

UNIT4

In Business for You

UNIT4 AND THE GENERAL DATA
PROTECTION REGULATION (GDPR)



Contents

| | |
|---|-----------|
| What is the GDPR? | 4 |
| GDPR definitions | 5 |
| Requirements of the GDPR | 6 |
| Appendix 1: Unit4 statement on the GDPR | 8 |
| Appendix 2: Unit4 data breach protocol | 10 |
| Appendix 3: Privacy by design at Unit4 R&D | 11 |

What is the GDPR?

On May 25, 2018, a new European privacy regulation called the General Data Protection Regulation (GDPR) came into effect.

This regulation is directly applicable across the entire EU and EEA region. It applies to all companies which are processing personal data about individuals who live in the EU/EEA, including companies based outside the EU. It does not take citizenship or residency as a criterion to protect personal data. From this perspective, it applies to the personal data of all individuals who live in the EU, regardless of whether or not they are EU citizens. Furthermore, the GDPR also applies to: a company or entity that processes personal data in the context of the activities of one of its branches established in the EU, regardless of where the data are processed; or a company based outside the EU that offers goods / services (paid or free) or tracks the behavior of individuals in the EU.

It provides individuals living in the EU/EEA with greater control over their personal data and assurances that their information is being securely protected across Europe.

The GDPR requires companies handling personal data from the EU to undertake major operational reform.

GDPR definitions

GDPR is all about privacy and data protection. To understand the law some knowledge on the “GDPR Language” is needed. The basic definitions can be found here.

Definitions:

Personal Data: means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person.

Data Subject: is an identified or identifiable natural person to whom personal data relates.

Controller: means the natural or legal person, public authority, agency or other body which – alone or jointly with others – determines the purposes and means of the processing of personal data. Sometimes the purposes and means of processing personal data are, instead, determined by Union or Member State law. In that situation, the controller (or the specific criteria for nominating a controller) may also be provided for by Union or Member State law.

Processor: means a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.

Consent: of the data subject) means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her.

(Personal) data breach: means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.

Processing: means any operation (or set of operations) that is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

Requirements of the GDPR

The General Data Protection Regulation (GDPR) contains many requirements about collecting, storing, and using personal data, including how you:

- Identify and secure the personal data in your systems.
- Accommodate new transparency requirements.
- Detect and report personal data breaches.
- Train privacy personnel and other employees.

We recommend that you begin your journey to compliance with the GDPR by focusing on 10 key steps, as defined by the Dutch Privacy Authority.

1. Awareness.
2. Rights of data subjects.
3. Overview of processing personal information.
4. Data Protection Impact Assessment (DPIA).
5. Privacy by design & privacy by default.
6. Data Protection Officer.
7. Data breach notification.
8. Data Processing Agreements.
9. Leading Privacy Authority.
10. Consent and legal right to process personal data.

1. Awareness

Make sure the relevant people in your organization are aware of the new privacy rules. They need to estimate what the impact of the GDPR is on your current processes, services and goods and what adjustments are needed to meet the GDPR requirements. Keep in mind that implementation can require a lot of the available manpower, resources and time to get it done.

2. Rights of data subjects

Under the GDPR, data subjects have more and improved privacy rights. Therefore, ensure that they are able to exercise their privacy rights properly. Consider existing rights, such as the right to access and the right to correction and removal.

But also keep in mind other rights, such as the right to data portability. With this right, you must ensure that your data is readily available to your data subjects.

3. Overview of processing Personal information

Record your data processing. Document what personal data you process and for what purpose. Document where this information comes from, where it is stored and with whom you share it. Under the GDPR you must be able to demonstrate that your organization is in compliance with the GDPR.

You may also need the overview, if data subjects execute their privacy rights. If they ask you to correct or delete their information, you must pass the request on to the organization(s) with which you shared their data.

4. Data Protection Impact Assessment (DPIA)

This is the process to describe the processing and assess privacy risks and determining countermeasures. A (D)PIA is only required when the processing is “likely to result in a high risk to the rights and freedoms of natural persons” (for example in the case of profiling, special personal data, camera surveillance, control employees, etc.).

5. Privacy by Design and privacy by Default

- **Privacy by design** means that protection of personal data in the design of products and services.
- **Privacy by default** means that you must take technical and organizational measures to ensure that, by default, processing of personal data is optimized for the specific purpose and that no more than the minimal personal data is then processed, to achieve to predefined goal. Privacy by default requires that the default settings are always as privacy friendly as possible.

Unit4 R&D has translated these principles into “The 7 Foundational Pillars of Privacy by Design Incorporated into Unit4 R&D Philosophy”, which can be found [here](#).

6. Data Protection Officer

Under the GDPR, organizations may be required to appoint a Data Protection Officer (DPO). Determine whether this applies to your organization.

7. Data Breach Notification

You must document all data breaches. In case of a data breach you have to inform the leading privacy authority of this breach in a well-documented way. The leading privacy authority must be able to verify that you have complied with the reporting obligation.

Unit4 has an internal data breach protocol that can be found [here](#). However, if Unit4 is hosting your organization's personal data, be aware that you can't just rely on Unit4's internal data breach protocol.

8. Data processing Agreement (DPA)

Did you outsource your data processing to a processor? Then evaluate whether the agreed measures in existing contracts and DPA with your processor are still sufficient and meet the requirements of the GDPR. If not, please make timely changes.

Unit4 has a standard DPA which is GDPR compliant.

9. Leading Privacy Authority

Does your organization have offices in several EU Member States? Or does your data processing affect multiple Member States? Then you only have to do deal with one privacy authority. This is called the leading Privacy Authority. If this applies to your organization, then determine which privacy authority is the one for your organization.

For Unit4, the Dutch Privacy Organization "Autoriteit Persoonsgegevens" is the leading authority.

10. Consent and legal right to process personal data

You must be able to prove that you have a valid principle to process the personal data of a data subject. Consent of the data subject is one of the legitimate grounds for processing personal data. However, consent must be given freely and actively. In addition, the data subject must also have the option to withdraw consent.

Under the GDPR, collecting and processing personal data of individuals is only legitimate in one of the following circumstances:

- Where the individual concerned, (the 'data subject'), has unambiguously given his or her consent, after being adequately informed; or
- if data processing is needed for a contract, for example, for billing, a job application or a loan request; or
- if processing is required by a legal obligation; or
- if processing is necessary in order to protect the vital interest of the data subject, for example, processing of medical data of a victim of a car accident; or
- if processing is necessary to perform tasks of public interests or tasks carried out by government, tax authorities, the police or other public bodies; or
- if the data controller or a third party has a legitimate interest in doing so, as long as this interest does not affect the interests of the data subject, or infringe on his or her fundamental rights, in particular the right to privacy. This provision establishes the need to strike a reasonable balance between the data controllers' business interests and the privacy of data subjects.

The GDPR prohibits the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life unless one of the exception criteria is met. Does your organization process this type of personal data? Then you should gain knowledge on the exception criteria.

Appendix 1:

Unit4 statement on GDPR

Privacy (and, therefore, the GDPR) is paramount for Unit4. Unit4 has worked hard on preparing its people, products and processes to comply with the requirements under GDPR, which became effective on May 25, 2018. It goes without saying that Unit4 will comply with the obligations under the GDPR as well as with obligations that may be imposed under national legislations.

This statement highlights the main topics under the GDPR and actions taken by Unit4.

Privacy by Design

Within the R&D processes for the various products of Unit4 an audit is conducted, together with an external auditing party, to determine the steps to be taken in order to implement the Privacy by Design concept in the development cycle.

The recommendations of the audit will be used as the baseline for development of new products and releases that are scheduled from May 25, 2018 onwards. In this process, the concept of Privacy by default will be considered as well. For other functions, like Support, Professional Service and Cloud Services, a review is undertaken to determine to what extent the Privacy by Design concept will impact and which measure must be put in place.

An overview of “Privacy by design at Unit4 R&D” can be found [here](#).

Data Processing Agreements

At this moment, Unit4 is already processing personal data on behalf of its customers. This processing is done – in most cases – based on a Data Processing Agreement. Unit4 has reviewed and made compliant its Data Processing Agreements with the new requirements under the GDPR, like (without limitation) the obligation of confidentiality for employees, a description of technical and organizational measures for data security, and the accountability and audit requirements. That implementation can require a lot of the available manpower, resources and time to get it done.

Processing Register

Unit4 will register all processing activities and document it in accordance with the GDPR requirements. The design and organization of the register will be handled by Unit4’s internal IT department and R&D Department.

Intra-group Data Processing Agreements

All Unit4 entities have signed up to an agreement relating to the intra-group transfer/processing of personal data (Agreement) in accordance with the European General Data Protection Regulations (GDPR). The entities of the same group of undertakings of Unit4 provide various services for each other. The Agreement stipulates the processing of Personal Data by the processor on behalf of the data controller. Each entity can be a data controller as well as data processor. The Agreement has been signed by the duly authorized representatives of all the Unit4 entities.

Data Security Requirements

Unit4 has made the necessary technical and organizational changes (if and where needed since it was already compliant with the requirements under the Dutch law which were very similar) to be compliant with the data security requirements of the GDPR.

Data Breaches

The obligations for Unit4 to report data breaches to the Responsible Authority for the processing will be adhered to, within the 72-hour time frame provided in the GDPR. Unit4 has an internal protocol in case of data breaches, which has been updated for GDPR compliance.

Data Protection Impact Assessment (“DPIA”)

Unit4 will perform a DPIA in case there is a probability for a high risk for the processing of personal data and will make DPIA an integral part of its processes where necessary.

Data Protection Officer

Unit4 has appointed a Global Data Protection Officer (Global DPO) - René Bentvelzen, Telephone number: +31882471777, email address: dpo@unit4.com. It is possible that Unit4 has also appointed a local DPO depending on the local needs in each Member State of the EU.

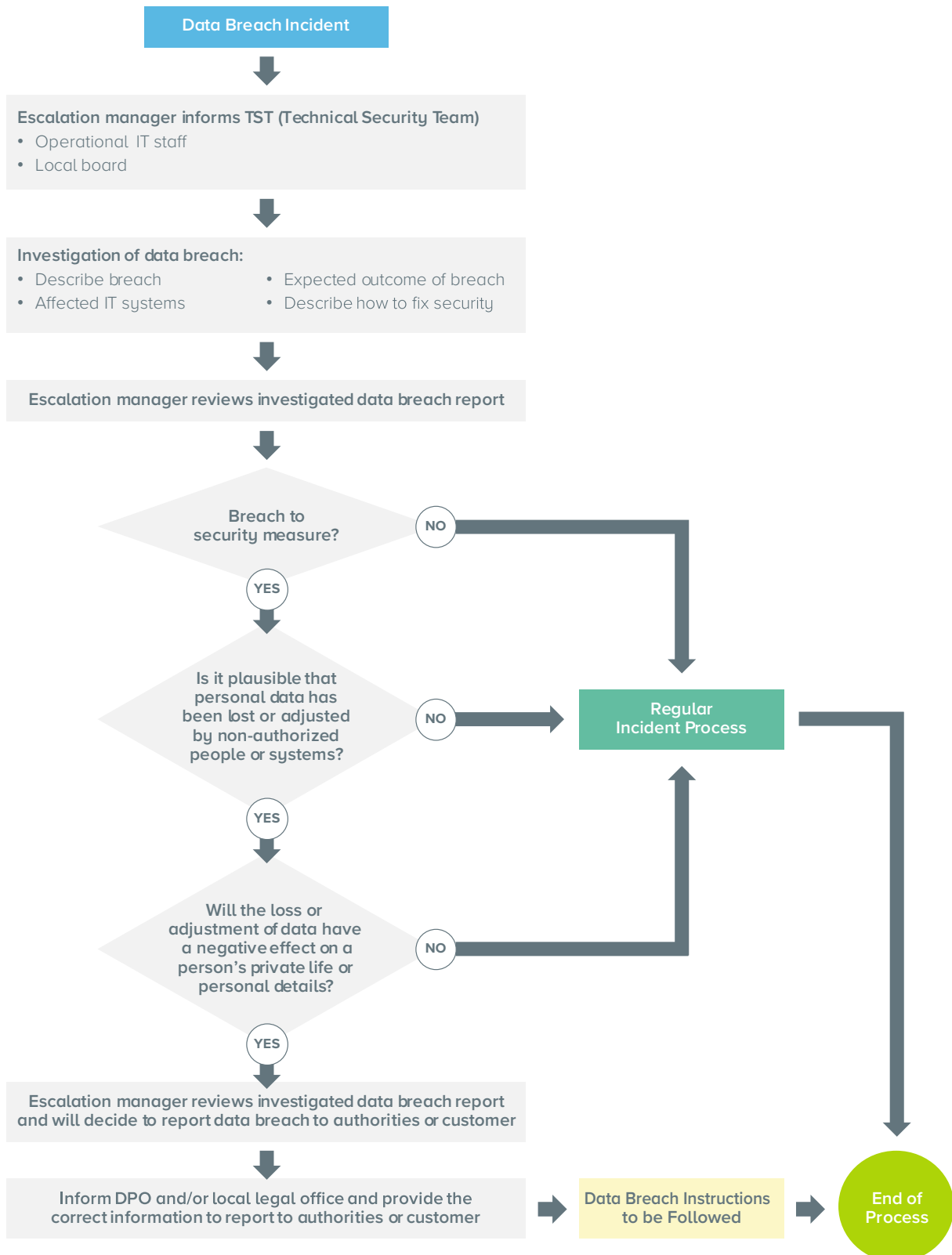
Audits and accreditations

Unit4 is assessing if and which audits and accreditations would be required for the services it provides and that may be affected by the GDPR. The accreditation may differ per product, service or country where it is offered to the public.



Appendix 2:

Unit4 data breach protocol



Appendix 3:

Privacy by design at Unit4 R&D

Background

The General Data Protection Regulation (GDPR) is aiming to harmonize the privacy and data protection legislation across the EU. The GDPR addresses data protection by design as a legal obligation for data controllers and processors; and introduces the obligation of data protection by default.

Privacy by design focuses on embedding privacy protection measures in products and 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, and is mandatory under GDPR.

Unit4 R&D Approach

Unit4 R&D believes the goals are best accomplished as part of an overall approach to protect privacy. One of the actions to achieve that is the assessment performed on yearly basis to identify/verify the product risk considering several aspects. One of the categories used to define the product risk index refers to the required levels of **confidentiality** and **integrity** for the data stored by the application.

Unit4 R&D recognizes the importance of privacy by design and by default approaches in minimizing privacy risk and building trust. Unit4 R&D adheres to previous privacy regulations and is in the process of incorporating privacy by design foundational principles as part of the software development lifecycle (SDLC). Our aim is to enhance and strengthen our built-in principles.

The 7 foundational pillars of privacy by design incorporated into Unit4 R&D philosophy

1st Pillar – Proactive and preventive

Our approach makes people, process and technologies primary agents to implement and enhance privacy protections. To provide privacy built into our products, Unit4 R&D is committed to provide training to its staff. Data protection, privacy by design and application security are part of the ongoing training curriculum.

2nd Pillar – Privacy by default

Privacy by default refers to implement mechanisms to ensure that only personal information needed for each specific purpose are processed “by default”.

It is a design concept, broadly defined, to prohibit the collection, display or sharing of any personal data without the explicit consent from the data subject. In a more detailed view, includes the most restrictive privacy settings by default. In other words, even if the user does nothing; privacy remains intact.

This concept is part of our standard requirements for new features and products. Our policy is to allow more control over privacy rather than less. Customers have the possibility to configure Unit4 products to meet their internal requirements.

Our privacy and cookie policies comply with GDPR requirements.

3rd Pillar – Embedded into design

Development guidelines and procedures about privacy by design are available in our internal technical knowledge base that is devoted to all Unit4 products.

Unit4 R&D works towards privacy embedded into the design, architecture and functionality from the very beginning.

Privacy becomes an integrated part of the system and not at the expense of less functionality.

4th Pillar – Full functionality

At Unit4 R&D, all efforts are made to assure privacy, security and functionality are implemented in our products. We are in the process of implementing the culture of the positive-sum concept, which means that there is no prevalent concept. Privacy should be considered at an early stage and throughout the software development lifecycle.

5th Pillar – End-to-end security

Our approach considers security a vital aspect to assure privacy. Unit4 R&D develops security guidelines, implements the security standard and trains the staff based on security frameworks from OWASP, as part of the software development lifecycle.

Unit4 has a Security Community with representatives from each product and other related areas. We have a Global Penetration Testing Program that ensures that security tests are performed on each major release of relevant products – based on risk and lifecycle – by an external and independent vendor. The purpose is to uncover and actively exploit vulnerabilities to prove or disprove real-world attack vectors.

6th Pillar – Visibility and transparency

Unit4 R&D provides our customers visibility and transparency by conducting and making available independent third-party audits and certifications.

We are providing our customers full transparency and visibility by producing documentation of the released functionality. If any 3rd party components that are handling private data are used, these will be specified in a data processor agreement.

7th Pillar – Respect for user privacy

Unit4 R&D is tying up privacy by design and by default to its core software development values. We believe that by following a user-centric approach; the other principles will fall into place.

We want to help our customers to meet their own GDPR compliance requirements by providing highly configurable functionality.

For more information go to:

unit4.com

Copyright © Unit4 N.V.

All rights reserved. The information contained in this document is intended for general information only, as it is summary in nature and subject to change. Any third-party brand names and/or trademarks referenced are either registered or unregistered trademarks of their respective owners. WP210317INT

UNIT4
In business for people