ACCOUNTANCY EUROPE.

WHAT DO THE NEW EU DATA PROTECTION RULES MEAN FOR YOU?

General Data Protection Regulation

SME Infopack

FACTS.

PROFESSIONAL MATTERS

APRIL 2017

HIGHLIGHTS

The new EU data protection rules entering into force on 25 May 2018 will apply to everyone dealing with personal data information, whether this is stored online or on paper. Professional accountants are directly impacted by these requirements as they deal with collecting, storing and processing personal data in relation to their clients, employees, and subcontractors. These data protection requirements need to be considered seriously as fines could go up to tens of millions of Euro.

The purpose of this factsheet is to help accountants understand how the new legislation impacts their work. We explain the legislative changes and provide examples of what these mean in practice, among others: to inform their client on their data rights, ensure proper cybersecurity, and better and timely respond to data breaches.

INTRODUCTION

The accountancy profession should carefully prepare for the *General Data Protection Regulation* (GDPR)[1], entering into force on 25 May 2018. It provides the mandatory legal framework for the protection of personal data within the EU. Accountancy practitioners process personal data and are therefore directly impacted by this legislation. The GDPR builds on and replaces the *EU Data Protection Directive*[2] (the Directive), which was adopted 21 years ago.

Since 1995, the ways in which personal data is communicated and used have changed. The new legislation has, therefore, a dual purpose - (i) to take into account these changes in the personal data landscape and (ii) to provide a more consistent regulatory framework across the EU. To this end, the GDPR introduces some new onerous obligations and increased penalties for non-compliance.

All organisations handling personal information should review their procedures as soon as possible to ensure compliance with the new provisions. A Google-funded paper estimates that the cost for an average SME to implement the GDPR could run up to EUR 7,200 annually[3].

This publication starts by providing an overview of the key concepts in the field of data protection. It then discusses the main principles that the GDPR prescribes for the processing of personal data. The third part of the publication includes aspects related to the supervision of and non-compliance with the GDPR. Before concluding with the main changes brought by the GDPR, some attention is dedicated to the transfer of personal data to third countries.

KEY CONCEPTS AND THE ROLE OF PRACTITIONERS IN DATA PROTECTION

Personal data includes any information relating to an identifiable natural person (the data subject). E.g. the home address, income, or telephone number of a certain individual. Accountancy practitioners regularly process personal data of their clients or employees.

Data processing is any operation performed on personal data. This includes collecting, recording, structuring, storing, adapting, consulting, using, disclosing, erasing or destroying data.

For example, accountants collect and store information related to the identity of a new client to comply with their Customer Due Diligence requirements under the *Anti-Money Laundering Directive*. When providing payroll services for their clients (and themselves), they also have relevant personal data for the employees. Auditors process personal data of their clients' employees.

Data can be processed by data controllers and data processors. Data controllers determine the purposes and means of the processing of personal data. Data controllers can call on data processors to process personal data on their behalf. Data controllers should keep in mind their responsibilities when working with a data processor.

Practitioners can be both data controllers and processors. For example, an accountant that stores in the cloud personal data of their clients is a data controller. The cloud service provider is, in this case, a data processor that processes the data stored by the data controller. However, the accountant keeps their responsibilities when outsourcing data processing, including ensuring the appropriate security of personal data.

---

[1] Regulation (EU) 2016/679, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32016R0679&from=EN

[2] Directive 95/46/EC, available at: http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=URISERV:l14012&from=EN

[3] L. Christensen, A. Colciago, F. Etro and G. Rafert, *The Impact of the Data Protection Regulation in the E.U* (13 February 2013), available at: http://bit.ly/2iTWy9r

The GDPR does not cover the processing of personal data by a natural person in the course of a personal or household activity. It also does not include information relating to corporations or other legal entities, i.e. non-personal information.

To exemplify, practitioners are not covered by the GDPR when they process information on the location of their client's business (non-personal information) or when they keep track of the grades of their own children (household activity).

PRINCIPLES FOR PROCESSING PERSONAL DATA

Data controllers have many responsibilities and limitations when processing personal data. This section discusses when personal data can be processed in a lawful manner, what is important to keep in mind to respect the data rights of data subjects, and how data controllers and processors should be able to prove that they are respecting their obligations.

GROUNDS FOR PROCESSING DATA

The processing of personal data is lawful when it is necessary to:

- perform a contract to which the data subject is a party
- comply with a legal obligation
- protect the vital interests of the data subject
- perform a task in the public interest or in the exercise of official authority
- pursue the legitimate interests of the data controller – except where this is overridden by the fundamental rights of the data subject

For example, practitioners can justify processing personal client information in the context of Costumer Due Diligence process as this is to perform a task in the public interest and to comply with their obligations under anti-money laundering legislation.

Aside from the options set out above, it is also possible to process data when the data subject gives their consent. However, the conditions under which this is possible are strictly regulated and the controller must be able to demonstrate that the data subject consented to processing. Importantly, the provision of a service doesn't require giving consent where the processing is not necessary in providing that service. Moreover, the data subject can withdraw its consent at any time.

The GDPR also introduces rules for when personal data is processed beyond its original purpose. It requires controllers to properly document this decision and describe the factors considered in coming to this decision.

DATA RIGHTS

Practitioners will have to inform the data subject from which they collect personal information, e.g. their clients on their data rights, and take action to facilitate these rights. This might require a review of the information provided to the data subject on how their personal data is processed. Such a review should include looking at whether the language that is used is clear and understandable by the data subject[4].

Data rights include the right to rectification, objection, erasure, subject access, data portability, restriction of processing, and certain rights in relation to profiling – some of these rights are described below. Practitioners involved in big data analytics are urged to take note of the new provisions on data profiling, which is considered a high-risk activity[5].

[4] Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU Data Protection Regulation.*
[5] Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU Data Protection Regulation.*

Practitioners will also have to act on and respond to any request of a data subject, e.g. their client, to exercise its rights. This might require creating new procedures to deal with such requests. Besides, unless data subject requests are manifestly unfounded or excessive, practitioners must perform any actions relating to the data subject's rights free of charge. If no action is taken in reaction to a request, then the practitioner has to advise the subject of its rights to complain.

The data protection obligations described above also apply to employment information. Member States or collective agreements between employers and employees may adopt more rules for the processing of employees' personal data in the employment context. This means that there might be variations in the requirements from Member State to Member State.

THE RIGHT TO INFORMATION

When data is collected directly from the data subject, the controller must provide information such as its contact details, the duration of the data retention, the purpose for processing, and its legal basis. Data controllers should thus provide the data subject (e.g. client, employee, etc.) with plain answers to these key questions:

- who are you?
- who (else) receives my data?
- why do you process my data?
- how long will you store my data?
- what are my data rights?

The controller must also inform the data subject when they intend to further process the data for a purpose other than which the data was initially collected. Where personal data has not been directly collected from the data subject, controllers must provide the data subject with similar information as where the data is collected directly.

For example, during the Costumer Due Diligence process, practitioners need to provide their clients with their contact details and explain that their information is gathered to perform a task in the public interest. Where a practitioner uses a cloud service provider whose servers are outside the EU, they will also need to inform the client about this and about the safeguards that are in place to ensure the protection of the data rights.

THE RIGHT TO ERASURE

The right to erasure or the 'right to be forgotten' requires controllers to erase personal data at the request of the data subject in certain circumstances. The right to erasure does not apply where processing is necessary for the controller to comply with legal requirements or where processing is in the public interest.

For example, clients can thus not request the erasure of personal information that was collected in the context of the Costumer Due Diligence process.

ACCOUNTABILITY

Controllers must implement the necessary measures to ensure and be able to demonstrate that data processing conforms in all aspects to the requirements of the GDPR. The obligations could be fulfilled by adherence to an appropriate certification procedure or to a code of conduct. Presumably, this also requires that the organisation has documented procedures and records of specific decisions. Controllers must also perform a data protection impact assessment before embarking on processing that is likely to carry a high risk to the rights and freedoms of data subjects. To ensure proper compliance with the GDPR, it will be important to go beyond a 'tick-the-box' exercise and build a proper data protection culture.

A new requirement of the GDPR is that the controller is obliged to take measures leading to "data protection by design and default"[6] and to ensure that only the strict necessary personal data is processed. For example, in the context of the Costumer Due Diligence, practitioners should not process personal data such as the political preferences of the client.

Controllers are obliged to keep a record of processing activities, including details of the technical and organisational security measures covering the data and its processing. However, there is an exemption for an organisation of less than 250 employees.

Both controllers and processors are required to designate a data protection officer in certain cases. For example, a data protection officer is necessary when the organisation's core activities require regular and systematic monitoring of data subjects on a large scale, or consist of large scale processing of special data or data relating to criminal convictions. The data protection officer must be a data protection expert and must monitor the compliance with the GDPR. The officer may be an employee of the organisation but must be independent in the exercise of their activities.

The principle of data accountability also extends to the interaction with data processors. The GDPR requires that controllers use only processors that provide sufficient guarantees to implement appropriate measures to fulfil the requirements of the GDPR. This means that controllers need to be aware of their own obligations, as well as of those of the processors.

Apart from provisions affecting both controllers and processors, specific requirements are imposed on processors. For example, a processor is prohibited from engaging another processor without prior specific consent from the controller.

The contract with the processor should set out the boundaries of the data processing work. It must stipulate that the processor will assist the controller to comply with a number of the latter's obligations, such as to fulfil the requests from the data subjects, to notify data breaches, or to notify the controller if it believes that a specific processing instruction will infringe the GDPR.

The new obligations that are applicable to data controllers and data processors will affect future contractual relationship between controllers and processors. As a result, contracts are likely to become much more detailed. The new obligations might also require a review of existing contracts[7].

Practitioners should thus be careful when making use of suppliers, such as cloud service providers. This can start already when selecting the supplier. For example, when organising a call for tenders for a cloud service, practitioners could provide criteria in the call related to the way the data processor deals with cybersecurity or whether there is an assurance report for compliance with relevant international standards.

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

[7] Hogan Lovells, *Future-proofing privacy: A guide to preparing for the EU Data Protection Regulation.*

DATA PROTECTION APPLIES ALSO TO FILING CABINETS

The United Kingdom (UK) Information Commissioner's Office (ICO), the authority that upholds information rights in the UK, fined Norfolk County Council (Norfolk) for non-compliance with data protection rules.[8]

As part of an office move, Norfolk got rid of some furniture, including filing cabinets that were used by the children's social work team. Norfolk did not have a written procedure to determine who was responsible for emptying the cabinets, which did not occur. As a result, one person buying some of the furniture got case files with sensitive information.

ICO found that Norfolk did not have appropriate measures in place against unauthorised processing of personal data and against accidental loss or destruction of personal data. Norfolk received a penalty of £60,000.

This case shows the importance of having proper data protection procedures, regardless of whether you are in the cloud or using paper files.

SECURITY

Both controller and processor must implement appropriate measures to ensure an appropriate level of security. Such measures should be based on a risk assessment.

The GDPR requires both the controller and the processor to consider the current "state of the art" when implementing measures for security and specifically mentions pseudoanonymisation and encryption as techniques that could be applied. This will put more pressure on organisations to at least consider whether these measures are necessary and cost effective and, if so, to implement them.

Such technical measures can rarely be implemented simply. For example, encryption is not likely to be effective when data is transferred to an online service (such as an accounting package), whereas pseudoanonymisation may be suitable, but only after customisation. Implementing such measures will thus have cost implications.

The GDPR also introduces new rules in respect of responding to data breaches. In such an event, controllers are obliged to report the breach to their supervisory authority as soon as possible. Where the breach has a high risk to the rights and freedoms of data subjects, controllers must also notify the data subjects of the breach. The obligation on the processor is to notify the controller without undue delay of any data breach.

For example, if someone hacks a practitioner's server and steals personal client information, (such as password, home address, age, and earnings), then the practitioner has to report this breach to the supervisory authority and to the clients[9]. If the practitioner stores the client data in the cloud, then the cloud service provider would need to inform the practitioner of any breach. The latter should then notify the supervisory authorities and the client.

DATA SECURITY GUIDELINES AVAILABLE FOR SMES

The European Union Agency for Network and Information Security (ENISA) published guidelines to help SMEs adopt a risk-based approach for the security of the personal data they process.[10]

The guidelines aim to help SMEs understand the context of the personal data processing and to assess themselves, through a questionnaire, the associated security risks. ENISA also proposes possible organisational and technical security measures which can be adopted by SMEs to be compliant with the GDPR.

[8] ICO, available at: https://ico.org.uk/media/action-weve-taken/mpns/2013720/mpn-norfolk-county-council-20170315.pdf
[9] You can check if you have an account that has been compromised in a data breach here: https://haveibeenpwned.com/
[10] ENISA, *Guidelines for SMEs on the security of personal data processing*, (January 2017), available at: https://www.enisa.europa.eu/publications/guidelines-for-smes-on-the-security-of-personal-data-processing

IMPLEMENTATION OF THE GDPR

SUPERVISION

The GDPR introduces the concept of the 'lead supervisory authority'. This is the supervisory body of the Member State where the data controller's or processor's main establishment is located within the EU. This authority will take the lead for all cross-border processing carried out by that organisation – effectively a "one-stop shop" for an organisation for all of its EU data processing.

Supervisory authorities of other Member States than the one where the lead supervisory authority is located may still be involved when a Member State is affected by an organisation's data processing. This is for example the case when there is processing solely in respect of data subjects within the national boundaries of that Member State.

This could be a valuable change for controllers or processors with establishments in more than one Member State as it should simplify their registration, regulatory, and reporting requirements. They are, therefore, advised to identify who their lead supervisory authority is.

For example, an audit network will predominantly have to deal with the supervisory authority of its EU headquarters. Where one practitioner of a network takes measures to comply with a decision issued by the lead regulatory authority, they only need to notify the lead supervisory authority of those measures. The latter will then notify the other supervisory authority concerned.

Member States may further regulate the power of supervisory authorities in relation to controllers and processors, which are subject to rules on professional secrecy.

NON-COMPLIANCE

Certain data breaches can result in fines of up to the higher of €20 million or 4% of worldwide turnover. Less severe breaches have fines of up to the higher of €10 million or 2% of worldwide turnover. In the majority of Member States, the GDPR will probably lead to a significant increase in the potential sanctions for breaches of data subject's rights.

Data subjects will have additional rights such as the right to lodge a complaint with a supervisory authority, to judicial remedy against a controller or a processor, and to compensation from the controller.

TRANSFERS OF PERSONAL DATA TO THIRD COUNTRIES

Personal data can only be transferred to countries outside the EU when the same level of data protection can be guaranteed. In practice, this means that either a country must have a similar data protection framework as the EU, or that data controllers ensure that certain measures are adopted to guarantee sufficient data protection.

The European Commission assesses the level of protection available in third countries and keeps a list of those that meet the criteria. Data transfers can be made to any third countries on the list without specific authorisation. So far, only a few countries have shown an adequate level of protection and made the European Commission's list[11].

Personal data can still be sent to a non-equivalent third country if appropriate safeguards are provided. Such safeguards can take the form of binding corporate rules, standard contractual clauses approved by the Commission, or approved codes of conduct or certification processes.

Practitioners will not need authorisation to store data in Switzerland, which is on the Commission list. On the other hand, if an audit network wants to store its data in Iceland, it could do this by adopting legally binding

[11] European Commission, *Commission decisions on the adequacy of the protection of personal data in third countries*, available at: http://ec.europa.eu/justice/data-protection/international-transfers/adequacy/index_en.htm

corporate rules. Such rules should include the acceptance of liability by the entities established within the EU for breaches by any member outside the Union.

TRANSFERS TO THE UNITED KINGDOM (UK): THE IMPACT OF BREXIT

When the UK (or other Member States) leaves the EU, it will be considered as a 'third country'. This means that UK data controllers and processers that process personal data coming from data subjects in the EU, or data controllers in the EU that make use of data processers which transfer data to the UK, will have to revise their current data processing practices.[12]

TRANSFERS TO THE UNITED STATES (US): THE PRIVACY SHIELD

The US is a particular case. It is allowed to transfer data from the EU to US companies when these US companies are part of the *Privacy Shield*[13]. When practitioners want to move personal client data to the US under the Privacy Shield, they need to make sure that the US companies they work with are on the Privacy Shield List and have taken all necessary measures to comply with the requirements. Alternatively, they can transfer data when using other authorised means to provide adequate data protection (e.g. through contractual clauses).

The EU-US *Privacy Shield* is currently being challenged because it allegedly provides insufficient privacy protection. When the predecessor of the *Privacy Shield*, the *Safe Harbour Agreement*, was struck down, it created major legal uncertainty for audit and accountancy firms that used servers in the US. It is therefore advisable for practitioners that store their data in the US to take this into consideration and to follow any relevant developments announced by the European Commission, as well as changes in the US data policy.

[12] The GDPR will be applicable by May 2018. This means that if the Brexit negotiations have not been concluded by then, the UK will be bound by the GDPR until the Brexit is finalised.
[13] European Commission, *The EU-U.S. Privacy Shield,* available at: http://ec.europa.eu/justice/data-protection/international-transfers/eu-us-privacy-shield/index_en.htm

CONCLUSION

This publication discussed some of the main obligations under the GDPR that might apply to practitioners when they process personal data. These new rules are likely to require a review of existing data processing procedures. Practitioners are advised to make sure they have the necessary expertise at hand when doing this.

EU institutions and national data protection authorities are likely to, or have already, published guidelines on how to comply with the GDPR. We recommend to closely look at any recommendations made by your authorities.

For example, the EU Article 29 Working Party, which is composed by the national Data Protection Authorities, published guidelines on data protection officers, data portability, and on how to identify your lead supervisory authority.[14] Besides, the Belgian Privacy Commission published a brochure with 13 steps to become GDPR compliant[15].

MAIN CHANGES BROUGHT BY THE GDPR

The main changes compared to the Directive include:

- inclusion of data controllers and processors based outside the EU who hold personal information on EU citizens
- new accountability obligations for data controllers
- new data rights for data subjects
- processing based on a data subject's consent becomes more strictly regulated
- some organisations will need to appoint a Data Protection Officer
- stricter rules on data breaches
- introduction of a "one-stop-shop" for supervision
- advance notification or approval from the Data Protection Agency has been removed in many circumstances
- introduction of direct obligations for data processors

[14] Article 29 Working Party, available at: http://ec.europa.eu/newsroom/just/item-detail.cfm?item_id=50083
[15] Belgian Privacy Commission, *Plan en 13 étapes,* available at: https://www.privacycommission.be/sites/privacycommission/files/documents/STAPPENPLAN%20FR%20-%20V2.pdf

Avenue d'Auderghem 22-28, 1040 Brussel

+32(0)2 893 33 60

www.accountancyeurope.eu

@AccountancyEU

Accountancy Europe

ABOUT ACCOUNTANCY EUROPE

Accountancy Europe unites 50 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).