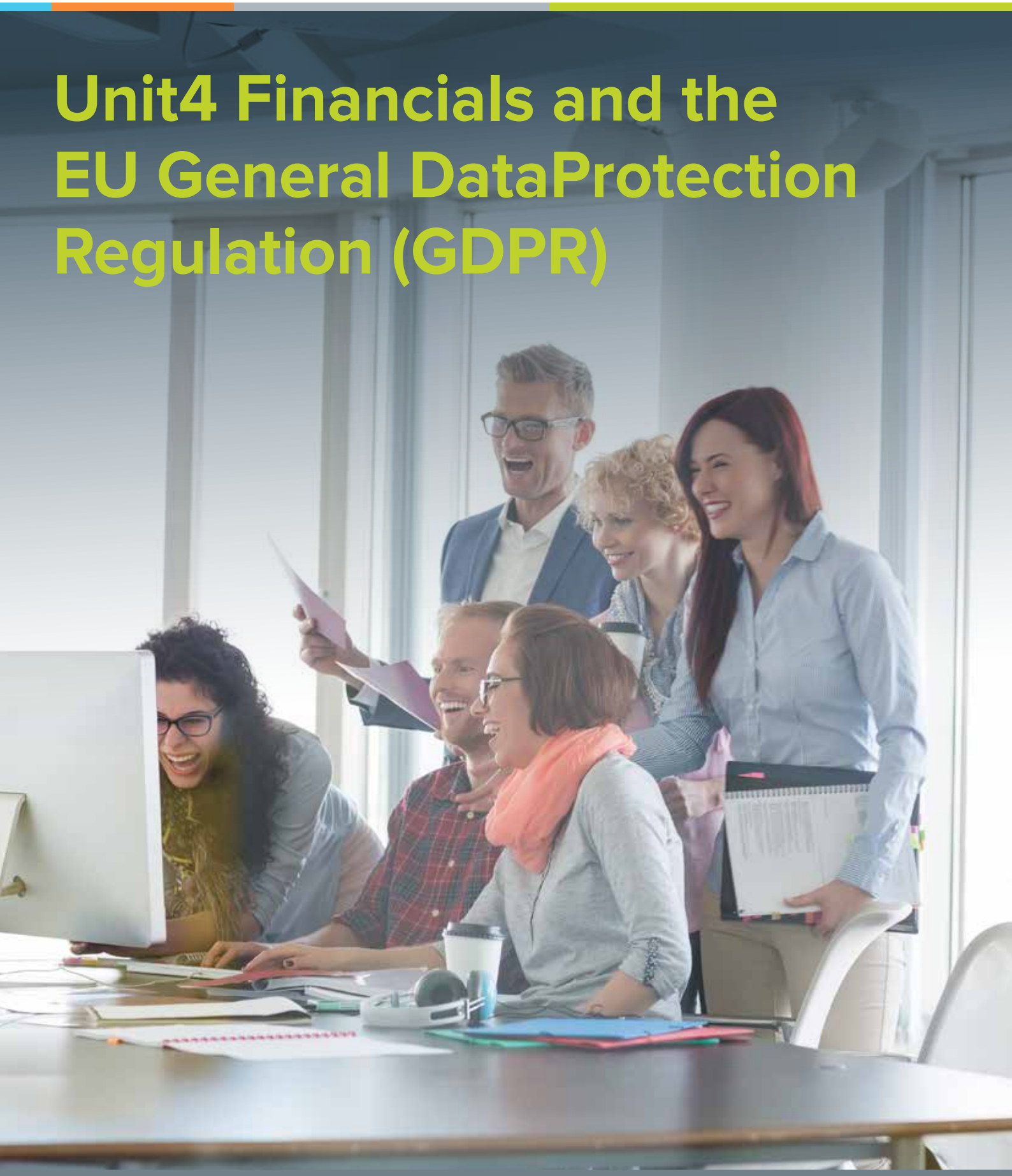
UNIT4

BRIEFING PAPER

Unit4 Financials and the EU General DataProtection Regulation (GDPR)



In business for people.

Disclaimer

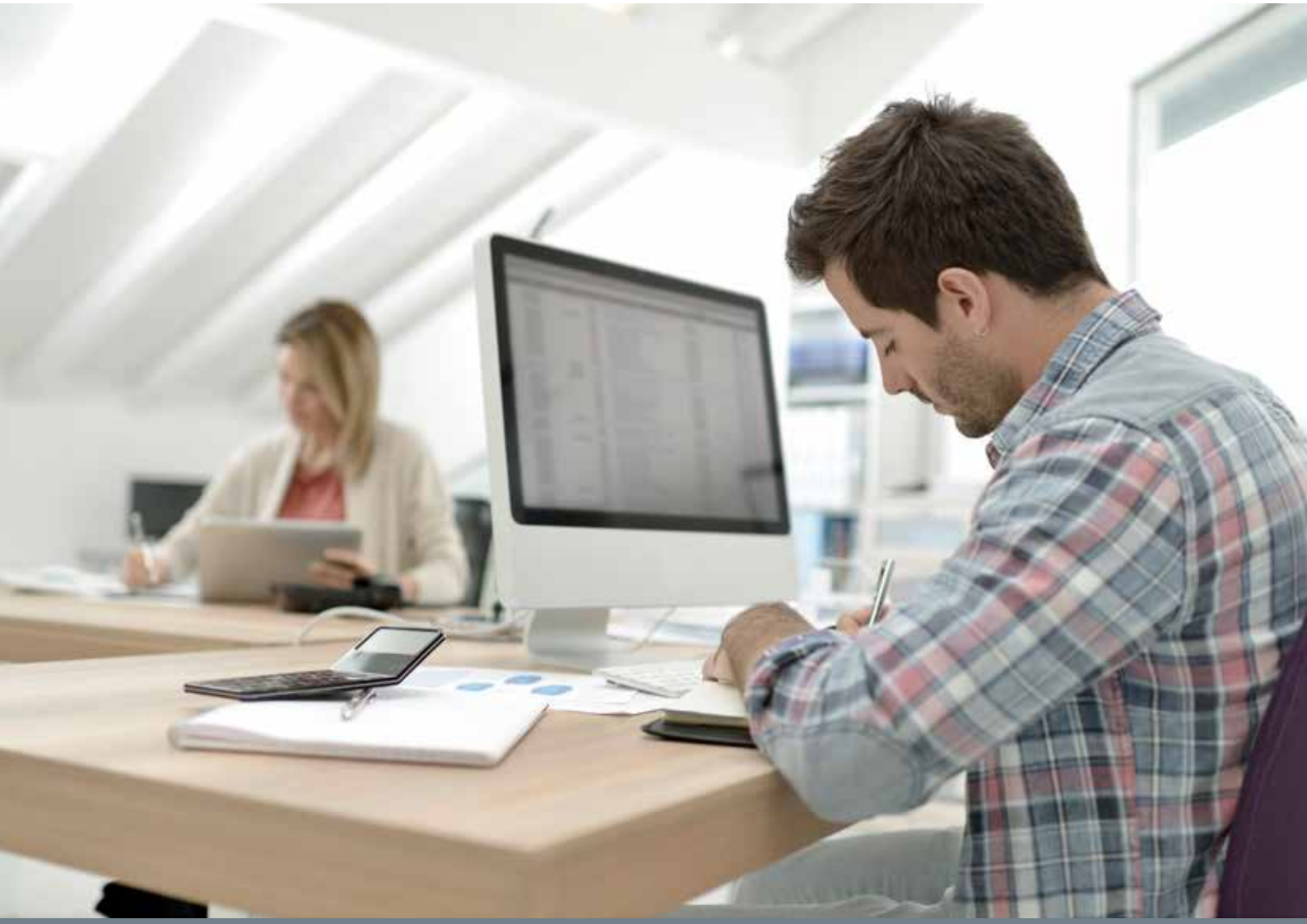
Every effort has been made to supply accurate information however the information in this document is subject to change without notice. Unit4 reserves the right to, at any time, make changes to the Roadmap, version names, delivery dates and any other information necessary for any reason deemed appropriate at the time. Unit4 assumes no responsibility for any errors that may occur in the documentation. No contractual commitments can be made regarding the content of this document. No rights can be derived from this document or claims can be made on the correctness and completeness of the content. Unit4 does not accept any liability.

Contents

1. Background to General Data Protection Regulation

General Data Protection Regulation (GDPR), is a regulation that is intended to strengthen and unify protection for all citizens within the EU, and to better protect their privacy. In addition, the regulation will give a unified data protection environment for organizations to operate in, as the regulation will be directly binding and applicable in all EU member states and organizations (Data Processors) which process data of EU citizens across the Globe.

The regulation was adopted by the European Parliament and European Council on April 27th 2016 and will be enforced by law from 25th May 2018, and will then replace the Data Protection Directive (Directive 95/46/EC) from 1995 (DPD).



2. Objective of this Whitepaper

This whitepaper is intended to communicate to customers how our product – Unit4 Financials – can help them comply with GDPR regulations and also identify areas where they are responsible for defining processes to enable their end-customers to exercise their rights (Data Subject Rights). GDPR provides the following rights for individuals (subjects):

a) The right to be informed

b) The right of access

c) The right to rectification

d) The right to erasure/ to be forgotten

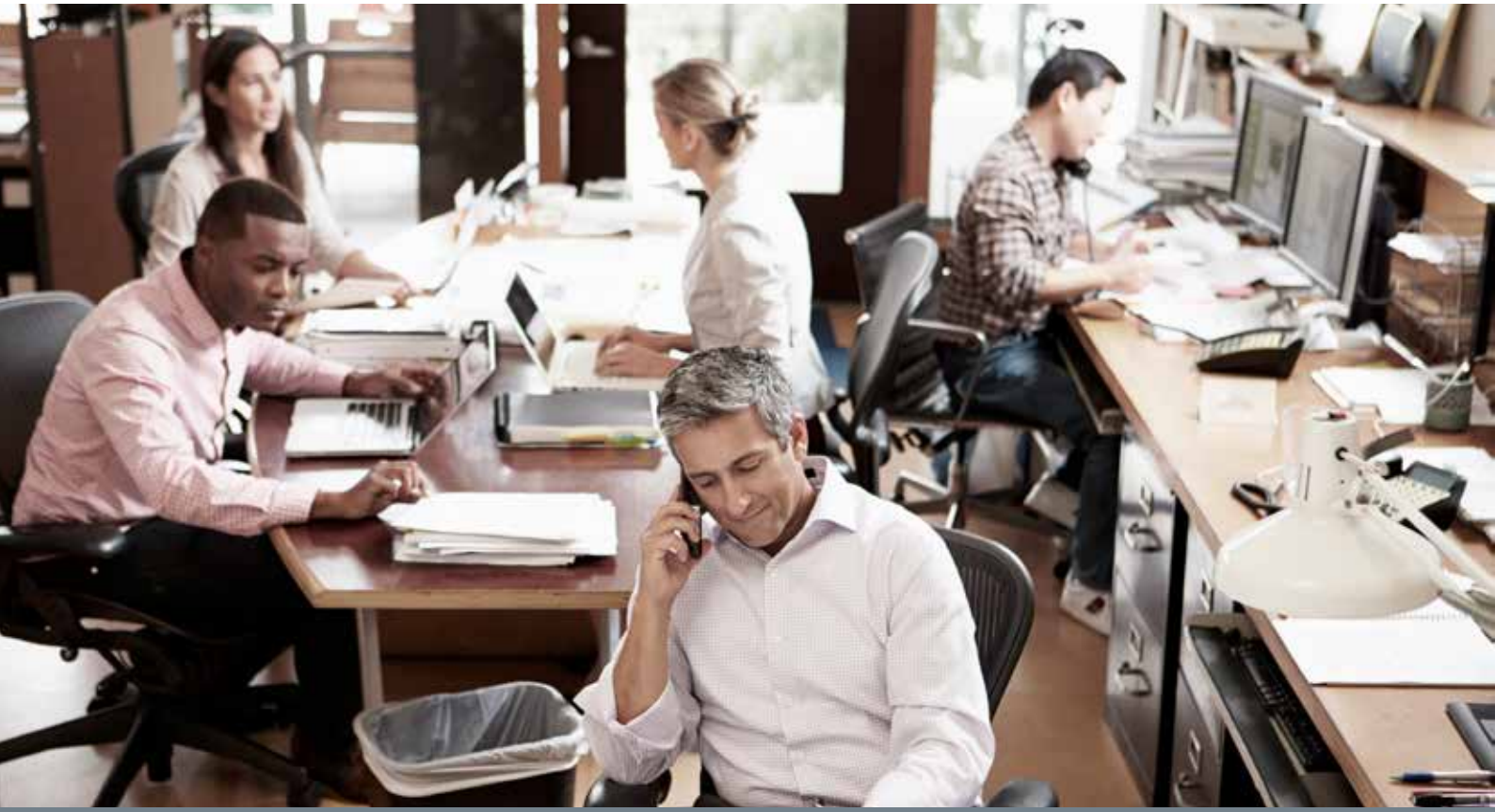
e) The right to restrict processing

f) The right to data portability

g) The right to object

h) The right in relation to automated decision making and profiling

This paper addresses the product capabilities in enabling our customers to execute the Data Subject Rights (DSRs) and addresses compliance on other processes such as consent, security, privacy by design/ default, breach notification and demonstrating compliance to the relevant supervisory authority.



3. Overview of the regulation

3.1 Principles of GDPR

The principles underpinning GDPR are:

Lawfulness, fairness and transparency	Communicating transparently about what the Data Controller is going to do with the data, how it is going to be processed, who it is to be shared with, etc.
Purpose limitation	Collecting and processing data for the specified purpose only
Data minimization	Only processing that data which is necessary for fulfilling the stated purpose
Data accuracy	Includes timeliness and outputs from processing
Storage limitation	Only storing the personal data for as long as is appropriate for the purpose identified
Integrity and confidentiality	Ensuring that personal data is secure from unauthorized, or unlawful processing and against accidental loss, destruction or damage
Accountability	Processing responsibly and demonstrating compliance

3.2 Key Stakeholders in GDPR

The GDPR identifies the following roles in its legislation:

a. *(Data) Subject* – means the person(s) to whom personal data (means any information relating to an identified or identifiable natural person directly or indirectly) relate or may relate to.

b. *Supervisory Authority* – a nominated public body responsible for monitoring the application of the GDPR.

c. *Data Protection Officer* – a Data Protection Officer (DPO) responds to compliance with privacy regulations in an organization.

d. *Data Controller* – the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes for which and the manner in which any personal data are, or are to be, processed.

e. *Data Processor* – a natural or legal person, public authority, agency or other body that processes personal data on behalf of the Data Controller.

f. *3rd Party* - a natural or legal person, public authority, agency or body other than the Data Subject, Data Controller, Data Processor and persons who, under the direct authority of the Data Controller or Data Processor, are authorized to process personal data.

4. Unit4 Financials – How our product complies with GDPR Regulations

Unit4 Financials is a best-in-class core financials solution designed for people-centric organizations. It provides a fully integrated data model, processing model and reporting model, enabling our customers to manage all their key business areas in a single suite:

- Corporate Financial Management, incorporating GL, AP, AR
- Procurement Management, including Invoice Matching
- Billing
- Fixed Assets

As Data Controllers, our customers will have responsibilities when it comes to GDPR compliance. With a strong history in focusing on security and privacy, by default Unit4 Financials can support them.

Some of the highlights of the functionality Unit4 Financials offers to our customers to meet their responsibilities as Data Controllers is described below.

4.1 Lawfulness of processing

What it means:

The GDPR defines that processing of personal data shall be lawful, done fairly and in a transparent manner in relation to the Data Subject and that processing shall be lawful only if and to the extent that at least one of the following applies:

a. The Data Subject has given consent to the processing for one or more specific purposes.

b. Processing is necessary for the performance of a contract to which the data subject is part of, or in order to take necessary steps at the request of the data subject prior to entering into a contract.

c. Processing is necessary for compliance with legal obligations of the Data Controller.

d. Processing is necessary in order to protect the vital interests of the Data Subject or of another natural person.

e. Processing is necessary for the performance of a task carried out in the public interest.

f. Processing is necessary for the purpose of the legitimate interests pursued by the Data Controller or by a third party except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

This means that any type of processing of PII data shall be tied to one of the legal grounds and the Data Controller is liable to inform the Data Subject about the processes for which the PII data is being used, the purpose of it and the lawfulness of it.

Consent may in some cases be required for the processing of personal data. The Data Controller is responsible for ensuring that the consent of the Data Subjects is obtained and that a person can also revoke/withdraw this consent. The proof that consent has been obtained is also with the Data Controller. The Data Controller must also register / document the consent or withdrawal. This does not have to be included into a product itself, but can also be done elsewhere.

The Data Controller's responsibility:

Ensure that any processing in Unit4 Financials can be tied to at least one of the legal grounds, and that this is documented for building up transparency through their processes. If consent is needed the Data Controller needs to assure that consent forms:

- are presented in an intelligible and easily accessible form.
- use clear and plain language.
- clearly distinguish the request for consent from other matters.

- refer to the Data Subject's right to withdraw his/her consent.
- contain a link to a privacy policy or statement, which includes all required information.
- document all consents (as well as any withdrawal of consent).
- ensure that consent is given by a clear affirmative action of the Data Subject.
- if a child's consent is involved, ensure that 'reasonable efforts' are made in order to verify that such consent is given or authorized by a parent.
- verify whether the privacy policy or statement needs to be updated.

How Unit4 Financials enables customers to execute this right:

For our customers, the personal data stored in Unit4 Financials may hold different types of information tied to the person; such as elements/master records of employees/suppliers/customers holding name, address, social security number, bank account number, expense claims, and so on. As a Data Controller, you will have legitimate interest as its processing is based on performance of a contract. Extending the categories of personal data is possible through flexi-fields, but it's advised to do this only when directly relevant and necessary for the purpose for which you obtained the data. In Unit4 Financials, consent is handled as part of performance of a contract. If needed, a contract can be stored in Document Repository in Unit4 Financials linked to the employee/user and/or customer/supplier.

4.2 How Unit4 Financials Enables Customers to execute Data Subject Rights

Under the GDPR, the Data Subjects now have a set of rights that companies that employ, interact with, or sell to them, will need to comply with – providing that the exercise of those rights does not compromise any other industry, or national, laws or regulations. Failure to comply within the timescales laid out in the regulations will entitle the Data Subject to file a claim for compensation. The paragraph below provides an explanation of these rights and also how Unit4 Financials enables our customers to execute the DSRs.

4.2.1 Right to be Informed

What it means:

The right to be informed obliges the Data Controller to provide 'fair processing information' to its Data Subjects. It requires that a Data Subject be sufficiently informed to ensure a fair and transparent data processing. The information must be provided to the Data Subject in a *'concise, transparent, intelligible and easily accessible form'*. It emphasizes the need for transparency at the point of collection, over how any personal data will be used by the Data Controller. The Data Controller also needs to be aware of how they obtained the personal data, for example directly from the Data Subject, or from some other source.

The Data Controller's responsibility:

Under the GDPR, Data Controllers will see their obligation to inform the Data Subject enhanced, as they will also have to inform the Data Subjects about inter alia:

- the envisaged retention period of the personal data.
- their right to withdraw their consent at any moment.
- the right to rectification.
- the right to erasure/ to be forgotten.
- the right to restrict processing.
- the right to object.

The GDPR specifically requires that the information is provided to the Data Subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language, especially when the information is addressed to a child.

How Unit4 Financials enables customers to execute this right:

Within Unit4 Financials, the customers have the ability to integrate data from other business applications with API interfaces. This will help our customers to display actual information from source systems in Unit4 Financials, providing transparency to the Data Subjects on personal data stored and processed with regards to the right to be informed.

a. *Personal data:* In Unit4 Financials there are various system-defined categories of personal data: System user information, employee, supplier and customer information. For most of our customers the personal data stored in these records will have legitimate interest. There are options available to extend

the diversity of personal data kept in the system through flexi-fields.

b. *Document Repository:* The document archiving functionality in Unit4 Financials, allows users to store digital documents including relevant metadata, making it easy to search and select for specific document types, dates or other characteristics. Documents can be stored on employee level, where access restrictions help prevent unwanted access to sensitive documents.

4.2.2 Right to Access

What it means:

The Data Subject has the right to obtain from the Data Controller confirmation as to whether or not personal data concerning him or her are being processed and, where that is the case provide the Data Subject with a copy of the data upon request. This means that the Data Subject can request, without undue delay, the right of access to their personal data, easily and at reasonable intervals, in order to be aware of and verify the lawfulness of the processing.

The Data Controller's responsibility:

As a Data Subject can request the right to access their personal data at any point in time it's important to determine how this data will be disclosed.

How Unit4 Financials enables customers to execute this right:

A pre-requisite for being compliant to the right to access, is that the Data Controller knows which personal data the organization holds on any person, where personal related information is stored and how to access the personal related information. In addition, the organization also needs to know which processes the personal-related information is used. In the appendix of this document you will find an overview of standard master data records, processes and Unit4 Financials standard functionality that supports the extraction of (personal) data directly upon request. This will help our customers to follow up a Data Subject's right to access.

a. *Data extraction:* Unit4 Financials offers a wide range of operational reporting tools for data extraction. Browse Details, Generic Browse, Browse Ledger, Browse Balances, XL for Unit4 Financials and Browse Ledger are ad hoc enquiry tools that enable users to quickly browse all types of business data in the system. Templates can be created on the fly for recurring enquiries. Data control can be used to "shield off" any sensitive data while users are still able to run the report.

4.2.3 Right to Rectification

What it means:

The Data Subject is entitled to have their personal data rectified if it is inaccurate or incomplete. If the data is incorrect, or incomplete, it must be corrected everywhere, without undue delay.

The Data Controller's responsibility:

Enabling change is business as usual in Unit4 Financials. The Data Controller will need to determine how the changes based on a right to rectification request will be effected. If a system administrator or super user is editing the data based on the rectifications provided by the Data Subject, the Data Controller is responsible for notifying the Data Subject once the updates have been completed.

How Unit4 Financials enables customers to execute this right:

In Unit4 Financials, users can logon and spot any inconsistencies by reviewing their personal master data. Fields regarding master data are amendable, either by the end user directly or by a system administrator, or super users, depending on the distribution of system access rights. If end users are granted rights to make changes themselves, the element authorization workflow can be used for reviewing the proposed changes.

4.2.4 Right to Erasure (Right to Be Forgotten)

What it means:

The right to erasure is commonly referred to as 'the right to be forgotten', however, erasure may only be partial and does not have to be complete. The broad principle underpinning this right is to enable an individual to request the deletion or removal of their personal data (or some of it) – without undue delay – when there is no compelling reason for its continued processing. In particular, the Data Subject will have the right to request erasure of his/her personal data on several grounds. These include the following situations:

1. when processing is no longer necessary for the intended purpose.
2. when the Data Subject withdraws his/her consent.
3. when the Data Subject objects to the processing and there are no overriding legitimate grounds for the processing.
4. when the processing is unlawful.
5. when erasure is necessary for compliance with a legal obligation; or
6. when the data concerns a child and has been collected via information society services.

The Data Controller's responsibility:

GDPR creates a broader right to erasure than the right available to Data Subjects under the directive. Consequently, our customers face a broader spectrum of erasure requests. Each person has the right to erase his personal data without unreasonable delay, in a number of cases, as mentioned under above clause (4.2.4). Not every request for erasure should be carried out. An erasure request shall not apply to the extent that processing is necessary:

- for exercising the right of freedom of expression and information.
- for compliance with a legal obligation.
- data that is stored and processed for the purpose of performing of the contract (and the contract still continues).
- for reasons of public interest in the area of public health.
- for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes, in so far as the right referred to is likely to render impossible or seriously impair the achievement of the objectives of that processing.
- for the establishment, exercise or defense of legal claims.

For example, if the data that is stored and processed on basis of a legal duty or is still necessary for the intended purpose (such as performing of the agreement), then a request for erasure can be rejected. The Data Subject should be notified about this, for example through a privacy notice and/or when he exercises his right to erasure.

Furthermore, the right to oblivion for Data Controllers imposes the additional duties to ensure that further disclosure of the data is made by those third parties to whom the person responsible has provided the personal data.

How Unit4 Financials enables customers to execute this right:

To support our customers' compliance with the right to be forgotten, Unit4 Financials offers options subject to applicable accounting principles and legislation.

Compliance can be achieved by manually anonymizing personal data in cases where deletion is not an option. The key to the right to be forgotten is that the link between the data and the living Data Subject is broken, so the remaining data can no longer be tied back to the Data Subject, which would be the case for anonymizing.

a. Document Repository: Documents in the Document Repository can contain personal data. A request for erasure will have an effect on this type of personal data. Documents can be anonymized or deleted from the Document Repository.

4.2.5 Right to Restriction of Processing

What it means:

A Data Subject can request a restriction of the processing of personal data. Restriction can be requested for example in case the personal data is inaccurate, or unlawful, or pending a decision on a complaint lodged by the Data Subject.

The Data Controller's responsibility:

Clear procedures are important to support requests to restriction of processing. To ensure compliancy, the procedure will need to cater for status control of the relevant personal data (that is make sure it's not processed).

A Data Subject who has obtained restriction of processing shall be informed by the Data Controller before the restriction of processing is lifted.

How Unit4 Financials enables customers to execute this right:

Given the fact that most processes in Unit4 Financials are run as part of the performance of a contract, impact will be low in this area. If needed, as support for following up on a Data Subject's objection to processing, this can be captured in flexi-fields on the element master files.

a. *Element values and status:* All (personal) master data in Unit4 Financials (such as employees, suppliers/customers, users, and user defined master files) are represented as element values. The status of an element value determines whether any data processing on it is possible and/or marks it for data purging. An easy way to exclude element values from any processes that is run.

b. *Flexi-field values:* these greatly contribute to Unit4 Financials' flexibility. They can be used to label certain (personal) data to create reporting hierarchies, distribute tasks, apply data control and group (or exclude) certain records for designated business processes.

c. *Data control:* Data control is a mechanism that allows access control at the level of a single or a group of records (for example element value(s)). It can be used to prevent people who normally have the proper authorization to under certain circumstance revoke the access to a record so they cannot adapt, alter, use, erase or disclose the data.

4.2.6 Right to Data Portability

What it means:

The Data Subject has the right to receive the personal data concerning them, which they have provided to a Data Controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another Data Controller without hindrance of the Data Controller that collected the data in the first place. In exercising their right to data portability, the Data Subject shall have the right to have their personal data transmitted directly from one Data Controller to another, where technically feasible.

The Data Controller's responsibility:

In context of the right to portability, the Data Controller needs to be able to provide personal data of a Data Subject in a machine-readable format. For Unit4 Financials, the most efficient way to that would be by extracting the data through one of the enquiry tools or directly via the API and transmitting it in a secure way.

How Unit4 Financials enables customers to execute this right:

Enquiry capabilities allow you to create reports on any type of personal data, both on stored data and on the processes in which the data is included. Contents of the enquiries can be used to create a report which is then exported to a machine-readable format like csv or xml. Unit4 Financials also provides web services (APIs) for extracting personal data and/or user data. When creating data extracts with the purpose of processing the data outside of Unit4 Financials, it's important for our customers to realize that when they hold personal data, these reports need to be used in a secure and controlled matter and defined by a Data Controller's internal processes around GDPR.

4.2.7 Right to Object

What it means:

The Data Subject can request in specific circumstances (personal to the Data Subject) that processing of their personal data is stopped. The objection can be conditional.

The Data Controller's responsibility:

As a Data Controller, the personal data that is objected to process needs to be removed from the respective masterfile. Information on the (conditions) of objection can be added to the masterfile to keep track of these requests, also for future reference. The Data Controller shall no longer process the personal data unless the Data Controller demonstrates compelling legitimate grounds for the processing which overrides the interests, rights and freedoms of the Data Subject or for the establishment, exercise or defence of legal claims.

How Unit4 Financials enables customers to execute this right:

Processing of personal data in Unit4 Financials has a lawful basis when it relates to the performance of contract. If a Data Subject successfully objects to processing (parts of) their personal data this can be followed up on by making changes to the master data (that is remove a specific part of the individual's identifiable information). An audit trail of these changes is maintained by the system.

4.2.8 Right not to be subjected to Automated Decision Making, including Profiling

What it means:

The GDPR introduces the following definition of 'profiling': "any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyze or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behavior, location or movements".

The Data Subject has the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her – unless the processing:

a. is necessary for entering into or performance of a contract between the Data Subject and the Data Controller.
b. is authorized by law (for example for the purposes of fraud or tax evasion prevention) to which the Data Controller is subject and which also lays down suitable measures to safeguard the Data Subject's rights and freedoms and legitimate interests.
c. is based on the Data Subject's explicit consent.

The Data Controller's responsibility:

This Data Subject Right is not applicable, as Unit4 Financials does not provide any automated decision-making functionality.

How Unit4 Financials enables customers to execute this right:

Unit4 Financials today doesn't have any automated decision-taking processes with regards to personal data. If included in any of our future developments and if not necessary due to a performance of contract (applicable to most of the processes in Unit4 Financials), we will add an explicit consent following the privacy by design guidelines.

4.3 Demonstrating Compliance

What it means:

Each Data Controller and, where applicable, the Data Controller's representative, shall maintain a record of processing activities under its responsibility.

Each Data Processor and, where applicable, the Data Processor's representative shall maintain a record of all categories of processing activities carried out on behalf of a Data Controller.

4.4 Security – Access and Data control

What it means:

Security of personal data and the controls associated with access privileges is of primary importance to safeguard information avoid data breaches. The Data Controller must work with the IT/ IS teams to make sure they implement appropriate technical and organizational measures to render the data unintelligible in case of unauthorized access.

The Data Controller's responsibility:

GDPR states that: "...the Data Controller shall implement appropriate technical and organizational measures to ensure and to be able to demonstrate that processing is performed in accordance ... [with the regulation]" It's the Data Controller's responsibility to implement these measures. In doing so, Unit4 Financials tooling as described below can help achieve compliance.

If Unit4 Financials is used as the source system in an integration scenario, then the Data Controller needs to ensure changes to the master data in Unit4 Financials are also reflected in the 3rd party systems through the integration solution configuration. Typically, this would be automated via the API webservices available with the solution.

How Unit4 Financials enables customers to execute this right:

Data security in Unit4 Financials has always been considered as a vital aspect to assure privacy. The principles that have been part of the product design so far will be further refined, based on GDPR requirements. In terms of existing functionality, Unit4 Financials already provides some strong mechanisms to prevent unwanted entry. Examples of these mechanisms are: Identity Services with two factor authentications, company access restrictions, menu access restrictions, data control restrictions, amendment logging. In addition, internal and independent external penetration tests are performed on each major release.

a. *Access control:* Access control is one of the key concepts in Unit4 Financials. It adheres to the privacy by default principles, so when setting up a system or extending it with new business functions, access levels can be defined for the roles and users that have access to it. Access control can be set at company level, menu item level, individual tabs within menu items and data level, through data control (e.g. limiting access to payroll accounts or employee elements in payroll transactions in the General Ledger).

   Note: A user, that due to his/her role, has been granted access to the "system" role (typically a system administrator) will have access to all companies, menu items and tabs. A user that has been granted access to the "super user" role will have access to all the data in the system as data control is overruled by this role.

b. *Identity:* An increasingly important requirement for users in an organization is to be able to log in with the same credentials in all applications they use, sometimes referred to as single sign-on (SSO) or federated authentication. Using the same credentials is convenient and an important security measure. Unit4 identity services (U4IDS) provides a single identity solution for the Unit4 ecosystem that allows users to have one single identity across multiple applications to provide a single sign-on experience. U4IDS integrates with

the organization's identity solution using industry standard protocols and is shared across Unit4 applications, acting as a common gateway for external authentication. U4IDS does not store any credentials locally and always relies on a trusted external identity provider for authentication.

c. *Activity logging:* To help our customers protect personal data against unauthorized access and security threats, Unit4 Financials logs the activity for each user account. System or security administrators can review the data on sign-on/ failed sign-on attempts.

d. *Amendment logging:* Amendment logging keeps track of any changes or additions to (business) data by users. Users with auditor type of role can run reports to view data changes any individual made in the system within a certain time period.

4.5 Privacy by design/ default

What it means:

Privacy by design: The Data Controller must consider the principles and obligations as laid down in the GDPR (such as data minimization and pseudonymizing) as from the early stage of designing the processing activities.

Privacy by default: The Data Controller also has to implement appropriate measures to ensure that, by default, only personal data that are necessary for each specific processing purpose are processed.

Privacy by design focuses on embedding privacy protection measures throughout the development process of products, processes, or services that could use personal data. While privacy by design has long been considered a best practice, it will be mandatory under the GDPR.

Unit4 R&D recognizes the importance of privacy by design and by default approaches in minimizing privacy risk and building trust. Therefore, Unit4 R&D has to adhere to previous regulations and is in process of incorporating privacy by design foundational principles as part of the software development lifecycle. We aim to enhance and strength our principles. More about the privacy by design and Unit4 approach can be found in the privacy by design whitepaper.

4.6 Breach Notification

What it means:

The GDPR introduces a reporting obligation to the data protection authority in the event of a data breach (similar to the obligation that is applicable in the Netherlands as of 1 January 2016). Such notification must take place within 72 hours after the Data Controller became aware of the data breach.

The Data Processor shall notify the Data Controller without undue delay after becoming aware of a personal data breach.

How has it been implemented within Unit4 Financials

Breach notification is not applicable on the product itself, but on the responsibility of the Data Controller and/or Data Processor. When Unit4 Financials is delivered as part of a cloud service by Unit4, Unit4 will act as a Data Processor, and in those cases a Data Protection Agreement (DPA) with detailed information on breach notification should be in place to highlight the joint responsibility.

Appendix 1 - Where is personal data stored?

Personal data is anything that can identify a 'natural person' and can include information such as a name, a photo, an email address (including personal work email address), bank details, posts on social networking websites, medical information or even an IP address. Personal data in Unit4 Financials is predominantly stored in the system due to the contractual agreement between employer and employee and/or customer, vendor and vice versa. The data model around personal data is for a large part predefined and its use depends on the customer's configuration. Below is an overview of the Masterfile and transactional records that cover the bulk of personal data.

Type of data	Data record or process	Data extraction options	Anonymization or deletion routine
Personal master data	User Masterfile	Can be achieved via any of the following enquiry tools: • Browse Details • Browse Transactions • Generic Browse • Browse Ledger • Account Summary • Webservices API • XL for Financials	Depending on your level of access, all fields in Element Master files and the documents in the Document Repository are editable, allowing for manual deletion or anonymization of the data. To fully forget an individual in the system a solution will be provided to meet the requirement.
	Employee Masterfile (i.e. Elements)		
	Customer/Supplier Masterfile (i.e. Elements)		
	Flexi-Field values		
Personal documents	Document Repository		
Transactional data (processed data)	GL transactions		
	Customer and supplier transactions		
	Expense transactions		
	Payroll transactions		
Logs	Workflow log	Browse Worklist	
	User access log	Session Management & Security reports	
	Change Log	Change Logging Master & Revision Browser	

In addition to personal master and transactional data, Unit4 Financials also allows its customers to create their own: flexi-fields, actions, notes, dynamic forms and rules (such as distribution rules). Based on the configuration chosen by the customer these could contain personal data. When making up the inventory on what personal data is controlled it's recommended to review the Unit4 Financials configuration that has been created, in addition to the system-defined data records and processes. It's recommended, and also an obligation of the GDPR, for customers to apply data minimization, which means actively limiting personal data collection, storage, and usage to only data that is relevant, adequate and absolutely necessary for carrying out the purpose for which the data is processed.

About Unit4

Unit4 is a leading provider of enterprise applications empowering people in service organizations. With annual revenue of close to 600M Euro and more than 4200 employees worldwide, Unit4 delivers ERP, industry-focused and best-in-class applications. Thousands of organizations from sectors including professional services, public services, not-for-profit, real estate, wholesale, financial services and education benefit from Unit4 solutions. Unit4 is in business for people.

unit4.com

Unit4
Papendorpseweg 100
3528 BJ Utrecht,
The Netherlands

T +31 88 247 17 77
E info.group@unit4.com