FOLKETINGET
STATSREVISORERNE

FOLKETINGET
RIGSREVISIONEN

May 2020
– 15/2019

Extract from Rigsrevisionen's report
submitted to the Public Accounts Committee

Outsourcing of personal data

1. Introduction and conclusion

1.1. Purpose and conclusion

1. Personal data about you are under attack. According to the Danish Centre for Cyber Security, cyber criminals are keenly interested in personal data and have been for several years. If the citizens' data end up with the wrong persons, it may lead to loss of reputation, identity theft or extortion, and if data are lost, the quality of public services delivered to the citizens may be adversely affected.

2. Denmark is among the most digitally advanced countries in the world. A broad range of digital services like, for instance, borger.dk (a national citizen portal), NemID (a national electronic identity and digital signature solution) and TastSelv (the tax administration's online self-service system) make life easier for both citizens, companies and the public authorities. E-government relies on the collection and processing of vast quantities of data about the citizens. Much of this information is sensitive or confidential like, for instance personal identification numbers, health data, data about political opinions and criminal records. If this information falls into the wrong hands or is lost, the consequences for the individual citizen and the public sector can be severe.

3. According to the report *Strategy for ICT management in central government* from 2017, Denmark is among the countries in the European Union that are outsourcing the largest share of central government IT systems. Outsourcing offers cost-effective running and better utilisation of expertise, but at the same time outsourcing imposes demanding requirements on the public authorities' management of the data processors that process data about the citizens.

Outsourcing
Outsourcing means that a task like, for instance, running, maintenance and development of IT services, is transferred to an external supplier, which can be either a private business or a public entity.

For example, the Ministry of Justice has outsourced storing of data from the Criminal Records Register to a private IT supplier.

4. The General Data Protection Regulation (the GDPR), which was adopted by the EU in April 2016, regulates the processing of personal data. The GDPR took effect on 25 May 2018 and replaced the Danish Data Protection Act from 2000, which implemented the EU directive on data protection in Danish legislation. The GDPR establishes some of the same requirements as the Data Protection Act like, for instance, the data controller's obligation to carry out risk assessments, enter into data processing agreements and monitor how the data is processed by the data processors.

GDPR
GDPR stands for the General Data Protection Regulation.

However, the GDPR also introduced new provisions like, for instance, the designation of a data protection officer and the right to impose substantial penalties for infringements of the provisions. The new provisions and the right to impose penalties have increased public interest in data protection and therefore the attention in the private as well as in the public sector.

5. This study looks across 17 ministries and one of the five regions. We have included Region Midtjylland (Central Denmark Region) as a case, because the five Danish regions handle large amounts of health data about citizens.

The public authorities
In this study, the term" public authorities" refers to the 17 ministries and the Central Denmark Region included in the study.

6. The purpose of the study is to assess the public authorities' effort to ensure that outsourced sensitive and confidential personal data about citizens are secure. The report answers the following questions:

- Have the public authorities' management of data processors that store sensitive and confidential personal data been satisfactory?
- Have the Ministry of Justice, including the Danish Data Protection Agency, and the Ministry of Finance adequately supported the public authorities in their management of data processors?

Rigsrevisionen initiated the study in February 2019.

Main conclusion

Overall, the public authorities have made an unsatisfactory effort to ensure that outsourced sensitive and confidential personal data about citizens are secure. The consequence is an enhanced risk of sensitive and confidential personal data being compromised.

Overall, the public authorities' management of outsourced sensitive or confidential personal data related to the digital services and IT-systems included in this study has been very unsatisfactory. This in spite of the fact that the public authorities, since 2000, have been required to make risk assessments, enter into data processor agreements and monitor data processors. Particularly, the Ministry of Immigration and Integration and the Central Denmark Region have managed data processors in an unsatisfactory manner. Overall, the Ministry of Finance performed better than the other public authorities did.
The public authorities have not carried out worked out risk assessments for 58% of the outsourced digital services prior to entering into data processing agreements with the external data processors. This means that in most instances the public authorities have lacked a proper basis for planning their monitoring and the establishment of an appropriate level of security in the data processing agreements, which Rigsrevisionen finds very unsatisfactory. When using global cloud-service providers, the public authorities are required to approve the standard terms and conditions, which generally cannot be adapted to the needs of the individual customer. Rigsrevisionen therefore finds it particularly unsatisfactory that the public authorities have only worked out risk assessments for six out of seventeen digital services that involve processing of personal data by global cloud-service providers. It is also unsatisfactory that several of the public authorities lacked detailed knowledge of the standard terms and conditions that they have accepted in relation to the outsourcing of data processing to global cloud-based service providers.

In spite of the fact that the public authorities had outsourced the storage of sensitive or confidential personal data, they had failed to enter data processor agreements for 14% of the outsourced digital services. This means that the public authorities did not have any legal basis for regulating the data processors' processing of personal data. However, in the course of Rigsrevisionen's study the public authorities entered data processor agreements for one third of these digital services that had been outsourced at an earlier stage.

The public authorities have not monitored the data processors' handling of the outsourced digital services in 23 % of the studied cases and have thus failed to check that the data processors comply with the terms of the data processor agreements and the data protection regulations. The public authorities have been unable to document that they have followed up on 40% of the completed inspections. Hence, they have failed to decide whether to take action against data processors in relation to the outcome of the inspections. This means that the inspections have not served their purpose.

Inadequate supervision carries the risk that the public authorities do not have sufficient knowledge of whether data processing takes place within the framework of the data processor agreements and data protection regulations. Rigsrevisionen's study found that the public authorities in 24% of the cases did not have knowledge of all sub-processors. In practise, this means that sub-processors have processed sensitive and confidential personal data without the knowledge of the public authorities.

The Ministry of Justice, including the Danish Data Protection Agency, and the Ministry of Finance have not adequately supported the public authorities' management of the data processors

The Ministry of Justice, the Danish Data Protection Agency and the Ministry of Finance have published 20 guidelines to support the public authorities in their implementation of the GDPR. Rigsrevisionen welcomes this initiative.

However, Rigsrevisionen finds it inadequate that eight of these guidelines were published after the GDPR took effect. Essential guidelines concerning risk assessments and the use of cloud services were published more than one year after the GDPR took effect. Moreover, the Ministry of Justice has not issued a departmental order or a guideline on the location requirement (formerly referred to as "rule of war") that defines which digital services that must be stored within the borders of Denmark, for national security reasons. This is not considered satisfactory by Rigsrevisionen either.

The Danish Data Protection Agency's has not had a risk-based approach to its supervision of public authorities and private companies. The agency has not worked out risk analyses to support its supervision and it has not updated its organization strategy since the GDPR took effect in May 2018. The agency has been unable to document that the inspections planned by the agency have been selected based on risk assessments. Thus, it is unclear whether the agency's resources have been used to supervise the data processing areas carrying the highest risks.

Since the GDPR took effect, the Danish Data Protection Agency has only completed 8 inspections of public authorities and 14 inspections of private companies. This means that the public authorities have very few inspection reports to rely on in their efforts to ensure adequate management of data processors and correct implementation of the GDRP. It also means that infringements of the GDPR carry a relatively low risk of detection, which reduces the preventive effect of the inspections.