availability of the material and human resources necessary for the contract's implementation. The guarantees will cover, at a minimum: ✓ The rate of unavailability of the service, networks, applications provided, etc. ; ✓ The corresponding penalties; ✓ The restoral of service time guarantee in the event of an incident or a disaster.		
Supplier's response: Notilus guarantee 99% of service availability per month described on page 27_28 of the appendix « Notilus Charte TnE SaaS- V2.3_en-GB ». ***Measures implemented:***		

EXT-I-02	Continuity of service	Service provider
The service provider will present the measures implemented in order to guarantee the continuity of activities, in the event of a major incident, for the services that it provides to the Plastic Omnium Group (e.g.: hardware or site redundancy, degraded solutions, business recovery plan and associated processes, etc.). The service provider will describe, in particular, the means and guarantees implemented in order to ensure the continuity of essential services (energy, air conditioning, telecommunications) on its operating site: ✓ Situation and general characteristics of the operating site: ✓ Electrical protection and redundancy (generator sets, power inverters, protection against overvoltage, etc.); ✓ Service contracts with access suppliers, characteristics of the back-up connections; ✓ Air-conditioning systems; ✓ Monitoring equipment and alarm systems; ✓ Equipment used by the IT system, particularly redundant components (power supplies, discs, controller cards, servers, network equipment, network links). The service provider will communicate the frequency at which the continuity plan is tested as well as the results of the business recovery plan tests that have already been carried out		
Supplier's response: A continuity plan is in place and described in the document "Notilus Charte TnE SaaS- V2.3_en-EN.pdf ". ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.2. *Compliance with the IT system's rules of use*

EXT-I-03	Protection of identifiers	Service provider
The service provider shall only use the authorisations given to it on the IT system dedicated to Plastic Omnium for the purposes of its assignment. The service provider is therefore forbidden from: ✓ Disclosing any of its identifiers, even between departments; ✓ Using an identifier other than its own, in the event it had knowledge of another identifier; ✓ Deleting, hiding or modifying its identity or its identifier; ✓ Using its identifier to access applications, data or an IT account other than those that were allocated to the service provider or to which it has been given access authorization. The service provider protects its identifiers and connection authenticators. Any incident (loss, theft, disclosure, etc.) concerning its identifiers and connection authenticators must be immediately brought to the attention of Plastic Omnium's CISO.		
Supplier's response: All accounts dedicated to manage the hosting platform are nominative and reviewed quaterly. Regarding security incident a process to inform the customer in less than 48h is in place. Q.V. "RGPD 07012021 EN - Notilus TnE - PCD Protection Policy Amendment .pdf" ***Measures implemented:***		

EXT-I-04	Responsibility in the event of misuse	Service provider
In the event of any misuse by the service provider's employees, the service provider is responsible for any direct damage to the IT system dedicated to Plastic Omnium.		
Supplier's response: Agreed by the supplier. ***Measures implemented:***		

3.3. *Partnership that does not imply the use of the Plastic Omnium IT system Plastic Omnium*

EXT-I-05	No access to the Plastic Omnium IT system Plastic Omnium	Service provider
In the case of a service provision that does not require the use of Plastic Omnium's IT system, the service provider agrees not to access the IT system either voluntarily or accidentally. If the service provider were to access Plastic Omnium's IT system by accident, it agrees to: ✓ Immediately exit the system; ✓ Inform the contract manager as quickly as possible.		
Supplier's response: The platform Notilus T&E is saas and Notilus employees will not access to Plastic Omnium's IT system. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.4. *Management of security incidents*

EXT-I-06	Obligation to report security incidents	Service provider
In the event of a security incident experienced by the service provider or by one of its subcontractors, and likely to harm Plastic Omnium, the service provider agrees to inform Plastic Omnium's CISO as quickly as possible.		
Supplier's response: Q.V. "RGPD 07012021 EN - Notilus TnE - PCD Protection Policy Amendment .pdf" ***Measures implemented:***		

EXT-I-07	Insurance	Service provider
The service provider must be insured against the risks inherent to its activities and that could cause direct, financial or operational damage to the Plastic Omnium Group.		
Supplier's response: Notilus has an insurance against cyber risks. ***Measures implemented:***		

3.5. *Conformity*

EXT-I-08	Compliance with laws and regulations	Service provider
In general, the service provider shall undertake to comply with the laws and regulations applicable to the activities performed on behalf of the Plastic Omnium Group, particularly: ✓ The French data protection law (law no. 78-17 of 6 January 1978 (amended)). In particular, the service provider ensures the security of personal data by protecting this data from accidental or unlawful destruction, accidental loss, alteration and unauthorized access or dissemination. Furthermore, the service provider may not subcontract all or part of the services without Plastic Omnium's prior written authorization. ✓ The General Data Protection Regulation (GDPR) ✓ The protection of intellectual property and the protection of software (article L111-1 and L113-9 of the intellectual property code); ✓ IT fraud and cybercrime (law no. 88-19 of 5 January 1988 on IT fraud); ✓ Cryptology (order no. 98-101 of 24 February 1998 defining the conditions in which declarations are submitted and licences granted for encryption products); ✓ The law on day-to-day security of 15 November 2001 on the fight against terrorism and, in particular, the conservation of connection data.		
Supplier's response: We are fully compliant with laws and GDPR. Q.V. "RGPD 07012021 EN - Notilus TnE - PCD Protection Policy Amendment .pdf" ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-I-09	Compliance with standards	Service provider
Depending on the nature of the outsourced service, the Plastic Omnium Group may require its service provider to apply the security measures or requirements laid down by: ✓ Standard ISO 27002 regarding best security practices; ✓ Any other standard whose application is necessary for the fulfilment of the outsourced service.		
Supplier's response: Notilus (company and product) are certified ISO27001. Q.V. "Notilus Charte TnE SaaS- V2.3_en-EN.pdf ". ***Measures implemented:***		

EXT-I-10	Traceability of actions	Service provider
Plastic Omnium's service provider ensures that the actions that it carries out as part of the service provided for Plastic Omnium remain traceable. Plastic Omnium reserves the right to request, at any time, the tracking records of this service kept by the service provider, particularly those records that concern access to personal data.		
Supplier's response: All actions regarding connections, page access… are logged and stored during a year. An access for audit may be granted on dmeand. ***Measures implemented:***		

EXT-I-11	Certification of the service provider	Service provider / CISO
The service provider will specify any certificates that it holds for the area concerned by the services offered (e.g.: ISO 27001 certification). The service provider undertakes to maintain, throughout the entire duration of the contract, the criteria that enables it to meet the requirements of the certificates obtained. If the service provider were to lose its certificate, it agrees to notify Plastic Omnium as quickly as possible. The CISO of the Plastic Omnium Group will stipulate any certificates that are expected in light of the specific characteristics of the service.		
Supplier's response: Q.V. "Notilus Charte TnE SaaS- V2.3_en-EN.pdf ". ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.6. *Development of applications made available*

EXT-I-12	Compliance with best development practices	Service provider
During the provision of services based on applications developed by the service provider in-house, the service provider must ensure the security of the developments, in accordance with best practice, in each technology implemented. Regarding the implementation of web technology, developments will be able to draw on recommendations from the OWASP (Open Web Application Security Project). The service provider undertakes to respect a project quality plan that it will describe while specifying, in particular, the security measures that are taken into account at the following stages: ✓ Design; ✓ Development; ✓ Test; ✓ Documents; ✓ Maintenance. **In the event the service provider is unable to apply certain best practice rules, it must explain why it cannot do so to Plastic Omnium.**		
Supplier's response: Security is one of the main point in the development pipeline, security reviews are done manually and automatically (Sonar Qube OWASP plugin) and a pen test campaign is done yearly. If we loose the certification, an alert will be send to all our customers. ***Measures implemented:***		

EXT-I-13	Separation of production and development environments	Service provider
The service provider differentiates between the development, test, pre-production and production environments. The security measures of these environments are at least equivalent to those of the production environment if these environments have to use data from the production environment for development requirements.		
Supplier's response: Test and production environmment are physically separeted. ***Measures implemented:***		

3.7. *Management of rights and access*

EXT-I-14	Authentication and authorization obligation	Contract manager / Service provider
Outsourced services must comprise an authentication and authorization management system regardless of the sensitivity level of the data and of the functionalities offered.		
Supplier's response: An authentification is mandatory to access Notilus T&E regardless of the user habilitation. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-I-15	Operating rules regarding the management of rights and access	Service provider
Depending on the level of confidentiality of data handled by any application or outsourced service, functionalities that enable the management of rights and access to be implemented will have to be put forward. These functionalities will include, in particular: ✓ A possible interface with an external directory; ✓ The parameterisation of the password policy, including: ✓ Rules on the complexity of passwords; ✓ The maximum duration of the passwords; ✓ The number of unsuccessful access attempts before access is blocked. ✓ The provision of a functionality that allows the user to change his password; ✓ The possibility of allocating to a user a temporary password that has to be changed the next time he logs on; ✓ The parameterisation of user rights on the basis of profiles or roles while respecting the principle of least privilege; ✓ The definition and use of user profiles and administrator profiles (functional and technical); ✓ The possibility of easily verifying the rights allocated to users; ✓ etc.		
Supplier's response: We highly recommend to use SSO and delegate authentification to your idenity federation services. If you still want to use the integrated diectroy, you may choose the compelxity, legnth, duration, number of passwords stored… The user may change his password thorugh his profile and receive a new one by mail if he forgot it. It's possible for administrators to extract all rights allocated to users. ***Measures implemented:***		

3.8. *Data protection*

EXT-I-16	Data security rules	Contract manager / Service provider
Depending on the data's level of confidentiality, the service provider will specify the security measures implemented in order to guarantee the security of data while it is stored (e.g.: encryption in the database) and exchanged (e.g.: encryption of data flows).		
Supplier's response: All data flow are encrypted using HTTPS (TLS1.2) and SFTP (SSH), regarding data at rest, all backups are encrypted using AES256. Sensible fields in the database like passwords or IBAN are also encrypted in SHA512+salt or AES256 if decoding is needed or not. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-I-16B	Personal data security rules	Contract manager / Service provider
The service provider agrees to comply with GDPR requirements, particularly article 28 regarding the protection of personal data. The service provider will indicate, in particular, the security measures taken to guarantee the security of data when it is stored, processed and exchanged (e.g.: encryption of data flows).		
Supplier's response: Q.V. "RGPD 07012021 EN - Notilus TnE - PCD Protection Policy Amendment .pdf" ***Measures implemented:***		

3.9. *Management of technical vulnerabilities*

EXT-I-17	Technical vulnerabilities	Service provider
The service provider will describe the methods and means implemented to identify and deal with technical vulnerabilities. These vulnerabilities may concern the application environments developed, the operating systems or the software programs of the contract. The service provider will list the elements considered in its vulnerability management system. The service provider will specify the extent to which Plastic Omnium may be informed of the vulnerability test results.		
Supplier's response: Scan for vulnerabilites are done weekly using Cyberwatch and result are monitored by the hosting service and the CISO. ***Measures implemented:***		

3.10. *Protection against malicious code*

EXT-I-18	Protection against malicious code	Service provider
The service provider will describe the means implemented to fight against malicious code. As an anti-virus program is no longer sufficient, the service provider will describe the means implemented to fight against malicious code that is persistent and not detected by a traditional anti-virus program.		
Supplier's response: To fight again malicious code we are using three level of defense: a WAF, an EDR and an antivirus. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.11. *Monitoring and control system*

EXT-I-19	Monitoring and control of infrastructure elements	Contract manager / Service provider
The service provider will specify the measures taken to monitor the infrastructure, as well as the monitoring times (e.g.: 24/7). The service provider will outline the alert and incident management process based on the level of severity. It will list the elements that are monitored and the corresponding means, for example: • Monitoring and management of the performance of the network connection that provides access to the Plastic Omnium environment • Monitoring and management of the performance of the internal network equipment • Firewalls and Intrusion Detection and Prevention Systems (IDS/IPS)		
Supplier's response: A SOC is in place 24/7 to monitor the platform: network, security quipement (firewall, reverse proxy, IDS/IPS, WAF and EDR). ***Measures implemented:***		

3.12. *Maintenance and updating rules*

EXT-I-20	Compliance with publisher rules	Service provider
The service provider respects the recommendations of manufacturers and publishers with regards to the development and maintenance of the components of Plastic Omnium's IT system for which it is responsible. The solutions implemented by the service provider will have to integrate the latest security patches (systems, applications, etc.). Similarly, the service provider shall avoid technical solutions whose sustainability is not guaranteed by the manufacturer or publisher.		
Supplier's response: A chapter about components maintenance and security patch is described in our ISMS as recommended by ISO 27002. Q.V. “Dimo_Extrait_DDA_2020.pdf” ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-I-21	Validation of updates	Service provider
The service provider will present the test process that it shall implement before a version or a patch is delivered. While carrying out the update validation or roll-out tests, the service provider undertakes not to cause any disruption to the production environments. Except in the case of an exemption duly approved by Plastic Omnium, the test sets used must be anonymised. They must not contain any confidential information, such as personal data. Otherwise, an exemption request must be submitted to Plastic Omnium's Controller and CISO.		
Supplier's response: Database used for tests are automatically anonymised when restored. Before being deployed in production, a new release passed different steps: unit tests, non-regression tests, security tests and functionnal tests. The results will allow the go live. ***Measures implemented:***		

EXT-I-22	Maintenance operations	Contract manager / Service provider
The maintenance operations carried out by the service provider in the production environment (applying corrections, direct access to the databases) must only take place with the contract manager's authorisation. They must give rise to a detailed report that specifies the following: ✓ The operation's start and end time and date; ✓ The identity of the employees; ✓ The nature and outcome of the operation.		
Supplier's response: Notilus T&E is a Saas platform, customers will be informed of maintenance operations at least seven days before excluding security cases). Cuts are mainly done during the night from friday to Saturday at 23h00 GMT+1. ***Measures implemented:***		

EXT-I-23	Management of functional developments	Service provider
Any functional or technical developments must not call into question the service provider's compliance with the security requirements or compromise a reversibility operation. In the event of a development, the service provider will have to make sure that its implementation complies with the contractual requirements. Plastic Omnium reserves the right to ask the service provider to justify the development.		
Supplier's response: The functionnal roadmap is defined and managed by Notilus in accordance with customers and market need. To avoid difficulties when delivering the last release, all new functionnalites are turned off. It's the customer choice to activate them or no. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-I-24	Change management	Service provider
The change management process will have to be described by the service provider. At a minimum, the change requests will have to be tracked and monitored. Commitments will have to be made with regards to the changes' application deadlines.		
Supplier's response: The change management is included in the project management (including build and run). It's followed by the project toolkit containing tracking and KPIs. ***Measures implemented:***		

3.13. *Physical security rules*

EXT-I-25	Disaster prevention measures	Service provider
The service provider undertakes to implement measures that ensure the physical security of the premises used to host the equipment and/or data belonging to Plastic Omnium. The service provider will describe, in particular, the means implemented to ensure: ✓ The prevention, detection and handling of fires; ✓ Protection against water damage (the partner will also specify whether the buildings hosting the facilities-management infrastructure are located in a flood prone area).		
Supplier's response: Q.V. "DIMO Software Notilus Security Insurance Plan V3_en-GB.pdf" ***Measures implemented:***		

EXT-I-26	Security of physical access points	Service provider
The service provider must implement a solution that restricts access to the premises hosting the IT resources (servers, workstations) that shall be used to provide the service to Plastic Omnium only to those individuals who require access in light of their assignment: filtering of access to the buildings and/or floors, and filtering of access to the computer room. If necessary, the service provider will specify the access conditions for Plastic Omnium employees (opening times, case of occasional unavailability, etc.).		
Supplier's response: Q.V. "DIMO Software Notilus Security Insurance Plan V3_en-GB.pdf" ***Measures implemented:***		

EXT-I-27	Security of the hosting premises	Service provider
The partner will specify all of the means implemented to ensure the security of the hosting premises, particularly: ✓ Monitoring equipment, anti-intrusion devices; ✓ Access control and recording devices (security guards, airlock doors, identification solution, etc.) ; ✓ Devices for the physical protection of the equipment (locking of bays, etc.).		
Supplier's response: Q.V. "DIMO Software Notilus Security Insurance Plan V3_en-GB.pdf" ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.14. *Location of data*

EXT-I-28	Data location rules	Service provider
The service provider will specify the data's storage location or, failing that, the country (or countries) in which the servers hosting the data are located. If personal data is hosted, the service provider agrees to host this data in France or, at a minimum, in a European Union country. If the location of the data is to change, the service provider shall inform Plastic Omnium beforehand and obtain its written approval.		
Supplier's response: All data in Notilus T&E are stored in Europe. Cf. "Notilus Charte TnE SaaS- V2.3_en-GB.pdf" ***Measures implemented:***		

4. CONTROL RULES

EXT-C-01	Traceability	Service provider
Any application outsourced to a service provider must allow the following to be tracked: ✓ Access to the application (successful or unsuccessful); ✓ Actions performed within the application (consultation, modification); ✓ Administration operations (deletion of accounts, modification of rights, etc.) and maintenance operations. These tracking records will contain the following information at a minimum: User identifier, date/time, action performed (to be supplemented in accordance with needs). The service provider will provide Plastic Omnium with documents that will specify the maintenance operations connected to the tracking records generated (storage, back-up, etc.).		
Supplier's response: All accounts dedicated to administrate the hosting platform are nominative. All actions are logged and stored during a year. ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

EXT-C-02	Inspection and audits	CISO / Service provider
The Plastic Omnium Group reserves the right to have audits conducted in order to make sure that the user instructions and the security rules are correctly applied to the IT resources used to provide the outsourced service. The audit may be conducted by in-house auditors or by an external audit firm; it will be coordinated by the CISO of the Plastic Omnium Group. The audit may be performed after the service provider has been notified of the audit eight days in advance, unless there is an emergency, in which case this notice period may be shortened. This notice period enables the service provider to organise itself, gather the documents requested and ensure those concerned are available. If the audit's results reveal IT system security shortcomings for which the service provider is responsible, the latter shall immediately resolve these shortcomings at its own cost.		
Supplier's response: It's possible for customers to do an audit yearly, we aask to be informed at least 3 weeks before the start to sign a protocol agreement. If the audit is done by a third party, we are requested a PSSI certified one. Q.V. "Notilus Charte TnE SaaS- V2.3_en-GB.pdf" ***Measures implemented:***		

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

6. GLOSSARY

6.1. *Cloud computing*

Cloud Computing, generally known as “the Cloud”, refers to the means and processes that enable an organisation to use the computing power and/or storage capacity of remote IT servers through the Internet.

6.2. *SAAS*

SAAS (Software As A Service) consists of the provision of means, services and expertise that enable an organisation to fully outsource a given part of its IT System (messaging, CRM, payroll, etc.) and to consider this service as an operating cost rather than an investment.

6.3. *IT hosting*

A service managed by a specialist supplier whose role is to provide dedicated premises and support infrastructure (electricity, air conditioning, network, etc.) that can host all or part of the servers, data and applications of an organisation.

7. REVISION OF THE DOCUMENT

This policy is periodically revised every year to remain in step with any changes to the risks.

Confidential and Proprietary - © 2018 Plastic Omnium

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

PLASTIC OMNIUM

SUPPLIER CHARTER

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Preliminary remarks

In acceding to the Global Compact of the United Nations as from 2003, Plastic Omnium undertook to promote and support the fundamental principles of Corporate Social Responsibility (CSR) in the context of its activities.

Plastic Omnium's aim is to have all of its suppliers, service providers and sub-contractors (hereafter the "Suppliers") involved in this continuous improvement approach.

The objective of this Charter is to express the expectations of Plastic Omnium and its subsidiaries ("Plastic Omnium") with regard to its Suppliers (current or potential) in terms of CSR.

This Charter applies to all the Suppliers of Plastic Omnium and shall be a part of the documentation issued by Plastic Omnium in support of its consultations. It is also intended to be included in contractual documents.

By acceding to this Charter, the Supplier shall undertake to respect, implement and have respected and implemented all the principles set forth therein by its own suppliers, service providers and sub-contractors, in compliance with contractual provisions and applicable national legislations.

The Supplier shall undertake to setup within its organization the rules and procedures required for compliance with the commitments referred to in this Charter and to make regular assessments.

The commitments defined herein may not be interpreted in a manner that would modify those taken by the supplier in its commercial agreements concluded with Plastic Omnium.

I – Supplier commitments required by Plastic Omnium

1. Regulatory compliance

The Supplier must respect all the laws and regulations applicable in the countries where it conducts its activities.

Furthermore, it specifically undertakes to respect:

- The Universal Declaration on Human Rights of the United Nations and its two complementary pacts (the international pact relating to economic, social and cultural rights and the international pact relating to civil and political rights)
- The ten principles of the United Nations Global Compact;
- The Fundamental Conventions of the International Labor Organization (ILO) as well as the ILO Declaration relating to the fundamental principles and rights at work
- The OECD guidelines

as well as any other international, national or local convention, in addition to the applicable contractual provisions.

In countries which have not ratified these texts, the Supplier undertakes to make its best efforts to reconcile as far as possible with the principles of the Global Compact.

2. Integrity and Business ethics

The Supplier shall endeavor to conduct its activities in accordance with the principles of loyalty, integrity and equity.

2.1 Respect of competition law

The Supplier undertakes, on behalf of all its employees, representatives and affiliates, to conduct its activity in compliance with laws on competition and to take any precautionary measures to avoid any anti-competitive practices or conduct.

In particular, the Supplier undertakes not to participate in cartels fixing prices, agreements on quotas, production or sales and, more generally, any unfair practices which impede free competition, in particular those intending to

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

oust a competitor from the market or restrict access by new competitors to markets by unlawful means.

2.2 Respect of the laws and regulations that aim to fight against corruption and money laundering

The Supplier undertakes, on behalf of all its employees, proxies, representatives, affiliates and any person who renders services in its name, to conduct its activity in strict compliance with the laws and regulations which aim to fight against corruption and money laundering, in all the countries in which it is registered as a company or established and in which it conducts its activities.

The Supplier undertakes in particular not to solicit or accept, for itself or for its relatives, or propose or offer to any associates at Plastic Omnium and any individuals or legal entities with whom it has business relations, any gift, reward, benefit in kind or in expenditure, that would be of a nature to influence business relations.

The Supplier undertakes to operate transparently and in particular shall ensure that its books, registers and all accounts accurately reflect all payments concerning its transactions.

The Supplier shall ensure that any sub-contractor or other person affiliated therein, in the context of the performance of its contractual obligations with Plastic Omnium, works on the basis of a written contract, which sets or guarantees the same level of commitment with regard to the fight against corruption and money laundering.

The Supplier undertakes to establish and implement policies and procedures for the fight against corruption and money laundering. It shall control compliance by all its employees and proxies, as well as any individuals or legal entities with whom it has business relations.

2.3 Conflict of interest situations

The Supplier is in a conflict of interest due to a personal connection between him and the people involved in the purchasing process or likely to influence the business relationships with Plastic Omnium.

When the Supplier is confronted with a risk of a potential or recognized conflict of interest, it undertakes to inform Plastic Omnium without delay.

3. Human Rights and working conditions

The Supplier undertakes to respect fundamental rights relating to working conditions, in particular, with regard to:

- recourse to any form of forced or compulsory labor in all its forms
- use of child labor
- discrimination in terms of employment and working conditions
- equal pay
- trade-union freedom and the protection of union rights

in compliance with the fundamental conventions of the International Labor Organization.

The Supplier shall undertake not to have recourse to illegal work such as defined by the rules of the countries in which it is involved.

The Supplier undertakes to be up-to-date with declarative obligations required by social protection bodies and the tax administration, and to pay the duties and contributions due in this regard.

The Supplier undertakes to respect local legislation with regard to the minimum wage, pay a regular salary and pay overtime due to employees at the legal rate stipulated by the host country. It also undertakes to ensure its employees benefit from applicable legal benefits.

The Supplier undertakes to respect local legislation with regard to working time.

4. Protection of health and safety

The Supplier undertakes to create and maintain a healthy and safe working environment to ensure the avoidance of any risk of accident or occupational illness of its employees, sub-contractors, other persons in the vicinity and users of its products.

The Supplier undertakes to implement both a policy and all procedures necessary for identifying and preventing health and safety risks not only for its employees, but also for any stakeholders likely to be affected. It shall take any relevant measures to limit and, insofar as is possible, eliminate these risks.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

The Supplier undertakes to inform Plastic Omnium of any dangers or risks related to its products or interventions on Plastic Omnium sites.

It shall ensure the respect by its employees, providers and sub-contractors of the health and safety rules applicable at the time of their interventions on Plastic Omnium sites.

Plastic Omnium incites the Supplier to obtain the OHSAS 18 001 standard for the management of Health and Safety issues.

5. Protection of the environment

Plastic Omnium expects its Suppliers to limit their environmental impact by controlling disturbances and pollution related to their activities, by making reasonable use of natural resources and by developing responsible waste management.

The Supplier undertakes to retain and keep up-to-date all approvals required with regard to the environment.

The Supplier shall wherever possible avoid the use of toxic products. In cases where there is no alternative solution to the use of such products, the Supplier shall limit use and ensure that their handling and use do not represent a danger for individual health. Concerning any other dangerous substances, elements or dangerous waste, of which use is limited, the Supplier shall strictly adhere to the applicable legal provisions.

The Supplier undertakes to implement traceability of raw materials, materials or components necessary for the provision of services or goods.

Plastic Omnium encourages initiatives that help reduce environmental impact, in particular by the use of environmentally friendly technology and the obtaining of ISO 14 001 for environmental management and ISO 50 001 for energy management.

II – Follow-up and respect of the Supplier commitments

1. Follow-up and control

The Procurement Departments of the entities of the Plastic Omnium Group may, depending on the circumstances, take measures they deem necessary to ensure full compliance with this Charter, in particular by sending questionnaires or performing, or tasking third parties to perform, specific audits at the Suppliers and sub-contractors premises.

The Supplier undertakes to provide reasonable support and act diligently for the completion of these audits, in particular by providing, at first request, as soon as possible and in a substantiated and complete manner, all the information, clarifications or explanations requested by Plastic Omnium.

If applicable, the Supplier shall ensure effective cooperation and coordination with its own suppliers and sub-contractors.

2. Non-compliance by the Supplier of its commitments

In cases where Supplier, due to specific circumstances, is unable to respect certain provisions of this Charter, it is obliged to inform Plastic Omnium without delay in order to agree upon corrective measures to be implemented.

If the Supplier discovers that it has or is likely to have violated any one of the provisions of this Charter, it shall immediately inform Plastic Omnium and cooperate in any investigation undertaken by Plastic Omnium in this regard.

Any serious and willful non-compliance with the commitments set forth in this Charter shall constitute non-compliance with the Supplier's contractual obligations.

In this specific case, Plastic Omnium may automatically and without prejudice to any damages:

- request that the Supplier implement the required corrective measures within a given time period and/or
- depending on the severity of non-compliance, terminate all or part of the contracts and/or business relations with this Supplier on the grounds of wrongful non-compliance.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

PLASTIC OMNIUM

Approval and signature

I, the undersigned....Bobichon gilles

in the name and on behalf of .NOTILUS..... (Name of the Supplier's company),

accept and undertake to comply with this Charter.

Date:....28 Juillet 2022

First name, Last name: .GILLES BOBICHON

Position:....DIRECTOR..

Representative of the Company ..NOTILUS....

Signature

NOTILUS
561, Allée des Noisetiers
69760 LIMONEST
Tél : 04.72.86.01.90
RCS LYON : 877 912 691

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

REMINDER OF CERTAIN FUNDAMENTAL TEXTS

1- THE EIGHT FUNDAMENTAL CONVENTIONS OF THE ILO

- Convention no. 29 on forced labor of 1930, ratified in 1937;
- Convention no. 87 on trade-union freedom and the protection of trade-union rights of 1948, ratified in 1951;
- Convention no. 98 on the right to organization and collective bargaining of 1949, ratified in 1951;
- Convention no. 100 on equal pay of 1951, ratified in 1953;
- Convention no. 105 on the abolition of forced labor of 1957, ratified in 1969;
- Convention no. 111 on discrimination of 1958, ratified in 1981;
- Convention no. 138 on the minimum age for admission to employment of 1973, ratified in 1990;
- Convention no. 182 on the worst forms of child labor of 1999, ratified in 2001.

2- THE 10 PRINCIPLES OF THE GLOBAL COMPACT

Human Rights

1- Businesses should support and respect the protection of internationally proclaimed human rights in their sphere of influence; and

2- Make sure that they are not complicit in human rights abuses.

Labor

3- Businesses should uphold the freedom of association and the effective recognition of the right to collective bargaining;;

4- The elimination of all forms of forced and compulsory labor;

5- The effective abolition of child labor; and

6- The elimination of discrimination in respect of employment and occupation.

Environment

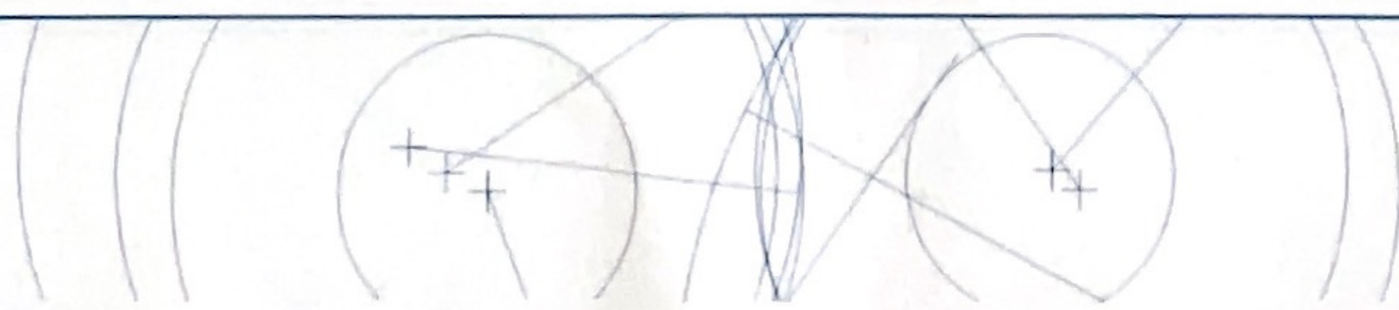
7- Businesses should support a precautionary approach to environmental challenges;

8- Undertake initiatives to promote greater environmental responsibility; and

9- Encourage the development and diffusion of environmentally friendly technologies.

Anti-corruption

10- Businesses should work against corruption in all its forms, including extortion and bribery.



DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

PERSONAL DATA PROCESSING CHARTER

Issued in accordance with Article 28 of Regulation (EU) 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.

In the context of the services entrusted under the **Contract**, the Customer ("the **Controller**") may entrust the Supplier ("the **Processor**") with the processing of personal data ("**Data**") on the Data Controller's behalf, in accordance with the provisions of Article 28 of Regulation (EU) 2016/679 of 27 April 2016 (the "**GDPR**"). In order to comply with the provisions of the GDPR, the Parties have agreed to enter into this charter (the "**Charter**").

PREAMBLE

1 PURPOSE

The Charter sets out the Processor's obligations in accordance with the provisions of Article 28 of the GDPR, in respect of any Processing carried out by the Processor on the Controller's behalf. The Charter forms an integral part of the Contract, in accordance with Article 7 below.

The Charter consists of this document and of the following annexes:

- Annex 1 Description of the Processing
- Annex 2 The Processor's Technical and Organisational Measures

Terms used in the Charter and beginning with a capital letter will have the meaning defined in Article 4 of the GDPR.

Thus, the term Processing means any processing of Data carried out by the Processor on the Controller's behalf pursuant to the services entrusted to it in the context of the Contract.

2 TERM

The Charter will take effect at the earliest from the date it is signed by both parties.

In the absence of any feedback from the Processor within thirty (30) days of the date of the Charter's transmission by the Controller, it will in any event be deemed to be agreed.

The Processor must comply with the provisions of the Charter throughout the period of the contractual relationship between the Processor and the Controller.

3 THE PROCESSOR'S OBLIGATIONS TO THE CONTROLLER

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.1 The obligation to have Technical and Organisational Measures in place specifically to protect the Data

3.1.1 In accordance with the provisions of Article 32 of the GDPR, the Processor undertakes to take any necessary precautions, having regard to the nature of the Personal Data and the risks posed by its Processing, to preserve the security and confidentiality of the Data, and, in particular, to prevent it from being distorted, damaged, or accessed by unauthorised third parties.

3.1.2 In this context, the Processor undertakes to complete Annex 1 of the Charter and to put in place and ensure the maintenance of any appropriate Technical and Organisational Measures of security and confidentiality and to list them in Annex 2 of the Charter entitled "The Processor's Technical and Organisational Measures".

3.1.3 The Processor undertakes to ensure that personnel authorised to process the Data for the purposes of performing the Contract, shall only have such access to the Data as is strictly necessary to carry out their functions, and shall undertake to observe the confidentiality of the Data.

3.1.4 Before making any substantial alteration to the Technical and Organisational Measures, the Processor must first inform the Controller, which reserves the right to make any observations and/or to refuse such alterations, giving reasons for its decision.

3.1.5 At the Controller's request, the Processor must be in a position to transmit documentary evidence that the Technical and Organisational Measures have been put in place – such as up-to-date certificates, reports or extracts issued by independent professionals (for example, external auditors, the internal audit department, an IT security department or quality auditors) – or to present adequate certification by means of an IT security audit or data protection audit.

3.2 The obligation to observe the Controller's power to give instructions

3.2.1 The Processor can only act in accordance with the Contract, and if applicable on documented instructions from the Controller to handle, correct, delete, lock or process the Data subject to Processing on the Controller's behalf.

3.2.2 The Processor undertakes to comply with the Contract and with the Controller's instructions relating to performance of the Charter. The Controller reserves a general right to give instructions regarding the nature, scope and method of processing of the Data, which may be supplemented by special instructions. The Processor can only transmit the Data to third parties or to Data Subjects with the Controller's prior written consent.

3.2.3 The Processor undertakes not to use the Data other than in accordance with the Charter and the Contract, and not to communicate them to third parties. It undertakes not to use the Data in any way on its own account, and not to use them in ways that are unfair, unlawful or contrary to the provisions of the GDPR. If the Processor is legally obliged to disclose the Data, it shall immediately inform the Controller.

3.2.4 The Processor must immediately inform the Controller if it thinks that any of the Controller's instructions is not compliant with the provisions of the GDPR. The Processor can then postpone performance of said instruction until it is confirmed or amended by the Controller.

3.3 The obligation to appoint a Data Protection Officer (DPO)

In accordance with Article 37 of the GDPR, the Processor must appoint a DPO, in writing when legally required. Any change in the contact details of the DPO must be communicated to the Controller.

3.4 The obligation to keep a record of Data processing

The Processor confirms that it keeps a record of all Processing carried out on the Controller's behalf, including the information provided for in Article 30(2) of the GDPR.

3.5 The notification obligation

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

In accordance with the provisions of the GDPR, the Processor is under an obligation to give notice in two cases:

- **In the event of an incident and/or Data Breach**

The Processor acknowledges that it has read Article 33 of the GDPR and that it is under an obligation to notify the Controller immediately of any incident and/or Data Breach, and to document them, regardless of their origin.

This notification obligation also applies to serious operational errors, to suspected breaches of the provisions relating to protection of the Data or to other irregularities in the Processing of the Controller's Data.

In agreement with the Controller, the Processor must take appropriate steps to secure the Data and as far as possible to limit the harmful effects on the Data Subjects.

The Processor also undertakes to provide the Controller with every assistance and with its full cooperation so that the Controller can report the Data Breach to the competent supervisory authority, and, if necessary, report it to the Data Subjects, in accordance with the provisions of the GDPR.

- **In the event of a request from the Data Subjects**

The Processor undertakes to immediately transmit to the Controller any request relating to the Data transmitted to it, and to do so no later than five (5) business days after receipt of such a request.

It is agreed that the Processor undertakes not to respond to such requests directly.

3.6 <u>The cooperation obligation between the Processor and the Controller</u>

In the context of the assistance and cooperation obligation provided for by Article 28 of the GDPR, the Processor undertakes to provide the Controller:

- With reasonable assistance to enable it to satisfy its obligations, particularly of a documentary nature;
- With the help necessary to enable the Controller to comply with its obligations arising in particular from Articles 32 to 36 of the GDPR (relating to security, notification of incidents/Data Breaches, Impact Analyses relating to data protection, and relations with the supervisory authorities);
- With assistance enabling the Controller to satisfy requests from Data Subjects who intend to exercise their rights in accordance with the provisions of the GDPR.

3.7 <u>The obligation to return and delete Data</u>

3.7.1 The obligation to return Data to the Controller

At the end of the Contract for any reason whatever, or at any time at the Controller's request, the Processor undertakes to return to it all documents, work carried out and the entirety of the Data processed and/or gathered in connection with the Charter and the Contract.

3.7.2 The obligation to prove the deletion of Data

The Controller can, at any time, require the Processor to provide evidence of the deletion of the Data.

It is also agreed that at the end of the Contract, the Processor will delete all the Data and provide evidence of its compliance with this obligation.

In the event that a legal obligation authorises the Processor to retain certain Data, documents, or any other information relating to the Data, beyond the period originally anticipated, the Processor undertakes to inform the Controller of the conditions in which such Data will be retained.

The Processor undertakes only to retain the Data for the period legally provided for that purpose. Upon the expiry of that period, the Processor shall delete the Data in accordance with the provisions of the Charter, the Contract and the GDPR.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.8 The obligation to provide information regarding the Data Processing location, and in the event of a transfer of the Data:

The Processor undertakes to inform the Controller of the location(s) where Processing of any nature (hosting, backup, maintenance, administrative management, support, etc.) will take place.

A list identifying the locations where Processing will take place on the date of entry into force of the Charter is attached in Annex 1 of the Charter.

In principle, the Processing entrusted by the Controller to the Processor must take place within the European Union.

On an exceptional basis, in the event that a transfer of Data outside the European Union is envisaged, notice of it must be given to the Controller in advance and it will be subject to the Controller's prior consent. If such a transfer is authorised by the Controller in advance, the Processor must then ensure that the transfer is covered by the guarantees provided for in Articles 45 to 49 of the GDPR.

4 THIRD-PARTY SERVICE PROVIDERS

The Processor can only sub-contract all or part of the Data processing services to third-party companies with the prior written consent of the Controller.

In the case of any service providers approved in advance by the Controller, the Processor undertakes to conclude contracts which contain the same obligations regarding the protection of the Data as are agreed between the Controller and the Processor.

The Controller will have a right to audit and supervise the third-party service provider in accordance with the Charter and the provisions of the GDPR.

The Processor guarantees compliance by its authorised third-party service providers with the Charter and with the Contract, and acknowledges that it is fully liable to the Controller for any failings by its authorised third-party service providers.

The Processor also undertakes to ensure that its authorised third-party service providers do not transfer the Data to a third country outside the European Union.

At the Controller's request, the Processor undertakes to provide it with information relating to the content of the sub-contract with the third-party service provider and its performance of its obligations relating to protection and processing of the Data, if necessary including checking the contractual documents relating thereto.

5 SUPERVISION AND AUDITING

The Controller is authorised to carry out inspections and audits (internally and/or with the appointment of an external auditor) at the Processor's place of business before Processing starts and then at regular intervals, subject to a maximum of one inspection per year, and subject to ten (10) days' notice being given.

The purpose of these inspections will be to verify whether the Processor is complying with Article 28 of the GDPR and the conformity of the Technical and Organisational Measures implemented by the Processor.

The Processor undertakes to contribute to the audit., and, at the Controller's or appointed auditor's request, to provide the information required to comply with the Controller's obligations relating to the processing of the Data, and to make available the documentation relating thereto.

No expenses will be reimbursed to the Processor by the Controller as a result of the audit.

6 LIABILITIES

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

The Processor undertakes to comply with all its obligations under the Charter.

The Controller will be entitled to terminate the Contract at any time if it finds that the Processor has breached any of the provisions of the Charter and/or any of its substantial obligations with regard to protection of the Data; one (1) month after service of a formal notice by registered letter with proof of receipt requested which has remained ineffective, and without prejudice to any action that might be taken by the Controller to obtain damages to compensate the loss suffered.

The Processor indemnifies the Controller against any claim made by a third party and undertakes to indemnify the Controller against any fine or judgment that might be issued against it. The Processor also undertakes to reimburse the Controller in respect of any costs or expenses that it might incur to defend itself in this respect.

None of the provisions of the Contract relating to the limitation of the Processor's liability will be applicable to the Processor's obligations under the Charter.

The Processor undertakes to take all necessary steps to help with the defence of the Controller in the context of any legal claim relating to the protection of the Data, or of any claim issued by a judicial or administrative authority.

The Processor undertakes to retain detailed documentation on the Processing and use of the Data, in order to enable the Controller to prove appropriate Processing and use of the Data to judicial and/or administrative bodies/authorities.

Even after the expiry of the Contract, the Processor will keep this documentation available for the Controller in the event that and insofar as the Controller has to defend itself against complaints from Data Subjects or any other third parties.

7 FINAL PROVISIONS

The Charter constitutes a written amendment to the Contract.

In the event of any inconsistency between the provisions of the Charter and any provision of the Contract, the provision of the Charter will prevail. All other provisions of the Contract which are not contradictory will remain in force in their current form.

All the provisions of the Charter expressly or impliedly intended to continue in force after the expiry of the Contract, in particular including the clauses relating to confidentiality, liability and indemnities, will remain applicable.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

List of Annexes:

Annex 1: Description of the Processing

Annex 2: The Processor's Technical and Organisational Measures

For the Controller	For the Processor
Signature:	Signature:
Forename, Family Name: Pascal ZEMBRA Function: VP Information System , Date: 29.09.2022	Forename, Family Name: Gilles BOBICHON Function: Chief Operating Officer, Date: 29.09.2022
pascal zembra	

ANNEX 1
DESCRIPTION OF THE PROCESSING IN ACCORDANCE WITH ARTICLE 28 OF THE GDPR

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

With reference to the Contract and the Personal Data Processing Charter referred to above, the Controller agrees to entrust the Processing of Personal Data to the Processor for the purposes of the Contract.

1. Principal and non-exhaustive purpose of the provision of services

For the record, the principal and non-exhaustive purpose of the provision of services by the Processor is as follows:

The contract is about the deployment of Notilus T&E, a platform dedicated to manage expense and travel.

2. Nature of the processing of personal data

The processing of personal data by the subcontractor is as follows:

The purpose of the platform is to reimburse expenses to employees and allow them to create bookings. To do so, the platform allow to collect, modify and consult personal data.

3. Categories of personal data:

Categories	**Data processed** (to be completed)
Identification (name, first name, date of birth, photo...)	Mandatory: Civility, identity, identification data, Contract execution period, Login, RLV (GDS), person identifier (number), sex, first name, surname, city birth, surname for travel, email addresses, business telephone details, employee category, traveller category, date of birth, business address, Logins, Person ID (Service Number), First Name, Last Name, Email Addresses, Password, Employee Category Non-mandatory: Middle name, maiden name, nationality, personal telephone details, residence address, national identity card, passport, visa, driving licence, ESTA, redress number, subscription and loyalty cards
Professional life (CV, diploma, position,...)	
Personal life (lifestyle, family situation,...)	Non-mandatory: Travel preferences, Emergency contact (entered by the traveller), Personal vehicle registration & Description (mandatory for mileage allowances)
Economic and financial information (income, , tax situation,...)	Bank details, Credit cards, Scanned expense receipts
Connection data (IP address, logs,...)	IP address, login date
Location data (movements, GPS data, GSM,...)	Business travel, spending location.
Sensitive data (health, genetic, biometric, sexual orientation, racial origin, trade union membership, religion, national identification number,...)	

Other (to be completed)	

4. **Categories of Data Subjects:**

☐ The Controller's customers
☐ The Controller's prospective customers
☒ The Controller's employees
☐ Suppliers, employees and partners
☐ Others: [to be completed]

5. **Geographical location(s) of the storage and Processing of the data entrusted by the Controller to the Processor (state the country or countries):**

All data are stored in France and managed in France, Germany and Belgium.

6. **Subsequent use by the Processor of subcontractors:**

Company name and registration number of any subsequent subcontractor	**Postal address of any subsequent subcontractor**	**Place of performance of the subcontracted services**	**Place of storage of the data processed (EU, or outside the EU)**	**Nature of the services subcontracted** (*e.g. hosting, maintenance, etc.)*
Google (OCR system)			Frankfurt & Bruxelles (Germany & Belgium)	Optical character recognition software
Visiativ managed services	Parc d'activité des, 5 Allée Du Crêt, Av. des Monts d'Or, 69890		La Tour de Salvagny – Vénissieux (France)	Hosting

	La Tour-de-Salvagny			
Arkhineo (Docapost Group)	24 Rue Drouot, 75009 Paris		Paris – Bordeaux (France)	Electronic Secured Safe for legal archiving purpose

7. Appointment of the Data Protection Officer

Please provide us below with information relating to your DPO, or if applicable, relating to the person responsible for matters relating to the Personal Data the subject of Processing:

Forename, Family Name: ……
E-mail: rgpd@dimosoftware.com.…

Any change in the contact details of the DPO must be communicated to the Controller.

ANNEX 2

THE PROCESSOR'S TECHNICAL AND ORGANISATIONAL MEASURES

The security measures are fully described in the Appendix 5 "PO Policy Security"

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Notilus

MOVING PEOPLE FURTHER

Cloud Charter Notilus T&E

Description & Operation

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Record of changes and validations

Date	Version	Nature of changes	Writer	Validation
20/03/2019	1.1	New charter	FDI, VMN	22/03/2019
19/4/2019	1.2	In-service support included	VMN	21/04/2019
27/05/2019	1.3	Service level table edited	CBG	20/06/2019
23/10/2019	1.4	RTO / RPO addition	FDI	23/10/2019
08/01/2020	1.5	In House server suppression + ISO certification update	FDI	08/01/2020
26/04/2020	1.6	SLA update	FPO	26/04/2020
08/09/2020	1.7	Support information update	DPD	08/09/2020
28/09/2020	1.8	Graphical charter update	DPD	28/09/2020
15/10/2020	1.9	Service level update	DPD	15/10/2020
03/12/2020	2.0	SaaS adjustment	DPD	03/12/2020
04/03/20201	2.1	BCP adjustment	DPD	04/03/2021
19/03/2021	2.2	HA infrastructure update	DPD	19/03/2021
29/09/2021	2.3	AI update	DPD	29/09/2021
16/12/2021	2.4	ISO27001 certificate update	DPD	16/12/2021

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Table des matières

1. Introduction 5

2. Client system 5

2.1 Service levels 5

2.2 Viewing and storing receipts and other documents 6

2.2.1 Storage of receipts 6

2.2.2 Legal archiving 6

2.2.3 Receipts consultation 7

2.3 Hosting location of customer data 7

3. Notilus T&E SAAS Architecture 8

3.1 Notilus architecture presentation at Visiativ Managed Services 8

3.2 General architecture diagram 10

3.3 Data exchange diagram 10

3.4 General flow chart 11

3.5 SFTP 12

3.6 Messaging 12

3.7 Notilus connection modes 13

3.7.1 Basic authentication 13

3.7.2 Identity federation WS-FED (IDP-Initiated) 13

3.7.3 Identity federation SAMLv2 (SP-Initiated) 13

3.7.4 Google OpenID Connect 13

4. ISO 27001 certification 13

4.1 What is ISO 27001? 13

4.2 Our goals 13

4.3 Certificates 15

4.3.1 NOTILUS 15

4.3.2 Visiativ Managed Services 17

4.3.3 ARKHINEO 17

4.3.4 Google cloud Platform 17

5. Notilus T&E SAAS operating model 18

5.1 Monitoring 18

5.2 Regular delivery of new versions 18

5.3 Hot maintenance 19

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

5.4 Business Continuity and Backup Policy ... 19
5.4.1 Service continuity ... 19
5.4.2 Data backup ... 19
5.5 Good practice guide ... 20
6. Notilus T&E SAAS security ... 20
6.1 Access management ... 20
6.2 Vulnerability and Intrusion Revenues ... 20
7. Audits and intrusion tests ... 20
7.1 Audits ... 20
7.2 Intrusion audits ... 21
8. MCO - Maintenance in Operational Conditions ... 21
8.1 Support ... 21
8.1.1 Composition ... 21
8.1.2 Languages ... 21
8.2 Scope of services ... 22
8.2.1 Adaptive maintenance ... 22
8.2.2 Corrective maintenance ... 22
8.2.3 Evolutive maintenance ... 22
8.2.4 Technical support ... 22
8.3 Our Missions ... 22
8.3.1 As a standard ... 22
8.3.2 Options ... 23
8.4 Operational functioning ... 23
8.4.1 Who can contact us? ... 23
8.4.2 How to contact us? ... 23
8.4.3 Receipt of a request ... 23
8.4.4 Consideration and Qualification ... 24
8.4.5 Hot incident management ... 24
8.4.6 Cold incident management ... 24
8.4.7 Closing ... 24
8.5 Definition of support and incident levels ... 25
8.6 Criticality of incidents and requests ... 25
8.7 Service Level Agreement (SLA) ... 28
8.7.1 Support service agreements ... 28

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.7.2 SaaS service engagement 29

8.8 Customer satisfaction 29

9. Termination of Service and Reversibility 29

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

1. Introduction

The purpose of this document is to provide a technical and operational description of the Notilus T&E SAAS service. It is intended for Notilus, its partners and customers.

Disclaimer: Notilus T&E is a Notilus registered trademark. All third-party trademarks communicated in this document are the property of their respective owners. Neither this document nor any part thereof may be communicated to a third party without the written permission of Notilus.

2. Client system

2.1 Service levels

The Notilus T&E SAAS service is composed of several levels to meet the different needs of our customers.

Function	Service level
Production environment	✔
Test environment	#
Additional environment (training...)	#
Storage of the data entered in the platform	Term of contract
On-line storage of receipts in EDM	✔ for 3 years plus the current year
Legal archiving of expenses reports receipts	✔ for 10 years
Storage of files on deposit directories	✔ for 30 days
Hosting location	EU
PGP encryption for import / export files	#
Possibility of audit, intrusion test (only in non-production environment)	#

Symbols: ✔ = included, # = Optional

At the deployment of the platform, a pre-production environment is made available to the customer. When production is launched, all the data entered during the pre-production phase is deleted (excluding parameterization and EDM/legal archiving), and this environment is then switched to production.
Optionally, you can request the implementation of a test environment.
Generally, the test environment is then installed after the switchover to production, and we restore a backup of the production database at a given time.
Three options are possible:

- TESTS NOTILUS environment, without automatic authentication, TRAVEL connection, interfaces, and ANALYSIS.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

- TESTS NOTILUS environment, with interfaces, and without automatic authentication, TRAVEL connection, and ANALYSIS.
- TESTS NOTILUS environment, with interfaces and ANALYSIS, excluding automatic authentication and TRAVEL connection

This environment is completely independent of the production environment.
If changes are made to the settings or interfaces or reports in the test environment, they must be carried over to the production environment.

NB: For the Travel module, the cohabitation of online or offline connections with return flows in test and production environments is to be validated with our partners. If necessary, additional services are to be provided to manage this double connection on the NOTILUS side.

2.2 Viewing and storing receipts and other documents

2.2.1 Storage of receipts

Expense receipts, downloaded via Notilus, are stored in the Notilus EDM.
By default, unless otherwise stipulated in the contract, they are kept for 36 months with a limit of 3Mb per file and up to 24Mb per active profile and per year (beyond that, additional fees will be charged).
At the end of the period, the documents can be downloaded by the customer as well as by an executable allowing the documents attached to the same expense report to be retrieved for a report number. This operation is invoiced.
The customer must be careful to request the documents before the end of the storage period. It is advisable to retrieve the documents at the end of each year to guarantee an exhaustive retrieval of the documents. It is not possible to retrieve a document beyond the 48 months of the Standard Storage Agreement or beyond the end of the Agreement.

2.2.2 Legal archiving

The SUPPLIER is setting up a process of Archiving with Probative Value in accordance with the Order of May 23, 2019 setting the terms of digitization of documents and documents prepared or received on paper in accordance with Article L. 243-16 of the Social Security Code.
The integrity of the supporting documents is guaranteed by an RGS 2* server stamp issued by a trusted third party. The Archiving at Probative Value is provided for a period of Ten (10) years at our partner ARKHINEO.
The proposed rate is fixed and includes a shared volume based on 24 MB per PA per year.
In case of overrun, a regularization will be made once (1) per year.
The consultation of the consumption of the Archiving Service with Evidential Value is accessible at any time by the CUSTOMER's Notilus administrator.
Billing will be established as soon as the Archiving Service is opened.

In case of termination of the Agreement the CUSTOMER has several options.

- The CUSTOMER wishes to keep a simple access to Notilus to allow consultation of the

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

documents archived at ARKHINEO, The SUPPLIER will maintain a restricted access (administrator profile only) to the Notilus database at a monthly rate of €1.50 excluding VAT x the number of existing APs, for a period of Twelve (12) months renewable => Advantage: consultation of the Data history via Notilus.

- The customer wishes to retrieve all the receipts archived at ARKHINEO. The client will be able to retrieve its documents archived at ARKHINEO, along with the sealing data, from its Notilus platform, until the date of termination. The supplier draws the client's attention to the fact that once the documents have been extracted from the ARKHINEO "safe", they will lose their Probative Value. For documents whose validity date in the event of a check is not exceeded, the customer must plan to archive them with another trusted third party.
- The customer wishes to continue to consult his documents archived at ARKHINEO, after the date of termination of his Notilus platform. The client will contact ARKHINEO to find out the access and financial terms and conditions. The latter will depend on the client's volume.

The archiving with probative value is the subject of an annexed contract.

2.2.3 Receipts consultation

Proof of expenses can be consulted via Notilus. Two modes of consultation are possible depending on the needs:

- Consultation of a copy of the receipts and data stored on our servers at each stage of the workflow and at any time depending on the user concerned (employee, controller, accountant, HR, etc.).
- In case of control, search, and consultation directly from Notilus by authorized persons of certified and archived PDF archive documents (internal audit, Urssaf control, tax audit, etc.).

2.3 Hosting location of customer data

Notilus chose multiple hosting/management partners:

- Visiativ Managed Services, a branch of the VISIATIV group, for hosting the platform. The main site is in La Tour de Salvagny (France) and the backup site in Vénissieux (France).
- ARKHINEO, as an electronic archiving system for the hosting of documents with probative value. The main site is in Paris (France) and the backup site in Bordeaux (France).
- Google Cloud Platform for AI services. The main site is in Frankfurt (Germany) and the backup site in Brussels (Belgium).

Notilus reserves the right to change its hosting provider while guaranteeing the quality of the service level and to remain within the European Union.

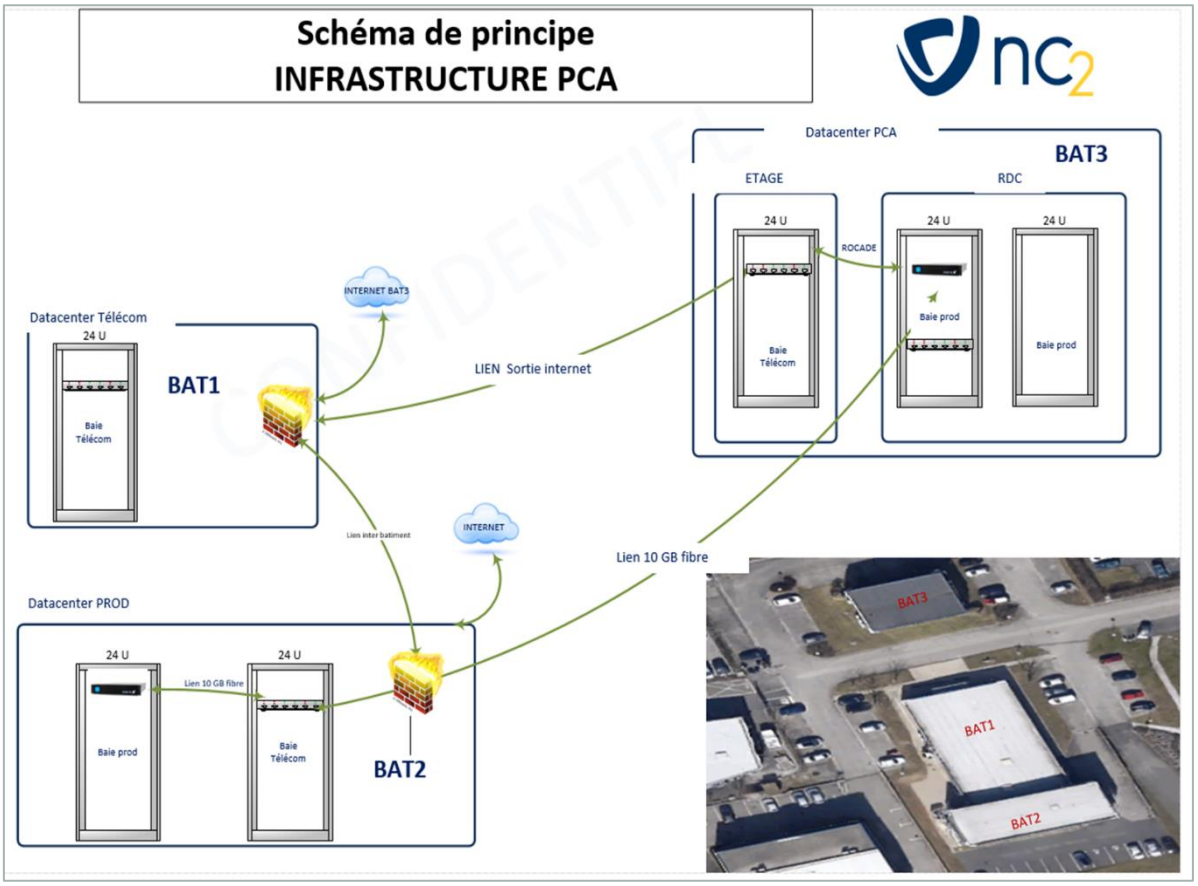
Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3. Notilus T&E SAAS Architecture

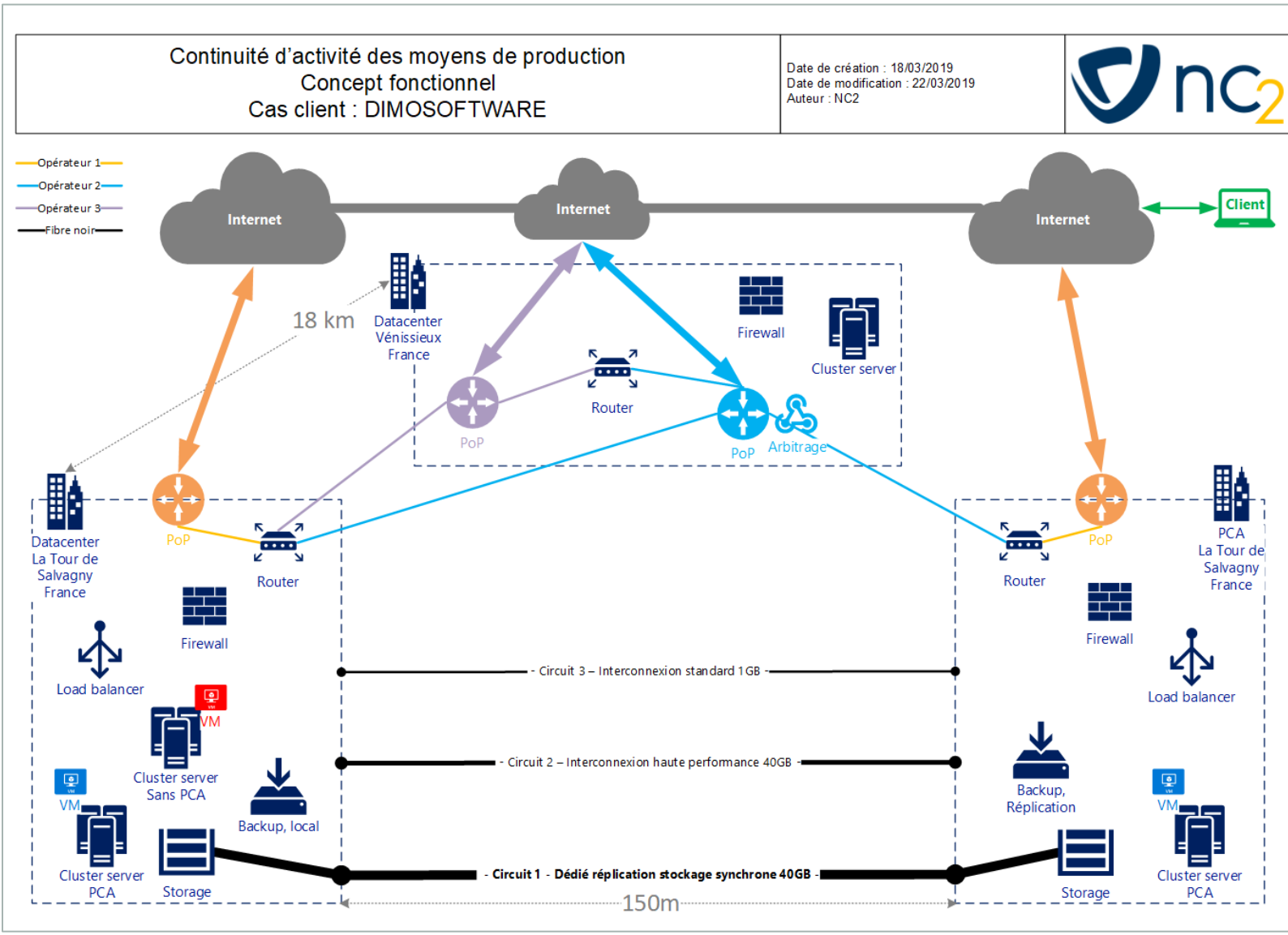
The Notilus software is designed for use in SAAS mode and runs on a modern and secure SAAS platform.
The design ensures that the application works well and completely securely when used on the Internet.

3.1 Notilus architecture presentation at Visiativ Managed Services



Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B



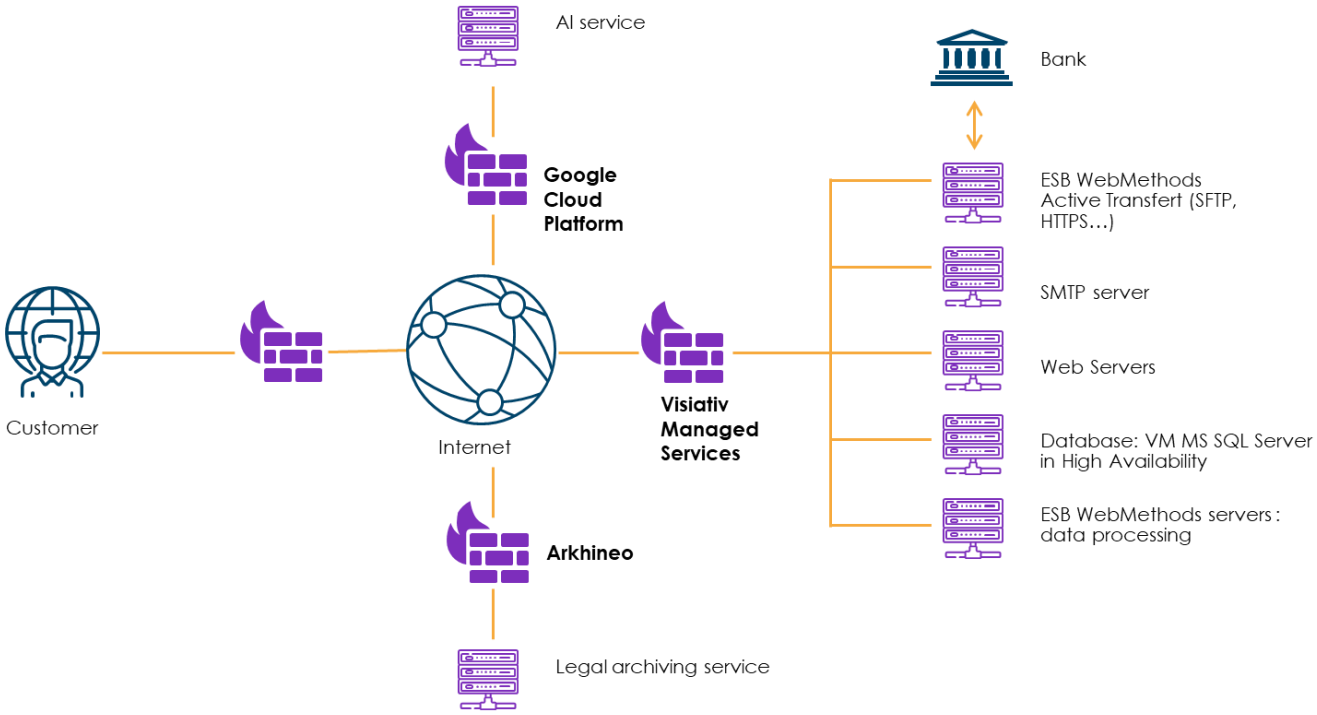
The Notilus T&E SAAS solution is designed to be scalable so that it can be scaled up as the load generated by customers increases. This ensures that performance does not degrade as more customers are added to the environment.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

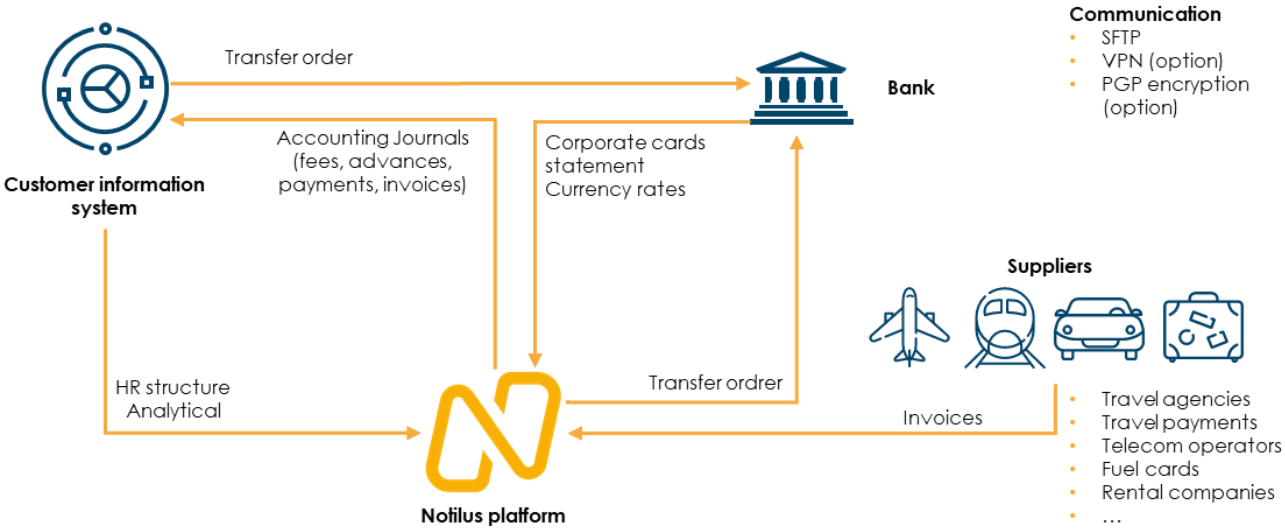
3.2 General architecture diagram

The following diagram shows the general architecture of the platform and the integration points.



- Users connect directly to our datacenter using the Internet in HTTPS.
- Exchanges with your information system are carried out by flat files. The protocol is SFTP.

3.3 Data exchange diagram



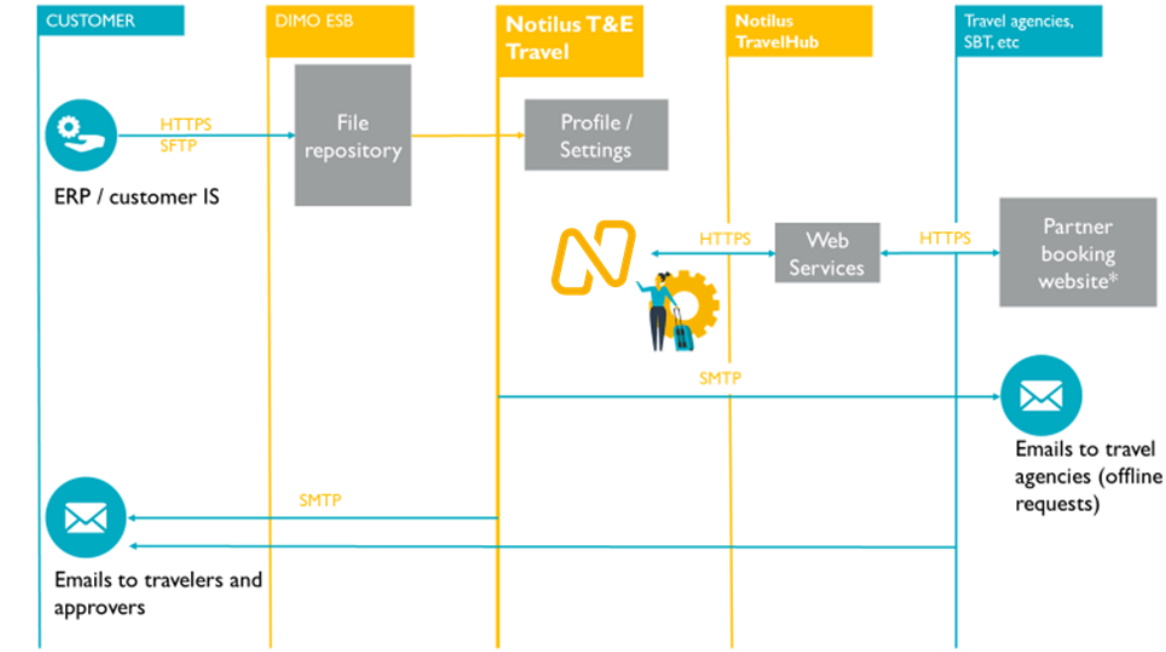
Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.4 General flow chart

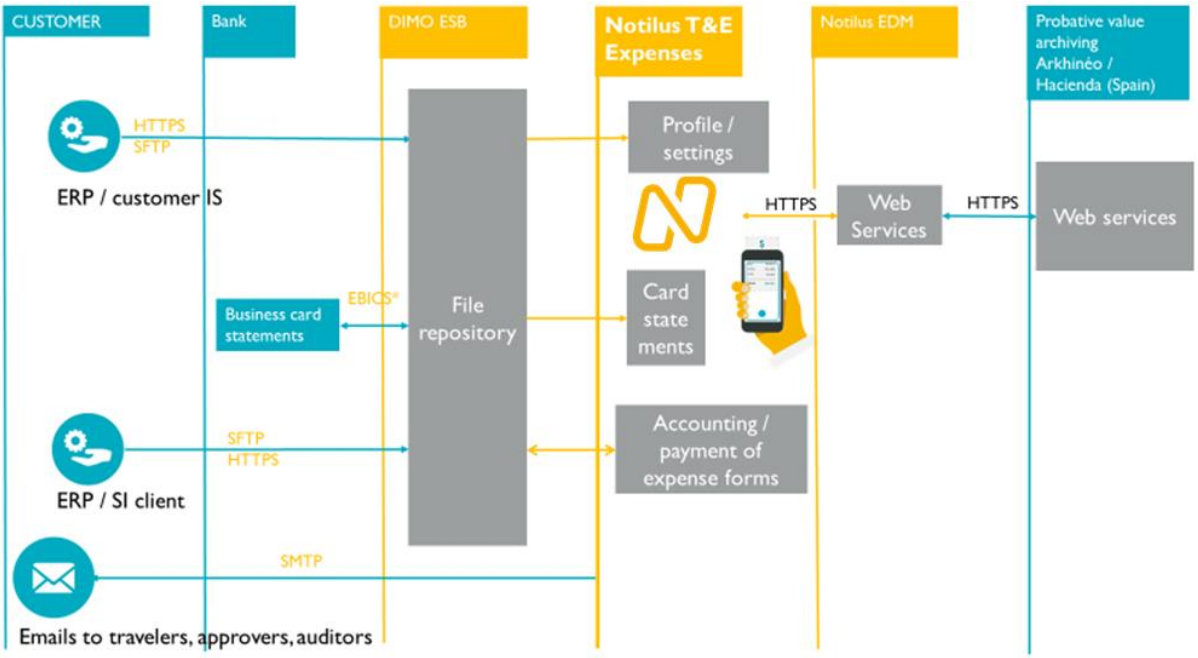
Notilus T&E SAAS supports the integration options shown in the diagram below.

For the management of travel and mission orders



* Communication with travel agencies and booking tools depends on partners, we recommend REST WebServices

For the management of expense reports

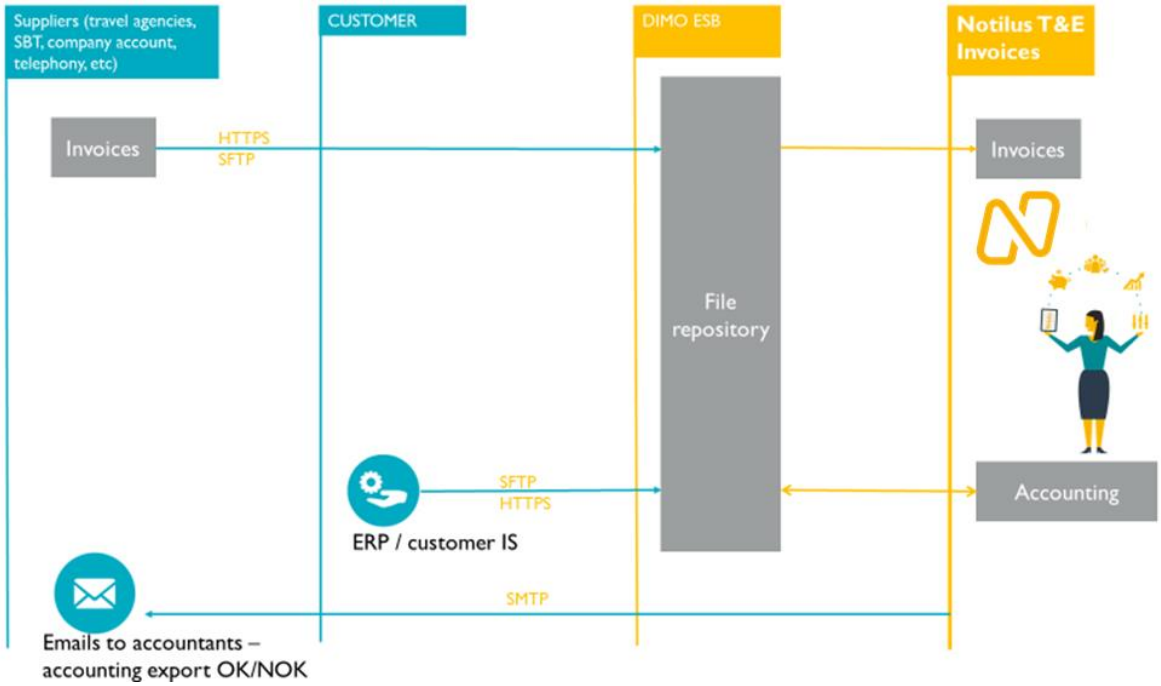


* Communication with banks depends on partner, we recommend EBICS

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

For invoice management



3.5 SFTP

Files are securely deposited (SFTP) by the client in the repository directory created for him. The automatic synchronization with NOTILUS T&E is adapted to the data types either:

- To the presence of the data file
- At a scheduled time
- When a commit file is detected

For all service levels, only files from an identified IP address (whitelist) will be processed.

3.6 Messaging

Notilus T&E will generate outgoing emails sent from the email noreply-notilus@mydimosoftware.com, to send booking requests to your travel agency, to inform travelers of the progress of their mission or trip and their expense report, to inform signatories and managers that action is expected from them and to follow up if necessary.

The recipients of the e-mails are travelers, signatories and their delegates, managers, and their delegates (advance managers, invoice managers, travel managers, etc.).

It is important that these emails are not "blacklisted" by the recipients' anti-spam filters.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

3.7 Notilus connection modes

3.7.1 Basic authentication

The login/password login credentials are managed by Notilus. This information is entered at the entrance of Notilus.

3.7.2 Identity federation WS-FED (IDP-Initiated)

Notilus can be connected to a compatible IDP via the WS-Federation protocol in IDP-initiated mode (e.g. ADFS: WS-FED in passive mode). The encryption of the authentication tokens between Notilus and the IDP is SAML V2. The implementation of the IDP configuration is the responsibility of the client.

3.7.3 Identity federation SAMLv2 (SP-Initiated)

Notilus can be connected to a compatible IDP via the SAML protocol in SP-initiated mode. The encryption of the authentication tokens between Notilus and the IDP is SAML V2. The implementation of the IDP configuration is the responsibility of the client.

3.7.4 Google OpenID Connect

Notilus can be connected to the Google OpenID connect authentication service which is based on the Oauth 2.0 protocol. The client is responsible for setting up the Google configuration.

⚠ **When using SSO login modes, it is imperative to provide Notilus support an access account on your directory.** This is necessary to allow them to connect for support and maintenance.

4. ISO 27001 certification

Notilus has been ISO 27001 certified for its Notilus SAAS offerings since 2015.
Similarly, our hosting provider NC2 is also ISO 27001 certified.

4.1 What is ISO 27001?

- An international standard for information security management
- A code of practice for information security management
- A basis for contractual relations
- A basis for third party certification
- May be certified by a certification body
- Applies to all industries and organizations of all sizes

4.2 Our goals

Within the framework of our ISO 27001 certification, we have chosen to prioritize the following objectives:

- Protect customer data

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

- Ensuring confidentiality
- Protecting integrity
- Ensuring the availability of client applications
- Protecting the heritage resulting from research and development

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

4.3 Certificates

4.3.1 NOTILUS

Bureau Veritas Certification

BUREAU VERITAS

NOTILUS

561 ALLÉE DES NOISETIERS
69760 LIMONEST
FRANCE

This is a multi-site certificate, additional site(s) are listed on the next page(s)

Bureau Veritas Certification Holding SAS – UK Branch certifies that the Management System of the above organisation has been audited and found to be in accordance with the requirements of the management system standards detailed below

ISO/IEC 27001:2013

Scope of certification

INFORMATION SECURITY MANAGEMENT SYSTEM DEDICATED TO NOTILUS SOFTWARE SOLUTIONS (BUSINESS TRAVEL AND EXPENSES) IN SAAS MODE AND ASSOCIATED SERVICES: RESEARCH AND DEVELOPMENT, SAAS OPERATIONS, CONSULTING, SUPPORT AND MAINTENANCE

SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION DÉDIÉ AUX OFFRES LOGICIELLES NOTILUS (VOYAGES ET FRAIS PROFESSIONNELS) EN MODE SAAS ET AUX SERVICES ASSOCIÉS : RECHERCHE ET DÉVELOPPEMENT, EXPLOITATION SAAS, CONSULTING, SUPPORT ET MAINTENANCE)

Statement of Applicability Version number and release date:
SOA version 18 of 08/09/2021

Original cycle start date:	**24 November 2015**
Expiry date of previous cycle:	**23 November 2021**
Certification / Recertification Audit date:	**07 October 2021**
Certification / Recertification cycle start date:	**24 November 2021**

Subject to the continued satisfactory operation of the organization's Management System, this certificate expires on: **23 November 2024**

Certificate No. *FR069761* *Version: 1* *Issue date: 23 November 2021*
Previous Certificate No. *FR050168*
Contract No. *10590572*

Laurent CROGUENNEC - President
Signed on behalf of BVCH SAS UK Branch

UKAS MANAGEMENT SYSTEMS 0008

Certification body address: 5th Floor, 66 Prescot Street, London E1 8HG, United Kingdom.
Local office: Bureau Veritas Certification France : 9, cours du Triangle - CS 40100, 92937 Paris-La-Défense Cedex – France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: ***+ 33(0) 1 41 97 00 60.***

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Bureau Veritas Certification

Appendix

NOTILUS

561 ALLÉE DES NOISETIERS
69760 LIMONEST
FRANCE

ISO/IEC 27001:2013

SITE NAME/LOCATION	SITE ADDRESS	SITE SCOPE
HEAD OFFICE	561 ALLÉE DES NOISETIERS 69760 LIMONEST FRANCE	INFORMATION SECURITY MANAGEMENT SYSTEM DEDICATED TO NOTILUS SOFTWARE SOLUTIONS (BUSINESS TRAVEL AND EXPENSES) IN SAAS MODE AND ASSOCIATED SERVICES: RESEARCH AND DEVELOPMENT, SAAS OPERATIONS, CONSULTING, SUPPORT AND MAINTENANCE SYSTÈME DE MANAGEMENT DE LA SÉCURITÉ DE L'INFORMATION DÉDIÉ AUX OFFRES LOGICIELLES NOTILUS (VOYAGES ET FRAIS PROFESSIONNELS) EN MODE SAAS ET AUX SERVICES ASSOCIÉS : RECHERCHE ET DÉVELOPPEMENT, EXPLOITATION SAAS, CONSULTING, SUPPORT ET MAINTENANCE) Statement of Applicability Version number and release date: SOA version 18 of 08/09/2021
SITE PARIS	56 BOULEVARD DE LA MISSION MARCHAND 92000 COURBEVOIE FRANCE	

Certificate No. FR069761 Version: 1 Issue date: 23 November 2021
Previous Certificate No. FR050168
Contract No. 10590572

Laurent CROGUENNEC - President
Signed on behalf of BVCH SAS UK Branch

UKAS MANAGEMENT SYSTEMS
0008

Certification body address: 5th Floor, 66 Prescot Street, London E1 8HG, United Kingdom.
Local office: Bureau Veritas Certification France : 9, cours du Triangle - CS 40100, 92937 Paris-La-Défense Cedex – France

Further clarifications regarding the scope of this certificate and the applicability of the management system requirements may be obtained by consulting the organisation.
To check this certificate validity please call: ***+ 33(0) 1 41 97 00 60.***

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

4.3.2 Visiativ Managed Services

afaq
AFNOR CERTIFICATION

Certificat
Certificate

N° 2013/55960.6

AFNOR Certification certifie que le système de management mis en place par :
AFNOR Certification certifies that the management system implemented by:

NC2 - NETWORK COMPUTER COMMUNICATION

pour les activités suivantes :
for the following activities:

ACTIVITES D'HERBERGEMENT ET D'INFOGERANCE CONCERNANT L'INFRASTRUCTURE (IAAS) OU LA PLATEFROME SYSTEME (PAAS) DE SYSTEMES D'INFORMATION, REALISEES EN DATACENTER INTERNE OU EXTERNE OU SUR LES INFRASTRUCTURES DU CLIENT. REALISATION DE PROJETS D'INTEGRATION.

DÉCLARATION D'APPLICABILITÉ DU 12 NOVEMBRE 2019

HOSTING AND OUTSOURCING ACTIVITIES CONCERNING THE INFRASTRUCTURE (IAAS) OR THE SYSTEM PLATFORM (PAAS) OF INFORMATION SYSTEMS, CARRIED OUT IN INTERNAL OR EXTERNAL DATACENTERS OR ON THE CUSTOMER'S INFRASTRUCTURES. IMPLEMENTATION OF INTEGRATION PROJECTS.

STATEMENT OF APPLICABILITY OF 12TH NOVEMBER 2019

a été évalué et jugé conforme aux exigences requises par :
has been assessed and found to meet the requirements of:

ISO/IEC 27001 : 2013

et est déployé sur les sites suivants :
and is developed on the following locations:

5, allée du Cret Pa des Monts d'Or FR-69890 LA TOUR DE SALVAGNY

Ce certificat est valable à compter du (année/mois/jour) 2019-12-16 Jusqu'au 2022-12-15
This certificate is valid from (year/month/day) Until

Franck LEBEUGLE
Directeur Général d'AFNOR Certification
Managing Director of AFNOR Certification

Flashez ce QR Code pour vérifier la validité du certificat

afnor CERTIFICATION

11 rue Francis de Pressensé - 93571 La Plaine Saint-Denis Cedex - France - T. +33 (0)1 41 62 80 00 - F. +33 (0)1 49 17 90 00
SAS au capital de 18 187 000 € - 479 076 002 RCS Bobigny - www.afnor.org

4.3.3 ARKHINEO

ARKHINEO's safety certifications are available at:
https://arkhineo.com/conformite/

4.3.4 Google cloud Platform

ARKHINEO's safety certifications are available at:
https://cloud.google.com/security

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

5. Notilus T&E SAAS operating model

5.1 Monitoring

Notilus T&E SAAS is monitored 24/7 to ensure service availability and performance and to detect possible service errors. Monitoring is divided into three areas: service level, application, and platform monitoring.

Service level monitoring

- services are supervised in real time by the supervision tools.
- Failures are reported as alerts to the operations team.
- Monitoring results are used for availability and performance reporting.

Application monitoring

- Application code is monitored for quality and security throughout the development process using static code analysis.
- Application behavior is monitored and analyzed using real-time log analysis. Alerts are used to detect anomalies and react proactively.
- Application performance is monitored for both user experience and document and data throughput.

Platform monitoring

- Real-time monitoring of shared infrastructure, operating systems, and applications
- Security monitoring includes vulnerability analysis, intrusion detection and information event management security.
- A PASSI certified SOC is in place 24 hours a day, 7 days a week.

5.2 Regular delivery of new versions

The application is regularly updated to the latest version of the NOTILUS T&E SAAS software. You will be informed of this update usually one month before the scheduled date. A documentation on the new features will be attached.

The new features are classified as follows:

Type of features	Description
Quiet improvement **(Delivered and activated as standard)**	Feature automatically implemented
Improvement to be studied! **(Delivered as standard and can be activated)**	Will require activation by the customer and/or communication to its users.
Requires support **(Delivered as standard and requires an analysis before activation)**	Requires the intervention of a Notilus consultant for its implementation

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Systematic updates are mandatory to guarantee the level of quality, service, and security of the software.

5.3 Hot maintenance

Notilus may need to perform maintenance between regular updates to maintain its level of service, in which case it will need to deploy important patches on critical bugs and security patches. The customer is always informed of these updates without any delay being required.

5.4 Business Continuity and Backup Policy

5.4.1 Service continuity

Data and applications are installed on HA (High Availability) dedicated hosts with 2 autonomous rooms in 2 separate buildings (see Diagram §3). This architecture allows real-time replication on both rooms, guaranteeing continuity of service in case of a major failure in one of the 2 rooms. Hot dedicated to software's and databases are different.
All our production servers therefore operate in BCP mode.

5.4.2 Data backup

Customer data is backed up and stored outside the data center.

Backups of the servers of the hosted platform are made by a specialized tool via agents installed on each server. This technology allows end-to-end encryption (AES 256) and is based on incremental block deduplication.
Backup jobs are performed daily according to the following backup plan:

- 1 daily backup available for 14 sliding days
- 1 monthly 12-month backup available for 365 sliding days
- Online restoration in https
- Usual retention on disk: 1 daily backup every business day, 1 encrypted set stored off-site in another datacenter.

Backup concerns all virtual machines: application servers and database servers.

Database backups are performed with maintenance plans, every night, in a dedicated backup environment. Transaction logs are backed up at 15-minute intervals for each database. The logging and full database backups allow restoring databases in case of crashes of client or server databases.

Databases are hosted in VMs and BCP storage arrays. In the event of a failure, the activity automatically switches to other nodes.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

5.5 Good practice guide

NOTILUS T&E SAAS relies on shared resources to serve end customers. To ensure good performance for all customers, Notilus has defined some usage rules such as:

- Scanned documents uploaded to the Notilus EDM are limited to 3 MB per file and up to 24 MB / Active Profile / year (beyond this limit, additional fees are charged).
- The formats accepted at the fee line level are only JPEG, PNG, PDF. Dangerous extensions such as .exe, .js, .bin, .bat, .vbs... are prohibited, as well as .TIFF .GIF .BMP images). Notilus Mobility users can scan their receipts directly from their smartphone.
- Direct access to the database with a system other than NOTILUS T&E is prohibited.

6. Notilus T&E SAAS security

6.1 Access management

Access management is the responsibility of the customer. When creating its environment, Notilus provides the customer with administrator access credentials that can then be used to control access to the application and related authorizations. When implementing an SSO connection, the customer will provide an account to Notilus teams to support the application.

6.2 Vulnerability and Intrusion Revenues

Vulnerability qualifications: Notilus performs its own vulnerability tests permanently on all exposed machines.
Intrusion tests: an independent security expert company performs external intrusion tests once a year, or more often if new publicly available components are added.
In both cases, Notilus does not share the results of these tests with its customers. Critical issues (that pose an immediate risk to customers' systems or data) will be classified as security incidents and resolved as quickly as possible, benefiting from development efforts as a top priority, while other issues will be dealt with as part of standard service maintenance and upgrades.

7. Audits and intrusion tests

7.1 Audits

Customers are entitled to audit the NOTILUS T&E SAAS service, subject to the following conditions:
The audit must be carried out by the customer or by a trusted third party bound by contract to professional secrecy. If the auditors are designated third parties, Notilus must be informed in advance and reserves the right not to approve the third-party auditor and therefore to deny access to conduct the audit.
The audit must comply with Notilus' audit security policies.
Only one audit per year may be performed.
Each party will be responsible for its own costs and time spent. An audit shall not take more than two business days at Notilus. Beyond two business days of Notilus' time, additional time will be charged at

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

the rate applied to the project manager's professional services.

7.2 Intrusion audits

Customers may perform or authorize third parties to perform vulnerability or intrusion tests on NOTILUS T&E SAAS environments, subject to the following conditions:
The customer must inform his Notilus customer service manager of the planned tests at least ten working days before the start of the tests. The customer shall specify the details of the planned revenues.
A test protocol must be signed between the parties and only one audit campaign may be carried out per year.
Notilus shall review the scheduled audit plan. Certain limits may be imposed by Notilus on validation efforts (including potentially invasive validations) to ensure the integrity of the overall production environment and continuity of service for other Notilus customers.
The audit must be performed by a competent party in accordance with industry best practices and applicable laws.
Audits for physical intrusion into the data centers used by Notilus are prohibited without prior authorization.

8. MCO - Maintenance in Operational Conditions

8.1 Support

8.1.1 Composition

The support team is made up of 22 people working on Notilus products, divided according to their specialization amongst different modules.

8.1.2 Languages

To cover the main languages of our customer contacts, support is available in English, Spanish and French.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.2 Scope of services

The Notilus Support service works in three areas of maintenance and one area of assistance:

8.2.1 Adaptive maintenance

It consists of providing:

- Assistance with the customer's dedicated contacts
- Access to the uses of the Notilus Expense / Travel platform
- Continuity of operation during upgrades of Notilus platform components and/or those interfaced with Notilus that are initiated by Notilus
- Upgrade management
- Maintenance operations

8.2.2 Corrective maintenance

It consists of ensuring:

- Corrective maintenance of the Notilus platform's application modules
- Associated assistance with the customer's dedicated contacts

8.2.3 Evolutive maintenance

This part concerns evolutive maintenance work carried out at the initiative of Notilus, such as security updates, as well as the associated customer support.

8.2.4 Technical support

Answers to administrators' questions about the use of the product are grouped together in the technical support mission. It covers functional, technical, and organizational issues.

8.3 Our Missions

Notilus support provides various assistance and maintenance missions for customers with different levels of involvement:

8.3.1 As a standard

- Support for your administrators on functional and technical issues.
- Monitoring and maintenance in operational conditions of your interfaces. The support team works in close cooperation with the hosting team in charge of the SaaS platform.
- Privileged contact for all issues related to the Travel / Mission Orders module (excluding pricing issues or navigation on the online booking portal). Support will manage the tripartite relationship with your travel agency and your SBT (Self Booking Tool).

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.3.2 Options

- ***TAM (third-party application maintenance)*** to benefit from personalized service with a dedicated contact person at your service throughout the support opening range.
- ***Specific developments*** according to your needs (reporting reports, mass integration of companies for example)

For this, we regularly exchange information by phone, email, and ticketing tool. All our answers are transcribed in the related ticket.

8.4 **Operational functioning**

8.4.1 Who can contact us?

The persons authorized to contact the support team are the functional or technical administrators defined by you during the project phase. They will have been trained by our consulting team in skill transfer mode to ensure their autonomy. End users can be called by the support on request of an administrator, but the opposite will not be possible. The customer always provides the first level of user support (Level 1).

8.4.2 How to contact us?

All tickets are entered into a tracking tool, regardless of their point of entry. This is a web portal accessible via the URL www.supportdimo.com and available in French, English and Spanish.
When you go into production, you will choose with your consultant which people are authorized to contact the support team. They will automatically receive their login IDs and passwords by e-mail.
Thanks to this tool, you can consult current or closed tickets, add information essential to the understanding of the context (files, texts...), carry out searches, trace the history of exchanges etc.
All status changes made to your tickets will be automatically notified to you by email.

If you have subscribed to the TMA option, you will have a Notilus Support contact dedicated to your company, who will personally handle all your requests and coordinate regular meetings with your departments to follow up on the actions to be taken.

8.4.3 Receipt of a request

The support service is open every French working day, from Monday to Thursday from 8:30 am to 6 pm (UTC+1) (5 pm on Friday). You can create your tickets 24 hours a day, 7 days a week on the customer extranet www.supportdimo.com. They will be processed as soon as the service opens.
The portal www.supportdimo.com is the request tracking tool (incidents, changes, assistance requests) used by the Notilus Support service.
Requests must describe as precisely as possible the need, the expected result, or the observed malfunction. Descriptive documents (screenshots, files, etc.) necessary for a proper understanding of the request must be attached whenever possible.
The level of urgency can be specified by the customer. It will be revised, if necessary, by Notilus

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Support after analysis.

8.4.4 Consideration and Qualification

The second level support confirms that the ticket has been considered at the ticket issuer, describing the first diagnosis in the case of an incident. It performs a first qualification to:

- Confirm or modify the severity level according to the intended definition (see Typology of criticality).
- Determine the need for referral.
- Analyze the problem.

The ticket is processed directly or forwarded to the next level up.

8.4.5 Hot incident management

The hot incident management procedure only concerns "Critical" or "Blocking" incidents. The correction of a hot incident consists in getting the application back up and running as quickly as possible. Either the malfunction is corrected directly, or a workaround is implemented.
NB: Support technicians are not authorized to modify the operation of the Notilus platform in depth. Their scope of intervention covers modifying application parameters, updating, and correcting data, restarting initialization processes, batch, or maintenance procedures.

8.4.6 Cold incident management

The cold corrective maintenance process includes the following main tasks:

- Functional and technical diagnosis
- Impact analysis
- Carrying out the correction
- Testing by the Provider
- Qualification (by the MOE) and Acceptance (if desired by the MOA)
- Upgrading of the documentation if necessary
- Planned delivery of the correction.

8.4.7 Closing

A ticket is closed when:

- An answer is given to the support request,
- Service is restored,
- An application modification is delivered to production.

The ticket is completed by describing the solution applied and delivered. If necessary, the documentation is updated before closing.
The closing of a ticket is not an end, but a status. If the error is reproduced, it can be reopened by the administrator from the portal www.supportdimo.com.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.5 Definition of support and incident levels

Level 1 (Customer support)

This is the internal customer support, made up of Notilus solution administrators, duly trained by Notilus Consultants during the deployment phase of the project.
They are the only people authorized to create tickets and to contact level 2 support (Notilus Support).

Level 2 (Notilus support)

Level 2 is made up of qualified technicians, specialized on the Notilus solution. They are in charge of considering, analyzing and resolving tickets. They establish telephone contact with Level 1 support if necessary.

Level 3 (Notilus business expertise centers)

Level 3 intervenes on complex incidents that Level 2 could not resolve. It consists of three areas of expertise:

- The Technical center (communication, security, interfaces)
- Travel / Mission Orders - Travel
- Expense - Invoice / Expense reports - Invoices

Level 4 (Notilus R&D)

Level 4 focuses on incidents requiring changes to the Solution. It is made up of product experts, functional designers, architects and software engineering experts.

Crisis unit

When a customer encounters a blocking problem and with agreement between the customer and Notilus, a crisis unit may be set up during the period necessary to resolve and/or implement a workaround.

8.6 Criticality of incidents and requests

All requests are classified according to a defined level of criticality in order to allow for processing within an appropriate timeframe. The first criticality is chosen during the creation of the request and will be modified if necessary, by the technician in charge.

Module	Functionality	CRITICAL	BLOCKING	MAJOR	MINOR
Advance	· Impossible to create an advance	NA	X		
	· Non mandatory field with an anomaly				X
	· Impossibility for a user to charge advances on expense reports · Incorrect automatic advance calculation · Mandatory field with an		If people impacted > 10	If people impacted > 1	If people impacted = 1

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

	anomaly · Information or registration of the form impossible				
Expense	· Impossible to create an expense · Impossible to approve an expense report	Access to Notilus impossible	X		
	· Non mandatory field with an anomaly				X
	· Non mandatory field with an anomaly · Impossible to send to the workflow		If people impacted > 10	If people impacted > 1	If people impacted = 1
EDM / Arkhineo	· EDM server KO	NA	X		
	· Impossible to attach receipts		If people impacted > 10	If people impacted > 1	If people impacted = 1
	· Unable to send receipts to Arkhineo				
Reporting	· Unable to run one or more reports · Unable to install/publish one or more reports · Unable to synchronize one or more reports	NA except Traveler Safety Alert Reporting	X		
	· Cube feeding impossible			X	
	· Incorrect data within a report				X
Interface (Import-export-Invoice)	· Interface in error and non-functional or generating empty file(s)	NA	X		
	· Expenses not accounted · Input file with incorrect data (invoice - HR) · Output file with incorrect data (advance, NDF, invoice, payment journal)			X	
	· Anomaly in the email notification				X
Connection	· Access to Citrix impossible	Access to Notilus impossible	X		
	· Access to Notilus impossible · KO referencing (email sending not possible from the application)		If people impacted > 10	If people impacted > 1	If people impacted = 1
Profile	· Profile synchronization not possible	NA	If people impacted > 10	If people impacted > 1	If people impacted = 1

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Travel	· Travel module inaccessible	Access to Notilus impossible	If people impacted = 1		
	· Creation of MO impossible · Problem entering an MO element		If people impacted > 1	If people impacted = 1	
	· Validation/refusal impossible for all MOs		From Notilus AND from emails	From Notilus OR from emails	
	· Problem sending Travel mail		If people impacted > 10	If people impacted > 1	If people impacted = 1
Online booking / Offline	· Cannot login or finalize online booking · Bookings non-integration · Non-compliance with workflow (approval/refusal/cancel)	Access to the SBT impossible	If people impacted > 1	If people impacted = 1	
	· Non-transmission of analytical axes to SBT · Distortion or non-transmission of information in mails/flows to the agency/internal service		If people impacted > 10	If people impacted > 1	If people impacted = 1

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.7 Service Level Agreement (SLA)

8.7.1 Support service agreements

Resource Commitment	Service level
Entry point	Web portal www.supportdimo.com : Access 24/24 – 7j/7
Concerned public	Notilus administrators only
Ticket processing schedules	From 8h30/12h30 to 14h/18h (17h on Friday) UTC+1, 5 days per week excluding French public holidays

Criticality	Consideration	Maximum processing time *	Product correction: patch or release)
Critical	1 hour	4 h	5 days
Blocking	2 h	8 h	R
Major	3 h	16 h	R
Minor	8 h	32 h	R
Evolution / Information	16 h	-	R

R: depending on the product roadmap (patches - 5 to 20 days and releases 1 to 3 months)

The above deadlines are calculated in working hours.

* Maximum processing time: in the case of the discovery of an anomaly requiring a correction of the product, the product will be reported to the R&D teams within the deadlines mentioned in column 3. The correction will be included in a cumulative Patch, or a Release (Notilus T&E only) according to the deadlines in column 4.
The times mentioned are maximum times (except in case of R&D correction: 4th column. The average processing time is usually half the maximum time.
For each criticality and each state of the ticket, Notilus Support ensures a minimum of 90% of tickets per category are processed, resolved and corrected within the specified time.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

8.7.2 SaaS service engagement

Engagement table

Resources engagement	Service level
Availability and monitoring of the application	7 days / 7 and 24h / 24
Application availability	99 % per month
Scheduled service interruptions	Maximum 4 working hours, planned at least 1 week in advance.
RTO (recovery time objective)	24H
RPO (recovery point objective)	8H

To achieve and comply with these objectives, all our technical means are covered by contracts with guaranteed service return time (DRG) within 4 hours.
Incidents are handled only during working hours.

8.8 Customer satisfaction

Our organization is built around customer satisfaction, and in order to measure its impact, we organize customer satisfaction surveys.

Monthly review 2019

- Average 9 /10 on 12 months;
- Recommendation rate: 90 %.

9. Termination of Service and Reversibility

In the event of service termination, all documents and associated metadata stored in the customer's systems can be exported by the customer using the application's export tool. The metadata will appear in a user-readable format (csv, XML). All Notilus services required in addition to existing functionality to assist the customer in exporting the data will be billed on a time and materials basis according to the Notilus Professional Services price list.
By default, Notilus agrees to provide a complete backup of the Notilus database.

Copyright Notilus – All rights reserved
Limited distribution

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Notilus rent in SaaS mode(*)			
OFFER		**Content**	
Rent **Hosting** **Maintenance** **Updates** **Support**	**Licenses & Technical infrastructure**	**Notilus Expense** **Notilus Decision** **Notilus Travel**	*Notilus Expense* *Notilus App* *Scan of receipts from Notilus app* *Technical infrastructure* *Credti card integration* *HTTPS* *Travel order / OnLine & OffLine booking* *Invoice Management* *Reporting*
Access to new version, correctiv			
POG will benefit. New conditio			
(**) : An active user is a person who submit at least one			
Monthly costs (without legal archiving)			
Sales discount Notilus client			
New cost per active profile			
New monthly costs (without legal archiving)			

Notilus options	
Notilus Invoice	**Invoice management import in Notilus (Airplus or other suppliers)**
Monthly costs	
Legal archiving	**Hosting with Arkhineo (legal archiving over 10 years with consultation of all receipts in Notilus).** **This option has to be defined according to the countries authorized to digitalize receipts**

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

36 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months
150 AP	**300 AP**	**350 AP**	**400 AP**	**450 AP**	**500 AP**	**600 AP**	**700 AP**
Price per active users (**) per month	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
7.30 €	5.51 €	5.22 €	4.88 €	4.54 €	4.53 €	4.18 €	3.96 €

e maintenance and support are included in the rent hereabove

ıns will apply upon CES full scope deployment

expense report per month.

1,095.00 €	1,653.00 €	1,827.00 €	1,952.00 €	2,043.00 €	2,265.00 €	2,508.00 €	2,772.00 €
22%	**22%**	**22%**	**22%**	**22%**	**22%**	**22%**	**22%**
5.69 €	**4.30 €**	**4.07 €**	**3.81 €**	**3.54 €**	**3.53 €**	**3.26 €**	**3.09 €**
854.10 €	**1,289.34 €**	**1,425.06 €**	**1,522.56 €**	**1,593.54 €**	**1,766.70 €**	**1,956.24 €**	**2,162.16 €**

Price per active users (**) per month	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
1,50 €/active profile	1,22 €/active profile	1,16 €/active profile	1,10 €/active profile	1,04 €/active profile	1,00 €/active profile	0,94 €/active profile	0,85 €/active profile
225.00 €	**366.00 €**	**406.00 €**	**440.00 €**	**468.00 €**	**500.00 €**	**564.00 €**	**658.00 €**

1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

36 months	36 months	36 months	36 months	36 months	36 months	36 months	36 months
800 AP	**900 AP**	**1000 AP**	**1200 AP**	**1500 AP**	**2000 AP**	**2500 AP**	**3000 AP**
Price per active users (**) per month	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
3.77 €	3.59 €	3.47 €	3.33 €	3.26 €	3.16 €	3.13 €	3.08 €

2,262.00 €	3,231.00 €	3,470.00 €	3,996.00 €	4,890.00 €	4,740.00 €	4,695.00 €	4,620.00 €
22%	**22%**	**22%**	**22%**	**22%**	**22%**	**22%**	**22%**
2.94 €	**2.80 €**	**2.71 €**	**2.60 €**	**2.54 €**	**2.46 €**	**2.44 €**	**2.40 €**
2,352.48 €	**2,520.18 €**	**2,706.60 €**	**3,116.88 €**	**3,814.20 €**	**4,929.60 €**	**6,103.50 €**	**7,207.20 €**

Price per active users (**) per month	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**	**Price per active users (**) per month**
0,81 €/active profile	0,78 €/active profile	0,75 €/active profile	0,71 €/active profile	0,69 €/active profile	0,67 €/active profile	0,65 €/active profile	0,63 €/active profile
648.00 €	**702.00 €**	**750.00 €**	**852.00 €**	**1,035.00 €**	**1,380.00 €**	**1,725.00 €**	**2,070.00 €**
1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile	1,20 €/active profile

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

36 months
3500 AP
Price per active users (**) per month
3.02 €
4,530.00 €
22%
2.36 €
8,244.60 €

Price per active users (**) per month
0,62 €/active profile
2,415.00 €
1,20 €/active profile

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Daily rate	Price/Day Project c Price/Day Project n

Level	NOTILUS attendee
Strategic	Project director, Account manager
Strategic	Project director, Account manager
Tactical	Project director, project manager
Operational	Project manager, Consultant
	Services sub-total

Notilus governance

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

director
manager

NOTILUS EXPENSE & DECISION services

[G] Strategic Committee - Initialization and review
A kick-off meeting, which presents the project(s) and sets the objectives;
A "Review and Outlook" feedback meeting, scheduled after the switchover to production, to review the project, report on the inventory and the recommendations made, and to launch the second phase, "running phase".

[G] Strategic Committee - Quarterly frequency
An operational management level focused on service to beneficiaries and stakeholder satisfaction, guaranteeing the optimization of resources and operational excellence.

[G] Tactical Committee - Monthly Frequency
A tactical management level that guarantees the respect of NOTILUS' contractual commitment and the permanent improvement of the quality of service, driving the development of value in response to the customer's challenges.

Operational Committee - Weekly Frequency
A strategic steering level that pilots the alignment of the proposed system with the client's challenges and in particular its development.

project total costs

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

	1,000.00 €
	900.00 €

Recommended services	
NOTILUS estimated workload	Price excl.tax in €
Unit load	
3.0	3,000.00 €
Quarterly load	
1.5	1,500.00 €
3.0	3,000.00 €
9.0	8,100.00 €
13.5	*12,600.00 €*

Recommended services
Price excl.tax in €
12,600.00 €

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Project phases	Consulting services - NOTILUS EXPENSE & DECISION : Pilot core model France		Estimation In number of days	Price in € excluding taxes	Options	Planning in week
Migration package of France Notilus Base	Migration package		offered	-		All project
Conception	Project management team		Flat fee	900.00 €		All project
	Functional analysis		1.0	900.00 €		W1-W4
	Functional analysis report		1.0	900.00 €		W4-W5
Installation	Notilus installation and report		flat fee	450.00 €		W1
Installation	Test platform installation (with interfaces)		flat fee	750.00 €		W1
Realisation	Assistance for settings (based on skills transfer)		3.0	2,700.00 €		W6 -> W12
Integration	HR interface already used in France by POG (the specifications of this interface need to be exactly the same)	HR interface with Success factor (establishments, cost centers people, users, signatories, approvers)	flat fee	750.00 €		W7 -> W12
	Incoming STANDARD interfaces (for each version of SAP/other ERP): analysis, report, development, tests, installation, automatisation and validation	Internal Code" interface (project code, client code, …)	flat fee	450.00 €		W7 -> W12
		Exchange rates interface (file from SAP)	flat fee	450.00 €		W7 -> W12
	Credit cards file : collect and integration	Per each bank file referenced in Notilus (mostly BNP)	flat fee	900.00 €		W7 -> W12
	Outcoming STANDARD interfaces (for each version of SAP/other ERP): analysis, report, development, tests, installation, automatisation and validation	Standard Accounting interface (expense report)	flat fee	450.00 €		W12 -> W15
		Standard Accounting interface (Advance Management)	flat fee	450.00 €		W12 -> W15
Validation	Check of the good running of the software	"Test group" training for CES (8 people maximum, trained on a half day)	1.0	900.00 €		W13 -> W17
		Feedback and adaptation of the parameters	1.0	900.00 €		
Deployment	Change management support	"Internal Support Team" training (8 persons trained per half day) for using if different from "Test group"	1.0	900.00 €		W18 -> W19
		User guide adatpation (if needed in french, standard guide are provided during the project)	1.0		900.00 €	
Reporting DECISION	Installation of Notilus analysis		flat fee	200.00 €		W1
	Training to Notilus analysis (data cube). 1 training session of half a day for 8 persons maximum		0.5	450.00 €		W25 -> W26
TOTAL Consulting services EXPENSE & DECISION			17.5	13,400.00		

Project phases	Additional options		Estimation In number of days	Price in € excluding taxes
Installation	SINGLE SIGN ON (analysis, report, installation and tests)		flat fee	900.00 €
Integration	Outcoming/Incoming STANDARD interfaces (If different from the pilot one): analysis, report, development, tests, installation, automatisation and validation	Intefaces to be define (examples : Custom interface, Trainings,...)	to be defined after the analysis	

Bank integrated :	AIRPLUS
	AMEX
	BANQUE POPULAIRE
	BBVA
	BNP
	CIC
	CITIBANK
	CORNER
	CREDIT DU NORD
	CREDIT MUTUEL
	HSBC
	SOCIETE GENERALE
	SWISSBANK
	UBS

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Phases deployment	Deployment pr
Project management	**Project management to deploy**
Conception	**Functionnal analysis workshop & report**
Realisation	**Assistance for settings** (depending on your optional, as you will have been trained in consider this type of configuration only for
	Functionnal deployment
Country interface options	**Incoming standard interface** ***(if different from the pilote core model)***
	Outgoing standard interface ***(if different from the pilote core model)***
	Incoming HR custom interface ***(if the same interface is needed for several countries on the same Notilus environment, the cost would be unique)***
	Outgoing accouting custom interface ***(if the same interface is needed for several countries on the same Notilus environment, the cost would be unique)***

Translation costs (other than english, french,
1500€/new language + annual maintenance co

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

ice per new country	Notilus estimate
	flat fee
	1.0
ability to set up, this type of service may be the administration of Notilus. We could therefore the first country)	2 days per country (to be adjusted with the project manager following the analysis & needs you may enhance)
costs	**3,600.0**

Notilus interfaces if applicable	
presentation, tests, installation, automatisation & validation	*flat fee*
presentation, tests, installation, automatisation & validation	*flat fee*
Analysis, development, tests, installation, automatisation & validation	flat fee
	flat fee

spanish, italien, dutch, portuguese, polish, german)
osts 300€/language

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Price in € excluding taxes
900.00 €
900.00 €
1,800.00 €
0 €

450.00 €
450.00 €
1,800.00 €
2,700.00 €

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Phases of the projet	Consulting service - NOTILUS TRAVEL: Pilot core model France		Estimation in nbr of days	Price in € excludding tax
Project Management	Project management team		Flat fee	1,800.00 €
	Start meeting		1.5	1,350.00 €
Conception	Functional analysis		1.0	900.00 €
	Functional analysis report		1.0	900.00 €
Installation	ON LINE : Installation of NOTILUS Travel Hub, test of the connection NOTILUS/OBT		Flat fee	1,350.00 €
Realisation	Assistance and training for settings		2.0	1,800.00 €
	ON LINE : Setting and test of the connection NOTILUS/EGENCIA		2.0	1,800.00 €
	OFF LINE: setting and test of the connection NOTILUS/TMC		Flat fee	450.00 €
Integration	Test of all exchanges		1.0	900.00 €
Validation	Check of the good runing of the software	"Test group" training (8 people maximum, trained on a half day)	1.0	900.00 €
Deployment	Creation of userguides (create and control of a travel request, reservations management)		1.0	900.00 €
	"Internal Support Team" training (8 persons trained during 1 day) for administration		1.0	900.00 €
TOTAL Consulting services TRAVEL per TMC/OBT			10.0	###########

Project phases	Consulting service - NOTILUS TRAVEL: New country online & offline connexion with new OBT	Estimation in nbr of days	Price in € excludding tax	Option
Project Management	Project management Actions necessary for the proper conduct of the project, and to be adjusted according to your needs.	Flat fee	900.00 €	
Conception	Functional analysis workshop	1.0	900.00 €	
	Writing of functional specifications	flat fee	900.00 €	
Realisation	Assistance and training for settings (only if administrated locally)	2.0		1,800.00 €
Installation	Implementation & Test of the OBT - Coordination with the TMC and/or the OBT for the implementation - Setting up and testing of the NOTILUS/OBT connection - Validation of flow exchanges from a technical point of view, according to established scenarios	flat fee	1,800.00 €	
Installation	Adjustment & Acceptance of the NOTILUS/AGENCY/CONNECTOR/your project team functional setu - Validation of the functional configuration and information exchanged, according to established scenarios (synchronization of the traveler's profile, reservation, order, modification, cancellation).	2.0	1,800.00 €	
TOTAL Consulting services TRAVEL per country and/or OBT		5.0	6,300.00 €	

Project phases	Consulting service - NOTILUS TRAVEL: New country offline connexion or same OBT (if only an offline connexion is possible)	Estimation in nbr of days	Price in € excludding tax
Project Management	Project management Actions necessary for the proper conduct of the project, and to be adjusted according to your needs.	Flat fee	450.00 €
Conception	Functional analysis workshop	0.5	450.00 €
	Writing of functional specifications	flat fee	450.00 €
Installation	Offline Implementation - Coordination with the TMC - Validation of flow exchanges from a technical point of view, according to established scenarios	flat fee	450.00 €
Installation	Adjustment & Acceptance of the NOTILUS/AGENCY/CONNECTOR/your project team functional setu - Validation of the functional configuration and information exchanged, according to established scenarios	1.0	900.00 €
TOTAL Consulting services TRAVEL per country and/or OBT		1.5	2,700.00 €

We consider for the deployment of new countries to rely on the admin we trained during the pilot phase

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Projet phases	CONSULTING SERVICE - NOTILUS INVOICE: CES PER REGION	Charge DIMO estimée	Base (prix net HT en €
Conception	**Functional analyses**	**0.5**	**450.00 €**
	Functional analyses report	**0.5**	**450.00 €**
Réalisation	**Setting and training based on skill transfer**	**2.0**	**1,800.00 €**
Intégration	**Incoming Interface Airplus - Analysis, report, develoment and test**	**Flat fee**	**1,800.00 €**
	Standard Accounting interface: Invoice Management Analysis, report and tests	**Flat fee**	**450.00 €**
TOTAL Consulting Service Invoice		**3.0**	**4,950.00 €**

Notilus interfaces if applicable			
Country interface options	**Incoming standard interface per provider** ***(if different from the pilote core model)***	*Flat fee*	*1,800.00 €*
	Outgoing standard interface ***(if different from the pilote core model)***	*Flat fee*	*450.00 €*

APPENDIX 3: IN-SERVICE SUPPORT

Availability

Department *	Availability
Web portal www.supportdimo.com	Accessible 24/7
Ticket handling times (working hours)	8:30 a.m. to 12:30 p.m. and 2 p.m. to 6 p.m. (5 p.m. on Fridays) UTC+1, 5 days a week, excluding French public holidays

*Notilus Support services are exclusively accessible to Notilus administrators who have received the appropriate training and been declared by NOTILUS teams.

All perimeter which belong to SLA including criterias listed in handling times and description of detailed service level are also applicable to POG and will be reported once per year in one shared POG and Plastic Omnium SLA report by Notilus in order to track their level of service performance, in consequence with penalties mechanism-referred to this appendix.

Handling times

Criticality *1	Maximum acknowledgement time	Penalties to take into consideration the acknowledgment time	Average handling time	Maximum handling time *2	Product correction (patch or release)	Penalties to take into consideration the handling time	Base
Critical	1 hour	1% per hour late	2 hours	4 hours	5 days	1% per hour late	Maintenance & Support
Blocking	2 hours	0.5% per hour late	4 hours	8 hours	R	0.5% per hour late	
Major	3 monthly fee hours	None	8 hours	16 hours	R	None	
Minor	8 hours	None	16 hours	32 hours	R	None	
Information	16 hours	None	24 hours	48 hours	R	None	
Change	16 hours	None	R	R	R	None	

The times above are shown and calculated in business days.
R: depends on the product Roadmap (patches - 5 to 20 days and releases 1 to 3 months)

- 1 the criticality is entered by the CLIENT and may eventually be re-evaluated by Notilus Support.
- 2 Handling time: after an anomaly is analysed, it is transferred to the R&D teams within the times shown. The correction is then included in a Cumulative Patch or a Release.

For each criticality and each ticket status, Notilus Support guarantees an acknowledgement, resolution and product correction time compliance rate of at least 90% of tickets. The penalties will be deemed on a monthly basis.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

SaaS Service Agreement

Department	Service level
Availability and monitoring	24/7
Application availability	99,5 % per month (87 hours of unavailability per year)*
Scheduled service interruptions	Duration 4 hours max, planned 1 week in advance.
Number of scheduled interruptions	Maximum once per month
Human management of the platform	8:30 a.m. to 6 p.m. (5 p.m. on Fridays) UTC+1, 5 days a week, excluding French public holidays

* Except in cases of force majeure or a cause beyond the host's control. Our technical resources are covered by contracts with a guaranteed service recovery time (GRT) of 4 hours maximum.

Penalties will be deemed as follows :

Availability of the system	Penalties applicable
98% to 98,99%	5% from the amount of the monthly Saas Services
96% to 97,99%	10% from the amount of the monthly Saas Services
95% to 96,49%	15% from the amount of the monthly Saas Services
<95%	20% from the amount of the monthly Saas Services

All indicators defined in the §8.7 "Definition of the Service Level agreements" of the appendix 8 are measured every month through the Service Provider's ticket tool , accessible to the Client.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

SERVICE AGREEMENT

POG-SA-22331

By and Between:
PO
&
NOTILUS

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

This Service Agreement, effective as of the date of the signature (the “Effective Date”), is made by and between:

PLASTIC OMNIUM GESTION

a company incorporated under French laws as, a “société par actions simplifiée”, whose registered office is located at 19 Boulevard Jules Carteret, 69007 LYON, FRANCE, registered under n° 410.314.207 CS LYON, acting both in his own name and on behalf of the companies owned directly or indirectly at 50% or more by Compagnie Plastic Omnium (“Client Affiliates”)
duly represented by Pascal ZEMBRA acting as VP Information Systems and having all powers for the purposes of representing

hereinafter referred to as the « **Client** » or **Plastic Omnium**

AND

NOTILUS a Cegid company

a company incorporated under French laws as a “Simplified joint stock company with a single shareholder”, whose registered office is located at 561 allée des Noisetiers 69760 Limonest, registered under n° B 877 912 691 , acting in its name and on its behalf and also in the name and on the behalf of its Affiliated Companies (as defined hereinafter)

duly represented by Gilles BOBICHON acting as Chief operating officer and having all powers for the purposes of representing Notilus

Notilus, a Cegid company

hereinafter referred to as the « **Service Provider** » or **Notilus**

hereinafter individually referred to as "Party" and collectively as "Parties"

WITNESSETH

WHEREAS, The Parties acknowledge and agree that the overall goals and objectives of the Client in entering into this Agreement are to: (i) benefit from the best practices in the area of business processes and services; (ii) add value to Client's business activities through better efficiency and processes; (iii) implement a comprehensive software solution to manage and streamline all travel requests and business expenses ; (iv) provide Client with the flexibility to quickly and effectively adapt to changing business requirements and changes in the Client business environment; and (iv) benefit from cost savings, Services of quality and continuous improvements.

WHEREAS, Service Provider represents to know and to understand the requirements and needs of Client and has submitted to this extent a commercial proposal to Client , and represents to Client it has the expertise, the Personnel, the services and the competencies required to satisfy Client's needs and requirements and to perform the Services in compliance with the terms and conditions set herein.

WHEREAS, Client, based upon the Commercial Proposal, the information it contains as much as upon the information provided by Service Provider during pre-contractual discussions and the contractual representations and warranties agreed between the Parties, wishes to engage Service Provider to provide professional service (the "Services") as set forth in the present Agreement.

WHEREAS, Client and Service Provider want to specify the terms and conditions under which Service Provider shall provide the Services and Deliverables to Client.

WHEREAS, this Service Agreement directly creates rights and obligations between Plastic Omnium Group and the Service Provider and/or its Affiliates Companies when applicable. Both Parties warrant and guarantee that their Affiliated Companies will agree and comply with the terms and conditions of this Service Agreement. Both Parties also warrant and guarantee that all companies that become their Affiliated Companies during the term of the Service Agreement will agree and comply with the terms and conditions of the latter. Any new company that becomes an Affiliated Company of a Party will be entitled to claim the benefit of the provisions of this Service Agreement for all the Contracts being performed. All perimeter which belong to SLA including criterias listed in handling times and description of detailed service level are also applicable to POG and will be reported once per year in one shared POG and Plastic Omnium SLA report by Notilus in order to track their level of service performance, in consequence with penalties mechanism referred to Appendix 3.

NOW, THEREFORE, in consideration of the agreements, representations, warranties, promises and covenants contained herein, and other good and valuable consideration, the receipt, sufficiency and adequacy of which are hereby acknowledged, the Parties, intending to be legally bound, agree to the foregoing and as follows:

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Article 1 - PRELIMINARY PRINCIPLES 6
1.1 - Due Diligence 6
1.2 - Best Practices 6
Article 2 - DEFINITION 6
Article 3 - CONTRACTUAL DOCUMENTS 8
Article 4 - COOPERATION 8
4.1 - Duty to Inform and of Loyalty 8
4.2 - Ongoing Cooperation 8
4.3 - Cooperation with Third Party Service Providers 8
4.4 - Governance 9
4.5 - Reports 9
Article 5 - PROVISION OF SERVICES 9
5.1 - Standards and Methodology 9
5.2 - Services Scope 9
5.3 - Services Description 10
5.4 - Planning 10
5.5 - Licensor Products 10
5.6 - Compatibility of Client Equipment and Interoperability 11
5.7 - Changes in Services - Services Change Requests 11
5.8 - Additional Services. 11
5.9 - Documentation 11
5.10 - Training 11
Article 6 - ACCEPTANCE 12
6.1 - Verification of Acceptability 12
6.2 - Acceptance Test 12
Article 7 - DELAYS 12
Article 8 - INTELLECTUAL PROPERTY 13
8.1 - Acquiring third-party rights 13
8.2 - Infringement and Indemnification by Service Provider 13
Article 9 - EMPLOYEES 13
9.1 - Expertise and management of Service Provider's Staff 13
9.2 - Key Personnel 13
9.3 - Employment law & Fight against illegal employment 14
9.4 - Tools 14
9.5 - Professional Messaging and Communications 14
Article 10 - CHARGES AND PAYMENTS 14
10.1 - Rates and Charges 14
10.2 - Rates and Terms for Additional Services 14
10.3 - Invoices 14
10.4 - Payment 15
10.5 - Disputed Invoices 15
10.6 - Modification of Bank Certificate 15
10.7 - Certificate of Tax Residence 15
10.8 - Travel Policy, Out-of-Pocket Expenses and Other Charges 15
Article 11 - REVERSIBILITY 15
Article 12 - CONFIDENTIALITY 16
Article 13 - REFERENCE TO CLIENT'S BRANDS AND NAMES 16
Article 14 - DATA PROTECTION – PROCESSING PERSONAL DATA 16
Article 15 - SECURITY 18

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

Article 16 - WARRANTIES 18
16.1 - Nature of Services 18
16.2 - Non-Interference 18
16.3 - Authority and Good Standing 18
16.4 - No Conflict 19
16.5 - Third Party Warranties 19
16.6 - Malicious Code 19
16.7 - Disabling Code 19
16.8 - Conflict of interest 19
Article 17 - AUDIT 19
17.1 - Record Keeping 19
17.2 - Audit Scope 19
17.3 - Periodicity 20
17.4 - Cooperation 20
17.5 - Report and Follow-up 20
17.6 - Costs 20
Article 18 - LIABILITY 20
18.1 - Liability Cap 20
18.2 - Exclusion of Liability 21
18.3 - Client Failure 21
18.4 - Liability Under Third Party Arrangements 21
Article 19 - INSURANCES 21
Article 20 - COMPLIANCE, PERFORMANCE OBLIGATIONS AND DELIVERY TIMEFRAMES – PENALTIES 22
Article 21 - FORCE MAJEURE 22
Article 22 - TRANSFER – SUBCONTRACTORS 23
22.1 - Transfer/Change of control 23
22.2 - Subcontractors 23
Article 23 - TERM AND TERMINATION 23
23.1 - Term 23
23.2 - Termination for breach 23
23.3 - Termination for Convenience 24
23.4 - Change in Control 24
23.5 - Cancellation for non-implementation 24
23.6 - Cancellation due to bankruptcy 24
23.7 - Survival 24
Article 24 - APPLICABLE LEGISLATION/DISPUTES 24
Article 25 - MISCELLANEOUS PROVISIONS 25
25.1 - Independence of the Parties 25
25.2 - Partial nullity 25
25.3 - Neither Party Considered Drafter 25
25.4 - Imprevision 25
25.5 - Non-waiver 25
25.6 - Counterparts; Digital signature. 25

ARTICLE 1 - PRELIMINARY PRINCIPLES

1.1 - Due Diligence

Service Provider acknowledges and agrees that it has entered into this Agreement in reliance of its own due diligence and therefore has not relied on any representation save for those expressly provided in this Agreement.

Service Provider represents and warrants it has entered into this Agreement in good faith and with loyalty and has given all necessary and relevant advises, warnings and information to Client related to Service Provider and the Services and Deliverables and which in its professional opinion would have had a detrimental impact on the Services and Deliverables or compromise the objectives of this Agreement.

1.2 - Best Practices

Service Provider shall inform Client on practices and processes it encounters or develops in its business activities where such practices and processes are of a higher standard than those contemplated under this Agreement. Service Provider shall advise Client of any new developments relating to the Services and Deliverables, including services, products and processes that could reasonably be expected to have an impact on Client business, and shall, upon Client request, assist in the evaluation and testing of such developments in connection with the Services and Deliverables.

ARTICLE 2 - DEFINITION

The following definitions apply in this document:

"Acceptance": shall mean that Client confirms in writing via an Acceptance Certificate, that the Acceptance Criteria has been fully satisfied in respect of the relevant Acceptance Tests and "Accept" and "Accepted" shall be construed accordingly.

"Acceptance Criteria": shall mean the criteria to be satisfied to demonstrate that the Acceptance Tests have been successful completed

"Additional Services": include consulting, expertise and study, development, integration, and any item to be delivered by Service Provider resulting from the additional service

"Affiliated Company(ies)", means any company (i) directly or indirectly controlled by a Party, or (ii) directly or indirectly controlling a Party, or (iii) under the same control as a Party. For the purpose of this definition the term "control" means the possession, directly or indirectly, of at least fifty percent (50 %) of the equity ownership or voting rights.

"Amendment": shall mean a written formal document signed by the Parties which purport to modify this Service Agreement.

"Attachment": means any attachment, schedule, appendix or the likes referenced in and appended to this Agreement and made a part hereof.

"Business Day": means a weekday (Monday through Friday) or a day on which normal business is conducted, excluding bank and other public holidays in the relevant Country.

"Change": means any actual or proposed change to the nature, level and/or extent of the Services or Service Levels or the manner in which the Service Provider implements or is to implement or provides or is to provide the Services (whether resulting in additions to, reductions in, or amendments to the Services or the Service Levels).

"Charges": means the charges set out in and/or calculated pursuant to Schedule 5: Charges and Financial Obligations.

"Conformity": the conformity of the Services is assessed based on:

- the specifications provided and/or agreed to by the Licensee and/or the performance and results described in the Contract, and
- other provisions of the Contract, and
- best industry practice, and
- legal provisions.

"Contract or Agreement", means the contractual relationship between the Parties arising out from the acceptance of a Purchase Order by the Licensor. The Contract is governed exclusively by the terms and conditions of the set of contractual documents concerning the Services as set forth in Article 3 "Contractual documents" below.

"Contractual Year": means a period of twelve (12) consecutive months starting on the Effective Date and each anniversary of it.

"Client": Any Plastic Omnium Group Company, which purchase the Services to Service Provider and/or Service Provider Affiliated Companies, or on whose behalf a Purchase Order is issued.

Service Provider expressly recognizes that there is no liability between the Client, on the one hand, and the Client's Affiliated companied acting as Client, on the other hand. Therefore, any entity making an order retains sole responsibility for any commitments entered into with Service Provider under the Contract.

"Data": all information and data that has been provided, taken, processed or stored and communicated to the Licensor, including personal data.

"Functional specifications": Appendix that describes the technical and functional specifications applied to the Services.

"Installation Site": shall mean any location for or to which Service Provider provides Service. Client may change Installation Sites from time to time upon notice to Service Provider in accordance with the terms of this Agreement.

"Intellectual Property Rights": shall mean all trade secrets, patents and patent applications, trademarks (whether registered or unregistered and including any goodwill acquired in such trade marks), service marks, trade names, business names, internet domain names, e-mail address names, copyrights (including rights in computer software), author rights, database rights, trade secrets, design rights, rights in know-how, rights in confidential information, rights in inventions (whether patentable or not) and all other intellectual property and proprietary rights (whether registered or unregistered, and any application for the foregoing), and all other equivalent or similar rights which may subsist anywhere in the world.

"Malicious Code": means any code, program, or sub-program whose knowing or intended purpose is to damage or interfere with the operation of the computer system or network containing the code, program or sub-program, or to halt, disable or interfere with the operation of software, code, programs or sub-programs, itself, any device, method or token that permits any user to circumvent the normal security of the software, network or system containing the code.

"Normal Business Hours": means 8:00 a.m. to 6:00 p.m. at the relevant location on a Business Day.

"Personal Data": data which is defined as any information relating to an identified or identifiable natural person who can be identified directly or indirectly by reference to a name, an identification number, location data, an online user ID, or any information relating to their physical, physiological, mental, economic, cultural or social identity. Personal data is legally protected.

"Plastic Omnium Group or POG ": means the Client and any Client's Affiliated Company(ies) or Joint Venture.

"Purchase Order or Order": the hardcopy or electronic (for online transactions) document by which the Licensee places the Services order with the Licensor.

In particular, it includes:

- a description of the Services;
- the Services price(s);
- the Site where the Services is to be implemented or delivered to;
- the timeframe and dates for the implementation or delivery of the Services;
- the Licensee's identification information;
- the Contract reference.

The Purchase Order is governed exclusively by the terms and conditions of the contractual documents relating to a Service, listed in Article 3 "Contractual Documents" below.

"Specifications": means, without limitation, the required organizational, functional, performance, qualities and technology requirements or any other requirements set forth in this Agreement or the applicable Transaction Agreement for Services and Deliverables provided by Service Provider, which may be modified at Client's option to incorporate any generally available service guarantee or assurance program that may be offered by Service Provider, or as otherwise provided in this Agreement.

"Rates and Charges": means the rates and charges for Services set forth in this Agreement and the applicable Attachment, as modified from time to time as permitted under or required by this Agreement.

"Security Policy": means security policy, guidelines and requirements in place within the organization of Client and notified to the Service Provider;

"Service Provider Personnel": means those personnel employed by Service Provider (including employees, contractors, subcontractors, agents, counsel, Service Providers and invitees of Service Provider or of its Affiliates, collectively or individually as applicable) whose functions or job assignments relate in whole or in part to the provision of Services. Service Provider Personnel shall include Key Personnel.

"Site": the place(s) where the Services is to be implemented or delivered.

Subcontractor: any subcontractor or Licensor that the Licensor uses to carry out the delivery of part of the Services.

"Third Party": means any person or entity which is not a Party to this Agreement. No Plastic Omnium Company shall be construed as a "Third Party".

ARTICLE 3 - CONTRACTUAL DOCUMENTS

The Service Agreement between Client and Service Provider is composed of the following documents, listed by decreasing order of priority :

- Service Agreement and its appendices:
  - Appendix 1 – Service Description+ Planning
  - Appendix 2 – Financial Conditions
  - Appendix 3 – In Service Support
  - Appendix 4 – Governance "Description and Operation 16.09.2021"
  - Appendix 5 - PO Policy Security
  - Appendix 6 - CSR Charter
  - Appendix 7 – GDPR
  - Appendix 8 – Notilus « Cloud Charter T&E 16.12.2021 »
  - Appendix 9 : Licence and Implementation Price conditions

- Purchase Order, as issued, as under which Client purchases the Services and accepted by Service Provider;

If there is a conflict among the terms in the various contractual documents listed in Article 3, the order of precedence set out in the said Article shall apply. In case of contradiction within the same contractual document, specific provisions shall prevail over general provisions.

ARTICLE 4 - COOPERATION

4.1 - Duty to Inform and of Loyalty.

Service Provider acknowledges that its covenants, representations and warranties are an express inducement for the entry of Client into this Agreement.

In performing this Agreement, Service Provider shall at all-time provide the Services and Deliverables in good faith and with loyalty to Client and shall advise and warn in writing Client on any event which Service Provider becomes aware of, or on any Client decision or request, which in his professional opinion may have a detrimental impact on the Services and Deliverables, or compromise the objectives of this Agreement.

4.2 - Ongoing Cooperation

Service Provider and Client shall cooperate in planning, implementing and providing Services, Additional Services, Services Upgrades, and Changes in an efficient, cost-effective manner. Such cooperation shall include each Party's prompt provision to the other of any information that the other may reasonably request to carry out its responsibilities hereunder and, in the case of Service Provider, cooperation with Third Party service provider of products and services to Client. Service Provider shall coordinate with Client all activities that could reasonably be expected to adversely impact Client's receipt of Services or provision of services to its Clients. Such coordination shall be designed to minimize any disruption to Client's business activities.

4.3 - Cooperation with Third Party Service Providers

Service Provider acknowledges that Client may be, during the Term of this Agreement, working with Third Parties which may require coordination with the Services Provider's own activities under this Agreement. Therefore, Service Provider, as part of the Services, shall cooperate with Client and such Third Parties. Such cooperation may include planning coordination, use of specific project management tools, exchange of information, including Services Provider's confidential information, and interface information.

Upon Client request, Service Provider agrees to fully cooperate with and work in good faith with any Third Party (and the agents, contractors and subcontractors of such Third Party) designated by Client in connection with this Agreement, including in the installation of services and resolution of troubles. Such cooperation may include: (a) providing access to any facilities being used to provide the Services, as necessary for such Third Parties to perform the work assigned to them; and (b) providing access to the equipment and software to the extent permitted under any underlying agreements with Third Party vendors of such equipment and software. Such Third Parties shall comply with Service Provider's reasonable security and confidentiality requirements, and shall, to the extent performing work on software or equipment for which Service Provider has operational responsibility, comply with Service Provider's reasonable standards, methodologies, and procedures. Service Provider shall immediately notify Client if an act or omission of a Client Third Party will cause, or has caused, a problem or delay in providing the Services, and shall work with Client to prevent or circumvent such problem or delay. Service Provider will coordinate with Client and such Third Parties to resolve differences and conflicts arising between the Services and other activities undertaken by Client or any of such Third Parties.

4.4 - Governance

Each Project Manager shall have direct access to the officers or other key decision-makers in his or her respective organization, and shall call upon the experience, expertise and resources of such organization to ensure proper performance of this Agreement. Service Provider's Project Managers shall be among the Key Personnel of Service Provider.

In no event shall any Party's participation in any meetings convened pursuant to this Section be deemed a waiver or alteration of any right or obligation imposed by this Agreement.

4.5 - Reports

Service Provider Project Manager and Client's appointed representative will act as interfaces between Service Provider and Client. Service Provider's Project Manager will provide Client's representative with status reports (at intervals determined by Client, on a monthly basis). At Client request, status reports may contain the following:

(a) a summary of the current status of the Services (including specific progress made since the immediately preceding status report);
(b) a summary of the status of, or progress made on, all problems identified in previous status reports (and not previously reported as corrected);
(c) a summary of any problems identified since the preceding status report and any recommended remedial action(s); and
(d) the amount of any anticipated delay in the completion of any milestone specified in this Agreement, the cause of such delay, any recommended remedial action(s) and other information requested by Client.
(e) SLA Reports will be both made for Plastic Omnium (monthly basis) and POG (annual basis)

As part of the project management during the run phase the Service Provider offers a 5-day package on demand (considering the price of a day at 810€) covering the training of new comers as well as the sending of SLA reports (new comers means all related admins who will be on boarded after origin implementation/development phase/country) :

- 3 days training of news comers in French and/or English (administrator training)
- SLA reports meeting review (minimum one per year)

ARTICLE 5 - PROVISION OF SERVICES

5.1 - Standards and Methodology

In the performance of their obligations under this Agreement, the Parties shall act fairly and in good faith. Where notice, approval or similar action by a Party is permitted or required by any provision of this Agreement, such action shall not be unreasonably delayed or withheld.

Service Provider shall provide the Services to Client in accordance with the terms and conditions of this Agreement, and is responsible for providing the Services in accordance with the performance criteria set forth in the applicable Schedule(s).

Service Provider represents and warrants to Client that Service Provider possess and shall maintain the skills, resources and expertise to provide the Services in accordance with the terms and conditions of this Agreement. Without limiting the generality of the foregoing, Service Provider represents and warrants to Client that:

(a) all Services provided under this Agreement shall be provided with all necessary efforts (i.e. "Obligation de Moyens Renforcée"), in a timely, professional and workmanlike manner consistent with the highest industry standards of quality and integrity; provided, however, that where this Agreement specifies a particular standard or criterion for performance, this warranty is not intended to and does not lower that standard or criterion for performance;
(b) Service Provider shall perform its obligations under this Agreement in a manner that will minimize any interference with Client's normal business operations and in accordance with:
(i) Client's policies as provided in writing to Service Provider from time to time;
(ii) Client's instructions and general guidelines relating to the System, the Services or Agreement; and,
(iii) Service Provider's own established procedures and practices (to the extent that compliance with the same does not conflict with Service Provider obligations under this Agreement);
(c) other than the applicable fees set forth in Schedule 2: Charges and Financial Obligations, no additional cost or expense shall be required of Client in order for Service Provider to be able to provide the Services as required under this Agreement.

Service Provider acknowledges that the timely performance of its obligations under this Agreement is of the essence and critical to Client business, and that Client is entitled to rely upon Service Provider to implement, under an obligation of results, the Services according to the implementation schedules agreed between the Parties.

5.2 - Services Scope

The Services and Deliverable(s) to be provided by Service Provider pursuant to this Agreement are specified in Annex 1: Services Description.

For the avoidance of doubt, shall be deemed to be included within the scope and price of the Services any activities or functions not specifically described in this Agreement which:

a) are an inherent, or necessary or customary part of the Services;
b) are required for proper performance of the Services or its delivery or its use by Client;
c) are required for proper delivery or usage of a Deliverable by Client;
d) include any assistance reasonably required by Client and/or its provider(s) of goods and/or services;
e) a project management and quality evaluation and oversight service for the co-ordination and quality assurance of all of the Service Provider's obligations.
f) Any additional activity required to meet Service Provider's legal obligations

5.3 - Services Description

Pursuant to the dispositions of this Agreement, Service Provider shall provide Client with the following Services more specified in the appendix 1 :

Notilus is publishing a Travel & Expense platform that allows its clients to manage the over whole process of the trip. Travellers will be able to book their trips directly from Notilus using the Plastic Omnium's nominated Travel Management Company booking tool. Expenses will be scanned from the mobile or the desktop application to ease expenses creation.
Managers will be able to validate or deny both travel & expense request on any devices.

Notilus will be central in the organization as it will be connected to Plastic Omnium IT systems (SAP HR and ERP).

Full service descriptions is available in the document attached "Appendix 1".

Any optional services shall be delivered by Service Provider, upon Client's request, according to the specific terms and conditions agreed in writing by the Parties (if any). The Change Request procedure provided in this Agreement shall apply accordingly.

5.4 - Planning

Service Provider shall meet with the estimated planning set forth in Appendix 1 and will perform the Services in consequence.
The planning services will be established between the parties upon signature of Notilus contract.
The Parties agree to define the planning following the kick-off meeting. This planning will be freezed and should be the starting point for the application of the mechanism of penalties.

Except as otherwise defined in this Agreement, all the dates, deadlines, or other statements related to the timeline, period or periodicity of any obligation contained in this Agreement, or its Appendix shall compose the planning with which Service Provider shall comply (the "Planning").

In the event of suspension of the service by the Client the Client remains obliged to pay the License Fees pro rata temporis to their consumption.

In case of any change of planning required by Client or Service Provider, the Project Managers of both Parties shall discuss in good faith and confirm, in writing, the new timelines, with reference to this Agreement which shall be deemed as a written amendment to this Agreement. In case of successive amending documents expressly agreed in written form by the Parties, the most recent shall prevail.

Client and Service Provider shall not unreasonably refuse, condition or delay its consent on any change of planning required by the other Party, to the extent that the concerned Phase falls during the then-agreed term of this Agreement. Also Service Provider cannot invoice any extra fees in case of change, if fees have not been pre-approved in writing by the Client according to the "change request" procedure.

If the Service Provider performs work outside the Normal Business Hours at the relevant Installation Site on its own, it shall not impose any premium or overtime rate for such installation or implementation work.

With respect to any Service moved, added or changed under this Agreement, Service Provider and Client shall establish a date for the implementation, effective operation and acceptance by Client of such Service.

5.5 - Licensor Products

The Service provider grants to Client, and Client hereby accepts a license to use the Software Products that is limited, nonexclusive, nontransferable, non sublicensable and revocable. Client may use the Software Product in the specified media and accompanying Documentation, for its Permitted use only.
. The appendix 1 specify relevant to the license being purchased, including: (a) the license type (e.g., Site, or User), (b) the license term (e.g., perpetual or term), and (c) the Software Product(s) being licensed

5.6 - Compatibility of Client Equipment and Interoperability

Service Provider shall ensure that all Client Systems shall be successfully integrated, interfaced and compatible with the Services and that adequate and appropriate (as determined by Client) architectural functions and structural integration exists between and among Client Systems and the Services such that the Services have the capability to communicate, execute programs or transfer data seamlessly.

Service Provider shall ensure that the Services shall not adversely affect the Client Systems, whether as to functionality, speed, service levels, interconnectivity, reliability, availability, performance, response times, or similar measures. The requirements of this Section "Compatibility of Client Equipment and Interoperability" shall be referred to as the "Interoperability Requirements".

The Client undertakes to observe the Software Package conditions for use that are indicated in the Documentation, in addition to any instructions given by the Service Provider. Notably, the Client undertakes to enter and send Data in a rigorous manner, observing the formats, conditions and frequency of scheduled transfers.

The Client shall only grant Software Package access to its authorised personnel. In particular, the Client undertakes to maintain the confidentiality of its identifiers.

It is incumbent upon the Client to ensure the accuracy and completeness of data transmitted under its responsibility.

It is incumbent upon the Client to ensure the suitability of the Software Package for its needs, notably with regard to its documentation.

It is incumbent upon the Client to have the appropriate configuration, notably pertaining to equipment, software, networks, terminals, connections and cabling compliant with the current version of the "Notilus Prerequisites" information document.

For the duration of this contract, the Client shall also designate an a single intermediary per region who has been trained on the technical and functional parts. Only this intermediary can use the assistance services offered by the Service provider.

5.7 - Changes in Services - Services Change Requests

During the course of this Agreement, Client may request Changes in the Services. Service Provider shall respond to such request with its best technical and financial proposal, under conditions no less favorable than those under which this Agreement was initially executed.

Service Provider shall also specify the impact of the Changes including the consequences on the Planning. Service Provider shall bear all the costs for this evaluation and proposal preparation for the requested Changes. Any such Change request shall be effective upon the execution of a Change Order setting forth the requested Changes and their impact (if any) on the compensation to be paid to Service Provider.

5.8 - Additional Services.

Client shall be entitled at any time during the Term to request the provision of additional services, and the parties agree to thereafter negotiate in good faith the detail of an appropriate Transaction Agreement to set out the provisions relevant to such services. Service Provider agrees to provide all of the Services listed in the completed Transaction Agreement once signed by Client Authorized Representative and the Service Provider Authorized Representative. For the avoidance of doubt, it is anticipated that any adjustments or extensions to existing Services be dealt with by way of the Change Procedure, and that a new Transaction Agreement will therefore only be required in relation to significant or entirely new requirements for Services by Client.

5.9 - Documentation

Service Provider shall deliver to Client a reasonable number (in relation to the number of individuals using the Services) of copies of its standard operational instructions and documentation for any Services or alternatively will allow Client to download any such documentation as reasonably required for the purpose of this Agreement.

If the Documentation described herein is revised at any time or if additional documentation is developed by Service Provider with respect to the Services, Client shall be entitled to receive, at no costs, copies of such revised or additional documentation produced by Service Provider.

Client shall have the right to reproduce and adapt any Documentation provided hereunder in order to meet its own internal requirements.

5.10 - Training

As part of the Services, Service Provider shall develop appropriate training materials and provide appropriate training with respect to the use of the Services and Client Personnel responsible for:

(a) administering or ordering Services;
(b) training end-users of the Services; or

(c) reporting and managing Performance Failures, delays or other troubles, including supporting the "level 1 help desk" functions performed by Client Personnel.

Service Provider shall cooperate with Client in the training of Service Provider Personnel on Client's Systems and practices so that Service Provider can properly and efficiently provide the Services.

Training for all Client Personnel shall be provided at the Installation Sites agreed between the Parties, which Client shall make available for this purpose.

As part of the project management during the run phase, Notilus offers a 5-day package (considering the price of a day at 810€) covering the training of new comers as well as the sending of SLA reports :

- 3 days training of news comers in French and/or English (administrator training)
- SLA reports meeting review

ARTICLE 6 - ACCEPTANCE

6.1 - Verification of Acceptability

Service Provider shall timely furnish the Services and the Deliverables to the Client in compliance with the Planning, Performance Specifications and descriptions as provided and agreed in this Agreement.

Upon implementation, provision, deliverance, repair or restoration of a Service or Deliverable, Client shall examine the Service or Deliverable to verify their acceptability by reference to their specifications in accordance to the defined acceptance tests defined in this Agreement. Service Provider will provide (at no additional cost for Client) such assistance as Client may reasonably require for such Verification of Acceptability.

6.2 - Acceptance Test

The Verification of Acceptability for any Service or Deliverable provided by Service Provider to Client shall be done according to the timing, procedure, and tests specified in the Appendix 1: Services Description.

Acceptance of a Service or a Deliverable will solely result from the Client's certificate of acceptance. Payment or use by the Client shall not be deemed as an acceptance or a waiver of any right or remedy by Client. Acceptance of the Services or Deliverables shall not be construed as a waiver from Client of any of its right or remedy based on Service Provider's representations and warranties.

If Client determines that a Service or Deliverable does not comply with the applicable Documentation, specifications, Service Levels and Interoperability Requirements as described in this Agreement, then Client will send Service Provider a notice describing the non-conformity. Unless otherwise specified in this Agreement or if the circumstances require a shorter period, Service Provider will have a five (5) days cure period from the date it receives Client's rejection notice to re-perform the Service or correct the Deliverable, at no additional cost for Client. Then Client will have ten (10) days from the date it receives the re-performed Services or corrected Deliverable to verify the conformity of the Service or Deliverable.

ARTICLE 7 - DELAYS

If, for any reason, Service Provider suspects or discovers that it or any Service Provider Subcontractor shall not be able to perform obligations hereunder, it shall immediately notify Client of that fact in writing. Such notification shall include a detailed description of the problem, the causes of the problem and Service Provider's or Service Provider Sub-contractor contingency plan. Such notification shall not relieve Service Provider of its obligations and shall not preclude any remedies available to Client hereunder.

In any event of failure by Service Provider or its Subcontractor to perform the Services as set forth in this Agreement, Service Provider shall as soon as possible, without prejudice to any specific response timing set forth in the applicable Schedules, take actions in order to diligently pursue the servicing of such Services in accordance with the terms and conditions of this Agreement and immediately commence and continuously and diligently exercise its best efforts to repair such Services until all necessary repairs are completed.

As soon as Service Provider fails to comply with the schedules set forth in the Implementation Plan, an implementation delay begins ("Implementation Delays"). The computing of an Implementation Delay ends when the Service is performed in a manner that meets the Specifications, Performance Standards and other applicable requirements of this Agreement and is accepted by Client for use. Any part of the Implementation Delay that is caused by the negligence or wilful misconduct, lack of avaibility of Client or persons authorized by Client or a breach of any of their obligations under this Agreement, shall not be computed in the Implementation Delay.

Service Provider acknowledges that in the event of any Implementation Delays, Client will suffer damages, the total of which cannot easily be computed, and the Service Provider's response to such Implementation Delays is therefore of paramount concern. Client shall not be obliged to pay any additional cost related to the remediation of such Implementation Delay nor to pay the Rates and Charges for any Service subject to any such Implementation Delay.

In the event that Implementation Delay constitute a material breach under this Agreement, Client may exercise any other remedies available, consistent with the applicable law and terms and conditions of this Agreement, including but not limited to the right to terminate this Agreement as described in Article 23-2.

ARTICLE 8 - INTELLECTUAL PROPERTY

8.1 - Acquiring third-party rights

Service Provider is responsible for acquiring all patrimonial copyrights before participating in any way in the fulfilment of this Agreement. In particular, they undertake to acquire these rights from their potential employees and subcontractors. Service Provider is also responsible for obtaining, at their own expense, all relevant third-party authorization, including patent holders and trademark owners, whose application or use would be necessary for the implementation of the additional service.

If Service Provider requires the use of one or more third-party software package(s), they must obtain a non-exclusive user license for the use of these third-party software packages as part of the Contract, at their own expense, for Service, and/or any authorized third party carrying out services for Service Provider, as well as for the entities of the authorized Plastic Omnium Group.

Service Provider must inform Client of their intention to use or incorporate, as part of the additional service, the deliverables described in the Contract and/or any other element arising from the additional service. Service Provider would not be able to assign all the rights as defined below Client for any pre-existing element. They must provide Client with a comprehensive document describing the pre-existing features concerned and specifying the terms of use for Client of these pre-existing features.

8.2 - Infringement and Indemnification by Service Provider

Service Provider warrants to Client a peaceful, uninterrupted use of the Services and Deliverables and all Intellectual Property Rights assigned or granted under this Agreement.

Service Provider shall protect Client against any third-party claim or action taken regarding counterfeiting or any other violation of the intellectual property rights and shall indemnify Client against all resulting consequences. If there is a risk of claim or action identified by Client or Service Provider, Service Provider shall take all necessary measures to eliminate the risk relating to counterfeiting or any other violation.

In the event of a ban in using a feature of the Services as part of the Agreement, Service Provider shall, at its own expense and as chosen by Client, either replace the feature which is subject to the alleged ban or amend it so that it eradicates the counterfeit or any other violation in accordance with the contractual provisions applicable to this Service feature. These replacements or changes must be carried out in a timeframe that suits the Client's needs. Failing this, Service Provider agrees to reimburse any amounts already paid to Client as part of the Contract.

The aforementioned provisions do not affect Client's right to claim damages from Service Provider and cancel the Contract under the terms provided in Article 22.5 ("Cancellation for non-implementation").

ARTICLE 9 - EMPLOYEES

9.1 - Expertise and management of Service Provider's Staff

For the implementation of the Services, Service Provider shall assign teams with relevant experience, expertise, qualifications and authorisation for the successful implementation of the Services.

Service Provider shall at all time and in all places, exert his employer authority on its Personnel, including when such Personnel provide Services outside Service Provider's premises. Service Provider Personnel shall not become Client Personnel for the reason that they are performing the Services.

Any instructions of requests by Client regarding the implementation of the Services may only be addressed to Service Provider's operational representative(s). This situation shall not lead to any subordinate relationship between the representative(s) and Client.

9.2 - Key Personnel

Service Provider Personnel whose involvement or role is especially important to a Service - such as the Project Manager, - may be specifically identified as "Key Personnel".

Subject to Laws, Service Provider shall not replace or reassign Key Personnel unless Client consents to such reassignment or requested such replacement or reassignment, or such Key Personnel (a) voluntarily resigns from Service Provider, or (b) is dismissed by Service Provider, (c) fails to perform his or her duties and responsibilities pursuant to this Agreement or (d) dies or is unable to work due to his or her disability.

In case of substitution, Service Provider shall replace the leaving Key Personnel with Similar Profiles.

9.3 - Employment law & Fight against illegal employment

Service Provider respects, and ensure the respect of its potential subcontractors, the employment law of the country or countries in which the Client's Site(s) are located and/or in which the Services are delivered and shall respect the regulations regarding illegal employment. In this respect, Service Provider shall declare that their staff, as well as the staff of their potential subcontractors assigned to the implementation of the Services, are lawfully employed and declared under the applicable legislation.
If Service Provider and their potential subcontractors intend to employ staff of a foreign nationality to implement the Services, Service Provider must also ensure that, while visiting the Client's site, these members of staff will be authorized to carry out professional activity in the country where the Site is located and that they have all the required working credentials and residence permits.

Service Provider is responsible for certifying that they or their Subcontractors do not use child labour or any type of labour that violated the fundamental principles of the International Labour Organization.

9.4 - Tools

Service Provider is responsible for procuring all tools, equipment and software, it needs for the performance of the Services ("Service Provider's Tools").

9.5 - Professional Messaging and Communications

Unless otherwise stated in the applicable Schedule, Service Provider agrees that its Personnel will exclusively use the e-mail address provided to him by Client in order to perform the Services. Service Provider acknowledge that the use of any other electronic mail account will constitute a breach of confidentiality.

ARTICLE 10 - CHARGES AND PAYMENTS

10.1 - Rates and Charges

Client shall pay the Rates and Charges set forth in Appendix 2: Charges and Financial Obligations. Subject to any adjustments permitted or required under this Agreement, these Rates and Charges constitute the totality of charges for which Service Provider may bill Client in connection with the provision of Services and performance of its obligations under this Agreement and will not exceed the amount resulting from the rates and methodologies set-forth in such Schedule 5: Charges and Financial Obligations.

The Rates and Charges include the remuneration for the Intellectual Property Rights assigned or granted to Client, and Service Provider may not claim any additional amount for such assignment or grant.

Payment of the Rates and Charges is conditional to the agreed payment Schedule.

Service Provider acknowledges that, except as expressly provided otherwise in this Agreement, expenses that Service Provider incurs in performing the Services are included in the Rates and Charges set forth in this Agreement. Accordingly, such Service Provider expenses are not separately reimbursable by Client unless Client has agreed in advance and in writing to reimburse Service Provider for such expenses.

10.2 - Rates and Terms for Additional Services

Service Provider may charge Client rates and charges that are mutually agreed upon by the Parties, provided that if the Parties cannot agree upon rates and charges for an Additional Service within thirty (30) days of the commencement of negotiations thereon, Client may seek bids from other service providers to provide the Additional Service, which Service Provider may then reasonably match.

Nothing in this Section "Rates and Terms for Additional Services" shall require Client to purchase any service that would qualify as an Additional Service from Service Provider.

10.3 - Invoices

All fees payable to Service Provider under this Agreement shall be detailed, categorized and clearly stated on an invoice in accordance with the terms and conditions set forth in this Agreement. When invoicing is linked to milestone payments, payments will be made as set forth in this Agreement, centrally controlled
If a new entity shall enter into the agreement, the invoicing process shall be determined.

10.4 - Payment

All undisputed invoices are payable within forty-five (45) days of invoice issuance date. In the event of payments not received from Client by the due date, any sum due to Service Provider will bear automatic late payment interest, starting on the day after the payment period's expiry date at three (3) times the rate of the statutory interest for commercial transactions. In addition, pursuant to Articles L. 441-10 and D. 441-5 of the French commercial Code, Client shall pay a fixed allowance of forty (40) euros for recovery costs per invoice.

10.5 - Disputed Invoices

Pending settlement or resolution of the dispute, Client's non-payment of such disputed items shall not per se constitute default by Client and shall not entitle Service Provider to suspend, delay or cease the performance or provision of the Services.

Service Provider shall promptly credit to Client any payment made to which Service Provider is not entitled hereunder, and shall refund to Client any such payment for which there are not sufficient charges against which to credit the overpayment.

10.6 - Modification of Bank Certificate

Service Provider acknowledges that Client may require a Bank Certificate from Service Provider's bank to be able to perform the payment of any charge due to Service Provider pursuant to this Agreement. In consequence, if any changes in Service Provider's bank information and related certificate(s) were to occur, a dated and signed original Bank Certificate must be sent to Client as early as possible after said change. Otherwise, Service Provider acknowledge that Client will not be in the capacity to pay any Service related invoice.

10.7 - Certificate of Tax Residence

For Services invoiced from a foreign country, Client reserves the right to ask Service Provider to provide a certificate of tax residence. Service Provider shall submit to Client a certificate of tax residence to its name and delivered by the authorized and applicable administrative authority (thereafter the "Certificate"). Payment to Service Provider of non-contested amounts pursuant to this Agreement will be contingent upon possession by Client of the Certificate and to its validity for the period of time corresponding to the concerned amounts. In consequence, Service Provider warrants, for the entire duration of this Agreement and on an annual basis, to provide Client with the appropriate Certificate.

10.8 - Travel Policy, Out-of-Pocket Expenses and Other Charges

Client shall reimburse Service Provider for all reasonable travel and out-of-pocket expenses incurred by Service Provider, provided that such expenses conform to the travel and out-of-pocket expenses policy.
Air, rail, underground, taxi, car rental and bus fares will be procured at the most economic rate. The approval is given upon travel cost estimates ex ante and the support documentation must be provided ex post. Accommodation will not exceed 100 € per nigh including breakfast
Such travel and out-of-pocket expenses shall not include Service Provider's overhead costs (or allocations thereof), general and/or administrative expenses or other mark-ups, and shall be calculated at Service Provider's actual incremental expense and shall be net of all rebates and allowances.

ARTICLE 11 - REVERSIBILITY

In the event of Contract termination, termination for part of the Services and/or Additional Services, Service Provider, upon Client's request, shall promptly carry out all necessary operations to allow Client to directly or indirectly take over the Services in the best possible way and during the time required to do this to ensure the continuity in the execution of the Services.

Service Provider shall thereby form a sufficient team from the people who participated in the implementation of the Services to carry out the reversibility process.

At the same time, Client shall set up a team sufficient in directly taking over or ensure the indirect take over by a third party, of the Services initially entrusted to Service Provider.

The reversibility operations shall include, in particular:

1/ Service Provider's return of a back-up, agreed between the Parties, of specific computer programs or software, data, files, outcomes and up-to-date operational documentation, now the property of Client;

2/ Communication by Service Provider of any information gathered that is necessary to Client in a reversibility folder which describes the scope of the Services, the latest account of the computer systems and the respective task to be carried out by Service Provider, on the one hand, and by Client or third parties, on the other hand, to ensure the reversibility. This reversibility folder shall be kept up to date throughout the duration of the Contract.

3/ Technical assistance from Service Provider, upon Client's request, to allow the acquisition of knowledge by Client or third parties.

The Parties agree to the following provisions regarding the bearing of costs for the reversibility process:

- if the reversibility is the result of a termination of the Contract at the fault of Service Provider, all reversibility process shall be carried out at the cost of Service Provider (paragraphs 1, 2 and 3);
- in other cases, the costs for reversibility process in paragraphs 1 and 2 are included in the fixed price of the Services initially entrusted to Service Provider. Client is responsible for the cost of any technical assistance (paragraph 3) that is carried out by Service Provider, at the fixed price agreed between the Parties.

ARTICLE 12 - CONFIDENTIALITY

All information provided by Client to Service Provider for the implementation of the Contract, as well as any Specific Features created by Service Provider for the implementation of the Services, are to be kept confidential.

All information of which Service Provider has knowledge in order to carry out the contract is also to be kept confidential. This includes, in particular, any information relating to Client's organisation, activities and results. The aforementioned information and/or Specific Features can only be used by Service Provider or their potential Subcontractors for the purposes of the Contract and for the implementation or delivery of the Services. They cannot be disclosed to any third party or any of Service Provider's staff members that are not assigned to the implementation or delivery of the Services, unless this disclosure is required for legal or jurisdictional reasons.

The confidentiality obligation does not apply to information provided by Client which is already in the public domain, without any breach by Service Provider of the obligation stipulated in Article 35, and/or which has been legitimately obtained by Service Provider from any third parties who have the right to disclose such information.

Service Provider undertakes to respect, and ensure their staff and potential Subcontractors respect, this confidentiality obligation for the entire duration of the Contract and for the three (3) years that follow its expiry or, regardless of the reason, for a longer duration if this has been stated in the Contract.
Service Provider shall return to Client, on expiry of the Contract regardless of the reason, all information provided by Client and data acquired by Service Provider, as well as any copies made which were held as part of the Contract implementation. On written request from Client, they shall also destroy any confidential information and data.

ARTICLE 13 - REFERENCE TO CLIENT'S BRANDS AND NAMES

Service Provider does not reserve the right to use or refer to Client's and/or the Plastic Omnium Group's company names, brands or logos, unless they have prior written consent from Client.

ARTICLE 14 - DATA PROTECTION – PROCESSING PERSONAL DATA

Service Provider declares that they have acknowledged the following legislation:

- Data protection principles,
- Regulation (EU) 2016/679 of 27 April 2016, relating to the protection of natural persons with regard to the processing of personal data and on the free movement of such data.

(Hereinafter referred to as "the Regulations").
The Client shall inform Service Provider that any information communicated to them is part of a database that benefits from the protection provided in the Regulations.
Each Party shall assume and fulfil their obligations within the meaning of Article 37.1 and 37.2.

The Client is hereinafter referred to as the exporter as they transfer all Personal Data to Service Provider.

Service Provider is hereinafter referred to as the importer as they receive the Personal Data from the Client.

Client Obligations

As an exporter, the Client accepts and guarantees the following:

- Any processing of Personal Data carried out by the Client, including its transfer, has been and will continue to be, up to the transfer, carried out in accordance with all the provisions of the Regulations.
- This processing of Personal Data shall comply with the Regulations.
- The Client shall respond, when possible, to any requests from CNIL (the national commission for information technology and civil liberties) in relation to the processing of Personal Data by the importer and any request by the person concerned in regard to the processing of their Personal Data by the importer.

With the exception of the hosting center for the solution, for which the Provider undertakes to inform the Client. The hosting center will be managed at the date of signature of the Contract by NC2 Groupe Visiativ, located in France. In the event of a change of hosting center, NOTILUS will have to inform the CLIENT beforehand, and the new hosting center will have to be located within the E.U.

Service Provider Obligations

As an importer, Service Provider accepts and guarantees and accepts sole responsibility for the following:

- They shall process any Personal Data in accordance with all legislation currently in force.
- They undertake to collect and process all Personal Data in accordance with the Regulations. In this respect, Service Provider is responsible for the processing of Personal Data.
- They shall deal with, in an appropriate and timely manner, all reasonable requests and information from the exporter or person concerned regarding the processing of the Personal Data they have transferred and will cooperate with the CNIL in any of their requests or information.
- At the request of the Personal Data exporter, the importer shall agree to an audit of their Personal Data processing methods, after a notice period of fifteen (15) days from the original request, which will be carried out by the Personal Data exporter or a regulatory body composed of independent members having the required professional skills, chosen by the Personal Data exporter and, where necessary, with the agreement of the CNIL.
- Consequently, Service Provider only has a right of access and, regarding Personal Data, a right of use limited to those necessary for the implementation of the Services, as well as the legal and/or regulatory and/or ethical obligations incumbent upon Service Provider in regard to their activity. These rights are only permitted for the duration of the Contract implementation. They are non-exclusive, non-communicable and non-transferable and shall end on the expiry date of the Contract for any reason whatsoever.
- Service Provider is prohibited from extracting and reusing all or part of the Personal Data entrusted to it.
- In particular, Service Provider undertakes not to exploit for its own account, concede or lease to third-party companies any nominative information collected in relation to the implementation of the Contract.
- The Contract does shall not lead to any transfer of ownership of such information or Personal Data.
- Service Provider undertakes to take all technical and operational measures in accordance with the best industry practice to assure the confidentiality, integrity and security of the information or Personal Data to which it has access, which is entrusted to them, or of which they have knowledge as part of the Contract, in particularly through a traceability process.
- Service Provider is strongly committed to ensuring compliance of this obligation to the Client through their staff and any of their subsidiaries and subcontractors.
- At the end of the Contract, regardless of the reason, Service Provider undertakes to immediately stop using the information contained in their database of Personal Data. They also agree to return any back-ups to the Client and to not keep any copies.
- Service Provider may only use another subcontractor after having obtained prior written agreement from the Client except for the hosting provider. For any service provider previously approved by the Client, Service Provider undertakes to conclude, and ensure that they have concluded, any contracts with their service providers that include the same obligations regarding the protection of Personal Data as those agreed between the Client and Service Provider.

The Client has the right to carry out audits and control checks of any third-party service providers in case of breach with a written prior notice. Service Provider shall ensure that their authorised third-party service providers do not transfer any Personal Data to non-member countries outside the European Union.

Upon request of the Client, Service Provider agrees to provide the Client with information relating to the content of their subcontracting agreement with any third-party service providers. This information must clearly indicate the sub-contracted processing activities, the subcontractor's identity and contact information, and the dates of the subcontracting agreement.

In the event of a Personal Data breach or violation, Service Provider shall inform the Client as soon as possible after having discovered it and shall take all appropriate corrective measures. Service Provider agrees to communicate to the Client, as soon as possible, all the information available to them in regard to the circumstances surrounding the security breach, including in particular the nature and extent of the Personal Data impacted, the number of people affected, the likely consequences and the technical conditions under which the incident occurred.

Exclusion of liability clause

Pertaining to data hosted on the servers
It is recalled that hosted data belongs to the Client which is responsible for its processing. Unless the Service Provider or a third party is involved with the data, the Client is solely responsible for the hosted dated and its accuracy.

The Service Provider undertakes to entrust the Service Provider with data that is gathered in accordance with GDPR requirements and has the characteristics of lawfulness and accuracy expected under the GDPR; does not infringe third-party rights, in particular intellectual property and privacy rights; in general, complies with the applicable French legislation and regulations.

Failing this, when notified by the Service Provider, the Client will take any action, within fifteen days, to ensure the hosted data complies with the requirements of this article. If the Client does not act, it must compensate the Service Provider for any damages it has been caused due to the non-compliance of hosted data with the requirements of this article.

Concerning processes on the servers
Consequently, and given the nature of public and private telecommunications networks, the Service Provider cannot be held liable for, among other things:

- The quality of data input by the Client users;
- Incorrect dimensioning of telecommunications lines or databases resulting from incorrect information provided by the Client;
- Contamination by computer virus by the Client users;
- Hijacking of passwords, PINs, and more generally, any information of a sensitive nature for the CLIENT, despite reasonable security measures implemented by the Service Provider;
- Bugs or faults in the Software Packages or applications used by the Client, responsibility for which is incumbent upon the respective publishers.

ARTICLE 15 - SECURITY

Service Provider agrees to comply with Client's Information Security Requirements for the provision of Services as described in Appendix 5 to this Agreement.

Client and Service Provider shall cooperate fully in efforts to prevent and cure unauthorized use of the Services by expeditiously informing each other of suspected abuse and, when known, the identity of the responsible individuals. Service Provider shall advise Client regarding methods to minimize Client's exposure to misuse and abuse of Client's service resulting from the operation of Client-provided systems, equipment, facilities or services interconnected with the Services. Service Provider shall provide assistance to Client upon request in its efforts to minimize ongoing misuse or abuse through timely reconfiguration and limitation of the Service. Appropriate representatives of Service Provider and Client shall meet at the request of Client to establish appropriate operational fraud control procedures.

Each Party shall advise the other as soon as it is aware of any security breach or potential security breach which may affect the Services or Plastic Omnium Group's reputation.

ARTICLE 16 - WARRANTIES

16.1 - Nature of Services

Service Provider warrants that (a) it has described its Services accurately and fairly and shall refrain from any misleading or unethical business practices; (b) the Services, Deliverables, processes and technologies used by Service Provider, meet highest industry standards and are flexible, scalable and modular enough, to allow integration with current and new technologies or processes, and changes in Client's objectives and organization; (c) it will perform the Services with all the dedication and expertise that one can expect from a leading information technology firm, on an obligation of results basis and, when applicable, in compliance with the agreed service levels; (d) the operation of the System and the delivery of the Services will, at least, meet and comply with the Service Levels or commitments;

16.2 - Non-Interference

The implementation, maintenance and provision of the Services shall be performed (a) in conformity with reasonable precautions designed to promote safety, avoid accidents and prevent injury to person or property at the Installation Sites; (b) in such a manner as will not, except as consented to in writing by Client in advance, (i) create any hazardous condition or interfere with or impair in any material respect the operation of the heating, ventilation, air conditioning, plumbing, electrical, fire protection, safety, security, public utilities or other systems or facilities at the Installation Sites; (ii) interfere with the use or occupancy of common areas of the Installation Sites or the premises of any tenant occupying any space therein; (iii) delay, restrict, impose any tasks, costs or obligations other than as set forth herein upon Client with respect to, or interfere in any material respect with, the use or operation of the Installation Sites; and (d) in such a manner as will minimize any financial, technical or operational burdens on Client or the disruption to Client's normal business operations that might arise as a result of such activities. Service Provider shall impose no premium charge for the performance of its installation, maintenance or repair obligations outside Normal Business Hours at any Installation Site.

16.3 - Authority and Good Standing

Service Provider and Client each have and shall maintain full power and authority to enter into this Agreement without the consent of any other person.

Service Provider warrants that this Agreement is not subject to or subordinate to any right of Service Provider's creditors or, if such subordination exists, this Agreement or instrument creating such subordination provides for the non-disturbance of Client as long as Client shall not be in default hereunder.

Service Provider warrants that it is not in default or otherwise in non-compliance in any material respect with any contract, agreement or other arrangement for goods, services or technology the termination of which might reasonably be expected to have a material adverse effect on Service Provider's ability to perform any of its obligations hereunder. Service Provider shall use its best efforts to remain in compliance with the terms and conditions of all such contract, agreements or other arrangements.

16.4 - No Conflict

This Agreement and the transactions contemplated hereby are not in conflict in any material respect with any other agreements or judicial or administrative orders to which Service Provider or Client are a Party or by which they may be bound.

16.5 - Third Party Warranties

Service Provider shall (at no additional cost to Client) pass through to Client and enforce on Client's behalf all of the representations, warranties, indemnifications (including reimbursement of expenses and attorneys' fees) and other benefits designed for protection of the user or purchaser that accrue to Service Provider under each agreement with any Service Provider Subcontractor or agent participating in the provision of Services.

To the extent Service Provider deems it necessary to effect such pass through, Service Provider shall cause Client to be named as a Third Party beneficiary of such agreements; provided that this Section does not contemplate formal assignment from Service Provider to Client of rights under any such agreement, except as otherwise provided in this Agreement.

16.6 - Malicious Code

Service Provider warrants that it shall take commercially reasonable actions and precautions to prevent the introduction and proliferation of any Malicious Code into Client's operating environment. Without limiting Service Provider's other obligations under this Agreement, Service Provider warrants that, in the event any Malicious Code is found in the systems used to provide the Services, (i) if such Malicious Code originated in the equipment, software or other resources provided by Service Provider under this Agreement, Service Provider shall remove such Malicious Code at its expense and indemnify Client for all losses incurred by Client as a result of such Malicious Code, and (ii) in any case (wherever such Malicious Code originated), Service Provider shall exercise commercially reasonable efforts at no additional cost to eliminate, and reduce the effects of, the Malicious Code and, if the Malicious Code causes a loss of operational efficiency or loss of data, to mitigate such losses and restore such data with generally accepted data restoration techniques.

16.7 - Disabling Code

Service Provider warrants that, without the prior written consent of Client, Service Provider shall not insert into the software any code that could be invoked to disable or otherwise shut down all or any portion of the Services. Service Provider further warrants that, with respect to any disabling code that may be part of the software, Service Provider shall not invoke or cause to be invoked such disabling code at any time, including upon expiration or termination of this Agreement for any reason, without Client's prior written consent.

16.8 - Conflict of interest

Service Provider shall maintain a process for identifying and managing conflicts of interest to ensure that no explicit or potential conflict of interests jeopardize the provision of the Services to Client and Service Provider shall notify Client as soon as practicable if the performance of the Services, or any instructions or directions from Client, pose a conflict of interest.

Without prejudice to the foregoing Service Provider shall take such action as is necessary to ensure that any identified conflict of interest is either eliminated or managed to Client's satisfaction whilst ensuring that the provision of the Services is not interrupted and the Services continue to be met to the standards required by this Agreement.

ARTICLE 17 - AUDIT

17.1 - Record Keeping

Service Provider shall keep detailed records of all activities carried out in connection with the provision of the Services ("Service Records") during the Term of this Agreement and for at least five (5) years after the expiry or earlier termination of this Agreement.

17.2 - Audit Scope

Subject to Service Provider's reasonable security requirements, Client may audit Service Provider's books, records and other documents to assess Service Provider's compliance with this Agreement (the "Audit"), including (without limitation):

(a) Service Records;
(b) Service Provider's performance of the Services notably but not exclusively with regard to the Service Levels, continuing improvement obligations and compliance with the Security Policy;
(c) all or any aspects of the provision of the Services including accuracy of the Charges and of the billing;
(d) the accuracy and truthfulness of any information or representation provided to Client in accordance with this Agreement;
(e) the nature and extent of the skills of those of Service Provider Personnel assigned to the Services;

(f) compliance with Service Provider's obligations under this Agreement relating to CONFIDENTIALITY, DATA PRIVACY AND SECURITY;
(g) compliance with Corporate Responsibilities.

For the avoidance of doubt, any and all records detailed herein shall be subject to the dispositions of ARTICLE 12 – CONFIDENTIALITY.

Service Provider shall cause each Service Provider Subcontractor if any, to permit Client to conduct an audit pursuant to this Section of such Subcontractor's provision of goods or performance of services at Service Provider's premises that are material components of the Services provided by Service Provider to Client.

17.3 - Periodicity

Audits may be carried out once per contractual year with a reasonable notice (which may be short, but no less than ten (10) Business Day) unless such Audit is required by Client for reasons of suspected fraud or noncompliance with the agreed security and data privacy requirements set out in this Agreement.

Service Provider shall give Client not less than sixty (60) days' notice of Service Provider's intention to destroy or otherwise dispose of any Service Records which are not required to be kept by it, and shall not destroy any such Service Records unless and until Client has had a reasonable opportunity to recover such Service Records and Client has not requested that the Service Records be delivered to it (together with the Retrieval Systems).

17.4 - Cooperation

Service Provider shall provide Client and its agents and representatives, and to any statutory or regulatory auditors of Client, reasonable assistance and access to its premises as may be necessary in order that they may fully and promptly carry out each Audit.

Access to premises or web links provided to Client as reasonably required to perform the Audit shall be subject to Client's strict adherence to Service Provider's safety, security and privacy policies and procedures then in effect and communicated in writing to Client.

Client will take all necessary care to avoid loss or damage to Service Provider property and to prevent unnecessary and excessive consumption of Service Provider Personnel's time. Client will indemnify Service Provider for any resulting damage to Service Provider's property and additional costs incurred by Service Provider in pursuant to facilitating the Audit.

17.5 - Report and Follow-up

A copy of the Audit report will be delivered to Service Provider when finalized. Should the Audit report identify a breach by Service Provider of its contractual obligations, Service Provider undertakes (i) to provide Client with an action plan to cure the default(s) within five (5) Business Days following the date of receipt of the Audit report by Service Provider and (ii), unless a longer time period is expressly agreed by Client in certain specific circumstances, to implement the corrective measures within ten (10) Business Days following Client's approval on the action plan proposed by Service Provider. This action plan may include making refund of any overpayment by Client in the form of a credit on the invoice for the first full billing cycle after the Parties have agreed upon the accuracy of the Audit results.

If Client determines that the required corrective measures have not been implemented by Service Provider within the aforementioned ten (10) Business Days period (or agreed longer period), Client may terminate this Agreement for breach of contract.

17.6 - Costs

It is hereby understood that, except as otherwise stated in this ARTICLE 17 – AUDIT, any fees or costs incurred by Client, or any incremental costs incurred by Service Provider in complying with Client audit requirements in connection with this ARTICLE 17– AUDIT, shall be the responsibility of Client.

In the event that any such Audit reveals any irregularities or breaches from Service Provider, without prejudice to any other remedies available to Client, Service Provider shall compensate Client for the internal and external cost of such Audit.

ARTICLE 18 - LIABILITY

18.1 - Liability Cap

Service Provider's and Client's liability to each other shall be limited to three (3) times the total value in its aggregate of this Agreement (the "Liability Cap").

THE FOLLOWING SHALL NOT BE COUNTED TOWARD THE LIABILITY CAP:
(a) AMOUNTS EXPENDED BY OR FOR SERVICE PROVIDER TO REMEDY NON-CONFORMING SERVICES OR DELIVERABLES;
(b) DELAY CREDITS, PERFORMANCE CREDITS AND PERFORMANCE FAILURE CREDITS ASSESSED AGAINST SERVICE PROVIDER; OR

(c) AMOUNTS WITHHELD BY CLIENT IN ACCORDANCE WITH THIS AGREEMENT DUE EITHER TO INCORRECT CHARGES BY SERVICE PROVIDER OR NON-CONFORMING SERVICES.

NOTHING IN THIS AGREEMENT SHALL EXCLUDE OR LIMIT:

(a) EITHER PARTY'S LIABILITY FOR DEATH OR PERSONAL INJURY OR LOSS OF OR DAMAGE TO TANGIBLE REAL OR TANGIBLE PERSONAL PROPERTY (INCLUDING DAMAGE TO THEIR PROPERTY) OR THE ENVIRONMENT CAUSED BY ITS (OR ITS AGENT'S OR SUB CONTRACTOR'S) NEGLIGENCE OR FOR FRAUD OR FRAUDULENT MISREPRESENTATION;
(b) SERVICE PROVIDER'S LIABILITY, WHETHER CATEGORIZED AS DIRECT OR INDIRECT DAMAGE, TO CLIENT ARISING OUT OF A BREACH OF ARTICLE XIV - REGULATORY REQUIREMENTS – COMPLIANCE WITH LAW, ARTICLE X – CONFIDENTIALITY, ARTICLE XI – DATA PRIVACY, ARTICLE XII - SECURITY, ARTICLE VIII – INTELECTUAL PROPERTY RIGHTS;
(c) CLIENT'S LIABILITY, WHETHER CATEGORIZED AS DIRECT OR INDIRECT DAMAGE, TO SERVICE PROVIDER ARISING OUT OF A BREACH OF ARTICLE X – CONFIDENTIALITY;
(d) LOSS OF, CORRUPTION TO, ALTERATION AND/OR RESTORATION OF CLIENT DATA
(e) EITHER PARTY'S LIABILITY FOR WILFUL OR INTENTIONAL MISCONDUCT OR GROSS NEGLIGENCE;
(f) SERVICE PROVIDER'S LIABILITY UNDER ANY WARRANTY AND/OR INDEMNITY SET OUT IN THIS AGREEMENT;
(g) EITHER PARTY'S LIABILITY THAT CANNOT, AS A MATTER OF LAW, BE LIMITED OR EXCLUDED.

18.2 - Exclusion of Liability

Neither Party will be liable to the other Party for any indirect, consequential or special loss arising out of, or in connection with this Agreement. The following types of Losses are agreed to be non-exhaustive, direct and recoverable Losses under this Agreement in each case to the extent caused by the Service Provider's failure to comply with the terms and conditions of this Agreement:

(a) Reasonably incurred additional and/or administrative costs and expenses incurred by Client arising from a Service Failure;
(b) the reasonably incurred cost of selecting, procuring and implementing any alternative or replacement or additional services which are intended to meet the same or substantially similar business requirements and objectives as those intended to be met by the Services, whether internally or through or with a Third Party;
(c) reasonably incurred additional costs of transferring the Services to a Replacement Service Provider arising from a Service Failure;
(d) any Losses incurred by a Client of Client, and any claims made by a Client of Client against Client in respect of such Losses; and
(e) any Operational Loss.

18.3 - Client Failure

Service Provider shall only not be in breach of this Agreement if and to the extent:

(a) Service Provider's non-performance results directly from a failure from Client to comply with its responsibilities as provided in this Agreement or a Force Majeure Event ("Relief Event");
(b) Service Provider uses its best efforts to mitigate the Relief Event and to perform the Services notwithstanding; and
(c) Service Provider notifies Client as soon as Service Provider becomes aware of the Relief Event via a written notice ("Relief Notice").

Such Relief Notice shall specify the following information:

(a) the affected Services;
(b) the cause(s) of the delay or interruption; and
(c) details of the extent of the likely delay or interruption.

Relief Notices shall only bind Client when it has confirmed in writing that it accepts the contents of the particular Relief Notice. Any dispute as to any submitted Relief Notice shall be submitted for resolution in accordance with ARTICLE XXVIII - DISPUTE RESOLUTION. Notwithstanding the submission of a Relief Notice, Service Provider shall perform and/or recommence performance of the affected Services as soon as possible.

18.4 - Liability Under Third Party Arrangements

No contract, subcontract, or other agreement entered into by Service Provider with any Third Party in connection with its provision of Services (including any such agreement assigned by Client to Service Provider) shall provide for any indemnity, guarantee, assumption of liability or other obligation of Client with respect to such arrangements, except as consented to in writing by Client.

ARTICLE 19 - INSURANCES

Service Provider agrees to take out and maintain, at their own cost, an insurance policy with a reputable and financially-sound insurance company that is able to cover Service Provider's towards Client and third parties. This insurance policy shall in no way be seen as a limitation of Service Provider's liability.

Service Provider shall, at the Effective Date of this Agreement and as when each policy of insurance is renewed (and, in any event, on request from Client), provide Client with certificates of insurance or such evidence that Client may reasonably require (including evidence of renewal of insurance) evidencing all of the coverage referenced above together with evidence of payment of the last premium.

ARTICLE 20 - COMPLIANCE, PERFORMANCE OBLIGATIONS AND DELIVERY TIMEFRAMES – PENALTIES

The Service provider is under an obligation of performance in regard to:

- attaining the service level agreements performance described in the Contract,
- keeping to delivery and implementation timeframes and dates.

When the Service provider is aware that a specified timeframe or date is going to be missed, the Service provider must inform the Client immediately, in writing, of the extent and reasons for this non-compliance and offer the appropriate corrective action. The Client is within their rights to refuse this action.

In case of non-compliance with the service levels or the respect of the planning for the project, the penalties will apply ipso jure and with prior written notice.

The Client's objective for the penalty system is to ensure the capacity of the Service Provider, to maintain its commitments in terms of Service Levels as and when the services are provided.

The penalties for the project

The penalty shall cover any damage resulting from the first week. Beyond this period, the Client can request compensation for damages resulting from the delay to cover any damages and costs.
They do not affect the Client's right to terminate the Contract under the provisions of Article 23.2 ("Termination for breach") and to claim damages from the Service provider, beyond the week-long delay in implementation or delivery, as well as a refund for the amount(s) already paid by the Licensee for the part of the Supply that has not yet been implemented on the date of the contract termination. The amount of penalties due will be deducted from the next invoice issued by the Service Provider or the CLIENT will issue a credit note.

The penalty analysis is based on pre-planning document per country attached in the Appendix 1. This planning which will be provided by the service provider within the Kick-off meeting(document freeze). The Parties agree to make this planning as an addendum to the main contract. As soon as on other entity will request the benefit of this contract, a dedicated planning will be established according to this clause. Within this document the main project milestones and performance dates are precisely described and imperative to follow. On this scale of milestones penalties shall apply within the following period, starting from milestone "assistance of settings" to final go live of each module (Expense/Travel) per dedicated country. This penalty in case the delay is due to the Service provider's fault. This logic shall apply for both modules which will be implemented one by one with the same milestones process. If any time deviation in this period occur following penalties shall apply: 800 €/ day of delay capped at 10 % of total development costs for each module (Expense and/ or Travel- see appendix 9 per dedicated country (without Governance costs).

The penalties for the SLA regulations

KPIs, Service Levels and the Penalty Calculation System are explained in the Appendix 3- "In service support".

The penalty shall cover any damage resulting from the first month. Beyond this period, the Client can request compensation for damages resulting from the delay to cover any damages and costs.
They do not affect the Client's right to terminate the Contract under the provisions of Article 23.2 ("Termination for breach") and to claim damages from the Service provider. The amount of penalties due will be deducted from the next invoice issued by the Service Provider or or the Client will issue a credit note.

Each month, Penalties may not exceed twenty (20%) of the monthly Saas invoice.

In case of non-compliance with the service levels, the penalties will apply ipso jure.

ARTICLE 21 - FORCE MAJEURE

No Party is seen to have failed in their contractual obligations if their non-implementation is the result of a case of force majeure as recognised by case law. A case of force majeure only releases the Party concerned from their contractual obligations insofar as and during the period in which they are not able to carry out such obligations. Each Party is responsible for any costs incurred by them as the result of a force majeure.

The Party affected by a case of force majeure shall immediately notify the other Party and provide all relevant information by fax, email or registered letter with an acknowledgement of receipt. The other Party reserves the right to check and verify the reality of the situation. The Party who invokes a case of force majeure shall make every effort to minimise any adverse effects resulting from the situation.

In any event, any strikes limited to Service Provider's staff or their potential Subcontractors do not relieve Service Provider of their responsibility in case of an implementation delay or impediment.

If the event which has given rise to a force majeure lasts more than fifteen (15) consecutive calendar days, the Party which the force majeure is opposed are within their rights to immediately cancel the Contract without any penalties. Service Provider shall reimburse any amounts already paid to Client as part of the Contract that do not relate to a Service that has already been implemented or delivered before the data the force majeure occurred.

ARTICLE 22 - TRANSFER – SUBCONTRACTORS

22.1 - Transfer/Change of control

Service Provider does not have the right to assign all of part of the Contract to a third party without the prior written consent of Client. Client may assign all or part of the Contract to an entity of the Plastic Omnium Group upon prior written notice to Service Provider.

In the event of a change of control, Service Provider must immediately notify Client. A change of control relating to Service Provider means any supply, transfer, merger or other operation that could modify the direct or indirect control of Service Provider; control is defined as directly or indirectly holding the majority of shares conferring the right to vote or the right to elect the majority of the Members of Service Provider's Board of Directors.

22.2 - Subcontractors

Service Provider may not outsource the Contract to a Subcontractor. If Service Provider wants to assign part of the Contract to a Subcontractor, they must:

- provide Client with information about their suppliers, in advance and in writing. They must specify the type and origin of the Services concerned and comply with any applicable legal provisions;
- receive prior written consent from Client in regard to subcontractors and comply with any applicable legal provisions. Any request for an agreement shall indicate, among other information, the type and extent of the Services they intend to outsource and the presented subcontractor's qualifications. Service Provider prohibits their subcontractors from outsourcing all or part of the Services subcontracted to them by Service Provider, unless Client agrees in accordance with the aforementioned provisions.

If Service Provider fails to comply with any legal obligations relating to subcontracting, Client reserves the right to immediately stop any payments to Service Provider and can continue to do so while Service Provider does not comply with said legal provisions. This does not entail any prejudice to the right of Client to cancel the Contract under the provisions of Article 22.5

Service Provider must ensure that any subcontracting agreement or supply of provisions concluded with any Subcontractor contains the same obligations between Service Provider and Subcontractor as those defined in the Contract. This is Service Provider's responsibility.
In any case, Client's permission for Service Provider to use a Subcontractor does not release Service Provider from any of their contractual obligations in regard to the part of the Services that has been outsourced. Service Provider remains solely responsible for the proper implementation of the Services. Additionally, Service Provider guarantees Client against any claim made by their Subcontractors or the Subcontractor's staff.

ARTICLE 23 - TERM AND TERMINATION

23.1 - Term

This Agreement shall commence as of the date of the signature and shall remain in force for a period of (36) months starting from the first invoice of licenses unless terminated earlier according to this Agreement provisions (the "Initial Term"). The Parties may extend the term of this Agreement for a period equal to or shorter than the Initial Term (the aggregate period thereafter designated as the "Term"). The Parties are free to extend the Term of this Agreement as often as they need to. Service Provider shall provide to Client a three (3) months advance written notice before the term of this Agreement in order to ascertain the will of Client to renew this Agreement.

23.2 - Termination for breach

Each Party shall be entitled to terminate the Contract in the case of breach of one of the other Party's obligations. This is done after a formal notice is sent by registered letter with an acknowledgement of receipt, fifteen (15) calendar days after the breach. The Client can especially terminate the Contract if there is a defect or failure in relation to Compliance or in the Services implementation conditions.

The Client has the right to terminate the Contract without formal notice (i) when there are repeated defects or failures from the Service Provider as provided in Article 22.2, or (ii) due to Service Provider's failure to comply with a regulation concerning health, hygiene, security, environment, or (iii) in any other cases of termination as provided in the Contract. This termination takes effect upon receipt of the termination notification by the Licensor.

If the Contract has been terminated by the Client for breach, the Service Provider must immediately reimburse the Client for any payments that have already been made by the Client, as they exceed the value of a Services that is recognised as Compliant by the Client, or any amounts that have been paid in advance, including any maintenance or governance fees which must be reimbursed pro rata temporis. The Client may also charge the Service Provider for any additional costs required for the completion of the Services by the Client themselves or through a third party.

23.3 - Termination for Convenience

Client may elect to terminate for convenience, upon a three (3) months prior written notice to Service Provider, this Agreement in totality or only partially. Client shall pay Service Provider, on a proportional basis, for the Services adequately performed before the effective date of termination. In case of such early termination initiated by Client, Client shall pay a lump-sum fixed indemnity, exclusive and in place of any other compensation, equal to fifty percent (50%) of the amounts still due to Service Provider for the current year.
The Termination could be total or partial restricted to one geographical area or one division.

With respect to any such termination: (i) Client shall in no event be required to pay any other fees, costs or expenses to Service Provider with respect to any such termination; and (ii) Client shall have no further liabilities or obligations to Service Provider under this Agreement.

23.4 - Change in Control

This Agreement is concluded intuitu personae, by express consideration of Service Provider and forms an essential element of this Agreement without which Client would not have entered into.
Therefore, if:

(a) Service provider is under control by a direct competitor of Plastic Omimum's affiliate.
(b) Service provider is under control by an entity which does not fulfill its obligations of security and compliance.

then, at any time within twelve (12) months after the last occurrence of such events, Client may, upon giving Service Provider prior written notice, as of right without judicial formalities terminate this Agreement without penalty and without payment of any termination fees.

23.5 - Cancellation for non-implementation

Each Party can, by law, cancel the Contract in the case of non-implementation of one of the other Party's obligations. This is done after a formal notice is sent by registered letter with an acknowledgement of receipt, fifteen (15) calendar days after the non-implementation. Client can especially cancel the Contract if there is a defect or failure in relation to Compliance or in the Services implementation conditions.

Client has the right, by law, to cancel the Contract without formal notice (i) when there are repeated defects or failures from Service Provider, or (ii) due to Service Provider's failure to comply with a regulation concerning health, hygiene, security, environment, or (iii) in any other cases of termination as provided in the Contract. This cancellation takes effect upon receipt of the cancellation notification by Service Provider.

If the Contract has been terminated by Client for non-implementation reasons, Service Provider must immediately reimburse Client for any payments that have already been made by Client, as they exceed the value of a Service that is recognised as Compliant by Client, or any amounts that have been paid in advance, including any maintenance fees which must be reimbursed pro rata temporis. Client may also charge Service Provider for any additional costs required for the completion of the Services by Client themselves or through a third party.

23.6 - Cancellation due to bankruptcy

Unless otherwise stated in public policy, Client may immediately cancel the Contract, by law and without formal notice, if Service Provider goes into liquidation, administration, settlement by mutual consent or becomes bankrupt.

23.7 - Survival

Notwithstanding the foregoing, any terms and conditions of this Agreement expressly identified or that would by their nature survive the expiration or termination of this Agreement, for any reason whatsoever, shall so survive including, by way of illustration only and not limitation, the terms of ARTICLE VIII – INTELECTUAL PROPERTY RIGHTS, ARTICLE XII – CONFIDENTIALITY, ARTICLE XIV – DATA PROTECTION-PROCESSING PERSONAL DATA, ARTICLE XVI - WARRANTIES, ARTICLE XXIV – APPLICABLE LEGISLATION/DISPUTES

ARTICLE 24 - APPLICABLE LEGISLATION/DISPUTES

UNLESS OTHERWISE STATED IN THE CONTRACT, ALL CONTRACT DISPUTES ARE SUBJECT TO FRENCH LAW AND THE TRIBUNAL DE COMMERCE (COMMERCIAL COURT) IN NANTERRE.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

CLIENT AND SERVICE PROVIDER EXPRESSLY WAIVE THE APPLICATION OF THE UNITED NATIONS CONVENTION ON CONTRACTS FOR THE INTERNATIONAL SALE OF GOODS, CONCLUDED IN VIENNA ON 11 APRIL 1980.

ARTICLE 25 - MISCELLANEOUS PROVISIONS

25.1 - Independence of the Parties

The Contract is concluded between independent parties. None of its provisions can be construed as giving any of the Parties the power or authorisation to act on behalf of another Party or as constituting any association or partnership between the Parties or as constituting any solidarity between them.

25.2 - Partial nullity

If a provision of the Contract becomes void under a law, regulation or decision taken by the court, it shall be treated as if it never existed. However, the other provisions of the Contract shall remain in force.

25.3 - Neither Party Considered Drafter

Despite the possibility that one Party may have prepared the initial draft of this Agreement and/or played the greater role in the preparation of subsequent drafts, the Parties agree that neither of them shall be deemed the drafter of this Agreement, and that, in construing this Agreement in case of any claim that any provision hereof may be ambiguous, no such provision shall be construed in favor of one Party on the ground that such provision was drafted by the other Party.

25.4 - Imprevision

The Parties hereby expressly waive all rights to invoke Article 1195 of French Civil Code. Each Party acknowledges and accepts all risks of significant change in the circumstances of this Agreement, except as expressly provided in this Agreement.

25.5 - Non-waiver

If one of the Parties does not at any time require the other Party to fulfil their obligations in full, this may in no circumstances be considered as a waiver of their obligation for their subsequent performance.

25.6 - Counterparts; Digital signature.

This Agreement may be executed in one or more counterparts, each of which shall be deemed an original, but all of which together shall constitute one and the same Agreement. The Parties agree that a digital signature may substitute for and have the same legal effect as the original signature.

DocuSign Envelope ID: 804D232C-F4D1-4D0C-A3B7-DD2E57C1BD4B

SERVICE PROVIDER	CLIENT
NAME : Gilles BOBICHON Acting as : Chief operating officer	NAME : Pascal ZEMBRA Acting as : VP Information Systems
Date : Signature :	Date : Signature :

DocuSign

Certificat de réalisation

Identifiant d'enveloppe: 804D232CF4D14D0CA3B7DD2E57C1BD4B

État: Complétée

Objet: Complete with DocuSign: Appendix 1 Service description+planning POG SA 22331 .docx, Appendix 2 ...

Enveloppe source:

Nombre de pages du document: 137

Signatures: 2

Nombre de pages du certificat: 5

Paraphe: 0

Signature dirigée: Activé

Horodatage de l'enveloppe: Activé

Fuseau horaire: (UTC+01:00) Bruxelles, Copenhague, Madrid, Paris

Émetteur de l'enveloppe:
Anne Hugonet
1 Allée Pierre BURELLE
LEVALLOIS PERRET CEDEX, . 92593
anne.hugonet@plasticomnium.com
Adresse IP: 46.235.153.61

Suivi du dossier

État: Original
29/09/2022 17:54:08

Titulaire: Anne Hugonet
anne.hugonet@plasticomnium.com

Emplacement: DocuSign

Événements de signataire	Signature	Horodatage
Gilles BOBICHON gbobichon@cegid.com Directeur Niveau de sécurité: E-mail, Authentification de compte (aucune)	Sélection d'une signature : Écrit sur un appareil En utilisant l'adresse IP: 86.248.23.87 Signé à l'aide d'un périphérique mobile	Envoyée: 29/09/2022 18:14:18 Consultée: 29/09/2022 21:44:19 Signée: 29/09/2022 21:49:17

Divulgation relative aux Signatures et aux Dossiers électroniques:
Accepté: 29/09/2022 21:44:19
ID: af50bafd-2d8e-4460-a934-8fbac60e6c1b

pascal zembra pascal.zembra@plasticomnium.com Directeur des Systèmes d'Information Groupe Plastic Omnium Gestion Niveau de sécurité: E-mail, Authentification de compte (aucune)	pascal zembra Sélection d'une signature : Style présélectionné En utilisant l'adresse IP: 46.235.155.239	Envoyée: 29/09/2022 18:14:18 Consultée: 30/09/2022 08:59:44 Signée: 30/09/2022 08:59:51

Divulgation relative aux Signatures et aux Dossiers électroniques:
Accepté: 30/09/2022 08:59:44
ID: 0335af68-15b9-49ba-935b-f07593bcfdd6

Événements de signataire en personne	Signature	Horodatage

Événements de livraison à l'éditeur	État	Horodatage

Événements de livraison à l'agent	État	Horodatage

Événements de livraison intermédiaire	État	Horodatage

Événements de livraison certifiée	État	Horodatage

Événements de copie carbone	État	Horodatage
alexandre fabbro afabbro@cegid.com Niveau de sécurité: E-mail, Authentification de compte (aucune)	**Copié**	Envoyée: 29/09/2022 18:14:19 Consultée: 29/09/2022 18:16:34

Divulgation relative aux Signatures et aux Dossiers électroniques:
Non offert par DocuSign

Événements de copie carbone	État	Horodatage
bruno TAMMARO bruno.tammaro@plasticomnium.com IT purchasing manager grp Plastic Omnium gestion Niveau de sécurité: E-mail, Authentification de compte (aucune) **Divulgation relative aux Signatures et aux Dossiers électroniques:** Accepté: 25/07/2022 16:41:50 ID: 85785d64-2b9f-414f-b048-9d73cf63c9e8	**Copié**	Envoyée: 29/09/2022 18:14:20
katja JUENGER katja.juenger@plasticomnium.com Niveau de sécurité: E-mail, Authentification de compte (aucune) **Divulgation relative aux Signatures et aux Dossiers électroniques:** Non offert par DocuSign	**Copié**	Envoyée: 29/09/2022 18:14:21 Consultée: 30/09/2022 07:36:51
melissa pires melissa.pires@plasticomnium.com MRO Buyer (IT) Clean Energy System Niveau de sécurité: E-mail, Authentification de compte (aucune) **Divulgation relative aux Signatures et aux Dossiers électroniques:** Non offert par DocuSign	**Copié**	Envoyée: 29/09/2022 18:14:20 Consultée: 30/09/2022 09:49:23
nicolas rousseau nrousseaux@cegid.com Niveau de sécurité: E-mail, Authentification de compte (aucune) **Divulgation relative aux Signatures et aux Dossiers électroniques:** Non offert par DocuSign	**Copié**	Envoyée: 29/09/2022 18:14:21
PO contract Leader lyesse.kouroughli_ext@plasticomnium.com Niveau de sécurité: E-mail, Authentification de compte (aucune) **Divulgation relative aux Signatures et aux Dossiers électroniques:** Accepté: 19/07/2022 11:42:57 ID: 8840b849-bf10-42e4-a80e-f4def0f023d2	**Copié**	Envoyée: 29/09/2022 18:14:19 Consultée: 30/09/2022 13:56:04

Événements de témoins	Signature	Horodatage

Événements notariaux	Signature	Horodatage

Récapitulatif des événements de l'enveloppe	État	Horodatages
Enveloppe envoyée	Haché/crypté	29/09/2022 18:14:21
Livraison certifiée	Sécurité vérifiée	30/09/2022 08:59:44
Signature complétée	Sécurité vérifiée	30/09/2022 08:59:51
Complétée	Sécurité vérifiée	30/09/2022 08:59:51

Événements de paiement	État	Horodatages

Divulgation relative aux Signatures et aux Dossiers électroniques

ELECTRONIC RECORD AND SIGNATURE DISCLOSURE

From time to time, PLASTIC OMNIUM GESTION (we, us or Company) may be required by law to provide to you certain written notices or disclosures. Described below are the terms and conditions for providing to you such notices and disclosures electronically through the DocuSign system. Please read the information below carefully and thoroughly, and if you can access this information electronically to your satisfaction and agree to this Electronic Record and Signature Disclosure (ERSD), please confirm your agreement by selecting the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

Getting paper copies

At any time, you may request from us a paper copy of any record provided or made available electronically to you by us. You will have the ability to download and print documents we send to you through the DocuSign system during and immediately after the signing session and, if you elect to create a DocuSign account, you may access the documents for a limited period of time (usually 30 days) after such documents are first sent to you. After such time, if you wish for us to send you paper copies of any such documents from our office to you, you will be charged a $0.00 per-page fee. You may request delivery of such paper copies from us by following the procedure described below.

Withdrawing your consent

If you decide to receive notices and disclosures from us electronically, you may at any time change your mind and tell us that thereafter you want to receive required notices and disclosures only in paper format. How you must inform us of your decision to receive future notices and disclosure in paper format and withdraw your consent to receive notices and disclosures electronically is described below.

Consequences of changing your mind

If you elect to receive required notices and disclosures only in paper format, it will slow the speed at which we can complete certain steps in transactions with you and delivering services to you because we will need first to send the required notices or disclosures to you in paper format, and then wait until we receive back from you your acknowledgment of your receipt of such paper notices or disclosures. Further, you will no longer be able to use the DocuSign system to receive required notices and consents electronically from us or to sign electronically documents from us.

All notices and disclosures will be sent to you electronically

Unless you tell us otherwise in accordance with the procedures described herein, we will provide electronically to you through the DocuSign system all required notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you during the course of our relationship with you. To reduce the chance of you inadvertently not receiving any notice or disclosure, we prefer to provide all of the required notices and disclosures to you by the same method and to the same address that you have given us. Thus, you can receive all the disclosures and notices electronically or in paper format through the paper mail delivery system. If you do not agree with this process, please let us know as described below. Please also see the paragraph immediately above that describes the consequences of your electing not to receive delivery of the notices and disclosures electronically from us.

How to contact PLASTIC OMNIUM GESTION:

You may contact us to let us know of your changes as to how we may contact you electronically, to request paper copies of certain information from us, and to withdraw your prior consent to receive notices and disclosures electronically as follows:
To contact us by email send messages to: bruno.asselin@plasticomnium.com

To advise PLASTIC OMNIUM GESTION of your new email address

To let us know of a change in your email address where we should send notices and disclosures electronically to you, you must send an email message to us at bruno.asselin@plasticomnium.com and in the body of such request you must state: your previous email address, your new email address. We do not require any other information from you to change your email address.

If you created a DocuSign account, you may update it with your new email address through your account preferences.

To request paper copies from PLASTIC OMNIUM GESTION

To request delivery from us of paper copies of the notices and disclosures previously provided by us to you electronically, you must send us an email to bruno.asselin@plasticomnium.com and in the body of such request you must state your email address, full name, mailing address, and telephone number. We will bill you for any fees at that time, if any.

To withdraw your consent with PLASTIC OMNIUM GESTION

To inform us that you no longer wish to receive future notices and disclosures in electronic format you may:

i. decline to sign a document from within your signing session, and on the subsequent page, select the check-box indicating you wish to withdraw your consent, or you may;

ii. send us an email to bruno.asselin@plasticomnium.com and in the body of such request you must state your email, full name, mailing address, and telephone number. We do not need any other information from you to withdraw consent.. The consequences of your withdrawing consent for online documents will be that transactions may take a longer time to process..

Required hardware and software

The minimum system requirements for using the DocuSign system may change over time. The current system requirements are found here: https://support.docusign.com/guides/signer-guide-signing-system-requirements.

Acknowledging your access and consent to receive and sign documents electronically

To confirm to us that you can access this information electronically, which will be similar to other electronic notices and disclosures that we will provide to you, please confirm that you have read this ERSD, and (i) that you are able to print on paper or electronically save this ERSD for your future reference and access; or (ii) that you are able to email this ERSD to an email address where you will be able to print on paper or save it for your future reference and access. Further, if you consent to receiving notices and disclosures exclusively in electronic format as described herein, then select the check-box next to 'I agree to use electronic records and signatures' before clicking 'CONTINUE' within the DocuSign system.

By selecting the check-box next to 'I agree to use electronic records and signatures', you confirm that:

- You can access and read this Electronic Record and Signature Disclosure; and
- You can print on paper this Electronic Record and Signature Disclosure, or save or send this Electronic Record and Disclosure to a location where you can print it, for future reference and access; and
- Until or unless you notify PLASTIC OMNIUM GESTION as described above, you consent to receive exclusively through electronic means all notices, disclosures, authorizations, acknowledgements, and other documents that are required to be provided or made available to you by PLASTIC OMNIUM GESTION during the course of your relationship with PLASTIC OMNIUM GESTION.