How accountants protect personal data (3/35/17)

Globalisation and rapid technological advance tend to make personal information publicly and globally available, especially via social networking sites. Yet everyone has the right to protect their personal data and to control third-party access. The General Data Protection Regulation, which Latvia must apply from 25 May 2018, focuses on the need to protect personal data in a big way and imposes stiff penalties for failure to comply with data protection requirements.

In practice, personal data is indispensable when it comes to signing a contract of employment, in payroll calculations, invoices, agreements etc. This article explores some of the statutory aspects to be considered by accountants routinely handling source documents and processing personal data.

The legal framework

The pieces of legislation applicable in Latvia already prescribe a fairly wide range of responsibilities for data controllers and data processors. Yet it is important to note that the Regulation imposes significant penalties for non-compliance with its requirements. An administrative fine can reach €20 million or 4% of the company's global revenue in the past financial year (whichever is higher).

Personal data can be processed if such processing has lawful grounds. External accounting service providers will commonly act as operators processing personal data on behalf of another person for the purpose of supplying accounting services. A company's internal accountants will process data as operators or as data controllers depending on whether the purposes and means of personal data processing are determined by the company itself or by another person.

The current version of the Personal Data Protection Act lists the following cases where a data controller may process data:

- the data subject has given their consent;
- data processing arises from an agreement with the data subject or is necessary for entering into one;
- data processing is necessary for the data controller to perform their statutory duties;
- data processing is necessary for protecting vital interests of the data subject;
- data processing is necessary for acting in the public interest or for performing the duties of a public authority;
- data processing is necessary for furthering the lawful interests of the data controller or of a third party to whom the personal data has been disclosed.

Accordingly, the data processor should be aware of whether data is being processed on behalf of another person or whether the company itself determines the purposes and means of data processing. An accountant who is processing personal data should check that there are lawful grounds for data processing, such as an agreement with the controller, or one of the conditions listed in section 7 of the Act is present.

Data processing principles

When it comes to processing personal data, a number of principles should be considered:

- Data should be processed in an honest and lawful manner, meaning there is a lawful basis for

personal data processing;

- Data should be processed for, and only in accordance with, particular purposes, meaning that particular personal data is being handled and stored for a particular purpose, e.g. the data processing is necessary for calculating and paying wages to employees;
- Data should be adequate, meaning that any data being stored and otherwise processed should not be excessive for achieving the stated purpose (the principle of data minimisation). For example, if data processing is necessary for calculating wages, the accountant will process only data that is necessary for that purpose;
- Data should not be stored for longer than necessary, meaning that data processing, which includes storage, should be allowed to continue only for as long as is necessary. The length of data processing can be determined by a number of factors, e.g. in certain cases the law prescribes the length of document storage, which implies how long the personal data included in such documents can be stored;
- Data should be processed according to the rights of the data subject, with the Act laying down particular rights of the data subject that the controller should consider. For example, in particular cases a data subject has the right to request information on individuals and entities that have received information on that data subject. In reply to such a request, the data processor should be able to gather information on organisations and persons that have received information on the individual, e.g. that tax payment data has been filed with the State Revenue Service for a particular period. If accounting services are supplied by an external provider, the data subject should be notified about that;
- Data should be in safe custody, meaning that an accountant should take necessary measures for protecting data to prevent unauthorised persons from gaining access to it. In practice this means that data should be stored in a place and manner that denies unauthorised access. This principle applies to documents containing personal data that are stored electronically or in hard copy. In accordance with this principle, personal data cannot be accessible to any other employees of the company whose job responsibilities do not include data processing;
- Data should not be forwarded to organisations or authorities nor outside Latvia without providing secure and adequate protection. Security requirements such as encryption should be fulfilled in forwarding to ensure that data will not become known to other persons.

An example of the data adequacy principle is processing a person’s identification documents. A copy of their passport or ID card is often made without a good cause, since these documents contain information that is not always necessary for the stated purpose. For example, a person’s nationality does not come into play when calculating their wages, and so there are no grounds for gathering and storing such information, unless these activities follow from the Act or from a lawful purpose of data processing.

Applying the Regulation

As stated above, the General Data Protection Regulation will govern personal data processing from 25 May 2018. It is important to note that the core principles for protecting and processing data that are currently prescribed by the Act largely match the requirements of the Regulation. The Regulation lays down the following obligations in data processing:

- the company’s employees should be well informed and trained in personal data protection matters;
- checks should be made to ensure that the company’s internal documents outline its data processing procedures, which would help it demonstrate compliance with the data protection principles laid down by the Regulation;
- when data processing is started, the company should already have appropriate data processing

procedures in place to satisfy the principle of data adequacy.

Statutory requirements for personal data protection create the need for companies undertaking personal data processing to review their processes and improve their procedures in order to meet the additional requirements, and if necessary bring in data protection professionals to mitigate the risks inherent in failure to comply with statutory requirements. Recommendations, practical advice and points to consider are also available from the website of the National Data Office.