GDPR Guidelines for Chartered Accountants, Tax Advisers and Payroll Professionals

regarding their status as 'controller' or 'processor' as referred to in the General Data Protection Regulation (GDPR) and the GDPR Implementation Act for the provision of services to clients

1 October 2019

Netherlands Institute of Chartered Accountants (NBA)
Dutch Association of Auditors and Auditing Firms (Novak)
Dutch Association of Tax Advisers (NOB)
Dutch Register of Tax Advisors (RB)
Dutch Institute of Register Payroll Accounting (NIRPA)

Contents

1 Status of the guidelines 3

2 Definitions and explanatory notes 4
2.1 Statutory framework 5
2.2 Engagements comprising more than one type of service 5
2.3 Guidance from government and supervisory authorities on the definitions of 'controller' and 'processor' 5
2.4 Conclusion 8

3 Rules governing professional ethics and conduct applicable to professional service providers 9

4 Statutory obligations applicable to professional service providers 11

5 Compilation, review and audit engagements; other assurance engagements and agreed-upon procedures 13

6 Tax advice and tax returns 15

7 Payroll processing 16

8 Administrative services 17

ANNEX 1 Overview of controllers' and processors' obligations 18

1 Status of the guidelines

These guidelines for chartered accountants ('accountants'), tax advisers and payroll professionals have been compiled by representatives of:

- NBA
- Novak
- NOB
- RB
- NIRPA

here jointly referred to as 'the professional bodies'.

In practice it can sometimes be unclear as to whether an accountant, tax adviser or payroll professional (henceforth also referred to as the 'professional service provider' or jointly as 'professional service providers', or as the 'service provider(s)') in performing services for clients is acting as a 'controller' or as a 'processor' as defined in the General Data Protection Regulation[1] (*Algemene verordening gegevensbescherming, "*GDPR"). These guidelines are intended to clarify the position. Please note that these guidelines do not address whether service providers are acting as controllers or processors in certain internal processes, such as when processing their own employees' personal data, maintaining their own client administration records or managing their own IT infrastructure.

The guidelines are based on a reasonable and practical understanding of the text of the GDPR, the GDPR Implementation Act [*Uitvoeringswet AVG*], the Guide issued by the Ministry of Justice and Security on the GDPR ('the Guide'), the Opinion issued by the Article 29 Working Party on the concepts of 'controller' and 'processor',[2] the information provided by the UK supervisory authority, the Information Commissioner's Office (ICO),[3] the position paper published by Accountancy Europe[4] and information available on the website of the Dutch Data Protection Authority (DPA). Where the regulations are unclear, these guidelines have set out to provide an interpretation that, as far as possible, reflects the essence and purport of the legislation and regulations and can be applied in practice in the Dutch context.

The DPA has been notified of the guidelines and its comments have been incorporated into the text.

The guidelines are not binding and do not discharge service providers and their clients from their responsibility to apply the regulations correctly. Consequently the professional bodies do not accept any liability for compliance with these guidelines and recommend that the relevant professionals should always consult the text of the GDPR and the official recommendations and information published by the DPA.

Any references in these guidelines using words in the masculine form to refer to service providers also include the feminine or gender-neutral forms of these words.

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council (EU) 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, and repealing Directive 95/46/EC.
[2] Opinion 1/2010 on the concepts of 'controller' and 'processor' (WP169), as approved on 16 February 2010.
[3] 'Data controllers and data processors: what the difference is and what the governance implications are', 20140506, version 1.0.
[4] 'GDPR: Implications for Auditors', Position paper, Accountancy Europe.

2 Definitions and explanatory notes

2.1 Statutory framework

The GDPR and the GDPR Implementation Act came into force in the Netherlands on 25 May 2018 in replacement of the Personal Data Protection Act [*Wet bescherming persoonsgegevens*]. The entry into force of the new legislation means that individuals whose personal data are processed now have more rights than previously, while organisations processing personal data now have more responsibilities.

Organisations that process personal data do so either in the capacity of a 'controller' or a 'processor'.

Article 4(7) GDPR defines a 'controller' as 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.' Article 4(8) of the GDPR defines a 'processor' as a 'natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller.' Parties may also be 'joint controllers' if they determine the purposes and means of processing jointly.[5]

The GDPR and the GDPR Implementation Act impose obligations on both controllers and processors. The obligations applying to controllers under the GDPR are more extensive than those applying directly to processors. You can find a summary of the applicable obligations in Annex 1.

If a controller outsources processing activities to a processor, the agreements they reach must be recorded in a contract or other legal act (often referred to as a data processing agreement).[6] As an example, the GDPR requires controllers to notify any breach of security ('a personal data breach')[7] to the relevant supervisory authority (in the Netherlands: the Dutch Data Protecting Authority, or DPA) without any unreasonable delay. Processors, by contrast, do not have a direct duty to notify such a personal data breach to the supervisory authority, but must inform the controller without undue delay as soon as they become aware of any personal data breach. Any further agreements relating to this duty of disclosure (such as the period within which a breach has to be reported and the information to be supplied) must be recorded in a data processing agreement.

Clients often assume that their service provider is acting as a processor simply because they have instructed the provider to perform a specific service. They then expect a data processing agreement to be signed as part of their contract with the provider. However, it is not always necessary for such an agreement to be signed. As the guidelines explain, service providers usually qualify as controllers rather than as processors. For each separate engagement, however, they have to assess whether they will be acting as a controller or processor. While the examples given here may provide guidance, please note that an engagement involving a hybrid or mixed form of the examples may result in the answer to the question of whether the provider is acting as a controller or processor being different from what is stated in these guidelines.

In many cases, clients themselves may also qualify as controllers. If the service provider and the client each independently qualify as a controller, both of them have to comply with the obligations imposed on controllers,[8] including establishing whether there is a legitimate interest for processing the data.[9]

If both the service provider and the client independently qualify as controllers, it is advisable to agree on how the GDPR obligations are to be met, including, for example, agreeing on procedures for reporting possible data leaks. However, these agreements will not release the service provider from the duty to perform the activities in line with the applicable professional rules and codes of conduct and any applicable statutory obligations.

---

[5] The professional bodies have not yet identified any activities performed by service providers that would involve 'joint controllers' as referred to in Article 26 GDPR. These guidelines do not, therefore, devote any further attention to 'joint controllers'.

[6] This arises from Article 28(3) GDPR.

[7] Unless the breach is unlikely to represent a risk to the rights and freedoms of natural persons.

[8] See Annex 1 for a summary of the obligations applying to controllers.

[9] Under Article 6 GDPR, data processing is lawful only if it meets at least one of the six stated conditions. The principles on which service providers usually base their data processing (depending on the type of processing) are:

- the processing is necessary for complying with a legal obligation to which the service provider is subject;
- the processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject before entering into a contract; or
- the processing is necessary for the purposes of legitimate interests pursued by the service provider or a third party, such as a client, except where such interests are overridden by interests or fundamental rights and freedoms of the data subject which require protection of personal data.

2.2 Engagements comprising more than one type of service

As service providers may perform various activities for their clients, their relationship with a client may involve them acting both as a controller and as a processor. For each type of service (including a series of services performed under one single engagement letter), providers have to establish whether they are acting as a controller or as a processor (i.e. whether they are also performing a 'processing activity'). Each service that the provider could perform as a separate engagement has to be assessed separately. All the personal data that could be processed as part of that engagement are regarded as one processing activity, for which the purposes and means of processing have to be determined.

Say, for example, a client asks a service provider to keep its books and records, to compile the annual financial statements and to prepare the VAT return. These three types of services (each of which is a separate processing activity) are recorded in a single engagement letter and are based on the same set of personal or other data supplied by the client. Whether the service provider is acting as a controller or a processor has to be determined separately for each of the three types of services (i.e. the financial administration, financial statements and VAT return). This is because each service could be provided separately. There is no need also to assess each individual action performed, using the required personal data, within the service in order to determine whether, in each case, the service provider is acting as a controller or processor.

If a service provider processes personal data as a processor, a data processing agreement will have to be signed.

2.3 Guidance from government and supervisory authorities on the definitions of 'controller' and 'processor'

Guide published by the Ministry of Justice and Security

The Guide published by the Ministry of Justice and Security in 2018 provides further clarification on the distinction between a controller and a processor.[10] It states that, in general, three situations can be distinguished when deciding which party is acting as a controller. Being a controller can derive from:

- an explicit legal power;
- an implicit power;
- factual influence exerted.

Situation 1 applies when, for example, a party providing professional services to a client has a statutory duty to disclose certain situations to a supervisory authority. See section 4 of these guidelines for more information.

Situation 2 applies when, for example, a party does not have explicit power to process personal data, but where widely applicable legal rules and standards assign responsibility as a controller processing the data to a specific natural or legal person, such as when employers process their employees' personal data.

In situation 3, being a controller depends on whether the parties can factually influence the processing of personal data, with account also being taken of aspects such as the legal relationships between parties. What matters here is who actually takes the decisions and determines what happens with the data.

Controllers regularly engage other parties to process personal data on their behalf. If a party processes personal data on behalf of a controller without being subject to the controller's direct authority, that party is regarded as a processor. The Guide explains that a party is regarded as processing personal data on behalf of a controller if the processing of personal data is that party's primary task. In other words, the services provided must be aimed at processing personal data for the controller. If processing personal data is not the primary task, but is instead the result of another service being performed, the service provider is a controller in its own right for the purposes of those processing activities. In other words, the sole fact that a party is engaged by a controller is not enough for that party to qualify as a processor. For this to be the case, the services in question must be aimed primarily at processing personal data.

[10] Section 3.5 of the Ministry of Justice and Security's Guide [*Handleiding Algemene verordening gegevensbescherming en Uitvoeringswet Algemene verordening gegevensbescherming*].

In the case, however, of the vast majority of activities performed by professional service providers, processing personal data is not the primary task. See sections 5, 6, 7 and 8 of these guidelines for more information.

Opinion issued by the Article 29 Data Protection Working Party[11]

In 2010, the Article 29 Data Protection Working Party (Article 29 WP) issued an important opinion[12] on the concepts of 'controller' and 'processor'. Although this opinion related to the meaning of these terms under Directive 95/46/EC, the considerations expressed by the Article 29 WP remain relevant with regard to the GDPR.

As far as interpreting the concepts of determining 'the purpose and means of the data processing', the Article 29 WP stated that:

> *Determination of the "purpose" of the processing is reserved to the "controller". Whoever makes this decision is therefore (de facto) controller. The determination of the "means" of processing can be delegated by the controller, as far as technical or organisational questions are concerned. Substantial questions which are essential to the core of lawfulness of processing are reserved to the controller. A person or entity who decides e.g. on how long data shall be stored or who shall have access to the data processed is acting as a "controller" concerning this part of the use of data, and therefore has to comply with all controller's obligations.*

With regard to the processor, the Article 29 WP stated that:

> *Two basic conditions for qualifying as processor are on the one hand being a separate legal entity with respect to the controller and on the other hand processing personal data on his behalf. This processing activity may be limited to a very specific task or context or may accommodate a certain degree of discretion about how to serve the controller's interests, allowing the processor to choose the most suitable technical and organizational means.*

The Article 29 WP then specified further criteria for determining the role of the various parties involved in processing data:

> *Some criteria may be helpful in determining the qualification of the various actors involved in the processing: the level of prior instruction given by the data controller; the monitoring by the data controller of the level of the service; the visibility towards data subjects; the expertise of the parties; the autonomous decision-making power left to the various parties.*

One of the relevant indicators for establishing the existence of a controller is the traditional role and professional expertise of the service provider. The Article 29 WP provides an example involving lawyers (barristers):

> *A barrister represents his/her client in court, and in relation to this mission, processes personal data related to the client's case. The legal ground for making use of the necessary information is the client's mandate. However, this mandate is not focused on processing data but on representation in court, for which activity such professions have traditionally their own legal basis. Such professions are therefore to be regarded as independent 'controllers' when processing data in the course of legally representing their clients.*

The above applies not only to lawyers, but also to service providers if their mandate is not aimed primarily at processing personal data.

[11] WP 169 - Opinion 1/2010 on the concepts of 'controller' and 'processor'.

[12] The Article 29 Working Party was established under Article 29 of Directive 95/46/EC. It is an independent European advisory body dealing with issues relating to the protection of personal data. Its tasks and responsibilities are described in Article 30 of Directive 95/46/EC and Article 15 of Directive 2002/58/EC. The Article 29 Working Party became part of the European Data Protection Board (EDPB) when the GDPR entered into force.

The Article 29 WP provides an example of work performed by accountants that is also relevant for tax advisers:

> *The qualification of accountants can vary depending on the context. Where accountants provide services to the general public and small traders on the basis of very general instructions ("Prepare my tax returns"), then - as with solicitors acting in similar circumstances and for similar reasons - the accountant will be a data controller. However, where an accountant is employed by a firm, and subject to detailed instructions from the in-house accountant, perhaps to carry out a detailed audit, then in general, if not a regular employee, he will be a processor, because of the clarity of the instructions and the consequent limited scope for discretion. However, this is subject to one major caveat, namely that where they consider that they have detected malpractice which they are obliged to report, then, because of the professional obligations they owe they are acting independently as a controller.*[13]

It follows from this that if a client engages a service provider, based on general instructions, to complete his tax return, this service provider qualifies as a controller in its own right. The second example covers situations where an accountant is engaged by a company as if he were their own employee – for example, as a member of the company's internal audit department or an accountant in business. This scenario does not apply to situations where the accountant is engaged by a company to perform assurance work required in the public interest. In those situations, the accountant obviously cannot act on instructions given by his principal because these would conflict with the fundamental principles of objectivity and independence that the accountant is required to observe. See section 5 in these guidelines for more information.

The Article 29 WP also notes in the above example that where accountants have a duty to report malpractice, they are always regarded as a controller. See section 4 of these guidelines for more information.

Guidance provided by the Information Commissioner's Office (ICO)

The UK data protection authority, the ICO, has also published guidance on 'controllers' and 'processors',[14] including information on the role of accountants and similar service providers:

> *44. A firm uses an accountant to do its books. When acting for his client, the accountant is a data controller in relation to the personal data in the accounts. This is because accountants and similar providers of professional services work under a range of professional obligations which oblige them to take responsibility for the personal data they process. For example if the accountant detects malpractice whilst doing the firm's accounts he may, depending on its nature, be required under his monitoring obligations to report the malpractice to the police or other authorities. In doing so an accountant would not be acting on the client's instructions but in accordance with its own professional obligations and therefore as a data controller in his own right.*
>
> *45. Where specialist service providers are processing data in accordance with their own professional obligations they will always be acting as the data controller and cannot agree to hand over or share data controller obligations with the client in this context.*

It follows from this that the ICO believes that service providers who perform their activities in accordance with the applicable legislation and professional standards are acting as controllers.

The ICO recently repeated this view in an interactive tool[15] that it has put on its website as part of the preparations for Brexit and in which it asks the following question:

> *Is the person sending you the data acting as a controller?*

---

[13] The professional bodies believe that the Dutch version of WP169 does not entirely correctly translate this example as included in the English version. The term 'employed by a firm', as used in the English version, has a wider meaning than the Dutch wording '*bij een bedrijf in dienst zijn*'. The Ministry of Justice and Security confirms in its Guide that if someone is in a subordinate relationship to a controller or if some other form of hierarchical relationship exists (e.g. an employee is seconded to a controller), this does not qualify as processing, but instead as 'internal management and control'.

[14] 'Data controllers and data processors: what the difference is and what the governance implications are', 20140506 Version 1.0.

[15] https://ico.org.uk/for-organisations/data-protection-and-brexit/standard-contractual-clauses-for-transfers-from-the-eea-to-the-uk-interactive-tool/.

Answer yes if the sender is a professional consultant or adviser with professional or regulatory obligations when they process personal data (e.g. a lawyer or accountant), even if they are acting for you.

2.4 Conclusion

The various guides and opinions published show that the following aspects should be considered when deciding whether a service provider is acting as a controller or as a processor when providing services to a client:

- The question of whether the engagement is primarily aimed at processing personal data or is only the result of another form of service;
- The service provider's professional expertise;
- The existence of rules governing professional ethics and conduct dictating how service providers have to perform their services; and
- Statutory obligations that require service providers to report certain situations to a supervisory authority.

3. Rules governing professional ethics and conduct applicable to professional service providers

For each separate type of service provided, professional service providers have to assess whether or not they are performing the services on behalf of and on the instructions of their clients. Indicators that point to service providers qualifying as controllers (i.e. where the providers determine the purposes and means of the data processing) include:

- Their own (or a statutory) requirement to store personal data;
- The requirement for service providers themselves to assess their use of the personal data (e.g. which data they need in order to perform the engagement);
- Monitoring the quality of the services to be provided;
- Controlling who has access to the data;
- Processing the personal data is not the primary task, but rather the result of another form of service; and
- Being subject to their own legislation and professional regulations.

The legislation and professional regulations applying to professional service providers are summarised below.

Accountants

Accountants in the Netherlands have to comply with the Regulation on the Code of Professional Ethics for Accountants [*Verordening gedrags- en beroepsregels accountants* or *VGBA*]. The *VGBA*, adopted by the NBA, stipulates, for example, that all accountants have to comply with the following fundamental principles in reflection of their responsibility to act in the public interest:

- Professionalism;
- Integrity;
- Objectivity;
- Professional expertise and the duty of care;
- Confidentiality.

Accountants have to ensure that anyone performing activities under their responsibility or whom they consult for advice or support also complies with these principles.

Acting as a processor, where the accountant would be acting on a client's instructions, would be at odds with the principle of independence. Independence is an important aspect of objectivity and is required when assurance engagements are being performed. More details on this can be found in the Regulation on Accountants' Independence [*Verordening inzake de onafhankelijkheid van accountants bij assurance-opdrachten*].[16]

When accepting or continuing any engagement, accountants have to assess whether the engagement could conceivably conflict with any of the fundamental principles. They also have to be familiar with the legislation and regulations applying to their clients and to take action if clients do not comply with those rules, as detailed in the *VGBA*, the Additional Regulations on Audit and Other Standards [*NV COS*] and the Further Regulations for Accountants' Conduct in the event of Non-Compliance with Legislation and Regulations by their own Organisation or Clients [*NV NOCLAR*].

Under the applicable disciplinary regulations, accountants can be called to account for their actions at any time during the ten years after the services were provided. This means they have to keep their files accessible for at least that period of time.

Tax advisers

Tax advisers who are members of the RB or NOB have to comply with the rules adopted by their , being the Professional Regulations of the RB and the Rules of Professional Conduct of the NOB. These rules require members to perform their work as tax advisers in an honest, conscientious and appropriate manner and to refrain from anything that is in conflict with the honour and dignity of the profession. Tax advisers must also ensure they demonstrate independence in practising their profession, including vis-à-vis their clients. These professional regulations additionally provide rules on:

[16] Independence is not a precondition for performing an 'assurance-related engagement' or 'other engagement'.

- Confidentiality;
- Professional competence;
- Services;
- Expertise.

Tax advisers who are members of the NOB can be called to account in disciplinary proceedings for any action conflicting with the applicable professional standards or for failing to act in accordance with these standards at any time in the ten years after the year of the relevant action or omission.

Tax advisers who are members of the RB can be called to account in disciplinary proceedings for any action conflicting with the applicable professional standards or for failing to act in accordance with these standards at any time in the five years after the year of the relevant action or omission.

Payroll professionals

Payroll professionals in the NIRPA's RPP (Registered Payroll Professional) or RSa (Registered Salary Administrator) register have to comply with the NIRPA code of conduct. This provides the framework within which they have to operate regarding:

- Professional conduct;
- Expertise (i.e. maintaining competencies through Continuing Professional Development and ensuring expertise both in terms of knowledge and skills);
- Integrity and confidentiality;
- Relationships between payroll professionals and those using their services.

NIRPA-certified payroll professionals found to have breached their code of conduct can be removed from the register and are then no longer allowed to use the title RPP or RSa.

4. Statutory obligations applicable to professional service providers

Professional service providers have to comply with various statutory obligations before and/or while providing services to their clients. Sometimes these obligations require them to process personal data.

Firms that employ such service providers have to structure their business activities so as to safeguard controlled and fair business operations. This means they have to avoid becoming involved in criminal activities or breaches of the law that could damage confidence in the firm or the financial markets. They also have to avoid becoming involved in any client relationship that could damage confidence in the firm or the financial markets.

In order to safeguard controlled and fair business operations, firms that employ these service providers need to know who they are doing business with. They do this by performing Client Due Diligence (CDD) to ensure they comply with the obligations in the Money Laundering and Terrorist Financing (Prevention) Act [*Wet ter voorkoming van witwassen en financieren van terrorisme* or *Wwft*]. CDD requires the firm that employs the service provider to process various categories of personal data of clients (or potential clients), including data relating to the identity of a client (where the client is a natural person), the client's representative and the ultimate beneficiary or ultimate beneficial owner (UBO). Not only do firms have to identify the client, the client's representative and the UBO, but these identities also have to be verified. Firms also have to have procedures in place to determine whether a client, a client's representative or UBO is a Politically Exposed Person (PEP).

Firms to which the *Wwft* applies have to report any unusual transactions (whether executed or intended) to the Dutch Financial Intelligence Unit (FIU). CDD enables a firm to report an unusual transaction, including identity details of the client and the UBO and, if necessary, the client's representative.

Personal data collected under the *Wwft* have to be retained for five years after the client relationship has ended. Afterwards, these data can in principle be destroyed because the processing will then no longer have any basis in law. This applies unless there are any other statutory grounds on which the firm is able or required to retain the data.

To avoid performing services for people or entities on sanctions lists, firms that employ service providers also need to screen their clients, both before and periodically during the relationship, to check that they are not on any sanctions lists. Publicly accessible sanctions lists are drawn up by the UN and EU, along with various national governments. If a client is found to be on a sanctions list, the firm must determine whether an engagement and/or the client can be accepted or whether any existing relationship has to be terminated. The firm has to ensure it does not provide any financial resources or services to such clients.

Accountants also have an obligation to report under various other regulations. If they are conducting a statutory audit engagement, for example, the Audit Firms Supervision Decree [*Besluit toezicht accountantsorganisaties or BTA*] requires them to inform the Authority for the Financial Markets (AFM) without delay of any incidents with serious consequences for their controlled and fair business operations. Under the Audit Firms Supervision Act [*Wet toezicht accountantsorganisaties or WTA*], accountants who obtain access, during the performance of a statutory audit, to information that justifies a reasonable suspicion of material fraud have to report this to the national police authorities (KLPD). Under the Financial Supervision Act [*Wet op het financieel toezicht* or *Wft]*, accountants who perform activities for entities required to be licensed, such as investment firms licensed under the *Wft*, may in certain circumstances be required to report to both the AFM and the central bank (DNB).

An example of regulations resulting in obligations for tax advisers is the obligation to report imposed on them under the Mandatory Disclosure Directive.[17] This requires any potentially aggressive tax arrangements to be reported to the tax authorities. Parties that have a Horizontal Supervision agreement with the Dutch tax authorities have an important monitoring role to play in the chain that is intended to result in correct tax returns being submitted.

The above examples are a non-exhaustive list. In the case of all the statutory obligations referred to above, the parties processing personal data do so in the capacity of controllers. With regard to complying with these statutory obligations, they cannot be regarded as operating on their clients' instructions. If, say, a service provider has to report an unusual transaction, the client cannot prevent the transaction from being disclosed. Indeed, the client is not even allowed to be informed of the actual or intended disclosure.

[17] Council Directive (EU) 2018/822 of 25 May 2018.

However, concluding that service providers qualify as controllers if they process personal data under an applicable statutory obligation is not the determining factor for deciding whether they are acting as processors or controllers when providing services to their clients. As explained in section 2.2, each type of service has to be assessed separately. A service provider may, for example, act as a processor when performing a certain service for a client, but at the same time also qualify as a controller because of being subject to a statutory obligation (such as the obligation, under the *Wwft*, to identify the client).

5. Compilation, review and audit engagements; other assurance engagements and agreed-upon procedures

As well as compilation, review and audit engagements, accountants' services can comprise other assurance engagements and agreed-upon procedures. When performing these activities, accountants have to comply with the rules governing professional ethics and conduct referred to in section 3. They are independently responsible for monitoring the quality of the services they provide and can be called to account in disciplinary proceedings.

After consulting with the DPA, the NBA provided the following explanatory information on the activities performed by accountants and whether they are then acting as controllers or processors:

Engagement	Client	Accountant
Standards 100 - 999 apply (audit of annual financial statements)	Controller	Controller
Standards 2000 - 2699 apply (review engagements)	Controller	Controller
Standards 3000 - 3850 apply (assurance engagements other than audits or reviews of historical financial information)	Controller	Controller
Standard 4400 (engagements to perform agreed-upon procedures regarding financial information)	Controller	Processor (if the service is aimed at processing personal data) or controller (if the service is not aimed at processing personal data, but is instead only the result of the service provided)
Standard 4410 (compilation engagements)	Controller	Controller
Engagements to which no standard applies and where the service is not aimed at processing personal data, such as consultancy or advisory services	Controller	Controller (providing the service is not aimed at processing personal data), but is instead only the result of the service provided)

Accountancy Europe[18] published a position paper in December 2018[19] in which it confirmed that auditors performing a statutory audit act as 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.*

[18] Accountancy Europe unites 51 professional organisations from 37 countries, together representing around one million qualified accountants, auditors and advisers.

[19] Accountancy Europe, 'GDPR: Implications for Auditors', December 2018.

With regard to other activities, Accountancy Europe states that whether the accountant is acting as a controller or a processor has to be analysed on a case-by-case basis. It gives the example of very general instructions to prepare a tax return, where the accountant is then regarded as a controller. Performing agreed-upon procedures (Standard 4400) is given as an example of an activity that is performed by a processor if the client has given detailed instructions on the personal data to be processed and on why and how these data have to be processed. This is in line with the explanation provided by the NBA in respect of Standard 4400 engagements: if the 4400 engagement is specifically aimed at processing personal data (i.e. the service is primarily aimed at processing personal data for a client), the accountant acts as a processor. If, however, the accountant determines which personal data are needed to perform the 4400 engagement (e.g. the accountant determines which data are to be included in a random check), the accountant acts as a controller.

In the case of Standard 4410 engagements (i.e. compilation engagements), the DPA has agreed with the NBA that the accountant is regarded as a controller, given that these types of engagements require the accountant to independently assess various matters (e.g. significant items) and, if the information is regarded as incomplete, inaccurate or otherwise unsatisfactory, to decide whether additional activities are required.

6. Tax advice and tax returns

Tax activities can roughly be divided into work involving the compiling and reviewing of tax returns (e.g. income tax, inheritance and gift taxes, corporate taxes, turnover tax, payroll taxes etc) and tax consultancy and advisory services. When performing these activities, tax advisers have to comply with the rules governing professional ethics and conduct referred to in section 3. They are independently responsible for monitoring the quality of the services they provide and can be called to account by a disciplinary tribunal.

The Article 29 WP Opinion stated that tax advisers compiling tax returns do so in the capacity of controllers. Clients, too, qualify as controllers. Although the clients issue generic instructions to the tax adviser to prepare their tax return, they generally engage the tax adviser precisely because the latter has the particular specialised knowledge required. Processing personal data is also not the primary aim of preparing or submitting a tax return. Instead, this processing is just the result of a different type of service provided. In short, the tax adviser determines the purpose for which and the means by which the data are processed. The same applies to engagements where the service provider is engaged to review tax returns and additional tax assessments and to prepare objections and appeals. A tax adviser can also be 'accesory to' a client's failure to comply with tax obligations[20] and so can also independently be regarded as a controller.

When giving advice, tax advisers also independently qualify as controllers because this work involves them using their specialised knowledge and the primary purpose of their engagement is not the processing of personal data. Tax advisers who provide advice determine the purpose for which and the means by which the data are processed. The GDPR does not apply to tax advice that does not involve the processing of personal data.

If, for example, a tax adviser is involved in assisting a financial institution to tTo ransfer data on US citizens under the Foreign Account Tax Compliance Act (FATCA) and the Intergovernmental Agreement between the Netherlands and the United States, the adviser qualifies as a processor if he submits data required under the FATCA to the Dutch tax authorities on his client's behalf. The same applies in the case of the Common Reporting Standard, where Dutch financial institutions are annually required to report information on their accountholders and accounts to the Dutch tax authorities. Tax advisers who report this information on behalf of their clients qualify as processors. Here, the engagement primarily focuses on the processing of personal data, and the client determines the purpose for which and the means by which the data are processed. If, however, as well as submitting personal data on the client's behalf, the tax adviser provides advice, and this advice requires him to process personal data, the tax adviser qualifies as a controller if the advice provided could also be performed as an independent, separate engagement. This is because the tax adviser is engaged for this service because of his specialised knowledge and the primary aim of this engagement is not the processing of the personal data. Here, the tax adviser qualifies as a processor when submitting the personal data to the Dutch tax authorities, but as a controller in respect of the additional advice provided.

A tax adviser advising a client on international mobility issues qualifies as a controller if this work involves him processing personal data (such as when arranging a visa for the client's employees or preparing income tax returns for employees). This work, however, is the result of another service; in other words, the service of advising the client on cross-border employment, including the consequences for the employer and employees of working abroad (e.g. immigration, social security, pensions and strategy). The primary purpose of the engagement is not the processing of personal data. When advising on international mobility, the tax adviser determines the purpose for which and the means by which the data are processed.

[20] Article 67o State Taxes Act [*Algemene wet inzake rijksbelastingen*].

7. Payroll processing

To conduct a client's payroll administration is regarded in the parliamentary history of the Dutch Personal Data Protection Act, the Ministry of Justice and Security's Guide[21] and the Opinion of the Article 29 WP as an example of activities where the client is regarded as the controller and the service provider as the processor. However, both this example and the basic presumption that the service provider always acts as a processor in such situations have to be qualified.

Essentially, there are two ways to perform a payroll processing engagement:

- 'Basic' payroll processing, where the service provider simply makes IT infrastructure (payroll software) available to the client so that the latter can prepare payroll calculations/payroll slips and/or where the data supplied by the client is simply inputted by the service provider into the payroll software without any additional checks or advice; or
- More extensive services, where not only the IT infrastructure is made available, but where the service provider also reviews the information or provides advice, such as advice on structuring the payroll administration, as well as assessing and, if necessary, correcting any data provided and checking whether the client has complied with the relevant legislation and regulations (tax regulations, collective labour agreements, pension arrangements etc.).

The latter, more extensive services are those that professional service providers are usually asked to perform. In both cases, service providers have to comply with the rules governing professional ethics and conduct referred to in section 3.

In the 'basic' payroll processing model, service providers act as processors because their processing of personal data is simply on the instructions and on behalf of the client. Here, the engagement is primarily aimed at processing personal data, and the client determines the purpose for which and the means by which the data are processed.

In the case, however, of more extensive payroll processing, service providers act as controllers. These services are comparable to a compilation engagement, where the DPA has confirmed that service providers act as controllers. When performing payroll processing engagements, service providers independently assess certain matters (e.g. whether the inputted data comply with legislation and regulations) and, where necessary, decide whether additional work is required. In this variant, service providers are engaged because of their specialised expertise, the services are not primarily aimed at processing personal data and the service providers are responsible for monitoring the quality of the services provided. In short, therefore, the service providers determine the purpose for which and the means by which the data are processed. The reviewing and advisory activities are so intertwined with the IT infrastructure (payroll software) that, as set out in section 2.2, they qualify as a type of service where the data are processed as one single activity and where the service provider acts as a controller.

If a service provider engages a subcontractor[22] to perform payroll processing (such as when an audit firm engages a specialised payroll processing company as a subcontractor), this subcontractor is regarded as a 'subprocessor' if the payroll engagement is a basic engagement in which the service provider acts as a processor under the instructions issued by the provider's client. In the event of more extensive services, the role of the subcontractor and the extent to which the latter receives instructions from the service provider on how to perform his work must be carefully assessed.

If the service provider simply passes on changes in client data to the subcontractor and the subcontractor has to check compliance with legislation and regulations, the subcontractor acts as a controller. In this scenario, the client, the service provider and the subcontractor are all independently regarded as controllers. If, however, the subcontractor only inputs the changes and the service provider has to check compliance with legislation and regulations, the client and the service provider are both independently regarded as controllers. The subcontractor then acts as a processor operating in line with the service provider's instructions.

If the client engages a third party (e.g. by purchasing a licence for payroll software directly from the software supplier), the client and the third party determine whether the third party is acting as a controller or a processor. This decision has no impact on the service provider.

[21] Section 3.5.1 of the Ministry of Justice and Security's Guide gives an example in which an administrative office does a company's payroll administration. The engagement is for the payroll administration, which essentially involves processing employees' personal data. In this case, the administrative office acts as a processor.

[22] If the service provider has a licence to use payroll software provided by a third party (i.e. a software supplier) and uses this software for all or almost all its payroll clients (i.e. not specifically at the request or on the instructions of a specific client), the software supplier is not regarded as a subcontractor. It is up to the service provider to decide which payroll software to use and the provider is not acting on the client's instructions. In this case, the service provider determines the purposes and means of data processing when selecting payroll software and so acts as a controller.

8. Administrative services

When preparing compilation, review and audit engagements or tax returns, service providers are often also engaged to perform bookkeeping services. In that case, keeping the client's books and accounts is a separate processing activity. Whether the service provider is then acting as a controller or a processor has to be determined separately (see section 2.2.). Bookkeeping is also a service that may be offered as a separate service.

As in the case of payroll processing engagements, a bookkeeping engagement also has to be assessed in terms of the nature and extent of the work to be performed by the service provider. Essentially, three different forms of service can be distinguished:[23]

- The service provider supplies the client with bookkeeping software (e.g. as a Software as a Service application);[24]
- The client itself licenses bookkeeping software. The service provider then checks the client's financial administration and gives advice on whether the client is keeping its books and accounts correctly and is compliant with the relevant statutory requirements, or
- The service provider keeps the books and records on behalf of its client (either using the provider's own bookkeeping software or software licensed by the client) and then gives advice on whether the client is keeping its books and accounts correctly and is compliant with the relevant statutory requirements.

If the service provider simply supplies the client with bookkeeping software, the service provider qualifies as a processor. The client has to maintain proper administrative records and it is the client who determines the purposes and means of processing the data. The service provider processes the data in line with the client's instructions and under the client's responsibility.

In the second and third variants, the service provider qualifies as a controller. Here, processing personal data is not the primary aim of the engagement. Instead, the processing is just the result of a different type of service. The service provider independently assesses certain matters (e.g. whether the books and records comply with the applicable legislation and regulations) and, where necessary, decides whether additional work is required. The service provider is also responsible for monitoring the quality of the services provided. In short, therefore, the service provider determines the purpose for which and the means by which the data are processed.

[23] If an engagement contains aspects of more than one of these variants, each part of the engagement has to be separately assessed to determine whether the service provider qualifies as a controller or processor.

[24] The service provider may qualify as a 'digital service provider', as defined in the Act on the Security of Network and Information Systems [*Wet Beveiliging Netwerk- en Informatiesystemen* or *Wbni]*, when providing cloud services such as Software as a Service, Platform as a Service or Infrastructure as a Service. The *Wbni* applies if the service provider provides a cloud service, has 50 or more employees and total assets or annual sales of EUR 10 million or more. The *Wbni* may apply, irrespective of whether the service provider qualifies as a controller or a processor under the GDPR.

ANNEX 1 Overview of controllers' and processors' obligations[25]

Controllers' obligations

Under the GDPR, any processing of personal data has to comply with the following principles:

- The processing must be lawful, fair and transparent ('lawfulness, fairness and transparency');
- The processing must be collected for specified purposes ('purpose limitation');
- The personal data must be adequate, relevant and limited to what is necessary ('data minimisation');
- The data must be accurate ('accuracy');
- The data must not be kept for longer than necessary ('storage limitation');
- The data must be appropriately secured and remain confidential ('integrity and confidentiality').

Controllers are responsible for and must be able to demonstrate compliance with these principles ('accountability'). Specifically this means that controllers have to:

- Maintain records of processing activities ('duty to record');
- Under certain circumstances, appoint a data protection officer;
- Carry out a data protection impact assessment before performing high-risk processing activities;
- Under certain circumstances, consult the Data Protection Authority before performing any new high-risk processing activities ('prior consultation');
- Structure processing activities in accordance with the principle of privacy by design and default;
- Take appropriate security measures to protect personal data;
- Report any personal data breach to the DPA and, under certain circumstances, also to the data subjects;
- Reach agreements with processors;
- Cooperate with the DPA;
- Respect the rights of the data subjects and interpret what they mean in practice.

Processors' obligations

The most important obligations applying to processors under the GDPR are that they must:

- Act only on instructions from the controller;
- Maintain a record of all categories of personal data processed on a controller's behalf (duty to record);
- Take appropriate technical and organisational measures to ensure the data subject is protected against the risks involved in the data processing;
- Not engage another processor or subprocessor without the controller's consent;
- Immediately notify the controller of any personal data breach;
- Cooperate with a request by the supervisory authority (the Data Protection Authority) relating to performance of the latter's tasks;
- Under certain circumstances, appoint a data protection officer.

[25] Overview based on Checklists 1 and 2 in the Ministry of Justice and Security's Guide to the GDPR and the GDPR Implementation Act.