Tax&Legal Highlights

Poland

VAT changes: No more traditional VAT returns and launch of the Central Invoice Register as of 1 July 2019

The draft amendments to the VAT Act and the Tax Code have been published by the Ministry of Finance. They eliminate the requirement to file some VAT returns, in addition to establishing the Central Invoice Register. It has been proposed that the new legislation come into effect as of 1 July 2019.

SAF_VDEK

The draft amendments do away with VAT-7 and VAT-27 returns, which will be replaced with a new, more complex structure of SAF with the working name of SAF_VDEK. The explanatory memorandum states that SAF_VDEK will contain data derived from both the VAT return and VAT records. At the moment, however, no details are available about the scope of data to be reported using the new SAF structure. According to the proposed amendments to the VAT Act, VAT records will have to contain not only information that is necessary for proper VAT reporting or return preparation but also data allowing the taxation authority to verify whether the related obligations have been fulfilled or not. These provisions are both imprecise and broad-ranging. Considering the above and the fact that a detailed scope of data is to be defined by a regulation and in the XSD structure of SAF, which

will be specified on the website of the Public Information Bulletin of the Ministry of Finance, the possibility of a considerable extension of the scope of information to be reported in the new structure as compared to the existing requirements may not be ruled out.

Appendices to the traditional VAT returns, including VAT-ZZ, VAT-ZT and VAT-ZD, are also planned to be eliminated and replaced with appropriate tags in the new SAF structure.

Additionally, the draft amendments address the issue of invoices raised to document sales transactions recorded by fiscal cash registers over which doubts exist at present about whether they should be included in SAF_VAT or not.
According to the proposed regulations, such sales should constitute an element of the daily fiscal cash register report and additionally, the relevant invoice ought to be reported in SAF_VAT for the current period but without an increase in the value of sales or output VAT for the period during which they were included in the daily report.

In the event of submission of SAFs which contain incorrect or incomplete information a financial penalty of PLN 500 may be imposed for each identified irregularity (provided that such irregularity has not been remedied within 14 days of a demand to do so).

Those taxpayers who report VAT on a quarterly basis will be allowed to continue to do it with the same frequency as before but they will be obliged to submit monthly information from their VAT records as well.

It will still be required to file the summary VAT-EU returns.

Central Invoice Register

Additionally, the proposed act provides for the establishment of the Central Invoice Register, which will be based, among other, on SAF_VAT submitted by taxpayers. As stated in the explanatory memorandum, the register is aimed to enable verification of the correctness of VAT invoices raised by taxpayers, in addition to eliminating such illegal practices as the issuing of "empty" invoices or carousel fraud.

What next?

Considering the planned date of the new legislation's entry into force as well as the scope of the proposed changes, taxpayers should begin their preparations for the implementation of the new reporting obligations now. The first step which may be taken at the moment, without any system modifications, is the introduction of controls over tax information quality.

Contact details

Krzysztof Wilk
Director
Tax Advisory Department
Email: kwilk@deloitteCE.com

Igor Roman
Director
Tax Advisory Department
e-mail: iroman@deloitteCE.com

Aleksandra Pacowska-Brudło
Senior Manager
Tax Advisory Department
e-mail: apacowska@deloitteCE.com

Limited number of goods that are subject to the requirements of the transport law package

The amended excise law, which reduces the list of goods the transport of which is subject to the monitoring obligation under the transport law package (SENT), come into effect as of 1 January 2019.

The provisions of the act of 9 November, which amends some laws with a view to introducing simpler requirements for business entities under tax and business law (the "amended act"), entered into force as of the beginning of the new year. They amend, among other, the Excise Law of 6 December 2008 (the "Excise Law"). The scope of the amendments introduced to the Excise Law includes revisions of the CN classification used for defining the majority of excise goods, by replacing the one which was in force in 2009 with the one which was still applicable in 2018, in accordance with the explanatory memorandum. However, the amendments to the Excise Law are not limited only to a simple replacement of all the CN codes of 2009 with those of 2018 but they also modify the list of goods that are considered excise goods. What is important, the change of the list determines the obligations in respect of the monitoring of the transport of some goods under the Act of 9 March 2017 on the road and rail goods transport monitoring system (the "transport law package").

What is it all about?

The amendments to Article 86 of the Excise Law and to Appendix 1 thereto replace CN codes 3824 90 91 and 3824 90 97 (from the Combined Nomenclature of 2009), which cover, among other, a wide spectrum of chemicals, with CN 3826 00 (from the Combined Nomenclature of 2018), which includes, among other, biodiesel and its blends. The legislator still requires that in order to be classified as excise goods, these goods need to be intended for heating or driving purposes. In effect, the amendments introduced in this regard as of 2019 should be interpreted as reducing the excise goods list to only a small part of products classified as CN 3824 in 2009.

As far as the transport law package is concerned, the list of goods the transport of which is subject to the SENT monitoring obligation includes products classified within CN 3824. According to the provisions of the transport law package, as enacted on 14 June 2018, goods which are classified within CN 3824 are subject to the monitoring obligation only if they are the excise goods specified in Appendix 1 to the Excise Law, whatever their purpose.

What does it mean?

Under the Excise Law which comes into effect on 1 January 2019, goods which are today classified within CN 3824 have been removed from the list of excise goods, whereas entities trading in such goods, the transport of which was subject to the monitoring obligation until the end of 2018, will be allowed to reduce the scope of the SENT monitoring duties performed by their staff.

What next?

Those entities whose business involves the goods that are classified today within CN 3824 and which fulfil the related SENT transport monitoring duties ought to check whether the same obligations will continue to apply as of the beginning of 2019. It is likely that a number of enterprises which carry on their business in the so called non-excise industries, such as construction or various types of manufacturing, and had to comply with the relevant SENT transport monitoring requirements in 2018, will no longer be subject to any such obligations under the transport law package.

Contact details

Anna Wibig
Senior Manager
Tax Advisory Department
Email: awibig@deloitteCE.com

Mateusz Jopek
Manager
Tax Advisory Department
e-mail: mjopek@deloitteCE.com

Support in cloud computing, big data, IoT or AI services

Regulation on a framework for the free flow of non-personal data in the European Union

Regulation (EU) No 2018/1807 of the European Parliament and of the Council of 14 November 2018 on a framework for the free flow of non-personal data in the European Union has come into effect. Its requirements will have to be complied with as of 28 May 2019.

What is the objective and the subject matter of the Regulation?

The primary objective of the Regulation is to support the development of the European economy and innovative technologies which are based on data and their flow by:

a) **improving the mobility of non-personal data within the European Union by prohibiting any data localization requirement within a specific territory**, unless it is justified on grounds of public security.

- Limitations in this regard have been imposed by some member states with respect to providers of financial services, entities from the healthcare industry or the public sector.

- **They are to be removed by 30 May 2021**, whereas any new draft regulations aimed to introduce or modify such limitations will have to be notified to the European Commission.

- **By 30 May 2021, the member states will have to notify the European Commission of any prohibitions that are in place and are justified on grounds of public security** – the notifications will be examined by the European Commission, which may express its comments and formulate recommendations as to modification or elimination of a specific measure, if necessary. The member states will also be obliged to disclose information regarding the localization requirements in place within their territories to the public.

b) encouraging self-regulation by EU codes of conduct (e.g. for cloud computing service providers).

- The said codes ought to comprise:

    - guidelines on best practices in **facilitating the switching of providers and the transfer of data to other providers or own IT systems, with the use of structured formats that are commonly used and machine-readable**, including those based on open standards, where it is required or requested by the service provider that is the data recipient;

    - minimum information requirements aimed to **provide those using such services for purposes of their business operations** – prior to the entry into a data processing agreement – with access to sufficiently **accurate, clear and transparent information concerning: processes** (including those for creating back-up copies of data and their location; technical requirements as well as the available data formats and supports, the required configuration of IT systems and the minimum network bandwidth);**the time framework** (e.g. the time required prior to initiating the porting process and the time during which the data will remain available for porting); **the fees applicable where a professional user wishes to switch service providers or transfer data back to its own IT systems**;

    - **the approach to certification schemes that facilitate the comparison of data processing products and services** for those who use them for purposes relating to their business operations, including quality management, information security management, continuity of business management and environmental management;

    - **communication action plans** with a multi-disciplinary approach to **sharing knowledge of codes of conduct among the relevant stakeholders.**

- Service providers have been encouraged by the Commission to develop their codes of conduct by 29 November 2019 and implement them effectively by 29 May 2020.

Additionally, the Regulation lays down the rules governing the competent authorities' access to data for purposes of fulfilment of their official duties and collaboration in this regard across the EU member states.

What is the scope of application of the Regulation?
The Regulation **applies to**:

a) the processing of **electronic non-personal data provided as a service within the European Union to users residing or having an establishment in the Union, regardless of whether the provider is established or not in the Union;** or

b) the processing of electronic non-personal data carried out by a natural or legal person residing or having an establishment in the Union for its own needs.

In practice, **the provisions of the Regulation will apply e.g. to entities which provide cloud computing, big data, IoT or AI services**.

What are non-personal data?

Non-personal data are **electronic data other than the personal data defined by GDPR.** Thus, they will include information which does not relate to an identified or identifiable natural person.

Examples of non-personal data are anonymized data sets used for big data analyses, IT algorithms, machine-generated data or information concerning websites visited by a user, the time spent on each site or the number of visits, provided that such information does not relate to an identified or identifiable natural person.

What is non-personal data processing?

The processing of non-personal data means **any operation or set of operations which is performed on non-personal data or on sets of non-personal data in electronic form, whether or not by automated means**, such as collection, recording, organization, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

The Regulation should apply to data processing in broad sense, encompassing **the usage of all types of IT systems, whether located on the premises of the user or outsourced to a service provider. It should cover different service models from Infrastructure-as-a-Service (IaaS) to Platform-as-a-Service (PaaS) or Software-as-a-Service (SaaS).**

The Regulation on a framework for the free flow of non-personal data versus GDPR

The Regulation on a framework for the free flow of non-personal data does not affect any personal data protection regulations, which means **that all the rights and obligations under GDPR will remain in full force and effect.**

As far as data sets encompassing both personal and non-personal data are concerned, the provisions of the Regulation will apply to the part which comprises non-personal data. Where the personal and

non-personal data contained in a set are inseparably connected, the Regulation will be without prejudice to GDPR.

As **in practice doubts may arise** as to the status of specific information, i.e. personal vs. non-personal data, **by 29 May 2019 the European Commission should issue guidance on the interrelations between the Regulation and GDPR**.

How will that work in practice?

Generally, it is hard to disagree with the direction of changes introduced by the Regulation. One should remember, though, that its scope may encompass a range of data that is considerably wider than the one covered by GDPR, as non-personal data may be in fact anything (as long as they are not personal data).

Therefore, laying down consistent rules for such a broad spectrum of data may be quite problematic. For instance, for services which are currently available in cloud computing, the challenges relating to the format and transfer of data from group work and collaboration platforms (e.g. documents, shared resources etc.) are entirely different from those concerning data that describe the cloud infrastructure (such as virtual machine pictures, network topology or database platform data). The Regulation fails to differentiate between these data types, and the establishment of consistent rules for such different information may turn out to be very hard in practice.

Contact details

Ewelina Witek
Senior Managing Associate
Deloitte Legal
Email: ewitek@deloitteCE.com

Jakub Garszyński
Director
Risk Advisory Department
e-mail: jgarszynski@deloitteCE.com

The geo-blocking prohibition comes into effect

Regulation (EU) No 2018/302 of the European Parliament and of the Council on addressing unjustified geo-blocking and other forms of discrimination based on customers' nationality, place of residence or place of establishment within the internal market and amending Regulations (EC) No 2006/2004 and (EU) 2017/2394 and Directive 2009/22/EC entered into force on 3 December 2018.

It introduces a number of prohibitions aimed to prevent discrimination in cross-border trade with customers from other EU member states.

Audio-visual, retail financial and transport services are excluded from the scope of the Regulation.

Prohibition to block or limit the customer's access to the trader's online interface

As the Regulation came into effect, a trader's unjustified blocking or limiting the customer's access to its online interface is no longer possible. It has also been prohibited to redirect customers to a version of the trader's online interface that differs from the one which the customer originally attempted to access. Situations where the customer is redirected by his explicit consent and the version of the interface that he originally attempted to display will remain easily accessible to the customer will be an exception.

Access to goods and services

In principle, traders may not apply different general conditions of access to goods or services without a justification. A foreign customer should be allowed to purchase goods on the same terms as customers residing in the trader's country. The said prohibition will not apply where the provisions of EU or national laws make it impossible for the trader to sell goods or provide services to specific customers or to customers in specific territories.

Means of payment

The Regulation prohibits discrimination of customers from other EU member states by applying certain different conditions of payment. This concerns payment transactions made in electronic form, by means of credit transfers, direct debits or card-based payment instruments within the same payment brand and category.

Polish law

The bill amending the Act on Competition and Consumer Protection, as proposed by the President of the Office of Competition and Consumer Protection, is aimed to bring the Polish law into line with the new regulations adopted by the European Union. It designates the President of the Office of Competition and Consumer Protection as the authority responsible for providing help to consumers, in addition to enforcing those provisions of the Regulation which apply to violation of collective interests of consumers and practices that limit competitiveness. Any other instances of non-compliance with the Regulation will be examined by courts of general jurisdiction.

Contact details

Monika Skocz
Senior Managing Associate
Deloitte Legal
Email: mskocz@deloitteCE.com

Grzegorz Olszewski
Senior Associate
Deloitte Legal
e-mail: golszewski@deloitteCE.com

Digital employee files – changes as of 1 January 2019

The Act of 10 January 2018 amending some laws due to the shortening of the employee file retention period and file digitization comes into effect on 1 January 2019. It introduces numerous changes to the way in which records related to the employment relationship are kept and retained.

Effective from 2019, employers will be allowed to maintain employee files also electronically instead of in paper form. However, this does not mean that the employment contract or the employer's termination notice will from now on be prepared in electronic form. Instead, this will be a new form in which such documents may be retained.

Additionally, under the new law, employee files ought to be **retained for the entire period of the employee's service and for ten years of the expiry of that period** (instead of a fifty-year period required thus far). However, a shorter retention period applies to those hired as of 1 January 2019. If certain conditions are met, the shorter retention period may also be applied to employees hired after 31 December 1998, which requires the submission of an information report to the Social Insurance Institution.

What is important, employee files should be kept in such a way as to guarantee their confidentiality, integrity, completeness and accessibility, in conditions which eliminate any threat of damage or destruction.

Details of the new procedures applicable to the maintenance and retention of employee records are to be provided in the new regulation, **the draft version of which, dated 13 September 2018, modifies the requirements for keeping the above-mentioned files**. It has been proposed that such records be divided into four parts and be more complex. What is more, the regulation sets out the conditions (including technical ones) for keeping employee files in electronic form, in particular the conditions to be satisfied to protect them against loss, damage or unauthorized access.

Employers will have to ensure compliance with the proposed regulation within a period of six months.

In view of the above, it may be useful and reasonable for employers to adopt additional procedures to be followed in respect of employee records, addressing such issues as digitization, access to documentation, back-up copy creation, storage, safeguards or control of their effectiveness.

Additionally, the amended act has **changed the default salary payment form, which will be a credit transfer to the employee's bank account as of 2019**. By 22 January 2019, employers are required – in line with their customary practices – to inform their staff who have thus far received their salaries in cash, of the obligation to provide the number of the payment account to which credit transfers will be made or to file a request for their salary payments to be made in cash.

Contact details

Agata Jost
Managing Associate
Deloitte Legal
Email: ajost@deloitteCE.com

Edyta Garlicka
Partner
Deloitte Legal
e-mail: egarlicka@deloitteCE.com