Requirements in data protection law for implementation of the new Cash Register Ordinance

Article by Dr. Carlo Piltz and Moritz zur Weihen

The Cash Register Ordinance, an Ordinance issued by the Finance Ministry specifying the duties for proper accounting in accordance with § 146a of the Tax Code, has been in effect since 1 January 2020. The Ordinance aims to prevent manipulation of cash registers and to facilitate data transmission and the satisfaction of tax documentation requirements. In essence, the Ordinance takes the existing statutory documentation requirements to the digital level.

As a result, the Cash Register Ordinance changes not only the technical requirements but also the substantive requirements for storage of relevant tax documents, such as receipts.

§ 2 of the Cash Register Ordinance defines the data from each transaction which is to be stored electronically, specifically:

- the time at which the transaction began;
- a clear and continuous transaction number;
- the type of transaction;
- the transaction data;
- the mode of payment;
- the time at which the transaction was completed or cancelled;
- a test value;
- the serial number of the electronic storage system or security module.

In addition, all cash registers in use must be equipped with a technical security device (TSD), i.e. a Blockchain-based method for secure storage of the cash register’s transactions which assigns a signature to each transaction ensuring that the data cannot be manipulated. The taxpayer’s data, such as address, Tax ID, etc., are to be entered into the cash register, ensuring that transactions are recorded automatically and with no gaps. The serial number of each cash register in use must be reported to the Tax Office by the operator.
If TSDs are implemented, it will no longer be necessary to certify the cash registers or cash register systems themselves: only the TSDs will have to be certified. But the precise technical specifications of the TSD may vary depending on the cash register’s manufacturer. The new rules will be binding as of 30 September 2020. From that point on, all cash registers will have to be equipped with a "TSD interface" and will have to comply with the provisions of the Cash Register Ordinance.

Export of the data secured by the TSD and export via the tax authorities' digital interface for cash register systems must be ensured for the duration of the document retention period in accordance with tax law, which is typically ten years (§ 147 of the Tax Code). This may take place either locally or through an outside service provider. Like other cloud storage services, such outside service providers perform the function of data processors in terms of Article 28 of the GDPR, whose requirements must be heeded in such a case. The controller for the data processing continues to be the cash register operator, which is the taxpayer in this case. Accordingly, the cash register operator should pay particular attention to the conclusion of an agreement with the processor (Article 28(3) of the GDPR) and ensuring that the service provider it uses takes appropriate technical and organizational security measures (Article 32 of the GDPR).

However, potential conflicts can be identified between provisions of data protection law and the technical requirements.

While the Ordinance does not require operators to store customers' personal data in a clear and direct manner, it may be possible to indirectly match the data to a specific person in certain cases, e.g. by combining the transaction number with the EC or credit card payment data. Cash register operators should therefore consider the option of anonymizing customer data, since storage of each customer’s specific EC Card data is not absolutely necessary for the purpose of processing, i.e. compliance with the statutory requirements established by the Cash Register Ordinance. Under the Ordinance, operators are only required to store the mode of payment, not to store data which identifies or makes it possible to identify the person making the payment.

Furthermore, the rules established by the GDPR state that data cannot be stored forever and that the controller’s ability to delete the data must generally be ensured. But the reason Blockchain systems are so secure against manipulation is that their technical features are such that data can never be completely deleted. Such a concept conflicts with the principle of storage limitation in accordance with Article 5(1)e of the GDPR.
A conceivable solution would be to replace the encryption key for journal data stored in Blockchain after ten years and then delete the old key so that readout of the old data would no longer be possible. But it remains questionable whether this approach is feasible in practice.

About us:
reuschlaw Legal Consultants advise companies active on a national and international scale in more than 30 countries in the areas of product liability, product safety law, recall management, insurance law, cybersecurity and data protection, compliance management and contract law.

Company contact: Melanie Schaumann I Head of Marketing & Communications I T: +49 30/ 2332895 0 I E: melanie.schaumann@reuschlaw.de