Annex A(i) – Unit4 Data Processing Terms

1. SUBJECT OF THESE DATA PROCESSING TERMS

1.1 The Customer (hereinafter referred to as the "**Controller**") is the Party, who (alone or in conjunction with others) determines the purposes and means of Processing of any Personal Data.

1.2 Unit4 and its Affiliates (hereinafter referred to as the "**Processor**") is the Party, who acts on behalf of the Controller without being subject to its direct authority.

1.3 The Processor will Process the Personal Data for the Controller (and Controller consents to the same) in accordance with applicable law and these Data Processing Terms including any schedules hereto.

1.4 Schedule 1 describes without limitation the purposes and means of the Processing, the categories of Personal Data that will be Processed and the retention period for such Personal Data and the country(ies) (or place(s)) where the Personal Data will be Processed.

1.5 Schedule 2 describes the applicable Security Measures adopted by the Processor, which the Controller confirms are adequate.

1.6 Schedule 3 sets out the details of any Sub-Processors.

1.7 Schedule 4 comprises the EU Standard Contractual Clauses, which apply where there is any transfer by the Controller of Personal Data from inside the EEA to the Processor located outside the EEA, as further described in paragraph 2.3 below.

1.8 The Schedules shall be updated from time to time during the term of these Data Processing Terms, if necessary.

2 PROCESSING

2.1 The Processor and the Controller shall, without undue delay, provide each other with all necessary information to enable proper compliance with the Data Protection Legislation.

2.2 The Processing of Personal Data takes place in the country/place or countries/places set out in Schedule 1and Controller gives its explicit permission for the Processing of the Personal Data in the countries/places mentioned in Schedule 1. If Processing will take place in another place (s) / country (s), the Processor will inform the Controller of this.

2.3 Where Processing of Personal Data takes place in a country outside the European Economic Area (EEA) for which the European Commission has not provided an adequacy decision, Processing will only take place provided that there are appropriate safeguards that provide an adequate level of protection for Personal Data. In such a case, to ensure appropriate contractual safeguards, the Parties will comply with their respective obligations in the EU Standard Contractual Clauses set out in Schedule 4 to these Data Processing Terms (or such other appropriate safeguards that the Data Protection Authority or a competent regulator decides provides for a sufficient level of protection) and the Controller hereby consents and instructs the Processor to carry out such Processing.

3 RESPONSIBILITIES OF THE PROCESSOR

3.1 The Processor will Process the Personal Data in a proper and careful manner in accordance with these Data Processing Terms and will ensure compliance with the Data Protection Legislation.

3.2 The Processor will only Process Personal Data in accordance with the performance of the Agreement and the written instructions provided by the Controller, unless the Processor is legally obliged to Process the Personal Data in a manner contrary to this. In the latter case, the Processor will inform the Controller of the relevant legal provisions and its obligations thereunder.

3.3 The Processor will only Process Personal Data for the purposes for which it has received instructions and to fulfil the obligations delegated under these Data Processing Terms. The Processor will not use the Personal Data for other purposes.

3.4 The Processor will not provide the Personal Data to a third party (other than the Data Subject or other persons approved by the Controller or the Processor to Process the Personal Data), unless this exchange takes place on the instructions of the Controller or in the context of the performance of the Agreement, these Data Processing Terms (including their respective Appendices or Schedules) or when this is necessary to comply with a legal obligation or court order.

3.5 The Processor will not alter, edit, amend or otherwise change the Personal Data without the Controller instructing it to do so.

3.6 The Processor shall give its reasonable cooperation to the Controller to fulfil requests of a Data Subject in relation to his/her rights under the Data Protection Legislation such as, but not limited to, (i) granting Data Subjects access to their Personal Data; (ii) rectifying or erasing Personal Data at the request of the Data Subject; (iii) presenting evidence of the rectification or erasure of his Personal Data; (iv) providing the Personal Data, which the Data Subject has provided to the Controller and the Controller has passed to the Processor and; (v) transmitting any Personal Data of the Data Subject to another Controller (data portability). If a request is made to return or provide a copy of the Personal Data, the Processor will provide the Personal Data in a structured, widely used and machine-readable format.

3.7 In the event the Processor receives a request or objection from a Data Subject (which could be a request for (without limitation) information, access, rectification, data transfer, introducing a processing restriction, or transfer of the Personal Data), the Processor will forward that request immediately to the Controller.

3.8 The Processor shall maintain a record of all categories of Processing activities carried out on behalf of Controller, in accordance with the Data Protection Legislation. The Processor shall provide the Controller with all necessary information in relation to the same.

3.9 The Processor shall support the Controller in complying with the legal information obligations of a Data Protection Authority or Data Subjects and, if necessary, shall, if it concerns technology of the Processor, assist the Controller where a Privacy Impact Assessment is required by the Data Protection Legislation.

3.10 If the Controller is subject to specific request for information from a Data Subject or third party (other than the Data Subject or other persons approved by the Controller or the Processor to Process the Personal Data) entitled to make such a request, the Processor will assist the Controller with this. The Processor shall not take any steps in relation to any enquiry received from a Data Subject or a third party (other than the Data Subject or other persons approved by the Controller or the Processor to Process the Personal Data), except in accordance with any previous instructions of the Controller. If a Data Subject contacts the Processor to enforce his or her claims related to Data Protection Legislation, the Processor shall forward this request promptly to the Controller.

4 RESPONSIBILITIES OF THE CONTROLLER

4.1 The Controller is responsible for the lawful Processing of the Personal Data and compliance with the Data Protection Legislation including, but not limited to, the protection of the rights of the Data Subjects.

4.2 The Controller shall be solely responsible for determining the purposes for which and the way in which the Personal Data is to be Processed.

4.3 The Controller is responsible for informing the Data Subjects and guaranteeing the rights that the Data Subjects can exercise based on the Data Protection Legislation and other applicable privacy laws and regulations and for communication with the Data Subjects.

4.4 The Controller warrants that the collected Personal Data is adequate, relevant and not excessive in relation to the purposes for which the Personal Data is transferred and (further) Processed.

4.5 The Controller shall make available all information that the Processor may need for the Processing, in a timely fashion and in the agreed format set forth in Schedule 1.

4.6 The Controller shall be responsible and liable (as between the parties themselves and to the Data Subjects and the Data Protection Authority) for: (i) ensuring Data subjects have given the appropriate consent to the Processing (whether by the Processor or any Sub-Processors) and/or ensuring they have the lawful basis to do so; and (ii) any claims or complaints resulting from the Processor's actions to the extent that those actions are the result of the Controller's instructions.

5 SUB-PROCESSORS

5.1 The Processor will engage the Sub-Processor(s) listed in Schedule 3 or in an Order Form by entering into the Agreement.

5.2 The Controller hereby consents to changes in Sub-Processors. The Processor will inform the Controller in writing in advance of any intended changes, for example regarding replacement, of any Sub-Processor. The Controller may object to such changes in writing, within 7 days of written notification of such a change to the Sub-Processors.

5.3 The engagement of a Sub-Processor does not affect the obligations of the Processor towards the Controller in any way. Access to the relevant Personal Data may only be granted when the Sub- Processor complies (or assures compliance) in all material respects with the obligations of these Data Processing Terms. The Processor will execute a written agreement with Sub-Processors in relation to the sub-processing of any Personal Data, which will comply with the Data Protection Legislation and, where practicable, be on materially the same terms as these Data Processing Terms.

5.4 Schedule 3 lists the current Sub-Processors, the Processing location and the description of the work. The Processor will, if necessary and within a reasonable time after a change, update this Schedule during the term of the Agreement.

5.5 Where the Processor sub-contracts any of its obligations to a Sub-Processor who has been approved by the Controller (under the Agreement or if different by subsequent approval), the Processor shall remain liable under these Data Processing Terms for the actions of those Sub-Processors.

5.6 Where the Processor sub-contracts any of its obligations to a Sub-Processor, Controller may (in some circumstances) provide instructions to the Sub-Processor in relation to the Processing of its Personal Data by the Sub-Processor. In such circumstances, Processor shall not be responsible for a breach of these Data Processing Terms that results from the Sub-Processor acting on the instructions of Controller, whether or not Processor is aware of the same.

6 SECURITY AND DATA BREACHES

6.1 The Processor will take the technical and organizational security measures that comply with Data Protection Legislation and industry good practice necessary to ensure the availability, integrity and confidentiality of the Personal Data and to protect it against loss or unlawful Processing. To be able to comply herewith, the Controller will inform the Processor of any reliability requirements that apply to the Processing and provide all necessary information sufficiently in advance in the event of any requested changes in reliability requirements for the Processing of Personal Data.

6.2 The technical and organizational security measures are described in Schedule 2 and comply with generally accepted security standards. The Controller acknowledges that it considers the arrangements set out in Schedule 2 are sufficient for the appropriate security of the Personal Data in accordance with Data Protection Legislation.

6.3 The Processor shall notify the Controller without undue delay after becoming aware of a Data Breach.

6.4 The notification mentioned in clause paragraph 6.3 shall contain at least:

6.4.1 the nature of the Data Breach including, where possible, the categories and approximate number of Data Subjects and the categories and approximate number of Personal Data records concerned;

6.4.2 the name and contact details of the Data Protection Officer or another contact person where more information can be obtained;

6.4.3 the likely consequences of the Data Breach;

6.4.4 the measures taken or proposed to be taken by the Processor to address the Data Breach, including, where appropriate, measures to mitigate its possible adverse effects.

6.5 The Processor shall support the Controller in fulfilling its statutory information obligations towards any supervisory authorities and/or the Data Subjects, in case of a Data Breach.

6.6 The Processor shall inform the Controller immediately if the Processor considers that any Processing instruction given by the Controller infringes any Data Protection Legislation.

7 ADDITIONAL CONFIDENTIALITY PROVISIONS

7.1 The Processor shall keep the Personal Data that it Processes under the Agreement confidential and shall take all necessary measures to ensure the confidentiality of the Personal Data. The Processor will also impose the obligation of confidentiality on its personnel and person engaged by it who have access to the Personal Data.

7.2 The confidentiality obligation referred to in this article shall not apply if the Controller has given written permission to provide the Personal Data to a third party, or in case of a legal obligation to provide the Personal Data to a Third Party.

8 DATA PROTECTION AUDITS

8.1 The Processor enables the Controller to review the compliance of the Processor with these Data Processing Terms or to allow a review through independent auditors, at the cost of the Controller, without the use of any company confidential information of the Processor and without disturbing the operations of the Processor. In case the audit shows that the Processor is not in compliance with its obligations under these Data Processing Terms, the Processor shall remedy or rectify the shortcomings identified by the review as soon as reasonably possible. In such a case the Processor will bear the reasonably incurred and justifiably demonstrable costs of the auditor (payment only being made on presentation of a valid invoice from the auditors for such costs).

8.2 An audit can take place no more than once a year, unless there is sufficient evidence that shows that the Processor is not complying with its obligations under these Data Processing Terms. The Processor shall provide the Controller with all information reasonably necessary to perform the audit.

8.3 In the event of an investigation by a Data Protection Authority or another competent authority ("**Authority**"), the Processor will provide all reasonable cooperation and inform the Controller as soon as possible.

8.4 The Processor shall designate an individual to be the point of contact who will support the Controller in the fulfilment of disclosure obligations arising from Processing and the Processor shall inform the Controller of the contact details for the point of contact.

9 CHANGES

9.1 Where any changes to the performance of an obligation under the Agreement has material consequences in respect of the Processing of Personal Data, the Processor will provide the Controller with a notification of the proposed amendments to these Data Processing Terms (such notification may be electronic mail, or via Unit4 Communities). The Controller will provide any objections, in respect of material changes only, to the amended terms within 7 days of receipt (of notification) and if it does not object, the Controller will be deemed to have accepted the changes and the updated version will apply on the effective date indicated.

9.2 Amendments to the schedules to these Data Processing Terms may be made by the Processor from time to time and published on its website. These changes will be notified to the Controller (such notification may be by electronic mail, or via Unit4 Communities), stating the version number and the date of entry of the updated version. Material changes to the schedules will not be made without providing the Controller the opportunity to object.

10 MUTUAL INDEMNITY

10.1 The Processor shall indemnify the Controller and hold it harmless from fines and / or penalties imposed on the Controller by or on behalf of a Data Protection Authority and for claims relating to any loss or damage suffered by a Data Subject, where it has been established that these penalties and / or penalty payments or claims are directly attributable to a failure by the Processor to Process Personal Data in accordance with Data Protection Legislation or other applicable privacy legislation.

To avail itself of this paragraph 10.1, the Controller shall:

(i) inform the Processor immediately in writing of the existence and the subject matter of the claim of a Data Subject or of any investigation or other instruction that could lead to determining the intention or decision of the Data Protection Authority to impose a penalty or order for a penalty;

(ii) to act and communicate to the Data Protection Authority or to the Data Subject in consultation with the Processor;

(iii) object and / or appeal against imposed fines if there is reason to do so; and

(iv) leave the handling of the case, including the making of any settlements, entirely to the Processor. To this end, the Controller will grant the necessary powers of attorney, information and cooperation to the Processor to defend itself against these legal actions, if necessary in the name of the Controller.

10.2 The Controller shall indemnify the Processor and hold it harmless from fines and / or penalties imposed on the Processor by or on behalf of the Data Protection Authority and for claims for loss or damage suffered by a Data Subject, where it has been established that these penalties and / or penalty payments or claims are attributable to the failure by the Controller to comply with Data Protection Legislation or other applicable privacy legislation.

To avail itself of this paragraph 10.2, the Processor shall:

(i) inform the Controller in writing without delay of the existence and the subject matter of a claim of a Data Subject or of any investigation or other instruction that could lead to determining the intention or decision of the Data Protection Authority to impose a penalty or order for a penalty;

(ii) to act and communicate to the Data Protection Authority or to the Data Subject in consultation with the Controller;

(iii) object and / or appeal against imposed fines if there is reason to do so; and

(iv) leave the handling of the case, including the making of any settlements, entirely to the Controller. To this end, the Processor will grant the necessary powers of attorney, information and cooperation to the Controller to defend itself against these legal actions, if necessary in the name of the Processor.

10.3 Insofar as the Parties share liability (whether joint and severally or otherwise) towards Third Parties, including Data Subject(s), or have a fine jointly imposed upon them by the Data Protection Authority, the Parties shall remain liable to indemnify each other under paragraphs 10.1 and 10.2 for such part of such liability to Third Parties and of any such joint fine that is proportionate to its degree of responsibility for the event giving rise to such liability or joint fine, taking account of the decision of any court or competent tribunal, the Data Protection Authority and the contribution made by any breach by a Party of its obligations under these Data Processing Terms.

11 TERM AND TERMINATION

11.1 These Data Processing Terms will take effect on the date of the Agreement.

11.2 Upon termination of the Agreement, the Processor shall return, or at the Controller's request either destroy or save, the Personal Data in the manner set forth in Schedule 1. In case the Personal Data are held or stored in a computer system or in any other form which reasonably cannot be handed over to the Controller, the Processor will destroy the Personal Data on its systems immediately, unless the Parties agree otherwise in writing.

Schedules:

Schedule 1: Description of the Processing of Personal Data

Schedule 2: Security measures

Schedule 3: Sub-Processors

Schedule 4: EU Standard Contractual Clause

SCHEDULE 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 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**") (generally) including IDS and Wanda	As the PPS 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	All categories of individual listed in this table. Depending on the application or service to which Wanda is

(together with any supporting services)	assignable to an individual; and Application Insights Logs (a Microsoft service utilised for performing diagnostics).	connected, the PPS could potentially Process Personal Data relating to any living individual that the User chooses to submit.

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 these Data Processing Terms, 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, Processing will include the following:

Product	Nature and Objective of Processing
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 Unit4 Cloud Services as set out in more detail in the Unit4 Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). Access to the Personal Data to provide support and maintenance of the Unit4 ERP 7 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 Unit4 Cloud Services as set out in more detail in the Unit4 Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description).

	Access to the Personal Data to provide support and maintenance of the Unit4 Financials 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 Unit4 Cloud Services as set out in more detail in the Unit4 Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). Access to the Personal Data to provide support and maintenance of the Unit4 Student Management 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 Unit4 Cloud Services as set out in more detail in the Unit4 Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). Access to the Personal Data to provide support and maintenance of the Unit4 FP&A 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 Unit4 Talent Management Cloud Services as set out in more detail in the Unit4 Talent Management Cloud Service Description. Access to the Personal Data to provide support and maintenance of the Unit4 Talent Management 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; • intergration of projects into other applications • perfoming 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 Unit4 Global Cloud Services as set out in more detail in the Unit4 Global Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). • Access to the Personal Data to provide support and maintenance of the Unit4 Assistance PSA Suite 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**") (generally) including IDS and Wanda (together with any supporting services)	Data will be processed by the PPS 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, Facebook Messenger 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 Unit4 Cloud Services as set out in more detail in the Unit4 Cloud Service Description or People Platform Services (as set out in the applicable People Platform Service Service Description). Access to the Personal Data to provide support and maintenance of the Unit4 PPS 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.

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 Cloud Services Descriptions.	<u>Personnel</u> The Unit4 Cloud Services operations team has personnel in Poland, Sweden, Norway, UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 Cloud Services. <u>Assets and Infrastructure</u> Unit4 utilises third party hosting infrastructure services to provide the Unit4 SaaS and employs other software systems for operation and management. See Schedule 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 Unit4 Talent Management	<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.

	Cloud Service Description and Solution Specific Service descriptions.	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 Schedule 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 these locations United Kingdom, Poland, Portugal, Norway, Germany, Sweden, Germany, US, Canada (and such other locations as required to support the 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 and/or consulting	The Processor will Process Personal Data in connection with the activities as described in the Agreement and more specifically in any more detailed Project documentation or statements of work agreed between the Parties following Project commencement.	Personnel 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 Schedule 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 these Data Processing Terms Further, the Controller has given the Processor permission to engage the applicable Sub-processor(s) as listed in Schedule 3 by entering into the Agreement.	See Schedule 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 Schedule 3 or the applicable Order Form and any additional provisions provided in further schedules or appendices to these Data Processing Terms if required by the Third Party Provider or Applicable Law.

People Platform Services ("**PPS**") (generally) including IDS and Wanda (together with any supporting services)	In addition to Unit4 SaaS, the PPS 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 Services operations team, which operates the PPS, has personnel in Poland, Sweden, Norway, UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 SaaS.
		
		Assets and Infrastructure
		
		Unit4 utilises its own and third party (shared) infrastructure services to provide the Unit4 People Platform services. This includes 3rd party systems (i.e. collaboration apps), over which Unit4 has no control. The PPS including Wanda 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*
		• 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/.

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>CLOUD MODEL</td><td>GEO-POLICITAL ZONE</td><td>LOCATION OF DATA CENTRE</td><td>FACILITY OR PARTNERSHIP</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 the Amazon Web Services (AWS) data centre in Frankfurt. All Customer data, save for sharing with selected sub-processors in Schedule 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">Customer Location</td><td colspan="2">Primarily Support is provided from:</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

(Enhanced and Premium Support Customers)</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.</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="3">People platform services ("PPS") (generally) including IDS and Wanda (together with any supporting services)</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>Service</td><td>Geo-political zone</td><td>Where Service Processes or Stores Data</td><td>Primarily Support is provided from:</td></tr>
<tr><td>Wanda</td><td>Any</td><td>Predominantly within the EU, but may be elsewhere.</td><td>Ireland, United States and other Global support where required</td></tr>
<tr><td></td><td>IDS</td><td>Depends on Cloud Deployment</td><td>As above for Unit4 SaaS</td><td>As above for Unit4 SaaS</td></tr>
<tr><td rowspan="2">Unit4 Professional Services and Unit4 customer</td><td>Topic</td><td colspan="3">Professional Services and customer success are provided from:</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>
</table>

success function	Data Migration	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).
	Trouble shooting	In applicable Unit4 Support Service location and Portugal.
	Customer Success	In applicable Unit4 Support Service location and Portugal.

6. CONTACT DETAILS

For questions or comments about these Data Processing Terms the contact person is

Controller: By letter (addressed to Global Data Privacy 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.

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

SCHEDULE 2 – SECURITY MEASURES

As stated in paragraph 6 of the Data Processing Terms, the technical and organisational security measures are listed in this schedule 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 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 in the ticketing system.
- 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 Global Information Security Manager and Global Data Privacy 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 Cloud Services:

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.
- Backups are encrypted using whole database encryption technology such as Transparent Database Encryption. Azure Storage Service Encryption to encrypt all data placed into a customer's storage account.
- 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 using for instance Dedicated Accounts and having separate database instances for all our customers.

Network isolation at several points:

- Each dedicated deployment is isolated from other deployments and communicate through private IP addresses.
- Customer VMs can only communicate with other VMs owned or controlled by the same Customer and with infrastructure service endpoints meant for public communications.
- Traffic between VMs always traverses through trusted packet filters.

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

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. Encryption of data at rest can be optionally ordered by the customers. 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 information 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.

As a proof of secure design and operations, Unit4 Cloud Services SaaS Ops holds ISO 27001:2013 certification and ISAE3402 (SOC1) report. Unit4 and the data centres operators hold various security certifications, for the details please refer to the Cloud 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 (1.2) 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.

Additional Elements for Unit4 Talent Management – SaaS (summary)

Talent Management SaaS is ISO27001 certified and has undergone an ISO27001 (phase 1 & 2) and GDPR audit. Most relevant information is included in the table, and extra documentation or information is available on request.

Domain	Practices
Information Security Management and Governance	The Talent Management SaaS Service has implemented an Information Security Management System (ISMS) under ISO27001. This contains, but is not limited to, an information security policy for all employees. The policy can be provided on request. Also, in order to provide information security, management measures are implemented that reduce the risks. These risks and the likelihood of them occurring are included in the ISO27001 ISMS.
Human Resources Security	The provision of the Talent Management SaaS Service provides that all confidential data in kept in a HRIS and complies with ISO27001 for which the information security department is responsible.
Asset Management	Assets (both digital and non-digital) are maintained under a data classification policy
Information Access Control	There are several policies that work according to the principle of least privilege, both for supplied applications, general information and own data. Access to own systems, hosted with Amazon (AWS), are restricted to the specific identified individuals and use of passwords are expressly forbidden. Only public/private key pairs are used to authenticate with servers. The access rights per user are determined in accordance with the established access policy. Specific questions about information access and its policies can be carried out to information security.
Operations Security	This falls under the scope of our ISMS (ISO27001).
Communications Security	All communication falls under a data classification policy. All network traffic runs over SSL/HTTPS, the most common and trusted communications protocol on the Internet. Internal infrastructure is isolated using strict firewalls and network access lists. Each system is designated to a firewall security group by its function. By default, all access is denied and only explicitly allowed ports are exposed. Persistence and storage layers are encrypted (also at-rest) and secured behind VPN & VPC firewalls. Offices use a network protected by a redundant Fortinet 200D Firewall, placed in the datacentre in Merelbeke, connected to the Ghelamco Arena via Dark Fiber. More information about this connection is given in the document “Continuity and Security measures”, also part of the ISMS of the ISO27001 certification.

SCHEDULE 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 Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	Microsoft Dynamics	As stated above in Schedule 2, paragraph 5.	Providing Software Services, in particularly Microsoft Dynamics (including some cloud infrastructure).
	Microsoft	As stated above in Schedule 2, paragraph 5.	Providing software tooling and Office
	Conapto	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
Unit4 SaaS – Talent Management	Amazon Web Services	Frankfurt, Germany	Providing solution - Suite
	Freshdesk	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	LogDNA	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Mandrill	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Mixpanel	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Pingdom	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Productboard	European Economic Area and United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Rustici Software	AWS US-East-1 (Privacy Policy)	Providing solution - Learn (SCORM only) (privacy shield link: Link)
	Sentry	United States of America (Privacy Policy)	Providing solution – Suite (privacy shield link: Link)
	Slack	United States of America (Privacy Policy)	Providing solution – Perform (privacy shield link: Link)
	Stripe	Countries in which Stripe operates (Privacy Policy)	Providing solution – Learn (privacy shield link: Link)
	Wistia	United States of America (Privacy Policy)	Providing solution – Learn (privacy shield link: Link)
People Platform Services ("**PPS**") (generally) including IDS and Wanda (together with any supporting services)	Microsoft Azure	As stated above in Schedule 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 2.

SCHEDULE 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 Schedule 1 and Schedule 3 of these Data Processing Terms
Appendix 2	The information required to complete this Appendix is set out in Schedule 2 of these Data Processing Terms

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 Schedule 1 of the Data Processing Terms (above).

Data importer

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

See Schedule 1 of the Data Processing Terms (above).

Data subjects

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

See Schedule 1 of the Data Processing Terms (above).

Categories of data

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

See Schedule 1 of the Data Processing Terms (above).

Special categories of data (if appropriate)

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

See Schedule 1 of the Data Processing Terms (above).

Processing operations

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

See Schedule 1 of the Data Processing Terms (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 Schedule 2 of the Data Processing Terms (above).