ACCOUNTANCY EUROPE.

GDPR: IMPLICATIONS FOR AUDITORS

Position paper

VIEWS.

AUDIT & ASSURANCE
DECEMBER 2018

HIGHLIGHTS

Statutory auditors regularly process personal data obtained from their clients. They are therefore directly impacted by the General Data Protection Regulation (GDPR) that entered into force in May 2018.

This publication aims to clarify what role auditors play under GDPR, i.e. whether they act as data controllers or as data processors. This distinction matters as the responsibilities allocated to each role are different.

We conclude that in principle, statutory auditors qualify as data controllers. For non-statutory audit services, we encourage practitioners to analyse the processing of personal data on a case-by-case basis to determine whether they will be considered data controllers or data processors. Respective role and responsibilities should be stated in the engagement letter.

NEW EU DATA PROTECTION RULES

The new General Data Protection Regulation (GDPR)[1] applies in all European Union (EU) Member States, as well as in Iceland, Norway and Liechtenstein[2], as from 25 May 2018. It lays out new rules with respect to the processing of personal data. This EU legislation may be supplemented by national legislation.

All organisations processing personal data should have reviewed and adapted their documents and procedures to ensure compliance with the new provisions.

In the course of a statutory audit, auditors regularly process personal data of or held by their clients. Therefore, they are directly impacted by the new legislation.

This publication does not constitute a legal opinion. Its purpose is to explain key concepts of GDPR, focusing on the role of statutory auditors and their main obligations stemming from the new data protection rules.[3] The implications of these new rules are still under discussion and the implementation of GDPR is work in progress in many EU Member States.

PERSONAL DATA

Personal data includes any information relating to an identified or identifiable natural person (the data subject), for example, a home address, income or a telephone number of a certain individual, even when this information is professional in nature and/or publicly available.

Data processing is any operation performed on personal data, whether or not by automated means. This includes consulting, collecting, recording, organising, storing, using, disclosing or destroying data.

Data can be processed by data controllers and data processors.

WHO ARE DATA CONTROLLERS AND DATA PROCESSORS?

For practitioners, it is important to identify what role they play under GDPR, i.e. whether they act as data controllers or as data processors. This distinction matters as the responsibilities allocated to each role are different.

DATA CONTROLLERS

DEFINITION

A data controller is a person/entity which, alone or jointly with others, determines the purposes and means of the processing of personal data. In other words, data controllers determine 'why' the data is used (the purposes) and 'how' the data is processed (the means).

RESPONSIBILITIES

- Comply with the seven key principles of data protection: (i) lawfulness, fairness and transparency, (ii) purpose limitation, (iii) data minimisation, (iv) accuracy, (v) storage limitation, (vi) integrity and confidentiality and (vii) accountability
- Where a type of processing is likely to result in a 'high risk' to the rights and freedoms of natural persons, perform a data protection impact assessment (DPIA) before processing the data

---

[1] *Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data*, available at https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679

[2] Iceland, Liechtenstein and Norway are part of the European Economic Area (EEA). GDPR is a text with EEA relevance.

[3] For more information on GDPR, refer to Accountancy Europe's publication *What do the new EU data protection rules mean for you?* (2017), available at https://www.accountancyeurope.eu/publications/new-eu-data-protection-rules-mean/

- Implement appropriate (technical and organisational) measures to ensure an appropriate level of data security
- Provide the data subjects with all necessary information about the processing of their personal data, e.g. the identity of the data controller and/or processor, how and why their personal data is processed, their rights including the right to rectification, objection, erasure, access, data portability, restriction of processing and certain rights in relation to automated decision-making (including profiling) – ideally this information is provided in a privacy policy
- Respond to any request of a data subject to exercise these rights
- Keep a record of processing activities available for the supervisory authority
- Only use data processors that provide sufficient guarantees in terms of data protection and enter into a data processing agreement with each further data processor
- Take measures leading to 'data protection by design and default'[4] and ensure that only the necessary personal data is processed
- Designate a data protection officer (DPO) (in certain cases)
- In the event of a personal data breach, in some cases, the data controller will have to report this breach to the supervisory authority within 72 hours after having become aware of it and/or to the individuals concerned
- Cooperate with the supervisory authority in the performance of its tasks

DATA PROCESSORS

DEFINITION

A data processor is a person/entity which processes personal data on behalf of data controllers. Data processors cannot decide themselves how to use the data but follow instructions of data controllers.

RESPONSIBILITIES

- Only act on documented instructions of the data controller, unless required to do so by EU/Member State law, and enter into a data processing agreement with each controller
- Implement appropriate (technical and organisational) measures to ensure an appropriate level of data security
- Obtain prior authorisation of the data controller when a sub-processor is appointed
- Keep a record of processing activities carried out for data controllers
- Designate a data protection officer (DPO) (in certain cases)
- Notify the data controller of any personal data breach without undue delay
- Cooperate with the supervisory authority in the performance of its tasks

WHAT HAPPENS IN CASE OF NON-COMPLIANCE?

Certain infringements of data protection legislation can result in fines up to EUR 20 million or 4% of the total worldwide annual turnover of the preceding financial year, whichever is higher. Less severe infringements face fines up to EUR 10 million or 2% of the total worldwide annual turnover of the preceding financial year.

Supervisory authorities can also carry out investigations and impose binding orders and corrective measures, such as stopping certain data processing activities, deleting certain data, making a public announcement, etc. In the majority of the EU Member States, GDPR will probably lead to a significant increase in the potential sanctions for infringements of data protection legislation.

[4] For more information and guidance see ENISA, *Privacy by design*, available at https://www.enisa.europa.eu/topics/data-protection/privacy-by-design

Non-compliance can also lead to complaints and damages claims from individuals. In addition to the above-mentioned data subject rights, GDPR provides data subjects with the right to lodge a complaint with a supervisory authority, the right to obtain an effective judicial remedy against a controller or a processor and to receive a compensation from the controller or processor for the damage suffered. Some national laws allow class actions to claim compensation.

STATEMENT ON THE ROLE OF AUDITORS UNDER GDPR

Based on thorough discussions, including discussions with national supervisory authorities, the European accountancy profession has come to the view outlined below on the auditors' role under GDPR. We draw your attention to the fact that it does not constitute a legal opinion and that the implications of these new rules are still being debated in certain Member States.

STATUTORY AUDITORS ARE DATA CONTROLLERS

Accountancy Europe believes that in principle, auditors qualify as data controllers in their own right.

Statutory audit legislation obliges auditors to be independent [of their audit clients] and for this reason, auditors are the ones that decide what data they need to perform the audit and how the data is used, stored, etc. Additionally, the auditor and client do not jointly determine the purposes and means of the processing, the purposes being determined by law and regulations. Therefore, auditors in the framework of statutory audit should be considered data controllers.

As a consequence, auditors should not enter into a data processing agreement with their audit clients, but are obliged to set up a privacy policy and notify their clients by including a data protection clause in the engagement letter. This privacy policy should clarify their role and responsibilities as data controllers in their own right (see above).

CAN ACCOUNTANCY FIRMS QUALIFY AS DATA PROCESSORS?

When performing an activity other than statutory audit, practitioners should base their decision as to their role of a data processor or a data controller on a careful case-by-case analysis of the service provided to the client. The question to ask is whether they as service providers have any control over the purposes and the means of the processing, for example:

- where a practitioner provides a service on the basis of very general instructions (e.g. tax return preparation), then the practitioner will be considered a data controller
- where a practitioner is subject to detailed instructions from the client as to what, why and how personal data is processed (e.g. detailed agreed-upon procedures), then the practitioner may be considered a data processor because of the consequent limited scope for discretion

As mentioned above, accountancy firms may act as data processors when dealing with personal data as part of work not linked to statutory audit, but for which they are only acting on behalf and under detailed instructions of the data controller. In such cases, it is the client who controls the use of the data, i.e. determines 'why' and 'how' the data is processed.

The above is, however, subject to one major caveat: whenever practitioners detect a malpractice which they are obliged to keep record of, then, because of their professional obligations, they will always be acting independently as a data controller for this specific purpose.

Where practitioners are acting as data processors, they are required to enter into a data processing agreement with their clients, which must comply with the strict requirements of article 28 of GDPR.

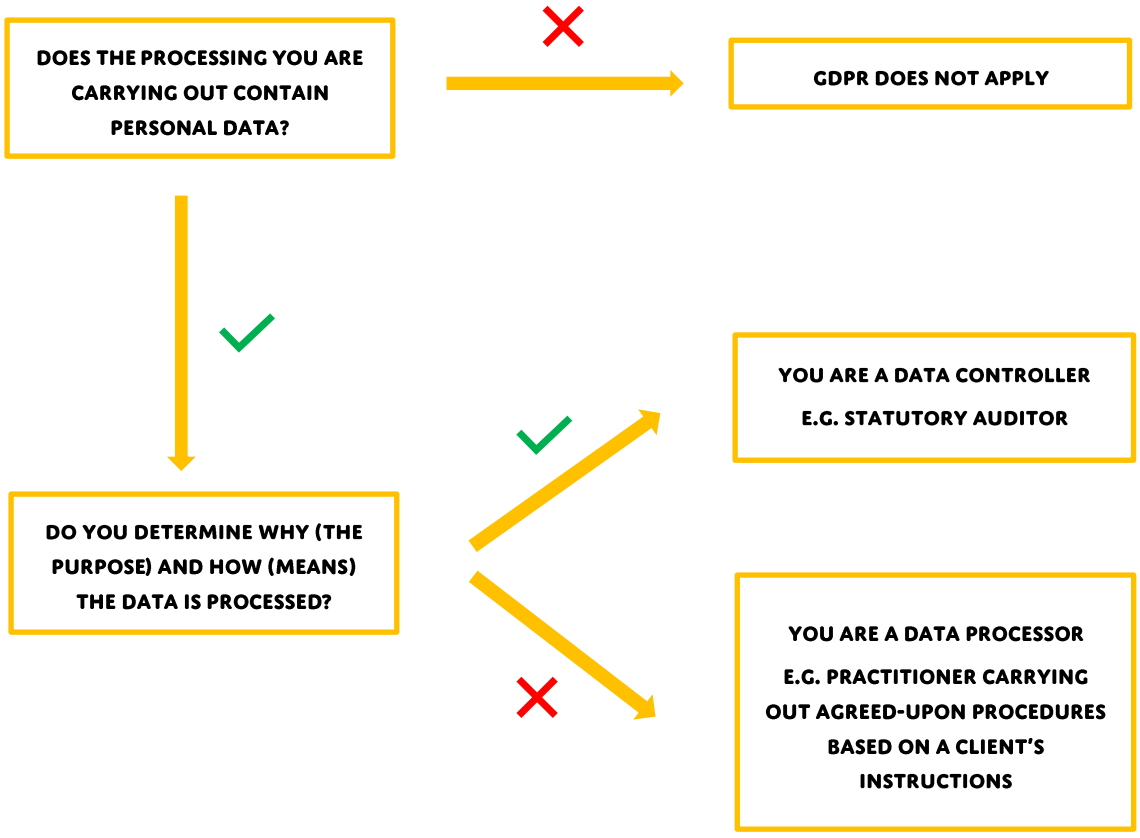
CONCLUSION

Statutory auditors decide how they process data obtained from their audit clients and are therefore considered data controllers in their own right under GDPR.

For non-statutory audit work, we encourage practitioners to analyse the processing of personal data on a case-by-case basis to determine whether they will be considered data controllers or data processors.

Respective role and responsibilities should be stated in the engagement letter.

GDPR: ARE YOU A DATA CONTROLLER OR A DATA PROCESSOR?



Avenue d'Auderghem 22-28, 1040 Brussels

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 51 professional organisations from 37 countries that represent close to **1 million** professional accountants, auditors and advisors. They make numbers work for people. Accountancy Europe translates their daily experience to inform the public policy debate in Europe and beyond.

Accountancy Europe is in the EU Transparency Register (No 4713568401-18)