# Summary of results from the audit of data protection officers in authorities and in private sector companies

**Summary of the results**
The audit shows that the majority of the authorities and companies investigated have notified and designated a data protection officer in time. More than 350 organizations were included in the audit and the Swedish Data Protection Authority (DPA) has identified deficiencies in approximately 16 percent of these cases. There is only a marginal difference in compliance between authorities and private sector companies.

Out of a total amount of 66 scrutinized cases, the Swedish DPA has decided to issue reprimands in 57 cases. In two other cases, the DPA issued an order to comply to the audited organization and seven cases were closed without further measures.

## Introduction

At the end of May 2018, the Swedish DPA initiated an audit of a number of organizations to see whether data protection officers had been designated. This is a compilation of the results from the audit.

According to article 37 of the General Data Protection Regulation[1] (GDPR), a public authority or public body shall designate a data protection officer. Private sector companies have the same obligation according to this article if

[1] Regulation (EU) 2016/679 of the European Parliament and of the Council of the 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

their core activities include regular and systematic monitoring of data subjects on a large scale or if their core activities include processing of sensitive data or data about crime on a large scale. According to this article, there is also an obligation to communicate the contact details of the data protection officer to the Swedish DPA.

The cases that were handled within this project can be divided into two categories; government administrative authorities and private sector organizations. The private sector organizations represent six different business sectors. They are banks, telecom providers, insurance companies, trade unions, public transportation companies and medical care providers.

A total amount of 362 organisations were checked, 66 organisations have been selected for a closer audit. Out of the 66, 35 are public authorities and 31 are private sector companies.[2]

## Results of the audit

The compilation of the audited cases shows that there are four different kinds of cases. The first category consists of organisations that have complied from the start and where a data protection officer has been designated and notified to the DPA by 25 May 2018 at the latest. The second category consists of organisations that have designated a data protection officer and/or communicated the contact details to the Swedish DPA after the 25 May 2018 but during the investigation, i.e. before the DPA issued a decision in the case. The third category consists of those organisations that, still at the time of the decision, had not designated a data protection officer or communicated the contact details to the Swedish DPA. To this can be added a fourth category consisting of one case where the DPA deemed that there was no obligation for the organisation to designate a data protection officer.

The cases in categories one and four were closed without further measures. These organizations have either complied from the start or the DPA has deemed that there was no obligation for the organisation to designate a data protection officer. Seven of the cases fall under these two categories. In

[2] The project group started the selection process by identifying more than 400 activities where the assumption was that there was an obligation to designate a data protection officer. Of these 400 activities, the Swedish DPA selected 362 organisations and checked them against the notifications of data protection officers that the DPA had received. Those 66 organisations that were finally audited in specific supervision cases are those where no such notification had been submitted to the DPA when the audit started. As shown below under the results of the audit, there are a few organisations which have shown that they had in fact designated and notified an officer in time despite the review of submitted notifications.

addition to this, all organisations that were part of the initial investigation, but where the Swedish DPA chose not to initiate a specific audit case, fall under these categories. Overall, 303 organisations out of the 362 that were included in the initial investigation fall under these two categories.

The cases in category two were closed with a reprimand to the audited organisations regarding the non-compliance. Failure to designate and communicate the contact details of a data protection officer to the Swedish DPA can result in an administrative fine.[3] The main reason why the DPA has not gone further than issuing reprimands is that a relatively short time has passed since the 25 May 2018.

Overall, category two includes 57 cases which are divided as follows:

- 31 public authorities
- 3 banks
- 4 insurance companies
- 1 public transportation company
- 4 telecom providers
- 12 trade unions
- 2 private medical care providers

The cases in category three, i.e. the two organisations which still at the time of the decision had not designated a data protection officer or communicated the contact details to the Swedish DPA, were closed with an order to comply to each organisation regarding the non-compliance.

## Conclusions on compliance

It is of interest to compare how the public authorities and the six different business sectors comply with the obligation to designate a data protection officer, in the light of the little more than 350 authorities and companies that the Swedish DPA included in the initial investigation. It is an indication both of the general picture but also of how authorities as a group and the different business sectors respectively comply with the obligation to designate a data protection officer.

Out of those more than 350 organisations that were checked initially, the Swedish DPA noted deficiencies in 16.3 % (59 out of 362). Divided according to each category and sector, this shows:

---

[3] Article 83 p. 4 (a) of the Data Protection Regulation and Chapter 6, section 2 of the Act (2018:218) on supplementary provisions to the EU Data Protection Regulation

- *Public authorities*: Of the 210 public authorities that were checked initially, the Swedish DPA noted deficiencies in 33 cases. This corresponds to approx. 16 percent.

- *Private sector organizations*: Of 152 private sector organizations that were checked initially, the Swedish DPA noted deficiencies in 26 cases which corresponds to just above 17 percent.

The private companies can be divided into the following business sectors:

- *Banks*: Out of 40 banks that were checked, the DPA noted deficiencies in 3 cases.
- *Insurance companies*: Out of 42 insurance companies that were checked, the DPA noted deficiencies in 4 cases.
- *Public transportation*: Out of 8 companies within public transportation that were checked, the Swedish DPA noted deficiencies in one case.
- *Telecom providers*: Out of 8 telecom providers that were checked, the Swedish DPA noted deficiencies in four cases.
- *Trade unions*: Out of 45 unions that were checked, the Swedish DPA noted deficiencies in 12 cases.
- *Private medical care providers*: Out of 9 medical care providers that were checked, the Swedish DPA noted deficiencies in two cases.

The Swedish DPA notes that, of those organizations that were audited, the majority has chosen to comply with the requirements during the pending investigation. Deficiencies only remain in two of the cases, something which has led to orders to comply from the DPA.

It can also be noted that there is only a marginal difference in compliance between public authorities and private sector organizations. Certain business sectors, however, stand out negatively.[4] This applies in particular to telecom providers where four out of eight companies have not complied with the requirements. Also, trade unions stand out negatively compared to the average.

/The Project Group

[4] Considering that the number of investigated organisations in some categories is relatively low, interpretation of the numbers on percentage must be interpreted with caution.

Annex

1. Overview of supervised organisations and corrective measures