

SCHEDULE 2 - DESCRIPTION OF THE PROCESSING OF PERSONAL DATA

The information below relates to Annex A(i) – Unit4 Agreement Regarding the Processing of Personal Data (“DPA”) a copy of which is available online at www.unit4.com/terms For these schedules to apply, Customer must enter into a DPA with Unit4.

1. THE PERSONAL DATA THAT WILL BE PROCESSED:

Product	Personal Data that may be processed might include:	To whom this may belong:
Unit4 Business World	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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.	<ul style="list-style-type: none"> • 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.

	<p>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.</p> <p>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.</p> <p>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.</p>	
Unit4 prevero	<p>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.</p>	<ul style="list-style-type: none"> • Current or former employees; • Sub-contractors (of any variety), agents or directors.
Unit4 Assistance PSA Suite	<p>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.</p>	<ul style="list-style-type: none"> • 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.

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 Master 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 this DPA, including the performance of functions required or requested by the Data Controller for the Data Controller's compliance with its statutory and/or contractual obligations. In relation to and depending on the Product, Processing will include the following:

Product	Nature and Objective of Processing
Unit4 Business World	<p>Personal Data will be entered into Unit4 Business World 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:</p> <ul style="list-style-type: none"> • Travel requests; • Expense claim processing;

	<ul style="list-style-type: none"> • Timesheet processing; • Absence management; • HR & Payroll related processes: <ul style="list-style-type: none"> ○ Payroll; ○ Course enrolment; ○ Competence management; ○ Appraisals; ○ Salary review; ○ Applicant registration; • Payment processing; • Billing; • Purchase requisitions; • People/Project Planning. <p>The Processing will involve:</p> <p>Product (software solution)</p> <ul style="list-style-type: none"> • Unit4 Business World 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. <p>Services</p> <ul style="list-style-type: none"> • 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. • Access to the Personal Data to provide support and maintenance of the Unit4 Business World 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.
<p>Unit4 Financials</p>	<p>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:</p> <ul style="list-style-type: none"> • Customer/Supplier/Employee registration; • Payment processing; • Billing; • Expense claim processing; • Travel requests; • Purchase requisitions & Orders; • People/Project Planning; • HR & Payroll related processes: <ul style="list-style-type: none"> ○ Payroll; ○ Timesheet processing; ○ Absence management ○ Course enrolment; ○ Competence management; ○ Appraisals; ○ Salary review; ○ Applicant registration; <p>The Processing will involve:</p> <p>Product (software solution)</p> <ul style="list-style-type: none"> • Unit4 Financials 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. <p>Services</p> <ul style="list-style-type: none"> • 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. • Access to the Personal Data to provide support and maintenance of the Unit4 Business World Product and assist the customer in the operation of the solution as set out in more detail in the Unit4 Support Terms

	<ul style="list-style-type: none"> 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	<p>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:</p> <ul style="list-style-type: none"> 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 <p>The Processing will involve:</p> <p>Product (software solution)</p> <ul style="list-style-type: none"> 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. <p>Services</p> <ul style="list-style-type: none"> 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. Access to the Personal Data to provide support and maintenance of the Unit4 Business World 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 prevero	<p>Personal Data will be entered into Unit4 prevero 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:</p> <ul style="list-style-type: none"> Budgeting; Financial and other reporting; Report distribution; Approval processing; People/Project planning. <p>The Processing will involve:</p> <p>Product (software solution)</p> <ul style="list-style-type: none"> Unit4 prevero 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. <p>Services</p> <ul style="list-style-type: none"> 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. Access to the Personal Data to provide support and maintenance of the Unit4 Business World 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	<p>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:</p> <ul style="list-style-type: none"> automation of a professional services organization, including financial and human resource management (HRM); daily time and project management;

	<ul style="list-style-type: none"> • 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 • performing accounting assisting the integration of financial data into other solutions. <p>The Processing will involve:</p> <p>Product (software solution)</p> <ul style="list-style-type: none"> • Unit4 Assistance PSA Suite 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 integations. <p>Services</p> <ul style="list-style-type: none"> • 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. • Access to the Personal Data to provide support and maintenance of the Unit4 Business World 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.
--	---

3. DESCRIPTION OF THE PROCESSING AND MEANS:

Processor 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
Global Cloud Services (Unit4 SaaS or Unit4 Managed Cloud)	The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically the Unit4 Global Cloud Services Description and Solution Specific Service descriptions.	<p><u>Personnel</u></p> <p>The Unit4 Global Cloud Services operations team has personnel in Poland, Sweden, Norway, UK, US, Canada, Malaysia and Singapore. These Processor personnel operate the Unit4 Global Cloud Services.</p> <p><u>Assets and Infrastructure</u></p> <p>Unit4 utilises third party hosting infrastructure services to provide the Unit4 Global Cloud Services and employs other software systems for operation and management. See Schedule 4.</p>
Support Services	The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically in the Unit4 Support Terms.	<p><u>Personnel</u></p> <p>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).</p> <p><u>Assets and Infrastructure</u></p> <p>Unit4 utilises other software systems for operation, delivery and management of these services.</p>
Professional Services and/or consulting	The Processor will Process Personal Data in connection with the activities as described in the Master Agreement and more specifically in any more detailed	<p><u>Personnel</u></p> <p>The Unit4 Professional Services team has personnel in all locations where Unit4 has a corporate group entity including United Kingdom,</p>

	Project documentation or statements of work agreed between the Parties following Project commencement.	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. <u>Assets and Infrastructure</u> 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 Master Agreement and (if any) the Third Party contractual and service documentation provided as part of the Master Agreement. For more details, See Schedule 4. The Processor will execute a written agreement with the Sub-processor(s), which will be in accordance with the relevant legislation and regulations and this DPA. Further, the Data Controller has given the Processor permission to engage the applicable Sub-processor(s) as listed in Schedule 4 by signing this DPA.	See Schedule 4.
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 Master Agreement and the Third Party contractual and service documentation provided as part of the Master Agreement.	See Schedule 4 and any additional provisions provided in further schedules or appendices to this DPA if required by the Third Party Provider or Applicable Law.

4. RETENTION PERIOD

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

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

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

Product - On premises	Data is stored on the servers of the Data Controller in their principal place of business or registered office as can be notified to Unit4 from time to time.			
Product - Unit4 Global Cloud Services	Unit4 Global 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.			
	CLOUD MODEL	ZONE	LOCATION	FACILITY OR PARTNERSHIP

	MANAGED CLOUD	BENELUX	AMSTERDAM / EDE	DIGITAL REALITY / BIT
	MANAGED CLOUD	SWEDEN	STOCKHOLM	SUNGARD
	MANAGED CLOUD	UK (WALES)	NEWPORT	NGD
	MANAGED CLOUD	UK (ENGLAND)	LONDON	DIGITAL REALITY
	MANAGED CLOUD	US	MULTIPLE LOCATIONS	AMAZON WEB SERVICES (AWS)
	MANAGED CLOUD	CANADA	TORONTO	IBM SOFTLAYER
	SAAS/MANAGED CLOUD	EU	DUBLIN / AMSTERDAM	MICROSOFT AZURE
	SAAS/MANAGED CLOUD	USA	MULTIPLE LOCATIONS	MICROSOFT AZURE
	SAAS/MANAGED CLOUD	CANADA	TORONTO / QUEBEC CITY	MICROSOFT AZURE
	SAAS/MANAGED CLOUD	UNITED KINGDOM	LONDON / CARDIFF	MICROSOFT AZURE
	SAAS/MANAGED CLOUD	ASIA	SINGAPORE / HONG KONG	MICROSOFT AZURE
	SAAS/MANAGED CLOUD	AUSTRALIA	VICTORIA / NEW SOUTH WALES	MICROSOFT AZURE
Unit4 Support – Standard Support and other standard support services	Unit4 Support uses SalesForce to register and process Cases. These Cases are accessible for any Unit4 employee that is provided access to SalesForce 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.			
	Customer Location		Primarily Support is provided from:	
	United Kingdom and Ireland		United Kingdom, Ireland, Portugal and Poland.	
	Sweden, Norway, Denmark, Finland and Iceland		Poland, Portugal, Norway and Sweden.	
	US & Canada		Poland, Portugal, US and Canada.	
	Europe rest		Poland, Portugal and Germany.	
	APAC		Poland, Portugal and Singapore/ Malaysia.	
Unit4 Support – 24/7 Support	Using a 'follow the sun' methodology, 24/7 support of Customer Cases could occur in any of the support locations listed above.			
Unit4 Support – EU Only Support	If EU Only support is elected, Cases are supported only within the EU locations listed above for standard support (during Business Hours).			
Unit4 Professional Services and Unit4 customer success function	Topic	Professional Services and customer success are provided from:		
	Implementation and other project services	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).		
	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 the DPA and Schedules the contact person is

Data 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 Master Agreement.

Processor: The Data Controller address for notices provided in the DPA or Master Agreement.

SCHEDULE 3 – SECURITY MEASURES

As stated in article 7 of the DPA, the technical and organisational security measures are listed in this schedule and are supplemented or amended if necessary. The Data 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 logical 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 the access to the system (including monitoring signs of unauthorised access to the Personal Data);
 - 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 approved 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 (including its General Business Principles found on www.unit4.com/about/ethics).
- 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/about/ethics.
- 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 Global Cloud Services (summary)

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

Data protection

Unit4 Global 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 our security posture to defend against potential breaches. The Unit4 Global Cloud operations team that closely monitor and secures Unit4's Global Cloud operations (cloud infrastructure, cloud services, products, devices and internal resources) simulate real-world breaches — 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 24x7 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 Global 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 Global Cloud Service Description.

SCHEDULE 4 – SUB-PROCESSORS

Service	Sub-processor (company name, location etc.)	Processing location	Type of service by Sub-processor
Unit4 Professional Services (if sub-contracted to a delivery partner)	As specified in the Master Agreement.	As specified in the Master 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 Master Agreement.	As provided in the Master 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 Global Cloud Services	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
	Sungard	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	Digital Realty	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	Amazon Web Services	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	Bit Data Center	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	IBM Softlayer	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services
	NGD	As stated above in Schedule 2, paragraph 5.	Providing Cloud Infrastructure and Services