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 <u>not</u> 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 <u>not</u> 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.	Personnel 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. Assets and Infrastructure 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.	Personnel 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. Assets and Infrastructure 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.	Personnel 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). Assets and Infrastructure 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	Personnel

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: o LUIS Cognitive Service - *language understanding.* o Text Translator API – *translating text* o 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 rowspan="10">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.</td></tr>
<tr><td><b>CLOUD MODEL</b></td><td><b>GEO-POLICITAL ZONE</b></td><td><b>LOCATION OF DATA CENTRE</b></td><td><b>FACILITY OR PARTNERSHIP</b></td></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>
<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 rowspan="7">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.</td></tr>
<tr><td colspan="2"><b>Customer Location</b></td><td colspan="2"><b>Primarily Support is provided from (but can include other EU countries):</b></td></tr>
<tr><td colspan="2">United Kingdom and Ireland</td><td colspan="2">United Kingdom, Ireland, Portugal and Poland.</td></tr>
<tr><td colspan="2">Sweden, Norway, Denmark, Finland and Iceland</td><td colspan="2">Poland, Portugal, Norway and Sweden.</td></tr>
<tr><td colspan="2">US & Canada</td><td colspan="2">Poland, Portugal, US and Canada.</td></tr>
<tr><td colspan="2">Europe rest</td><td colspan="2">Poland, Portugal and Germany.</td></tr>
<tr><td colspan="2">APAC</td><td colspan="2">Poland, Portugal and Singapore/ Malaysia.</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 rowspan="4">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.</td></tr>
<tr><td><b>Service</b></td><td><b>Geo-political zone</b></td><td><b>Where Service Processes or Stores Data</b></td><td><b>Primarily Support is provided from:</b></td></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>
<tr><td rowspan="5">Unit4 Professional Services and Unit4 customer success function</td><td><b>Topic</b></td><td colspan="3"><b>Professional Services and customer success are provided from:</b></td></tr>
<tr><td>Implementation and other project services</td><td colspan="3">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 colspan="3">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 colspan="3">In applicable Unit4 Support Service location and Portugal.</td></tr>
<tr><td>Customer Success</td><td colspan="3">In applicable Unit4 Support Service location and Portugal.</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

This table contains the information that is required to be inserted into the EU Standard Contractual Clauses that are set out below this table:

Parties	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.
Clause 9 and 11(3)	The data exporter is based in the Territory specified in the Agreement.
Appendix 1	The information required to complete this Appendix is set out in Section 1 and Section 3 of the Data Processing Information
Appendix 2	The information required to complete this Appendix is set out in Section 2 of the Data Processing Information

STANDARD CONTRACTUAL CLAUSES (PROCESSORS)

For the purposes of Article 26(2) of Directive 95/46/EC for the transfer of personal data to processors established in third countries which do not ensure an adequate level of data protection

Parties

Name of the data exporting organisation: …

Address: …

Tel. …; fax …; e-mail: …

Other information needed to identify the organisation

…

(the data **exporter**)

And

Name of the data importing organisation: …

Address: …

Tel. …; fax …; e-mail: …

Other information needed to identify the organisation:

…

(the data **importer**)

each a 'party'; together 'the parties',

HAVE AGREED on the following Contractual Clauses (the Clauses) in order to adduce adequate safeguards with respect to the protection of privacy and fundamental rights and freedoms of individuals for the transfer by the data exporter to the data importer of the personal data specified in Appendix 1.

Clause 1

Definitions

For the purposes of the Clauses:

a) 'personal data', 'special categories of data', 'process/processing', 'controller', 'processor', 'data subject' and 'supervisory authority' shall have the same meaning as in Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data ([1]);

b) 'the data exporter' means the controller who transfers the personal data;

c) 'the data importer' means the processor who agrees to receive from the data exporter personal data intended for processing on his behalf after the transfer in accordance with his instructions and the terms of the Clauses and who is not subject to a third country's system ensuring adequate protection within the meaning of Article 25(1) of Directive 95/46/EC;

d) 'the sub-processor' means any data processor engaged by the data importer or by any other sub-processor of the data importer who agrees to receive from the data importer or from any other sub-processor of the data importer personal data exclusively intended for processing activities to be carried out on behalf of the data exporter after the transfer in accordance with his instructions, the terms of the Clauses and the terms of the written subcontract;

e) 'the applicable data protection law' means the legislation protecting the fundamental rights and freedoms of individuals and, in particular, their right to privacy with respect to the processing of personal data applicable to a controller in the Member State in which the data exporter is established;

f) 'technical and organisational security measures' means those measures aimed at protecting personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing.

Clause 2

Details of the transfer

The details of the transfer and in particular the special categories of personal data where applicable are specified in Appendix 1 which forms an integral part of the Clauses.

Clause 3

Third-party beneficiary clause

1. The data subject can enforce against the data exporter this Clause, Clause 4(b) to (i), Clause 5(a) to (e), and (g) to (j), Clause 6(1) and (2), Clause 7, Clause 8(2), and Clauses 9 to 12 as third-party beneficiary.

2. The data subject can enforce against the data importer this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where the data exporter has factually disappeared or has ceased to exist in law unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law, as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity.

3. The data subject can enforce against the sub-processor this Clause, Clause 5(a) to (e) and (g), Clause 6, Clause 7, Clause 8(2), and Clauses 9 to 12, in cases where both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, unless any successor entity has assumed the entire legal obligations of the data exporter by contract or by operation of law as a result of which it takes on the rights and obligations of the data exporter, in which case the data subject can enforce them against such entity. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

4. The parties do not object to a data subject being represented by an association or other body if the data subject so expressly wishes and if permitted by national law.

Clause 4

Obligations of the data exporter

The data exporter agrees and warrants:

a) that the processing, including the transfer itself, of the personal data has been and will continue to be carried out in accordance with the relevant provisions of the applicable data protection law (and, where applicable, has been notified to the relevant authorities of the Member State where the data exporter is established) and does not violate the relevant provisions of that State;

b) that it has instructed and throughout the duration of the personal data-processing services will instruct the data importer to process the personal data transferred only on the data exporter's behalf and in accordance with the applicable data protection law and the Clauses;

c) that the data importer will provide sufficient guarantees in respect of the technical and organisational security measures specified in Appendix 2 to this contract;

d) that after assessment of the requirements of the applicable data protection law, the security measures are appropriate to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access, in particular where the processing involves the transmission of data over a network, and against all other unlawful forms of processing, and that these measures ensure a level of security appropriate to the risks presented by the processing and the nature of the data to be protected having regard to the state of the art and the cost of their implementation;

e) that it will ensure compliance with the security measures;

f) that, if the transfer involves special categories of data, the data subject has been informed or will be informed before, or as soon as possible after, the transfer that its data could be transmitted to a third country not providing adequate protection within the meaning of Directive 95/46/EC;

g) to forward any notification received from the data importer or any sub-processor pursuant to Clause 5(b) and Clause 8(3) to the data protection supervisory authority if the data exporter decides to continue the transfer or to lift the suspension;

h) to make available to the data subjects upon request a copy of the Clauses, with the exception of Appendix 2, and a summary description of the security measures, as well as a copy of any contract for sub-processing services which has to be made in accordance with the Clauses, unless the Clauses or the contract contain commercial information, in which case it may remove such commercial information;

i) that, in the event of sub-processing, the processing activity is carried out in accordance with Clause 11 by a sub-processor providing at least the same level of protection for the personal data and the rights of data subject as the data importer under the Clauses; and

j) that it will ensure compliance with Clause 4(a) to (i).

Clause 5

Obligations of the data importer **([2])**

The data importer agrees and warrants:

a) to process the personal data only on behalf of the data exporter and in compliance with its instructions and the Clauses; if it cannot provide such compliance for whatever reasons, it agrees to inform promptly the data exporter of its inability to comply, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

b) that it has no reason to believe that the legislation applicable to it prevents it from fulfilling the instructions received from the data exporter and its obligations under the contract and that in the event of a change in this legislation which is likely to have a substantial adverse effect on the warranties and obligations provided by the Clauses, it will promptly notify the change to the data exporter as soon as it is aware, in which case the data exporter is entitled to suspend the transfer of data and/or terminate the contract;

c) that it has implemented the technical and organisational security measures specified in Appendix 2 before processing the personal data transferred;

d) that it will promptly notify the data exporter about:

i. any legally binding request for disclosure of the personal data by a law enforcement authority unless otherwise prohibited, such as a prohibition under criminal law to preserve the confidentiality of a law enforcement investigation;

ii. any accidental or unauthorised access; and

iii. any request received directly from the data subjects without responding to that request, unless it has been otherwise authorised to do so;

e) to deal promptly and properly with all inquiries from the data exporter relating to its processing of the personal data subject to the transfer and to abide by the advice of the supervisory authority with regard to the processing of the data transferred;

f) at the request of the data exporter to submit its data-processing facilities for audit of the processing activities covered by the Clauses which shall be carried out by the data exporter or an inspection body composed of independent members and in possession of the required professional qualifications bound by a duty of confidentiality, selected by the data exporter, where applicable, in agreement with the supervisory authority;

g) to make available to the data subject upon request a copy of the Clauses, or any existing contract for sub-processing, unless the Clauses or contract contain commercial information, in which case it may remove such commercial information, with the exception of Appendix 2 which shall be replaced by a summary description of the security measures in those cases where the data subject is unable to obtain a copy from the data exporter;

h) that, in the event of sub-processing, it has previously informed the data exporter and obtained its prior written consent;

i) that the processing services by the sub-processor will be carried out in accordance with Clause 11;

j) to send promptly a copy of any sub-processor agreement it concludes under the Clauses to the data exporter.

Clause 6

Liability

1. The parties agree that any data subject, who has suffered damage as a result of any breach of the obligations referred to in Clause 3 or in Clause 11 by any party or sub-processor is entitled to receive compensation from the data exporter for the damage suffered.

2. If a data subject is not able to bring a claim for compensation in accordance with paragraph 1 against the data exporter, arising out of a breach by the data importer or his sub-processor of any of their obligations referred to in Clause 3 or in Clause 11, because the data exporter has factually disappeared or ceased to exist in law or has become insolvent, the data importer agrees that the data subject may issue a claim against the data importer as if it were the data exporter, unless any successor entity has assumed the entire legal obligations of the data exporter by contract of by operation of law, in which case the data subject can enforce its rights against such entity.

3. The data importer may not rely on a breach by a sub-processor of its obligations in order to avoid its own liabilities.

4. If a data subject is not able to bring a claim against the data exporter or the data importer referred to in paragraphs 1 and 2, arising out of a breach by the sub-processor of any of their obligations referred to in Clause 3 or in Clause 11 because both the data exporter and the data importer have factually disappeared or ceased to exist in law or have become insolvent, the sub-processor agrees that the data subject may issue a claim against the data sub-processor with regard to its own processing operations under the Clauses as if it were the data exporter or the data importer, unless any successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law, in which case the data subject can enforce its rights against such entity. The liability of the sub-processor shall be limited to its own processing operations under the Clauses.

Clause 7

Mediation and jurisdiction

1. The data importer agrees that if the data subject invokes against it third-party beneficiary rights and/or claims compensation for damages under the Clauses, the data importer will accept the decision of the data subject:

a) to refer the dispute to mediation, by an independent person or, where applicable, by the supervisory authority;

b) to refer the dispute to the courts in the Member State in which the data exporter is established.

2. The parties agree that the choice made by the data subject will not prejudice its substantive or procedural rights to seek remedies in accordance with other provisions of national or international law.

Clause 8

Cooperation with supervisory authorities

1. The data exporter agrees to deposit a copy of this contract with the supervisory authority if it so requests or if such deposit is required under the applicable data protection law.

2. The parties agree that the supervisory authority has the right to conduct an audit of the data importer, and of any sub-processor, which has the same scope and is subject to the same conditions as would apply to an audit of the data exporter under the applicable data protection law.

3. The data importer shall promptly inform the data exporter about the existence of legislation applicable to it or any sub-processor preventing the conduct of an audit of the data importer, or any sub-processor, pursuant to paragraph 2. In such a case the data exporter shall be entitled to take the measures foreseen in Clause 5(b).

Clause 9

Governing law

The Clauses shall be governed by the law of the Member State in which the data exporter is established, namely …

Clause 10

Variation of the contract

The parties undertake not to vary or modify the Clauses. This does not preclude the parties from adding clauses on business related issues where required as long as they do not contradict the Clause.

Clause 11

Sub-processing

The data importer shall not subcontract any of its processing operations performed on behalf of the data exporter under the Clauses without the prior written consent of the data exporter. Where the data importer subcontracts its obligations under the Clauses, with the consent of the data exporter, it shall do so only by way of a written agreement with the sub-processor which imposes the same obligations on the sub-processor as are imposed on the data importer under the Clauses ([3]). Where the sub-processor fails to fulfil its data protection obligations under such written agreement the data importer shall remain fully liable to the data exporter for the performance of the sub-processor's obligations under such agreement.

The prior written contract between the data importer and the sub-processor shall also provide for a third-party beneficiary clause as laid down in Clause 3 for cases where the data subject is not able to bring the claim for compensation referred to in paragraph 1 of Clause 6 against the data exporter or the data importer because they have factually disappeared or have ceased to exist in law or have become insolvent and no successor entity has assumed the entire legal obligations of the data exporter or data importer by contract or by operation of law. Such third-party liability of the sub-processor shall be limited to its own processing operations under the Clauses.

The provisions relating to data protection aspects for sub-processing of the contract referred to in paragraph 1 shall be governed by the law of the Member State in which the data exporter is established, namely …

The data exporter shall keep a list of sub-processing agreements concluded under the Clauses and notified by the data importer pursuant to Clause 5(j), which shall be updated at least once a year. The list shall be available to the data exporter's data protection supervisory authority.

Clause 12

Obligation after the termination of personal data-processing services

The parties agree that on the termination of the provision of data-processing services, the data importer and the sub-processor shall, at the choice of the data exporter, return all the personal data transferred and the copies thereof to the data exporter or shall destroy all the personal data and certify to the data exporter that it has done so, unless legislation imposed upon the data importer prevents it from returning or destroying all or part of the personal data transferred. In that case, the data importer warrants that it will guarantee the confidentiality of the personal data transferred and will not actively process the personal data transferred anymore.

The data importer and the sub-processor warrant that upon request of the data exporter and/or of the supervisory authority, it will submit its data-processing facilities for an audit of the measures referred to in paragraph 1.

The parties agree that these Standard Contractual Clauses become binding on the entering into an order form for services between the parties, which form an agreement.

[1] Parties may reproduce definitions and meanings contained in Directive 95/46/EC within this Clause if they considered it better for the contract to stand alone.

[2] Mandatory requirements of the national legislation applicable to the data importer which do not go beyond what is necessary in a democratic society on the basis of one of the interests listed in Article 13(1) of Directive 95/46/EC, that is, if they constitute a necessary measure to safeguard national security, defence, public security, the prevention, investigation, detection and prosecution of criminal offences or of breaches of ethics for the regulated professions, an important economic or financial interest of the State or the protection of the data subject or the rights and freedoms of others, are not in contradiction with the standard contractual clauses. Some examples of such mandatory requirements which do not go beyond what is necessary in a democratic society are, inter alia, internationally recognised sanctions, tax-reporting requirements or anti-money-laundering reporting requirements.

[3] This requirement may be satisfied by the sub-processor co-signing the contract entered into between the data exporter and the data importer under this Decision.

Appendix 1

to the Standard Contractual Clauses

This Appendix forms part of the Clauses and must be completed and signed by the parties

The Member States may complete or specify, according to their national procedures, any additional necessary information to be contained in this Appendix

Data exporter

The data exporter is (please specify briefly your activities relevant to the transfer):

See Section 1 of the Data Processing Information (above).

Data importer

The data importer is (please specify briefly activities relevant to the transfer):

See Section 1 of the Data Processing Information (above).

Data subjects

The personal data transferred concern the following categories of data subjects (please specify):

See Section 1 of the Data Processing Information (above).

Categories of data

The personal data transferred concern the following categories of data (please specify):

See Section 1 of the Data Processing Information (above).

Special categories of data (if appropriate)

The personal data transferred concern the following special categories of data (please specify):

See Section 1 of the Data Processing Information (above).

Processing operations

The personal data transferred will be subject to the following basic processing activities (please specify):

See Section 1 of the Data Processing Information (above).

Appendix 2

to the Standard Contractual Clauses

Description of the technical and organisational security measures implemented by the data importer in accordance with Clauses 4(d) and 5(c) (or document/legislation attached):

See Section 2 of the Data Processing Information (above).