EuroCloud
TRUSTED DIGITAL COMPETENCE PLATFORM

CLOUD PRIVACY CHECK (CPC) NETWORK
OFFICIAL PUBLICATION NO. 02

GDPR: 20 MOST RELEVANT QUESTIONS & ANSWERS

09/2017 VERSION 1.0

The Cloud Privacy Check (CPC)

LawyersforIT
Cordemeyer & Slager Advocaten

02

Irvette Tempelman
Cordemeyer & Slager / advocaten – CS Law
+31 (0)23 5340100
i.m.tempelman@cslaw.nl

Hanneke Slager
Cordemeyer & Slager / advocaten – CS Law
+31 (0)23 5340100
j.slager@cslaw.nl

EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://eurocloud.org

PUBLICATION CONTRIBUTORS

- Austria, Götzl Thiele EUROLAWYER® Rechtsanwälte
- Belgium, Time.lex
- Czech Republic, Nielsen Meinl
- Germany, Derra, Meyer & Partner
- Estonia, PwC Legal
- France, Alain Bensoussan Avocats Lexing
- Greece, Zepos & Yannopoulos
- Ireland, William Fry
- Luxembourg, Etude REDING Avocats à la Cour
- Latvia, Njord Latvia
- Malta, Malta IT Law Association
- Netherlands, Cordemeyer & Slager
- Norway, Grette
- Portugal, Abreu Advogados
- Romania, Wolf Theiss
- Slovenia, JK Group ltd.
- Slovakia, Bukovinsky & Chlipala, s.r.o.
- Spain, Miliners
- Sweden, Synch
- Switzerland, Laux Lawyers AG
- Turkey, Gün + Partners

TABLE OF CONTENTS

QUESTION #1

WHEN DOES THE GDPR APPLY TO PRIVATE ENTERPRISES? DOES IT EVEN APPLY IF MY COMPANY DOESN'T HAVE CUSTOMERS THAT ARE INDIVIDUALS?

In short, the GDPR must be observed by natural and legal persons who process personal data by automated means. In detail: The GDPR applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system (Art. 2 Para. 1 GDPR). In order to prevent creating a serious risk of circumvention, the protection of natural persons should be technologically neutral and should not depend on the techniques used (Recital 15 GDPR).

Personal data means any information relating to an identified or identifiable natural person (Art. 4 Para. 1 GDPR). It makes no difference whether the data themselves are to be additionally considered in need of protection, worthy of protection or sensitive. Data of legal persons are not protected by the GDPR. To clarify: The GDPR explicitly does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity. While these 20 Q&A deal with the private sector, it should be noted that the GDPR does not apply only to the private sector.

QUESTION #2

DOES THE GDPR ALSO APPLY TO ENCRYPTED, ANONYMISED AND PSEUDONYMISED DATA?

The GDPR also applies to pseudonymised data (Art. 4 No. 5 GDPR) as they are considered personal data as well (Recital 26 GDPR). The only type of personal data that the GDPR does not apply to are anonymised data (Art. 2 Para. 1, Recital 26 GDPR). Whether encrypted data are anonymised or have merely undergone pseudonymisation cannot be answered unequivocally for all data, as the answer depends on the specific form of encryption used, as well as on whether there is a decryption key and who possesses it.

Nevertheless, pseudonymisation and encryption are considered and encouraged as means of mitigating the risks of processing where appropriate (Recital 83, Art 6 Para 4 Subpara e, Art 32 Para 1 Subpara a, Art 34 Para 3 Subpara a GDPR).

QUESTION #3

DOES THE GDPR ALSO APPLY TO MY BACKUP AND/OR ARCHIVED DATA?

The GDPR also applies to backup and archived data. The regulation stipulates no exceptions from its area of application regarding archived or backup data.

QUESTION #4

WHAT IS THE GEOGRAPHICAL COVERAGE OF THE GDPR? WHAT ABOUT NON-EU STATES? WHAT ABOUT THE USA?

The GDPR must be observed by private enterprises (cf. Answer 1) if they process personal data in an automated fashion within the EU. Specifically, the regulation must be observed if the processing takes place within the context of the activities of an establishment of a controller or processor within the EU, regardless of whether the processing takes place in the EU or not (Art. 3, Para. 1 GDPR). The GDPR applies to the processing of personal data of data subjects within the EU by a controller or processor not established in the EU only if the processing activities are related to:

a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
b) the monitoring of the behaviour of data subjects as far as their behaviour takes place within the Union (Art. 3 Para. 2 GDPR). Although the GDPR only mentions EU Member States, the EEA countries that are not EU Member States are obligated to apply the GDPR as a condition for being part of the EEA.

QUESTION #5

WHAT ARE THE NEW PRINCIPLES CREATED BY THE GDPR? WHAT ARE THE KEY DIFFERENCES BETWEEN THE GDPR AND DIRECTIVE 95/46/EC?

The GDPR does not abrogate current principles of personal data processing. In particular, the GDPR maintains the four elementary principles of Directive 95/46/EC:

1. Prohibition unless consent is obtained or processing is based on another legal ground (""Processing shall be lawful only if and to the extent that at least one of the following applies …"") (Art. 6 Para. 1 GDPR). This states a general prohibition unless authorised.
2. Purpose limitation (Art. 6 Para. 4, Art. 5 Para. 1 Subpara. b GDPR);
3. Transparency (Art. 13 & 14 GDPR);
4. Rights of data subjects (Art. 15 ff. GDPR).

Compared to Directive 95/46/EC, the GDPR does stipulate more obligations for data controllers and data processors in regard to their documentation of fulfilment of the GDPR requirements by organisational measures, as well as changes in the territorial scope of EU privacy regulation. In particular: territorial scope (Art. 3 GDPR), accountability (Art. 5 Para. 2 GDPR), obligations for controllers relating to the rights of data subjects (Art. 12 GDPR), obligation for organisation of the controller (Art. 24 GDPR), data protection by design and by default (Art. 25 GDPR) (combined with ""data minimisation"" (Art. 5 Para. 1 Subpara c GDPR)), data breach notification (Artt. 33 & 34 GDPR), data protection impact assessment (Art. 35 GDPR), consultation of controlling authorities (Art. 36 GDPR) and, within a defined scope, the data protection officer (Artt. 37 ff. GDPR), administrative sanctions (Art. 83 GDPR) as well as joint liability of controller and processor under the requirements of Art. 82 GDPR. This means that the fundamental new aspect is the principle of comprehensive obligations for documentation and organisation of the observance of data security at the controller (enterprise).

QUESTION #6

WHAT ARE THE ESSENTIAL NEW REGULATIONS ON DATA SECURITY UNDER THE GDPR?

The GDPR emphasizes the obligation to safeguard personal data. Under the GDPR, data security is still a substantial element of privacy and data protection. In comparison to Directive 95/46/EC, the regulations on data security are redesigned in the GDPR so that more and new aspects must be considered for defining adequate measures for data security.

Under the GDPR, the performance of appropriate documentation becomes an element of the evaluation whether data may be processed. In the course of a data protection impact assessment in particular, the provision of adequate data protection must be evaluated and documented (Art. 35 GDPR).

QUESTION #7

WHAT ARE THE NEW OBLIGATIONS CONCERNING INFORMATION TO BE PROVIDED TO DATA SUBJECTS?

Transparency obligations relating to the data subject have been significantly expanded by the GDPR. The controller is obligated to provide the data subject with certain legally defined information in a multi-level process (Artt. 13 & 14 GDPR). In particular, this information must include the purpose of processing, the legal basis for processing, and the company's internal regulations regarding deletion of the data.

The GDPR stipulates the obligation to inform the data subjects of their right to withdraw consent (Art. 7 GDPR) and their right to object (Art. 21 GDPR) to data processing. Furthermore, the GDPR stipulates an obligation to notify the data subject of personal data breach incidents under certain circumstances (Art. 34 GDPR).

QUESTION #8

DOES THE GDPR CONFER NEW RIGHTS TO DATA SUBJECTS?

Fundamentally new are the right to erasure ('right to be forgotten', Art. 17 Para. 2 GDPR) and the right to data portability (Art. 20 GDPR). According to Art. 17 Para. 2 GDPR, the data subject has the right (if no exceptions apply) to demand from the controller the erasure of personal data concerning him or her, including data at any third party to which the controller has transmitted the data.

This regulation differs from the 'right to be forgotten' established by the EU Court of Justice, which is ultimately a normal request for deletion. Under Art. 20 GDPR, the data subject has the right to have his or her personal data transmitted directly from one controller to another where this is technically feasible, except under certain circumstances.

QUESTION #9

DOES THE GDPR REQUIRE CONSENT BY THE DATA SUBJECT FOR ANY AND ALL DATA PROCESSING?

No. According to the GDPR, the lawfulness of data processing can result from a legal permissibility regulation (cf. Art. 6 Para. 1 Subpara b to f GDPR) like performance of a contract (Art. 6 Para 1 Subpara b GDPR) or from consent given by the data subject (Art. 6 Para. 1 Subpara a GDPR).

However, the special regulations in Artt. 9 & 10 GDPR stipulate more restrictive requirements for the processing of special categories of personal data (Art. 9 GDPR) and the processing of personal data relating to criminal convictions and offences (Art. 10 GDPR).

QUESTION #10

WHAT ARE THE MAIN DIFFERENCES IN REGARD TO OBTAINING CONSENT COMPARED TO DIRECTIVE 95/46/EC?

The main differences concerning the obtainment of consent compared to Directive 95/46/EC are threefold:

1. Transparency for the data subject is emphasized more heavily (cf. Art. 4 No. 11 GDPR);
2. The data subject must be informed about his or her right to withdraw consent (cf. Art. 7 Para. 3 GDPR);
3. Special conditions apply to consent given by children relating to online services (cf. Art. 8 GDPR). Furthermore, there is doubt whether implied consent is sufficient under the GDPR. If there are multiple purposes for the processing, consent should be obtained for all of them.

QUESTION #11

IS IT NECESSARY TO OBTAIN CONSENT ANEW UNDER THE GDPR (I.E. TO "RENEW" CONSENT)?

Consent to data processing does not need to be re-obtained if the previously given consent conforms to the requirements of the GDPR (Recital 171 GDPR). This cannot be decided in the abstract and for all situations, but must instead be evaluated for each individual case.

QUESTION #12

WHAT ARE THE "RECORDS OF PROCESSING ACTIVITIES"? DO I NEED TO KEEP THESE RECORDS AND WILL MY DATA PROCESSOR HELP ME IN DOING SO? HOW CAN A CLOUD SERVICE PROVIDER CONTRIBUTE TO MAINTAINING RECORDS OF THE PERSONAL DATA THAT IT PROCESSES?

The so-called records of processing activities are a register of all processing activities by the data controller (Art. 30 Para 1 GDPR) as well as the data processor (Art. 30 Para. 2 GDPR). Their purpose is to make the controller and processor aware of their processing activities and to simplify control of these activities by the supervisory authority. The records must contain specific information defined by the GDPR for each processing activity (cf. Art. 30 Para. 1 & 2 GDPR). Art. 30 Para. 5 GDPR exempts SME from this obligation under certain conditions; in practice, however, it is doubtful whether the range of application of this exemption will be very significant.

The processor is obligated to maintain a special separate register concerning his processing activities (Art. 30 Para. 2 GDPR), and must support the controller in the keeping of the controller's records (Art. 28 GDPR). It should also be noted that regardless of the abovementioned exception, records of processing activities will effectively need to be compiled frequently to be able to carry out a data protection impact analysis.

QUESTION #13

WHAT ARE THE REPORTING OBLIGATIONS IN THE EVENT OF BREACHES OF DATA PROTECTION? DO I HAVE TO INFORM THE DATA PROTECTION AUTHORITY? CAN I BE FACED WITH A PENALTY OF UP TO 20 MILLION EUROS?

Every controller is obligated to notify the competent supervisory authority of a "personal data breach" within 72 hours of becoming aware of the breach (Art. 33 Para. 1 GDPR). According to Art. 33, the breach must only be reported when there is a "risk" to the rights and freedoms of natural persons. However, it is not yet certain at what (low) level the data protection authorities will consider this requirement ("risk") to be met. Under the requirements of Art. 34 GDPR (in particular: a "high risk" to the rights and freedoms of natural persons), every controller is also obligated to notify the affected data subject.

According to Art. 4 No. 12 GDPR, a "personal data breach" means a breach of security leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed. If the 72-hour deadline cannot be met, the notification must include a justification for the delay. If the data controller does not report an incident, the data controller must be able to justify why the incident was not reported. A data processor must notify the respective controller, not the supervisory authority, of a personal data breach. Any violation of the obligation to report is punishable with fines up to 10 million Euros or 2 % of the respective company's worldwide revenue for the previous fiscal year (Art. 83 GDPR).

QUESTION #14

WHO IS RESPONSIBLE UNDER THE GDPR FOR MAKING A NOTIFICATION IN THE EVENT OF A BREACH OF DATA SECURITY: THE DATA CONTROLLER OR THE DATA PROCESSOR?

The data controller is obligated to notify the supervisory authority as well as the affected persons according to Artt. 33 & 34 GDPR. The data processor is obligated to notify the data controller of any incidents. Each entity is liable for compliance with its reporting obligations. Liability for the underlying incident depends on the type of incident.

QUESTION #15

DOES EVERY COMPANY NEED A DATA PROTECTION OFFICER (DPO)? WHEN MUST A DPO BE DESIGNATED? AM I ALLOWED TO APPOINT AN EXTERNAL DPO INSTEAD OF AN INTERNAL DPO?

The data controller and the data processor must designate a data protection officer in any case if:

a) the processing is carried out by a public authority or body, except for courts acting in their judicial capacity;
b) the core activities of the controller or the processor consist of processing operations which, by virtue of their nature, their scope and/or their purposes, require regular and systematic monitoring of data subjects on a large scale; or
c) the core activities of the controller or the processor consist of processing on a large scale of special categories of data pursuant to Article 9 GDPR and personal data relating to criminal convictions and offences referred to in Article 10 GDPR.

(Art. 37 Para. 1 GDPR)
National legislations have the right to define further circumstances in which a data protection officer must be designated below the abovementioned thresholds (e.g. BDSG-neu in Germany). The data protection officer may be a staff member of the controller or processor or fulfil the tasks on the basis of a service contract (Art. 37 Para. 6 GDPR), provided that the DPO fulfils the requirements set forth in the GDPR and is capable of handling his or her tasks without any conflict of interests. Not every enterprise is required to designate a separate data protection officer. For example, a group of companies may designate a joint data protection officer. Associations and organizations of which the controller or processor is a member may also designate a data protection officer.

QUESTION #16

IS THERE AN OBLIGATION UNDER THE GDPR FOR CERTIFICATION DEMONSTRATING COMPLIANCE?

Certifications are not mandatory under the GDPR but may be established (Artt. 42 & 43 GDPR). Moreover, certification mechanisms are to be encouraged according to the GDPR.

Appropriate certifications should serve to simplify verification of compliance with the respective requirements of the GDPR relating to the object of certification. However, an issued certification cannot protect a company from the stipulated sanctions.

QUESTION #17

WHAT IS A DATA PROTECTION IMPACT ASSESSMENT (DPIA) AND WHEN DOES IT NEED TO BE PERFORMED?

A data protection impact assessment (DPIA) serves to estimate risks regarding the protection of personal data. It shall be carried out if a type of processing, in particular using new technologies and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons (Art. 35 Para. 1 GDPR).

This evaluation and the execution of a DPIA are a complex process for which several different models are currently being developed. The DPIA is a fundamental instrument of data protection under the GDPR and should not be disregarded. As an example, a DPIA should be carried out in the case of processing on a large scale of special categories of data referred to in Art. 9 Para 1 GDPR (cf. Art. 35 Para. 3 GDPR).

QUESTION #18

WHO IS LIABLE IN CASE OF VIOLATIONS OF THE GDPR?

In principle, everyone is liable for their own actions. This includes data controllers as well as data processors. The GDPR explicitly stipulates the data processor's direct liability to the data subject for data infringements (Art. 79 Para. 2 GDPR). But the GDPR even goes one step further by stipulating that data controller and data processor are jointly and severally liable for any incidents (Art. 82 Para. 4 GDPR). Although the GDPR includes some restrictions concerning liability of the data processor (Art. 82 Para. 4 GDPR), this means that data processors in particular are subject to increased risk, since they are not privileged or even free of liability even though they do not control the processing of data and act under the authority of the controller.

The liability regulation is directly applicable only to claims by the data subject under civil law. The data processor is only liable for damage suffered by a natural person as a result of processing if the data processor has not complied with obligations of the GDPR specifically directed at processors, or where the data processor has acted outside or contrary to lawful instructions by the data controller (Art. 82 No. 2 GDPR).

QUESTION #19

WHAT IS THE DEADLINE FOR ENSURING GDPR COMPLIANCE? DO THE FINES STIPULATED IN THE GDPR APPLY IMMEDIATELY STARTING ON 25 MAY 2018? MY BUSINESS OPERATES IN SEVERAL EU MEMBER STATES; WHO IS MY COMPETENT SUPERVISORY AUTHORITY?

The GDPR will be directly applicable in all EU Member States starting on 25 May 2018 (Art. 99 GDPR). This also applies to the stipulated sanctions. The GDPR considers the time between its entrance into force on 25 May 2016 and the beginning of its application on 25 May 2018 as a transition period for adaptation to its regulations (Recital 171 GDPR). There is no protection of status quo and no further transition or grace period after 25 May 2018.

This means that 24 May 2018, 12.00 pm is the definitive deadline for implementation of the regulations. The competent supervisory authority is the supervisory authority of the main establishment or single establishment of the controller or processor (Art. 56 Para. 1 GDPR). Nevertheless, it remains to be seen how the data protection authorities across the EU will begin enforcing the GDPR. The German Data Protection Authority has made it clear that there will be no additional transition or grace period. Nevertheless, sanctions require at least negligence, and there will thus remain some leeway to fulfil the obligations of the GDPR in detail.

QUESTION #20

DOES THE GDPR ALLOW THE PARLIAMENTS OF MEMBER STATES TO PASS LAWS REFINING OR LIMITING THE REGULATIONS OF THE GDPR? WILL THERE STILL BE DIFFERENT NATIONAL LAWS REGULATING DATA PROTECTION?

As an EU Regulation, the GDPR is binding and directly applicable within all EU Member States (Art. 99 GDPR). Deviating national regulations are only permitted in areas specified in the GDPR and in the scope provided by the GDPR. In particular, the Member States have some scope of discretion to impose national legislation (see Art. 88 in regard to the processing of personal data in the employment context.

Nevertheless, any national legislation exceeding these restrictions will not be valid as it is supplanted by the GDPR.

WHAT IS THE DPC/CPC PROJECT?

53 lawyers from 33 countries are contributing to the project "Data Privacy Compliance (DPC)/Cloud Privacy Check (CPC)" in 26 different languages.

Understanding the complexity of current European data protection laws and regulations is already difficult enough for an IT engineer, buyer, or business user. In combination with the often small but nevertheless significant differences between various EU member states, however, it can become an almost insurmountable challenge without proper juristic accompaniment from the very start.

Unfortunately, here in Europe it is not only our many different languages that make things difficult for us: Cloud service providers and users alike are faced with major obstacles in regard to data protection, causing us to suffer massive and unacceptable competitive disadvantages in comparison with, for example, the USA. It is a reality that the many different European data protection rules act as a significant hurdle to IT service (and cloud) customers as well as providers.

The Cloud Privacy Check (CPC) is intended to simplify certain decisions and processes for most affected persons. Naturally, it cannot replace legal expertise, but it structures and breaks own a complex topic without withholding any vital information. And the Data Privacy Check (DPC) provides highly relevant legal information for 33 countries that can easily be compared with each other.

Dr. Tobias Höllwarth,
CPC Project Manager
EuroCloud Europe
tobias.hoellwarth@eurocloud.org

Jens Eckhardt
CPC 20Q&A Project Editor
Derra, Meyer & Partner
EuroCloud Deutschland_eco e.V.
eckhardt@derra-d.de

HOW DOES THE CPC WORK?

The purpose of the CPC is to determine actions from a data protection perspective on the basis of four simple tests. The CPC contains the methodology (4 steps), a short video explaining the project, a brochure and a whitepaper (all available on this website).

The CPC methodology:

- Simplification. Simplification of a complex subject matter without loss in terms of content. The goal of the CPC is to elucidate the topic of data protection in the cloud to 90 percent on a single page, thus providing a comprehensible and workable basis of information for 90 percent of the people having to deal with the topic.
- Structuring. Structuring of a plethora of questions into individual topical blocks which can then be approached step by step – from the simplest to the most complex case. Simultaneous correlation of the respectively required legal tools to be generated and evaluated in detail by jurists.
- Separation. Separation of the generally applicable from the specific. This is probably the most significant aid for managing a complex trans-border endeavour. By identifying what is the same throughout all countries, the CPC allows the user to focus on the differences – if they actually apply to him. The CPC aims to provide access to relevant information affecting another country quickly and easily, without having to deal with those aspects that are the same as “at home”.

By applying the CPC method, the legality of using a particular cloud solution can be ascertained quickly and easily, and the required legal action items can be determined.

HOW DOES THE DPC WORK?

In addition to the CPC features, the DPC web offers the possibility to understand the difference between generic data protection regulations (similar in all countries) and the country-specific differences (delta reports). This helps to quickly evaluate the requirements for being legally compliant in various countries.

The DPC has a strongly structured methodology (generic report, country report, differential report) and a uniform legal wording. This was essential once the legal framework of 33 countries was added to the DPC content.

CPC PARTNERS

- Austria, Götzl Thiele EUROLAWYER® Rechtsanwälte
- Belgium, Astrea Advocaten
- Belgium, Time.lex
- Bulgaria, Kambourov & Partners
- Czech Republic, Nielsen Meinl
- Cyprus, Tassos Papadopoulos & Associates LLC
- Germany, Derra, Meyer & Partner
- Denmark, NJORD Advokatpartnerselskab
- Estonia, PwC Legal
- Finland, Hannes Snellman Attorneys Ltd
- France, Alain Bensoussan Avocats Lexing
- Greece, Zepos & Yannopoulos
- Ireland, William Fry
- Italy, C-LEX STUDIO LEGALE
- Italy, R&P legal
- Luxembourg, Etude REDING Avocats à la Cour
- Latvia, Njord Latvia
- Monaco, Giaccardi Avocats
- Malta, Malta IT Law Association
- Republic of Macedonia, Directorate for Personal Data Protection
- Netherlands, Cordemeyer & Slager
- Norway, Grette
- Poland, Bird & Bird
- Portugal, Abreu Advogados
- Romania, Wolf Theiss
- Serbia, Ražnatović / Ognjanović & Partners
- Slovenia, JK Group ltd.
- Slovakia, Bukovinsky & Chlipala, s.r.o.
- Spain, Miliners
- Sweden, Synch
- Switzerland, Laux Lawyers AG
- Turkey, Gün + Partners
- United Kingdom, Osborne Clarke LLP
- United Kingdom, Bond Dickinson LLP

EuroCloud Europe a.s.b.l.
L1013 Luxembourg
7, Rue Alcide de Gasperi. Luxembourg

E-Mail: contact@eurocloud.org
Web: https://eurocloud.org