

Summary:

Processing of personal data in Norwegian organisations

This report presents the results of a survey based on self-administered questionnaires on the processing of personal data by Norwegian organisations. Among the 424 organisations that are the questionnaire respondents, there are public and private businesses, public bodies and public service providers and others (for example non-profit organisations). In this summary the term “organisations” is used to refer to all of these.

The survey seeks to reveal:

- What personal data are processed in organisations.
- To what extent do organisations fulfil the requirements for processing of personal data which stem from the Personal Data Act or the regulations issued under this law.
- The organisations’ knowledge and attitude towards the legal framework and to the central public organs for the protection of privacy.
- The organisations’ attitude to the protection of privacy when weighed up against certain other interests.

Main conclusions

The survey suggests a basic positive attitude towards the protection of privacy among the organisations. Knowledge of the Personal Data Act and the duties which stem from it are meanwhile little known. Quite a lot of the organisations hold that the requirements do not apply to them, even though they process personal data and therefore are covered by the law. A small part of the organisations say that they completely agree that they fulfil the concrete requirements which stem from the law or the regulations. This applies to the requirement for data security, internal control and information to those to whom the data refers.

The organisations process many types of personal data

The organisations in the survey process many types of personal data on their own employees and customers, clients, users and other third parties. A large number of them also process information that in the law is defined as sensitive personal data. One out of three organisations process, for example, health data about their own employees and one out of three process data about their employees’ trade union membership. This is information that, according to the law, is sensitive.

Processing of such data requires a licence, unless the information was handed over unsolicited.

77 percent of the organisations say that they process information on customers, clients, users and other third parties, also information which according to the law is defined as sensitive. There are more bodies within the public service and administration which process information about third parties than among the remaining organisations. This group comprises health and social services and education, something that explains why a large group process personal data on third parties.

Weak compliance with the Personal Data Act

The questionnaire respondents consist of organisations that have four or more employees. All the respondent organisations consequently process personal data and therefore fall within the Personal Data Act.

The law or the regulation issued under the law lay down a number of duties which should be complied with when personal data is processed. This applies to the requirement for *data security* and *internal control* and *an obligation to provide information* to those people to whom the personal data refers. The survey reveals that a considerably large part of the organisations hold that measures which should be taken in order to comply with these duties, are not relevant for them. This shows a low level of knowledge among the organisations as to which duties they have under the law.

We have asked representatives of the organisations to what extent they agree that they carry out different measures that are required in order to claim that they are in compliance with the duties.

Internal control and data security

With a division of the answers into three as being either "agree", "neither nor" and "disagree", approximately half say that they have established a system for internal control. Nevertheless there is a good part of these who do not agree that they have routines for deletion of data which no longer is necessary for the purpose for which it was originally collected. Without routines for deletion, it is difficult to claim that one is carrying out an acceptable internal control. To not delete data which is no longer necessary for the original purpose, is also a direct breach of the law and not just an indication of a lack of internal control. 40 percent of all the organisations say that they have such routines.

Only one of three organisations say that they carry out a systematic survey over what personal data is processed in the organisation. It is absolutely not possible to comply with the different requirements of the Personal Data Act without such an overview. 44 percent of the organisations say either that such an overview is not relevant or that they *completely disagree* that they have such an overview.

Of the different requirements for data security and internal control that we asked about, there are only 4 percent of the organisations which say they *completely agree* that they have carried out the different measures. 30 percent cannot completely agree that they have carried out even one measure.

There is not a large difference among private and public businesses on the one side, and public bodies and public service providers on the other as regards the

carrying out of different measures required to comply with the requirements for data security and internal control. The size of the organisations (measured according to the number of employees) has little meaning on whether the requirements for data security and internal control are fulfilled.

Obligation to provide information

Only between one-fourth and one-half of the organisations always give the type of information that we have asked for, to the person to whom the information refers. The purpose for which the information will be used and the right of access, are what the organisations most often reply that they always inform about. There are nevertheless only 35 percent who always give information about this. Only one out of four always inform that it is voluntary to give information or otherwise, and only 30 percent always give information whether the data will be disclosed to third parties or not.

The organisations that process information on third parties do not comply with the duty to provide information any more than all the organisations taken together. Among these organisations there are just 6 percent who reply that they always give *all* the types of information we have asked about. 33 percent cannot answer “yes, always” to even one of them.

Public bodies and public service providers are better than the others in fulfilling the different facets of the duty to provide information. There is not much difference between large and small organisations.

Positive attitude to the protection of privacy, laws and rules, but little knowledge

There is broad agreement on the need for a strong Data Inspectorate. There is meanwhile only 16 percent who say that they have good knowledge of the role and tasks of the Data Inspectorate and only 4 percent say the same about the Privacy Appeals Board. With the answers being split into three as being either “agree”, “neutral” or “disagree”, among those who say they have some knowledge of the Personal Data Act, 70 percent hold that the law is necessary. There is only 6 percent of them who hold that the law is only necessary for some special sectors and activities.

Positive attitude, but little knowledge of the Personal Data Act

One out of three say that they have little knowledge of the Personal Data Act. Among those who say they *have* some knowledge of the law, there are 28 percent who cannot answer whether the law is easy to understand and 21 percent *cannot answer* whether the law is easy to comply with. Among the organisations which have a clear standpoint with regards to this, there are more who hold that the law is both easy to understand and easy to comply with, than those who hold the opposite.

The assertion that the laws and rules which protect personal privacy are too strict does not find support among the organisations. When asked what can be the most important reason why some organisations do not comply with the requirements of the law, three out of four reply that it is a *lack of knowledge* of the legal framework. That the legal framework is too little flexible or that it is too time-consuming to comply with it, finds little support among the organisations.

Privacy considerations have weight

When the organisations were asked to assess privacy protection when weighed against other interests, a preponderance of them *gave most weight* to the protection of privacy. A large majority of the organisations disagree that the employer shall have unlimited right to access the employees' e-mails and that the employer shall have the opportunity to have hidden camera-surveillance at the workplace in order to reveal possible breaches of the law. Almost half of the organisations say that they *completely disagree* with this. There is somewhat more agreement that the employer without warning could see what Internet websites the employees have visited. Three out of four organisations hold that there should be strict rules for the exchange of information, even if a freer exchange can give better products and services. One out of three say they *completely agree* with this.