Unit4 Data Processing Information incorporating EU SCCs

SECTION 1 - DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

1. THE PERSONAL DATA THAT WILL BE PROCESSED:

Product	Personal Data that may be processed might include:	To whom this may belong:
Unit4 ERP x	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
Unit4 ERP 7	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
Unit4 Financials	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above.	Current or former employees; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
Unit4 Student Management	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information; date of birth; age; place of birth; nationality or citizenship; residency; domicile; spoken language(s); passport number; national security number or social security number or ID card reference; marital status; beneficiary details under benefits; gender; employment information (including: salary; position; pay scale; pay step; competences and personal notes); tax information; benefits information; union membership; next of kin provided (name; address; birthdate; phone number; emergency contact details); start and end dates of employment; bank account or credit card details; personal service company details (name; registration number and registered office); directorships; VAT numbers; documents (written or electronic) containing any of the above. Additional Personal Data for former and current employees: staff type (e.g. faculty, advisor, housing director); academic department; hire status; employment status; workload; faculty rank; publications; work status tracking; education details and qualification details. Additional Personal Data for former and current applicants: prior college information; transcripts and/or (additional) test results; physical health status; former employer letters; and workplace information. Additional Personal Data for former and current students: academic record including results and goals; enrolment details; academic progression details (including grades); academic achievements; work or academic placements; course planning details; billing and payment history; housing preferences and history; financial aid details; health record (including vaccinations, allergies, medical conditions), insurance information and health documentation.	Current or former employees (including any faculty or personnel); Contractors or Sub-contractors (of any variety), agents or directors; Applicants or prospective employees; and Current, former and prospective students.
Unit4 FP&A	Names; addresses; telephone numbers (including mobile); email address(es); other contact information. Other Personal Data is not required to be stored or processed to achieve the objectives of the Product (as set out below), but other Personal Data may be stored or processed by the Product if it is configured in such a way to do so (e.g. salary data) or is inputted into the Product by the Customer.	Current or former employees; Sub-contractors (of any variety), agents or directors.
Unit4 Assistance PSA Suite	Names; addresses; telephone numbers (including mobile); email address(es); other contact information. Other Personal Data is not required to be stored or processed to achieve the objectives of the Product (as set out below), but other Personal Data may be stored or processed by the Product if it is configured in such a way to do so or is inputted into the Product by the Customer.	Current or former employees; Sub-contractors (of any variety), agents or directors; Anyone else who is a member of a project team (including non-employees) applicants or prospective employees. Customer's customer contacts and supplier contacts.
Unit4 Talent Management	Names; addresses; contract details; telephone numbers (including mobile); email address(es); other contact information (street address and country); date of birth; age; place of birth; job title; department. By using the Learn module: course enrolments; session enrolments; quiz results and reviews; video engagement data; slide engagement data; text engagement data; badges; certifications. By using the perform module: check-in data; OKR data; feedback and praise. By using the Engage module: answers and feedback on engagement questions.	Current or former employees; Current or former job candidates; Contractors or Sub-contractors (of any variety), agents or directors; and Applicants or prospective employees.
People Platform Services ("**PPS**"), Localisations Services and Unit4 Apps	As the PPS, Localisation Services and/or Unit4 Apps are services that work and interface with Unit4's other Products or Services, they may process any or all types of Personal Data set out in this table in relation to the listed Products and Services. Additionally, Wanda may process: Unit4Id (which identifies the user of IDS); any Personal Data or information submitted by the user into an application to which Wanda may be connected (such information being processed or stored unless User elects to have it deleted); any other conversation and dialog data; metadata where assignable to an individual; and Application Insights Logs (a Microsoft service utilised for performing diagnostics).	All categories of individual listed in this table. Depending on the application or service to which Wanda is connected, the PPS could potentially Process Personal Data relating to any living

		individual that the User chooses to submit.
Unit4 Property Management	Names; addresses; telephone numbers (including mobile); email address; homepage address; national security number or social security number or ID card reference; date of birth; customer identity; language; marking for protected identity; marking for estate; VAT numbers; contact persons information (including: title/position, interests); bank account details; employment information (including: employer, address information); applicant details (including: profession, annual income, employed year, number of persons in household, previous landlord, assessment of credit report, date of credit assessment); applicant and other attributes (defined by the Controller); queue position; membership (including: member number, status, membership start/end date, reason for entry/resignation, first entry date, main membership, related membership, tenancy points, home savings points); roles/categories of persons; Users (user id, type of user, signature); Lease agreement and tenant ownership details (including: identity of the invoice recipient for e-invoice, mandate information deposit, guarantee, warranty); case management information; contractor (assignments for mailing); Notes (registered by the Controller); documents (written or electronic) containing any of the above.	Current or former employees; Contractors or Sub-contractors (of any variety), agents or directors; Applicants or prospective employees; and consumers (e.g. property applicants and tenants) of management services.

2. NATURE AND OBJECTIVE(S) OF PROCESSING:

Generally, the nature of the Processing by the Processor will only be as is necessary to enable the Processor to comply with its obligations and exercise its rights under the Agreement, including (in relation to the Personal Data) collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure, or destruction. The objective or purpose of the Processing is the performance of the Processors obligations and exercise of its rights under the Agreement, including the performance of functions required or requested by the Controller for the Controller's compliance with its statutory and/or contractual obligations. In relation to and depending on the Product or Service. Processor will also Process your Personal Data to improve her products and services (e.g. for product improvement via artificial intelligence, machine learning etc.) or data analysis. Processing will include the following:

Product	Nature and Objective of Processing
Unit4 ERP x	Personal Data will be entered into Unit4 ERP x to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Travel requests; • Expense claim processing; • Timesheet processing; • Absence management; • HR & Payroll related processes: • Payroll; • Course enrolment; • Competence management; • Appraisals; • Salary review; • Applicant registration; • Payment processing; • Billing; • Purchase requisitions; • People/Project Planning. The Processing will involve: ***Product (software solution)*** Unit4 ERP x executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. ***Services*** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 ERP 7	Personal Data will be entered into Unit4 ERP 7 to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Travel requests; • Expense claim processing; • Timesheet processing; • Absence management; • HR & Payroll related processes: • Payroll; • Course enrolment; • Competence management; • Appraisals; • Salary review; • Applicant registration; • Payment processing; • Billing; • Purchase requisitions; • People/Project Planning. The Processing will involve:

	Product (software solution) Unit4 ERP 7 executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. ***Services*** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 Financials	Personal Data will be entered into Unit4 Financials to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Customer/Supplier/Employee registration; • Payment processing; • Billing; • Expense claim processing; • Travel requests; • Purchase requisitions & Orders; • People/Project Planning; • HR & Payroll related processes: • Payroll; • Timesheet processing; • Absence management • Course enrolment; • Competence management; • Appraisals; • Salary review; • Applicant registration; The Processing will involve: **Product (software solution)** Unit4 Financials executing programmable software code to provide that the activities set out (as detailed above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. **Services** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 Student Management	Personal Data will be entered into Unit4 Student Management to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Recruiting prospective students, • Responding to information requests • Processing applications • Managing the academic lifecycle of a student including onboarding, course scheduling, academic progression, advisory, housing and other facilities, graduation • Planning and scheduling faculty staff The Processing will involve: **Product (software solution)** Unit4 Student Management executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. **Services** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 FP&A	Personal Data will be entered into Unit4 FP&A to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Budgeting; • Financial and other reporting; • Report distribution; • Approval processing; • People/Project planning.

	The Processing will involve: **Product (software solution)** Unit4 FP&A executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. **Services** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 Talent Management	Personal Data will be entered into Unit4 Talent Management to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Human capital management; • Employee performance management; • Talent enablement; • Candidate assessment; • Learning; • Feedback and praise; and • People analytics and engagement. The Processing will involve: **Product (software solution)** Unit4 Talent Management executing programmable software code to provide that the activities set out (as detailed above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. **Services** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
Unit4 Assistance PSA Suite	Personal Data will be entered into Unit4 Assistance PSA Suite to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • automation of a professional services organization, including financial and human resource management (HRM); • daily time and project management; • booking time and expenses with receipts; • transitioning opportunities into projects, budget and forecasting hours and planning projects and resources; • tracking time and expenses and execute invoicing; • integration of projects into other applications; and • performing accounting assisting the integration of financial data into other solutions. The Processing will involve: **Product (software solution)** • Unit4 Assistance PSA Suite executing programmable software code to provide that the activities set out (as detailed above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. **Services** • Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. • Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. • Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.
People Platform Services ("**PPS**"), Localisations services and Apps	Data will be processed by the PPS, Localisation Services and/or Apps to permit the stated purposes of the services as set out in the applicable PPS Service Description on www.unit4.com/terms. In addition, Personal Data will be inputted into Wanda using third party software of choice (e.g. Slack Integration, or other Microsoft Applications (including Microsoft Teams)). Dependent on the Unit4 Product or Service used by Customer, Wanda can help to complete administrative tasks for Customer's employees. Tasks may include: • Timesheet entries • Expense entries • Travel requests • Payslip enquiries • Absence entries • Balance enquiries • Purchase requisitions. The Processing will involve:

	Product (software solution) Wanda executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. ***Services*** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 PPS, Localisation Services and/or Apps and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data in order to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer. Access to Personal Data for product improvement via AI machine learning or data analysis.
Unit4 Property Management	Personal Data will be entered into Unit4 Property Management to allow Customer to organise and manage processes related to the operational functioning and management and/or administrative processes of its internal business. Processes may include: • Applicant registration • Lease out management • Lease agreement processes • Tenant ownership processes • Electronic signing processing • Debiting incl. invoice printing • Payment processing • Dunning processing • Rental change. The Processing will involve: ***Product (software solution)*** Unit4 Property Management executing programmable software code to provide that the activities set out (above) are able take place. This may involve transferring data to or from third party solutions not under the control of the Processor through integrations. ***Services*** Transfer and storage of Personal Data to provide additional Services as set out in more detail in the Service Description or People Platform Service Description as applicable. Access to the Personal Data to provide support and maintenance of the Unit4 Product and assist the Customer in the operation of the solution as set out in more detail in the Unit4 Support Terms. Access to the Personal Data to provide configuration and/or customisation and/or data migration (e.g. from its legacy systems) and/or other Professional Services as purchased by Customer.

3. DESCRIPTION OF THE PROCESSING AND MEANS:

Processer will Process the aforementioned Personal Data in connection with the following activities (the activities below are mentioned as example only):

Type of Processing	Description	Means and resources
Unit4 SaaS (General)	The Processor will Process Personal Data in connection with the activities as described in the Agreement and more specifically the Unit4 Service Descriptions.	<u>Personnel</u> The Unit4 Cloud operations team has personnel in countries in the EU (including, but not limited to, Poland, Sweden, Norway, Netherlands, Spain and Portugal), UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 SaaS. <u>Assets and Infrastructure</u> Unit4 utilises third party hosting infrastructure services to provide Unit4 SaaS and employs other software systems for operation and management. See Section 3.
U4 Talent Management SaaS	The Processor will Process Personal Data in connection with the activities as described in the Agreement and more specifically the applicable Service Description.	<u>Personnel</u> The Unit4 Talent Management Cloud Services operations team has personnel predominantly in Belgium and some other EEA countries. These Processor personnel operate the Unit4 Talent Management SaaS Service. <u>Assets and Infrastructure</u> Unit4 utilises third party hosting infrastructure services to provide the Unit4 Talent Management SaaS Service and employs other software systems for operation and management. See Section 3.
Support Services	The Processor will Process Personal Data in connection with the activities as described in the Agreement and more specifically in the Unit4 Support Terms.	<u>Personnel</u> The Unit4 Support team has personnel in countries in the EU (including, but not limited to, Poland, Sweden, Norway, Germany, Ireland, Netherlands, Spain and Portugal), UK, US, Canada (and such other locations as required to support Unit4's business needs). These Processor personnel provide the Unit4 Support Services (set out in the Unit4 Support Terms in Section B of the SLA). <u>Assets and Infrastructure</u> Unit4 utilises other software systems for operation, delivery and management of these services.
Professional Services	The Processor will Process Personal Data in connection with the activities as	<u>Personnel</u>

and/or consulting	described in the Agreement and more specifically in any more detailed Project documentation or statements of work agreed between the Parties following Project commencement.	The Unit4 Professional Services team has personnel in all locations where Unit4 has a corporate group entity including United Kingdom, Ireland Poland, Portugal, Norway, Spain, France, Germany Sweden, US, Canada, Singapore/Malaysia (and such other locations as required to support Unit4's business needs). These Processor personnel provide the Unit4 Professional Services. Assets and Infrastructure Unit4 utilises other software systems for operation, delivery and management of these services.
Unit4 Professional Services (if sub-contracted to a delivery partner)	The Processor and its sub-processors will Process the aforementioned Personal Data in connection with the activities as described in the Agreement and (if any) the third party contractual and service documentation provided as part of the Agreement. For more details, See Section 3. The Processor will execute a written agreement with the Sub-processor(s), which will be in accordance with the relevant legislation and regulations and the Agreement Further, the Controller has given the Processor permission to engage the applicable Sub-processor(s) as listed in Section 3 by entering into the Agreement.	See Section 3 or the applicable Order Form.
Third Party Products and Services	The Processor and its sub-processors will Process the aforementioned Personal Data in connection with the activities as described in the Agreement and the Third Party Provider contractual and service documentation provided as part of the Agreement.	See Section 3 or the applicable Order Form and any additional provisions provided in further schedules or appendices to the Data Processing Information if required by the Third Party Provider or Applicable Law.

People Platform Services ("**PPS**"), Localisation Services and/or Apps	In addition to Unit4 SaaS, the PPS, Localisation Services and/or Apps will (where applicable) process Personal Data in connection with a privacy statement as presented to the end user, asking for consent, where such Personal Data is processed.	Personnel
		
		The Unit4 Cloud operations team, which operates the PPS, Localisation Services and/or Apps has personnel in countries in the EU (including, but not limited to, Poland, Sweden, Norway, Netherlands, Spain and Portugal), UK, US, Canada, Malaysia and Singapore. These Processor personnel operate Unit4 SaaS.
		
		Assets and Infrastructure
		
		Unit4 utilises its own and third party (shared) infrastructure services to provide the Unit4 People Platform services, Localisation Services and/or Apps. This includes 3rd party systems (i.e. collaboration apps), over which Unit4 has no control. The PPS including Wanda, Localisation Services and/or Apps make use of a number of Microsoft products and services, as follows:
		
		• Cognitive services:
		  ○ LUIS Cognitive Service - *language understanding.*
		  ○ Text Translator API – *translating text*
		  ○ QnA Maker Cognitive service – *provides a questions and answers service*
		• Bot framework connectors – *provides for the connection of Wanda to the supported social channels*.
		• Traffic manager – *used for disaster recovery and failover if the primary region is unhealthy*
		• Web apps / web jobs – *hosts web APIs and long running web-based processes*
		• Service bus – *provides internal communication in the Wanda ecosystem*
		• Storage accounts – *used to store conversation state and user settings*
		• Cosmos DB –*provides storage*
		• *Functions – provides logical algorithms for extensions*
		• Event grid – *provides communication*
		• API management – *to manage APIs*
		• Service Plans – *Linux and dynamic service plans to run the Service in*
		• Storage accounts – *used for storage*
		• Key vault – *stores confidential data that is used to communicate with Microsoft services and for internal services*
		• Redis cache – *provides caching capabilities*
		• Application Insights – *Monitoring of system, includes telemetry and logging*
		• *SQL server – provides storage*
		• Kubernetes – *open source container*
		
		Further information and details relating to those Microsoft products and services can be found here: https://azure.microsoft.com/en-us/services/.
		
		Next to that the PPS, Unit4 Localisation Services and/or unit4 Apps make use of:
		
		Twilio – sendgrid – *to send mail messages*

4. RETENTION PERIOD

The Processor will keep the Personal Data **for the duration of the Agreement**.

After the agreed period of retention, the Processor will return the Personal Data to the Controller, on a migration-capable format set by Processor **or** immediately destroy the Personal Data without retaining a copy, upon first request of Controller.

5. INFORMATION REGARDING COUNTRY (OR PLACE) OF PROCESSING OF PERSONAL DATA

<table>
<tr><td>Product - On premises</td><td colspan="4">Data is stored on the servers of the Controller in their principal place of business or registered office as can be notified to Unit4 from time to time.</td></tr>
<tr><td>Product - Unit4 SaaS</td><td colspan="4">Unit4 Cloud operates in several data centres, including a worldwide presence in Microsoft Azure. Unit4 will deploy the customer in the most logical location dependent on where the Customer resides (as set out in an Order Form). All Customer data will be stored only in the selected geo-political zone and won't be moved outside of it without explicit customer consent.
<table>
<tr><th>CLOUD MODEL</th><th>GEO-POLICITAL ZONE</th><th>LOCATION OF DATA CENTRE</th><th>FACILITY OR PARTNERSHIP</th></tr>
<tr><td>SAAS CLOUD</td><td>EU</td><td>DUBLIN / AMSTERDAM</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>USA</td><td>MULTIPLE LOCATIONS</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>CANADA</td><td>TORONTO / QUEBEC CITY</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>UNITED KINGDOM</td><td>LONDON / CARDIFF</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>ASIA</td><td>SINGAPORE / HONG KONG</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>AUSTRALIA</td><td>VICTORIA / NEW SOUTH WALES</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>NORWAY</td><td>OSLO / STAVANGER</td><td>MICROSOFT AZURE</td></tr>
<tr><td>SAAS CLOUD</td><td>SWEDEN (NORDICS)</td><td>SÄTRA AND SOLLENTUNA</td><td>CONAPTO</td></tr>
</table></td></tr>
<tr><td>Product – Talent Management SaaS</td><td colspan="4">Talent Management SaaS operates in Microsoft Azure, covering both the EU and UK Geo-Political Zones (above), with the zone being allocated based on Customer's location. All Customer data, save for sharing with selected sub-processors in Section 3, will be stored only in the selected geo-political zone and won't be moved outside of it without explicit customer consent.</td></tr>
<tr><td>Unit4 Support – Standard Support and other standard support services</td><td colspan="4">Unit4 Support uses third party software (such as salesforce / ServiceNow) to register and process Cases. These Cases are accessible for any Unit4 employee that is provided access to third party software such as support engineers, cloud engineers, Professional Services consultants and service management. Access is controlled by internal management and organisational processes, to ensure that Personal Data is not accessed by consultants or engineers in locations that should not have access to particular Customer details.
<table>
<tr><th>Customer Location</th><th>Primarily Support is provided from (but can include other EU countries):</th></tr>
<tr><td>United Kingdom and Ireland</td><td>United Kingdom, Ireland, Portugal and Poland.</td></tr>
<tr><td>Sweden, Norway, Denmark, Finland and Iceland</td><td>Poland, Portugal, Norway and Sweden.</td></tr>
<tr><td>US & Canada</td><td>Poland, Portugal, US and Canada.</td></tr>
<tr><td>Europe rest</td><td>Poland, Portugal and Germany.</td></tr>
<tr><td>APAC</td><td>Poland, Portugal and Singapore/ Malaysia.</td></tr>
</table></td></tr>
<tr><td>Unit4 Support – 24/7 Support</td><td colspan="4">Using a 'follow the sun' methodology, 24/7 support of Customer Cases could occur in any of the support locations listed above as well as Netherlands, Spain and such other locations as required to support Unti4's business needs.</td></tr>
<tr><td>Unit4 Support – EU Only Support</td><td colspan="4">If EU Only support is elected, Cases are supported only within the EU locations listed above for standard support (during Business Hours).</td></tr>
<tr><td>People platform services ("PPS") (generally) including IDS and Wanda (together with any supporting services), localisation services and/or Apps</td><td colspan="4">PPS are cloud services that use shared infrastructure and 3rd party services that might not provide geopolitical zone isolation. Below is an overview of the PPS and the country (or place) of Processing of Personal Data using that service.
<table>
<tr><th>Service</th><th>Geo-political zone</th><th>Where Service Processes or Stores Data</th><th>Primarily Support is provided from:</th></tr>
<tr><td>Wanda</td><td>Any</td><td>Predominantly within the EU, but can be anywhere globally where there is an Azure data centre (e.g. US).</td><td>EU countries including Ireland, Poland and Spain, United States and other Global support locations where required.</td></tr>
<tr><td>PPS, Localisation Services and/or Apps</td><td>Depends on Cloud Deployment</td><td>Service is processed and data is stored in the selected Geo-Political zone.</td><td>As above for Unit4 SaaS</td></tr>
</table></td></tr>
<tr><td>Unit4 Professional Services and Unit4 customer success function</td><td colspan="4">
<table>
<tr><th>Topic</th><th>Professional Services and customer success are provided from:</th></tr>
<tr><td>Implementation and other project services</td><td>In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable).</td></tr>
<tr><td>Data Migration</td><td>In the Territory or Customer location of registered office/principal place of business (as applicable) and/or Portugal depending on what is agreed between the Parties in the project documentation or a statement of work (if applicable).</td></tr>
<tr><td>Trouble shooting</td><td>In applicable Unit4 Support Service location and Portugal.</td></tr>
<tr><td>Customer Success</td><td>In applicable Unit4 Support Service location and Portugal.</td></tr>
</table></td></tr>
</table>

6. CONTACT DETAILS

For questions or comments about the Data Processing Information the contact person is:

Processor: By letter (addressed to Global Data Protection Officer copy to Corporate Legal Department) P.O. Box 5005, 3528 BJ Utrecht, the Netherlands or by email to privacy@unit4.com or to the Unit4 address for notices provided in the Agreement.

Controller: The Controller address for notices provided in the Agreement.

SECTION 2 – SECURITY MEASURES

As stated in paragraph 6 of the Data Processing Terms, the technical and organisational security measures are listed in this Section and are supplemented or amended if necessary. The Controller considers these measures suitable for the processing of Personal Data.

Unit4 Business Security Measures (Internal business operations summary)

Description of the technical and organisational security measures implemented by the Processor in its organisation (generally):

Physical Security:

- Physical access control is managed by Unit4 facilities.
- All offices have security systems in place in respect of controlling access through barriers, e.g. entry gates, manned reception desks, alarmed fire doors, intruder detection systems and/or lockable offices.
- Unit4 operates access controls with the help of what people know, such as password or personal access code; or with the help of what people carry, such as a security pass;
- On-site server rooms (where applicable) have additional physical controls.
- Access to secure areas or sensitive information is restricted to prevent unauthorized access by visitors / unauthorized staff (by way of lockable offices or lockable cabinets) and operating clear desk policies where appropriate.
- Unit4 visitors are controlled at reception (whether by a dedicated receptionist or other member of staff).
- Shredders or other suitable secure disposal method for sensitive documents are used.

Virtual and computing Security:

- The responsible line manager will ensure employees and contractors return all Unit4 assets in their possession upon termination of their employment or contract agreement. Records of this return of asset are maintained.
- Unit4 aims to classify information as either public, confidential, proprietary or sensitive. Information would then be protected according to its classification.
- Media (including hard drives) are disposed of securely and safely when no longer required. All sensitive material (hard disks, floppies, etc.) is removed by guaranteed removal software, (not by reformatting or deletion) before disposal or physical destruction.
- Anti-malware - we use the latest version of industry standard solutions to provide virus and anti-malware protection.
- Further, Unit4 utilises:
- control on assigned rights;
- logging and controlling access to the system;
- recovery measures;
- the ability to ensure the ongoing confidentiality, integrity, availability and resilience of Processing systems and services; and
- systems and processes to allow it to restore the availability and access to Personal Data in a timely manner in the event of a physical or technical incident.
- Business Continuity and Disaster Recovery plans have been prepared which include information security considerations.

Security Policies and Documentation:

- The Global Leadership Team for Unit4 and/or its respective local management teams have oversight of both global and local information management and security plans including any information security policies that meet identified information security risks and supports the business goals.
- Information security and management is assigned globally to the Chief Information Security Officer and Global Data Protection Officer, who manage resources to deliver strategic and overall compliance with information security policy and process.
- Unit4 has implemented security policies updated and amended regularly to comply with good industry practice.
- Unit4 has a privacy policy and white paper on GDPR published on www.unit4.com/terms.
- Unit4 enters into non-disclosure and confidentiality agreements with Third Parties when sharing confidential information relation to its business.
- Unit4 ensures all employees and contractors enter into standard confidentiality clauses in their contracts.
- Unit4 provides all employees with training in relation to: data protection; security and its core business principles as stated above.

Additional Elements for Unit4 SaaS on Microsoft Azure (summary)

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 SaaS:

Data protection

Unit4 Cloud utilizes several mechanisms to protect Personal Data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
- System security – Logical authentication and authorization mechanism in place
- Firewalls – next generation firewall technology to ensure inbound and outbound traffic is controlled.

Database level security features, process and protocols

- Data security – Logical authentication and authorization mechanism in place.
- Database security – Every customer has their own secure database which means partitioning of databases is not required and customer data not co-mingled. The outcome is that a customer's data is never inadvertently shared with others.
- Database backups are encrypted using whole database encryption technology such as Transparent Database Encryption.
- Non-transactional data and files will be secured by standard symmetric encryption (AES).
- Unit4 uses Azure Key Vault to maintain control of keys used by cloud applications and services to encrypt data.

Continually tested and evolving security

To uncover unforeseen vulnerabilities and refine our detection and response capabilities, we are continually looking into how we can improve out security posture to defend against potential breaches. The Unit4 Cloud operations team that closely monitor and secures Unit4's Cloud operations (cloud infrastructure, cloud services, products, devices and internal resources) — testing penetration and improving our ability to protect, detect and recover from cyber threats.

Threat detection, mitigation and response

As the number, variety and severity of cyber threats have increased, so has our diligence in threat detection and response. Centralized monitoring systems provide continuous visibility and timely alerts. Frequent application of security patches and updates helps protect systems from known vulnerabilities. Intrusion and malware detection systems are designed to detect and mitigate risks from outside attacks. In the event of malicious activity, our incident response team follows established procedures for incident management, communication and recovery. The team uses industry best practices to alert both internal teams and customers. Finally, security reports monitor access patterns to help proactively identify and mitigate potential threats.

Data segregation

Data is the currency of the digital economy and we take the responsibility of protecting customer data very seriously. Both technological safeguards, such as encrypted communications and operational processes help keep customer data secured. In the Cloud, data from multiple customers may be stored on the same IT resources. Unit4 uses logical isolation to segregate each customer's data from that of others. Unit4 SaaS is designed to counter risks inherent in a multitenant environment. Data storage and processing is logically separated among consumers having separate database instances for all our customers.

Data encryption

Unit4 provides, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS, using latest security ciphers. The mechanism used is a transparent, whole database encryption – TDE. Microsoft Azure customers in the Public SaaS offering get the TDE data at rest encryption as a standard.

Access control

Customers using Unit4 products in the Cloud are fully empowered to conduct front-end access control to their application. This means that the responsibility for creating new accounts, account termination and review for Unit4 application is with the customer.

Unit4 will retain limited back-end access to customer data (by direct database connection). Access by Unit4 to Personal Data shall be strictly limited to activities necessary for installing, implementing, maintaining, repairing, troubleshooting or upgrading the solution. All access is logged and limited to a small group of Cloud Engineers and Support Consultants. Access logs are saved in the centralized monitoring solution for 365 days. In case of data breaches, Unit4 can provide the access log on request.

Data breach notification

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

Data privacy and security by design

Unit4 Cloud platform was designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

Unit4 and the data centres operators hold various security certifications, for the details please refer to the applicable Service Description.

Additional Elements for Unit4 People Platform Services (summary)

Description of the technical and organisational security measures implemented by the Processor in relation to the provision of the Unit4 People Platform Services (Cloud only):

Data protection

Unit4 People Platform utilizes several mechanisms to protect Personal Data in the cloud. Below is a comprehensive overview of applied controls.

Network level security features, process and protocols

- Secure data transmission over public networks – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.

Authentication

- All services follow the principle of least privilege and authentication towards services and their APIs are secured using industry standard mechanisms. OpenID Connect and the underlying oAuth 2.0 protocol is used to securely perform authentication of users and/or client services with trusted parties and validate identity and access using claims-based tokens.
- HMAC (Hash-based Message Authentication) is used as alternative method to secure communication between services.

Database level security features, process and protocols.

- A data stored in storage accounts are encrypted at rest.
- All storage accounts require secure transfer – all traffic is secured using industry standard protocols such as SSL/TLS and HTTPS.
- All data stored in Azure Cosmos DB is encrypted at rest and in transport.
- All Azure SQL Servers are enabled with Transparent Data Encryption (TDE).
- All Azure SQL Servers are running with Threat detection and auditing enabled.
- Azure KeyVault is used to secure particular sensitive information like service principal credentials.

Messaging level security features, process and protocols.

- All data stored by Azure Service Bus instances are encrypted at rest.
- All traffic (in transit) on the Azure Service Bus is secured using industry standard protocols such as SSL

More details about the Security Policy and Security Program can be found at www.unit4.com/terms.

Data encryption

Unit4 People Platform services provide, as a standard, secure access to all its services by encrypting all data in transit traveling on public networks. This is done by using only secure protocols, like HTTPS over TLS (1.2), using latest security ciphers. All data stored are encrypted.

Data breach notification

Unit4 shall notify the Customer without undue delay after becoming aware of a data breach. Customer should make sure that the contacts listed in Unit4 Support Portal are always up to date, as they will be used for all communication.

Data privacy and security by design

Unit4 People Platform services were designed from the ground up with data security and privacy in mind. Unit4 is continually improving the security of the solution, by applying lessons learned from annual penetration tests and audits.

SECTION 3 – UNIT4 SUB-PROCESSORS

Service	**Sub-processor** (company name, location etc.)	**Processing location**	**Type of service by Sub-processor / Module used with**
Unit4 Professional Services (if sub-contracted to a delivery partner)	As specified in the Agreement.	As specified in the Agreement.	As specified in Order Form or agreed in writing with Customer.
Third Party Products and Services only applicable when purchased by customer	As specified in the Agreement.	As provided in the Agreement or in any further schedules or appendices to the Agreement relating to the Third Party Provider processing.	Software and//or Support Services and/or Cloud Services.
Unit4 SaaS	Microsoft Azure	As stated above in Section 1, paragraph 5.	Providing Cloud Infrastructure and Services
	Microsoft Dynamics	As stated above in Section 1, paragraph 5.	Providing Software Services, in particularly Microsoft Dynamics (including some cloud infrastructure).
	Microsoft	As stated above in Section 1, paragraph 5.	Providing software tooling and Office
	Conapto	As stated above in Section 1, paragraph 5.	Providing Cloud Infrastructure and Services
	Twilio - Sendgrid	United States of America (Privacy Policy)	Sending mail (EU SCCs – See Section 4)
Unit4 SaaS – Talent Management	Microsoft Azure	Dublin, Ireland	Providing solution - Suite
	LogDNA	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs – See Section 4)
	Mandrill	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs – See Section 4)
	Mixpanel	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs – See Section 4)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Providing solution - Learn (SCORM only) (EU SCCs – See Section 4)
	Sentry	United States of America (Privacy Policy)	Providing solution – Suite (EU SCCs – See Section 4)
	Slack	United States of America (Privacy Policy)	Providing solution – Perform (EU SCCs – See Section 4)
	Wistia	United States of America (Privacy Policy)	Providing solution – Learn (EU SCCs – See Section 4)
People Platform Services ("**PPS**") (generally) including IDS and Wanda (together with any supporting services)	Microsoft Azure	As stated above in Section 1, paragraph 5 and as provided by Microsoft here: https://www.microsoft.com/en-us/trustcenter/privacy/where-your-data-is-located.	Providing Cloud Infrastructure and platform Services (as set out above) in Section 1.
	Twilio - Sendgrid	United States of America (Privacy Policy)	Sending mail (EU SCCs – See Section 4)

SECTION 4 – EU STANDARD CONTRACTUAL CLAUSES

STANDARD CONTRACTUAL CLAUSES ("SCC")

Controller to Processor

The data exporter is the Controller whose details appear in an Order Form (as Customer) in the Agreement between Controller and Processor.

The data importer is the Processor whose details appear in an Order Form (as Unit4) in the Agreement between Controller and Processor.

Module Two (Transfer controller to processor) of the SCC is applicable.

These SCC only apply where there is any transfer by the Controller of Personal Data from inside the EEA to the Processor located outside the EEA, also known as a third country, and where no adequacy decision applies.

SECTION I

Clause 1

Purpose and scope

(a) The purpose of these standard contractual clauses is to ensure compliance with the requirements 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 (General Data Protection Regulation) ([i]) for the transfer of data to a third country.

(b) The Parties:

(i) the natural or legal person(s), public authority/ies, agency/ies or other body/ies (hereinafter 'entity/ies') transferring the personal data, **as listed in the Agreement ("Customer"**) and as listed in Annex I.A (hereinafter each 'data exporter'), and

(ii) the entity/ies in a third country receiving the personal data from the data exporter, directly or indirectly via another entity also Party to these Clauses, **as listed in the Agreement ("Unit4")** and as listed in Annex I.A (hereinafter each 'data importer')

have agreed to these standard contractual clauses (hereinafter: 'Clauses').

(c) These Clauses apply with respect to the transfer of personal data as specified in Annex I.B.

(d) The Appendix to these Clauses containing the Annexes referred to therein forms an integral part of these Clauses.

Clause 2

Effect and invariability of the Clauses

(a) These Clauses set out appropriate safeguards, including enforceable data subject rights and effective legal remedies, pursuant to Article 46(1) and Article 46(2)(c) of Regulation (EU) 2016/679 and, with respect to data transfers from controllers to processors and/or processors to processors, standard contractual clauses pursuant to Article 28(7) of Regulation (EU) 2016/679, provided they are not modified, except to select the appropriate Module(s) or to add or update information in the Appendix. This does not prevent the Parties from including the standard contractual clauses laid down in these Clauses in a wider contract and/or to add other clauses or additional safeguards, provided that they do not contradict, directly or indirectly, these Clauses or prejudice the fundamental rights or freedoms of data subjects.

(b) These Clauses are without prejudice to obligations to which the data exporter is subject by virtue of Regulation (EU) 2016/679.

Clause 3

Third-party beneficiaries

(a) Data subjects may invoke and enforce these Clauses, as third-party beneficiaries, against the data exporter and/or data importer, with the following exceptions:

(i) Clause 1, Clause 2, Clause 3, Clause 6, Clause 7;

(ii) Clause 8 – Module One: Clause 8.5 (e) and Clause 8.9(b); Module Two: Clause 8.1(b), 8.9(a), (c), (d) and (e); Module Three: Clause 8.1(a), (c) and (d) and Clause 8.9(a), (c), (d), (e), (f) and (g); Module Four: Clause 8.1 (b) and Clause 8.3(b);

(iii) Clause 9 – Module Two: Clause 9(a), (c), (d) and (e); Module Three: Clause 9(a), (c), (d) and (e);

(iv) Clause 12 – Module One: Clause 12(a) and (d); Modules Two and Three: Clause 12(a), (d) and (f);

(v) Clause 13;

(vi) Clause 15.1(c), (d) and (e);

(vii) Clause 16(e);

(viii) Clause 18 – Modules One, Two and Three: Clause 18(a) and (b); Module Four: Clause 18.

(b) Paragraph (a) is without prejudice to rights of data subjects under Regulation (EU) 2016/679.

Clause 4

Interpretation

(a) Where these Clauses use terms that are defined in Regulation (EU) 2016/679, those terms shall have the same meaning as in that Regulation.

(b) These Clauses shall be read and interpreted in the light of the provisions of Regulation (EU) 2016/679.

(c) These Clauses shall not be interpreted in a way that conflicts with rights and obligations provided for in Regulation (EU) 2016/679.

Clause 5

Hierarchy

In the event of a contradiction between these Clauses and the provisions of related agreements between the Parties, existing at the time these Clauses are agreed or entered into thereafter, these Clauses shall prevail.

Clause 6

Description of the transfer(s)

The details of the transfer(s), and in particular the categories of personal data that are transferred and the purpose(s) for which they are transferred, are specified in Annex I.B.

Clause 7 – Optional

Docking clause

(a) An entity that is not a Party to these Clauses may, with the agreement of the Parties, accede to these Clauses at any time, either as a data exporter or as a data importer, by completing the Appendix and signing Annex I.A.

(b) Once it has completed the Appendix and signed Annex I.A, the acceding entity shall become a Party to these Clauses and have the rights and obligations of a data exporter or data importer in accordance with its designation in Annex I.A.

(c) The acceding entity shall have no rights or obligations arising under these Clauses from the period prior to becoming a Party.

SECTION II – OBLIGATIONS OF THE PARTIES

Clause 8

Data protection safeguards

The data exporter warrants that it has used reasonable efforts to determine that the data importer is able, through the implementation of appropriate technical and organisational measures, to satisfy its obligations under these Clauses.

8.1 Instructions

(a) The data importer shall process the personal data only on documented instructions from the data exporter. The data exporter may give such instructions throughout the duration of the contract.

(b) The data importer shall immediately inform the data exporter if it is unable to follow those instructions.

8.2 Purpose limitation

The data importer shall process the personal data only for the specific purpose(s) of the transfer, as set out in Annex I.B, unless on further instructions from the data exporter.

8.3 Transparency

On request, the data exporter shall make a copy of these Clauses, including the Appendix as completed by the Parties, available to the data subject free of charge. To the extent necessary to protect business secrets or other confidential information, including the measures described in Annex II and personal data, the data exporter may redact part of the text of the Appendix to these Clauses prior to sharing a copy, but shall provide a meaningful summary where the data subject would otherwise not be able to understand the content or exercise his/her rights. On request, the Parties shall provide the data subject with the reasons for the redactions, to the extent possible without revealing the redacted information. This Clause is without prejudice to the obligations of the data exporter under Articles 13 and 14 of Regulation (EU) 2016/679.

8.4 Accuracy

If the data importer becomes aware that the personal data it has received is inaccurate, or has become outdated, it shall inform the data exporter without undue delay. In this case, the data importer shall cooperate with the data exporter to erase or rectify the data.

8.5 Duration of processing and erasure or return of data

Processing by the data importer shall only take place for the duration specified in Annex I.B. After the end of the provision of the processing services, the data importer shall, at the choice of the data exporter, delete all personal data processed on behalf of the data exporter and certify to the data exporter that it has done so, or return to the data exporter all personal data processed on its behalf and delete existing copies. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit return or deletion of the personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process it to the extent and for as long as required under that local law. This is without prejudice to Clause 14, in particular the requirement for the data importer under Clause 14(e) to notify the data exporter throughout the duration of the contract if it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under Clause 14(a).

8.6 Security of processing

(a) The data importer and, during transmission, also the data exporter shall implement appropriate technical and organisational measures to ensure the security of the data, including protection against a breach of security leading to accidental or unlawful destruction, loss, alteration, unauthorised disclosure or access to that data (hereinafter 'personal data breach'). In assessing the appropriate level of security, the Parties shall take due account of the state of the art, the costs of implementation, the nature, scope, context and purpose(s) of processing and the risks involved in the processing for the data subjects. The Parties shall in particular consider having recourse to encryption or pseudonymisation, including during transmission, where the purpose of processing can be fulfilled in that manner. In case of pseudonymisation, the additional information for attributing the personal data to a specific data subject shall, where possible, remain under the exclusive control of the data exporter. In complying with its obligations under this paragraph, the data importer shall at least implement the technical and organisational measures specified in Annex II. The data importer shall carry out regular checks to ensure that these measures continue to provide an appropriate level of security.

(b) The data importer shall grant access to the personal data to members of its personnel only to the extent strictly necessary for the implementation, management and monitoring of the contract. It shall ensure that persons authorised to process the personal data have committed themselves to confidentiality or are under an appropriate statutory obligation of confidentiality.

(c) In the event of a personal data breach concerning personal data processed by the data importer under these Clauses, the data importer shall take appropriate measures to address the breach, including measures to mitigate its adverse effects. The data importer shall also notify the data exporter without undue delay after having become aware of the breach. Such notification shall contain the details of a contact point where more information can be obtained, a description of the nature of the breach (including, where possible, categories and approximate number of data subjects and personal data records concerned), its likely consequences and the measures taken or proposed to address the breach including, where appropriate, measures to mitigate its possible adverse effects. Where, and in so far as, it is not possible to provide all information at the same time, the initial notification shall contain the information then available and further information shall, as it becomes available, subsequently be provided without undue delay.

(d) The data importer shall cooperate with and assist the data exporter to enable the data exporter to comply with its obligations under Regulation (EU) 2016/679, in particular to notify the competent supervisory authority and the affected data subjects, taking into account the nature of processing and the information available to the data importer.

8.7 Sensitive data

Where the transfer involves personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, genetic data, or biometric data for the purpose of uniquely identifying a natural person, data concerning health or a person's sex life or sexual orientation, or data relating to criminal convictions and offences (hereinafter 'sensitive data'), the data importer shall apply the specific restrictions and/or additional safeguards described in Annex I.B.

8.8 Onward transfers

The data importer shall only disclose the personal data to a third party on documented instructions from the data exporter. In addition, the data may only be disclosed to a third party located outside the European Union ([ii]) (in the same country as the data importer or in another third country, hereinafter 'onward transfer') if the third party is or agrees to be bound by these Clauses, under the appropriate Module, or if:

(i) the onward transfer is to a country benefitting from an adequacy decision pursuant to Article 45 of Regulation (EU) 2016/679 that covers the onward transfer;

(ii) the third party otherwise ensures appropriate safeguards pursuant to Articles 46 or 47 Regulation of (EU) 2016/679 with respect to the processing in question;

(iii) the onward transfer is necessary for the establishment, exercise or defence of legal claims in the context of specific administrative, regulatory or judicial proceedings; or

(iv) the onward transfer is necessary in order to protect the vital interests of the data subject or of another natural person.

Any onward transfer is subject to compliance by the data importer with all the other safeguards under these Clauses, in particular purpose limitation.

8.9 Documentation and compliance

(a) The data importer shall promptly and adequately deal with enquiries from the data exporter that relate to the processing under these Clauses.

(b) The Parties shall be able to demonstrate compliance with these Clauses. In particular, the data importer shall keep appropriate documentation on the processing activities carried out on behalf of the data exporter.

(c) The data importer shall make available to the data exporter all information necessary to demonstrate compliance with the obligations set out in these Clauses and at the data exporter's request, allow for and contribute to audits of the processing activities covered by these Clauses, at reasonable intervals or if there are indications of non-compliance. In deciding on a review or audit, the data exporter may take into account relevant certifications held by the data importer.

(d) The data exporter may choose to conduct the audit by itself or mandate an independent auditor. Audits may include inspections at the premises or physical facilities of the data importer and shall, where appropriate, be carried out with reasonable notice.

(e) The Parties shall make the information referred to in paragraphs (b) and (c), including the results of any audits, available to the competent supervisory authority on request.

Clause 9

Use of sub-processors

(a) GENERAL WRITTEN AUTHORISATION The data importer has the data exporter's general authorisation for the engagement of sub-processor(s) from an agreed list. The data importer shall specifically inform the data exporter in writing of any intended changes to that list through the addition or replacement of sub-processors at least 30 days in advance, thereby giving the data exporter sufficient time to be able to object to such changes prior to the engagement of the sub-processor(s). The data importer shall provide the data exporter with the information necessary to enable the data exporter to exercise its right to object.

(b) Where the data importer engages a sub-processor to carry out specific processing activities (on behalf of the data exporter), it shall do so by way of a written contract that provides for, in substance, the same data protection obligations as those binding the data importer under these Clauses, including in terms of third-party beneficiary rights for data subjects. ([iii]) The Parties agree that, by complying with this Clause, the data importer fulfils its obligations under Clause 8.8. The data importer shall ensure that the sub-processor complies with the obligations to which the data importer is subject pursuant to these Clauses.

(c) The data importer shall provide, at the data exporter's request, a copy of such a sub-processor agreement and any subsequent amendments to the data exporter. To the extent necessary to protect business secrets or other confidential information, including personal data, the data importer may redact the text of the agreement prior to sharing a copy.

(d) The data importer shall remain fully responsible to the data exporter for the performance of the sub-processor's obligations under its contract with the data importer. The data importer shall notify the data exporter of any failure by the sub-processor to fulfil its obligations under that contract.

(e) The data importer shall agree a third-party beneficiary clause with the sub-processor whereby – in the event the data importer has factually disappeared, ceased to exist in law or has become insolvent – the data exporter shall have the right to terminate the sub-processor contract and to instruct the sub-processor to erase or return the personal data.

Clause 10

Data subject rights

(a) The data importer shall promptly notify the data exporter of any request it has received from a data subject. It shall not respond to that request itself unless it has been authorised to do so by the data exporter.

(b) The data importer shall assist the data exporter in fulfilling its obligations to respond to data subjects' requests for the exercise of their rights under Regulation (EU) 2016/679. In this regard, the Parties shall set out in Annex II the appropriate technical and organisational measures, taking into account the nature of the processing, by which the assistance shall be provided, as well as the scope and the extent of the assistance required.

(c) In fulfilling its obligations under paragraphs (a) and (b), the data importer shall comply with the instructions from the data exporter.

Clause 11

Redress

(a) The data importer shall inform data subjects in a transparent and easily accessible format, through individual notice or on its website, of a contact point authorised to handle complaints. It shall deal promptly with any complaints it receives from a data subject.

[OPTION: The data importer agrees that data subjects may also lodge a complaint with an independent dispute resolution body ([iv]) at no cost to the data subject. It shall inform the data subjects, in the manner set out in paragraph (a), of such redress mechanism and that they are not required to use it, or follow a particular sequence in seeking redress.]

(b) In case of a dispute between a data subject and one of the Parties as regards compliance with these Clauses, that Party shall use its best efforts to resolve the issue amicably in a timely fashion. The Parties shall keep each other informed about such disputes and, where appropriate, cooperate in resolving them.

(c) Where the data subject invokes a third-party beneficiary right pursuant to Clause 3, the data importer shall accept the decision of the data subject to:

(i) lodge a complaint with the supervisory authority in the Member State of his/her habitual residence or place of work, or the competent supervisory authority pursuant to Clause 13;

(ii) refer the dispute to the competent courts within the meaning of Clause 18.

(d) The Parties accept that the data subject may be represented by a not-for-profit body, organisation or association under the conditions set out in Article 80(1) of Regulation (EU) 2016/679.

(e) The data importer shall abide by a decision that is binding under the applicable EU or Member State law.

(f) The data importer agrees that the choice made by the data subject will not prejudice his/her substantive and procedural rights to seek remedies in accordance with applicable laws.

Clause 12

Liability

(a) Each Party shall be liable to the other Party/ies for any damages it causes the other Party/ies by any breach of these Clauses.

(b) The data importer shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data importer or its sub-processor causes the data subject by breaching the third-party beneficiary rights under these Clauses.

(c) Notwithstanding paragraph (b), the data exporter shall be liable to the data subject, and the data subject shall be entitled to receive compensation, for any material or non-material damages the data exporter or the data importer (or its sub-processor) causes the data subject by breaching the third-party beneficiary rights under these Clauses. This is without prejudice to the liability of the data exporter and, where the data exporter is a processor acting on behalf of a controller, to the liability of the controller under Regulation (EU) 2016/679 or Regulation (EU) 2018/1725, as applicable.

(d) The Parties agree that if the data exporter is held liable under paragraph (c) for damages caused by the data importer (or its sub-processor), it shall be entitled to claim back from the data importer that part of the compensation corresponding to the data importer's responsibility for the damage.

(e) Where more than one Party is responsible for any damage caused to the data subject as a result of a breach of these Clauses, all responsible Parties shall be jointly and severally liable and the data subject is entitled to bring an action in court against any of these Parties.

(f) The Parties agree that if one Party is held liable under paragraph (e), it shall be entitled to claim back from the other Party/ies that part of the compensation corresponding to its/their responsibility for the damage.

(g) The data importer may not invoke the conduct of a sub-processor to avoid its own liability.

Clause 13

Supervision

(a) **[Where the data exporter is established in an EU Member State:]** The supervisory authority with responsibility for ensuring compliance by the data exporter with Regulation (EU) 2016/679 as regards the data transfer, as indicated in Annex I.C, shall act as competent supervisory authority.

[**Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) and has appointed a representative pursuant to Article 27(1) of Regulation (EU) 2016/679:]** The supervisory authority of the Member State in which the representative within the meaning of Article 27(1) of Regulation (EU) 2016/679 is established, as indicated in Annex I.C, shall act as competent supervisory authority.

[Where the data exporter is not established in an EU Member State, but falls within the territorial scope of application of Regulation (EU) 2016/679 in accordance with its Article 3(2) without however having to appoint a representative pursuant to Article 27(2) of Regulation (EU) 2016/679:] The supervisory authority of one of the Member States in which the data subjects whose personal data is transferred under these Clauses in relation to the offering of goods or services to them, or whose behaviour is monitored, are located, as indicated in Annex I.C, shall act as competent supervisory authority.

(b) The data importer agrees to submit itself to the jurisdiction of and cooperate with the competent supervisory authority in any procedures aimed at ensuring compliance with these Clauses. In particular, the data importer agrees to respond to enquiries, submit to audits and comply with the measures adopted by the supervisory authority, including remedial and compensatory measures. It shall provide the supervisory authority with written confirmation that the necessary actions have been taken.

SECTION III – LOCAL LAWS AND OBLIGATIONS IN CASE OF ACCESS BY PUBLIC AUTHORITIES

Clause 14

Local laws and practices affecting compliance with the Clauses

(a) The Parties warrant that they have no reason to believe that the laws and practices in the third country of destination applicable to the processing of the personal data by the data importer, including any requirements to disclose personal data or measures authorising access by public authorities, prevent the data importer from fulfilling its obligations under these Clauses. This is based on the understanding that laws and practices that respect the essence of the fundamental rights and freedoms and do not exceed what is necessary and proportionate in a democratic society to safeguard one of the objectives listed in Article 23(1) of Regulation (EU) 2016/679, are not in contradiction with these Clauses.

(b) The Parties declare that in providing the warranty in paragraph (a), they have taken due account in particular of the following elements:

(i) the specific circumstances of the transfer, including the length of the processing chain, the number of actors involved and the transmission channels used; intended onward transfers; the type of recipient; the purpose of processing; the categories and format of the transferred personal data; the economic sector in which the transfer occurs; the storage location of the data transferred;

(ii) the laws and practices of the third country of destination– including those requiring the disclosure of data to public authorities or authorising access by such authorities – relevant in light of the specific circumstances of the transfer, and the applicable limitations and safeguards ([v]);

(iii) any relevant contractual, technical or organisational safeguards put in place to supplement the safeguards under these Clauses, including measures applied during transmission and to the processing of the personal data in the country of destination.

(c) The data importer warrants that, in carrying out the assessment under paragraph (b), it has made its best efforts to provide the data exporter with relevant information and agrees that it will continue to cooperate with the data exporter in ensuring compliance with these Clauses.

(d) The Parties agree to document the assessment under paragraph (b) and make it available to the competent supervisory authority on request.

(e) The data importer agrees to notify the data exporter promptly if, after having agreed to these Clauses and for the duration of the contract, it has reason to believe that it is or has become subject to laws or practices not in line with the requirements under paragraph (a), including following a change in the laws of the third country or a measure (such as a disclosure request) indicating an application of such laws in practice that is not in line with the requirements in paragraph (a).

(f) Following a notification pursuant to paragraph (e), or if the data exporter otherwise has reason to believe that the data importer can no longer fulfil its obligations under these Clauses, the data exporter shall promptly identify appropriate measures (e.g. technical or organisational measures to ensure security and confidentiality) to be adopted by the data exporter and/or data importer to address the situation. The data exporter shall suspend the data

transfer if it considers that no appropriate safeguards for such transfer can be ensured, or if instructed by the competent supervisory authority to do so. In this case, the data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses. If the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise. Where the contract is terminated pursuant to this Clause, Clause 16(d) and (e) shall apply.

Clause 15

Obligations of the data importer in case of access by public authorities

15.1 Notification

(a) The data importer agrees to notify the data exporter and, where possible, the data subject promptly (if necessary with the help of the data exporter) if it:

(i) receives a legally binding request from a public authority, including judicial authorities, under the laws of the country of destination for the disclosure of personal data transferred pursuant to these Clauses; such notification shall include information about the personal data requested, the requesting authority, the legal basis for the request and the response provided; or

(ii) becomes aware of any direct access by public authorities to personal data transferred pursuant to these Clauses in accordance with the laws of the country of destination; such notification shall include all information available to the importer.

(b) If the data importer is prohibited from notifying the data exporter and/or the data subject under the laws of the country of destination, the data importer agrees to use its best efforts to obtain a waiver of the prohibition, with a view to communicating as much information as possible, as soon as possible. The data importer agrees to document its best efforts in order to be able to demonstrate them on request of the data exporter.

(c) Where permissible under the laws of the country of destination, the data importer agrees to provide the data exporter, at regular intervals for the duration of the contract, with as much relevant information as possible on the requests received (in particular, number of requests, type of data requested, requesting authority/ies, whether requests have been challenged and the outcome of such challenges, etc.).

(d) The data importer agrees to preserve the information pursuant to paragraphs (a) to (c) for the duration of the contract and make it available to the competent supervisory authority on request.

(e) Paragraphs (a) to (c) are without prejudice to the obligation of the data importer pursuant to Clause 14(e) and Clause 16 to inform the data exporter promptly where it is unable to comply with these Clauses.

15.2 Review of legality and data minimisation

(a) The data importer agrees to review the legality of the request for disclosure, in particular whether it remains within the powers granted to the requesting public authority, and to challenge the request if, after careful assessment, it concludes that there are reasonable grounds to consider that the request is unlawful under the laws of the country of destination, applicable obligations under international law and principles of international comity. The data importer shall, under the same conditions, pursue possibilities of appeal. When challenging a request, the data importer shall seek interim measures with a view to suspending the effects of the request until the competent judicial authority has decided on its merits. It shall not disclose the personal data requested until required to do so under the applicable procedural rules. These requirements are without prejudice to the obligations of the data importer under Clause 14(e).

(b) The data importer agrees to document its legal assessment and any challenge to the request for disclosure and, to the extent permissible under the laws of the country of destination, make the documentation available to the data exporter. It shall also make it available to the competent supervisory authority on request.

(c) The data importer agrees to provide the minimum amount of information permissible when responding to a request for disclosure, based on a reasonable interpretation of the request.

SECTION IV – FINAL PROVISIONS

Clause 16

Non-compliance with the Clauses and termination

(a) The data importer shall promptly inform the data exporter if it is unable to comply with these Clauses, for whatever reason.

(b) In the event that the data importer is in breach of these Clauses or unable to comply with these Clauses, the data exporter shall suspend the transfer of personal data to the data importer until compliance is again ensured or the contract is terminated. This is without prejudice to Clause 14(f).

(c) The data exporter shall be entitled to terminate the contract, insofar as it concerns the processing of personal data under these Clauses, where:

(i) the data exporter has suspended the transfer of personal data to the data importer pursuant to paragraph (b) and compliance with these Clauses is not restored within a reasonable time and in any event within one month of suspension;

(ii) the data importer is in substantial or persistent breach of these Clauses; or

(iii) the data importer fails to comply with a binding decision of a competent court or supervisory authority regarding its obligations under these Clauses.

In these cases, it shall inform the competent supervisory authority of such non-compliance. Where the contract involves more than two Parties, the data exporter may exercise this right to termination only with respect to the relevant Party, unless the Parties have agreed otherwise.

(d) Personal data that has been transferred prior to the termination of the contract pursuant to paragraph (c) shall at the choice of the data exporter immediately be returned to the data exporter or deleted in its entirety. The same shall apply to any copies of the data. The data importer shall certify the deletion of the data to the data exporter. Until the data is deleted or returned, the data importer shall continue to ensure compliance with these Clauses. In case of local laws applicable to the data importer that prohibit the return or deletion of the transferred personal data, the data importer warrants that it will continue to ensure compliance with these Clauses and will only process the data to the extent and for as long as required under that local law.

(e) Either Party may revoke its agreement to be bound by these Clauses where (i) the European Commission adopts a decision pursuant to Article 45(3) of Regulation (EU) 2016/679 that covers the transfer of personal data to which these Clauses apply; or (ii) Regulation (EU) 2016/679 becomes part of the legal framework of the country to which the personal data is transferred. This is without prejudice to other obligations applying to the processing in question under Regulation (EU) 2016/679.

Clause 17

Governing law

These Clauses shall be governed by the law of one of the EU Member States, provided such law allows for third-party beneficiary rights. The Parties agree that this shall be in accordance with, the law that govern the Agreement.

Clause 18

Choice of forum and jurisdiction

(a) Any dispute arising from these Clauses shall be resolved by the courts of an EU Member State.

(b) The Parties agree that those shall be the courts of the law that govern the Agreement.

(c) A data subject may also bring legal proceedings against the data exporter and/or data importer before the courts of the Member State in which he/she has his/her habitual residence.

(d) The Parties agree to submit themselves to the jurisdiction of such courts.

APPENDIX

EXPLANATORY NOTE:

It must be possible to clearly distinguish the information applicable to each transfer or category of transfers and, in this regard, to determine the respective role(s) of the Parties as data exporter(s) and/or data importer(s). This does not necessarily require completing and signing separate appendices for each transfer/category of transfers and/or contractual relationship, where this transparency can achieved through one appendix. However, where necessary to ensure sufficient clarity, separate appendices should be used.

ANNEX I

A. LIST OF PARTIES

Data exporter(s): [*Identity and contact details of the data exporter(s) and, where applicable, of its/their data protection officer and/or representative in the European Union]*

As listed in the Agreement

Activities relevant to the data transferred under these Clauses:

As described in the Agreement

2. Role (controller/processor):
As described in the Agreement

Data importer(s): [*Identity and contact details of the data importer(s), including any contact person with responsibility for data protection]*

As listed in the Agreement.

Activities relevant to the data transferred under these Clauses:

As described in the Agreement

2. Role (controller/processor):

As described in the Agreement.

B. DESCRIPTION OF TRANSFER

Categories of data subjects whose personal data is transferred

As described in Section 1 and 3 of the Data Processing Information.

Categories of personal data transferred

As described in Section 1 and 3 of the Data Processing Information.

Sensitive data transferred (if applicable) and applied restrictions or safeguards that fully take into consideration the nature of the data and the risks involved, such as for instance strict purpose limitation, access restrictions (including access only for staff having followed specialised training), keeping a record of access to the data, restrictions for onward transfers or additional security measures.

As described in Section 1 and 3 of the Data Processing Information.

The frequency of the transfer (e.g. whether the data is transferred on a one-off or continuous basis).

As described in Section 1 and 3 of the Data Processing Information.

Nature of the processing

As described in Section 1 and 3 of the Data Processing Information.

Purpose(s) of the data transfer and further processing

As described in Section 1 and 3 of the Data Processing Information.

The period for which the personal data will be retained, or, if that is not possible, the criteria used to determine that period

As described in Section 1 and 3 of the Data Processing Information.

For transfers to (sub-) processors, also specify subject matter, nature and duration of the processing

As described in Section 1 and 3 of the Data Processing Information.

C. COMPETENT SUPERVISORY AUTHORITY

Identify the competent supervisory authority/ies in accordance with Clause 13

The competent supervisory authority will be the authority of The Netherlands:

"De Autoriteit Persoonsgegevens".

(Unless otherwise required under clause 13).

ANNEX II

TECHNICAL AND ORGANISATIONAL MEASURES INCLUDING TECHNICAL AND ORGANISATIONAL MEASURES TO ENSURE THE SECURITY OF THE DATA

EXPLANATORY NOTE:

The technical and organisational measures must be described in specific (and not generic) terms. See also the general comment on the first page of the Appendix, in particular on the need to clearly indicate which measures apply to each transfer/set of transfers.

Description of the technical and organisational measures implemented by the data importer(s) (including any relevant certifications) to ensure an appropriate level of security, taking into account the nature, scope, context and purpose of the processing, and the risks for the rights and freedoms of natural persons.

As described in Section 2 of the Data Processing Information

ANNEX III

LIST OF SUB-PROCESSORS

EXPLANATORY NOTE:

This Annex must be completed in case of the specific authorisation of sub-processors (Clause 9(a), **Option 1).**

N/A

---

[i] Where the data exporter is a processor subject to Regulation (EU) 2016/679 acting on behalf of a Union institution or body as controller, reliance on these Clauses when engaging another processor (sub-processing) not subject to Regulation (EU) 2016/679 also ensures compliance with Article 29(4) of Regulation (EU) 2018/1725 of the European Parliament and of the Council of 23 October 2018 on the protection of natural persons with regard to the processing of personal data by the Union institutions, bodies, offices and agencies and on the free movement of such data, and repealing Regulation (EC) No 45/2001 and Decision No 1247/2002/EC (OJ L 295, 21.11.2018, p. 39), to the extent these Clauses and the data protection obligations as set out in the contract or other legal act between the controller and the processor pursuant to Article 29(3) of Regulation (EU) 2018/1725 are aligned. This will in particular be the case where the controller and processor rely on the standard contractual clauses included in Decision 2021/915.

[ii] The Agreement on the European Economic Area (EEA Agreement) provides for the extension of the European Union's internal market to the three EEA States Iceland, Liechtenstein and Norway. The Union data protection legislation, including Regulation (EU) 2016/679, is covered by the EEA Agreement and has been incorporated into Annex XI thereto. Therefore, any disclosure by the data importer to a third party located in the EEA does not qualify as an onward transfer for the purpose of these Clauses.

[iii] This requirement may be satisfied by the sub-processor acceding to these Clauses under the appropriate Module, in accordance with Clause 7.

[iv] The data importer may offer independent dispute resolution through an arbitration body only if it is established in a country that has ratified the New York Convention on Enforcement of Arbitration Awards.

[v] As regards the impact of such laws and practices on compliance with these Clauses, different elements may be considered as part of an overall assessment. Such elements may include relevant and documented practical experience with prior instances of requests for disclosure from public authorities, or the absence of such requests, covering a sufficiently representative time-frame. This refers in particular to internal records or other documentation, drawn up on a continuous basis in accordance with due diligence and certified at senior management level, provided that this information can be lawfully shared with third parties. Where this practical experience is relied upon to conclude that the data importer will not be prevented from complying with these Clauses, it needs to be supported by other relevant, objective elements, and it is for the Parties to consider carefully whether these elements together carry sufficient weight, in terms of their reliability and representativeness, to support this conclusion. In particular, the Parties have to take into account whether their practical experience is corroborated and not contradicted by publicly available or otherwise accessible, reliable information on the existence or absence of requests within the same sector and/or the application of the law in practice, such as case law and reports by independent oversight bodies.