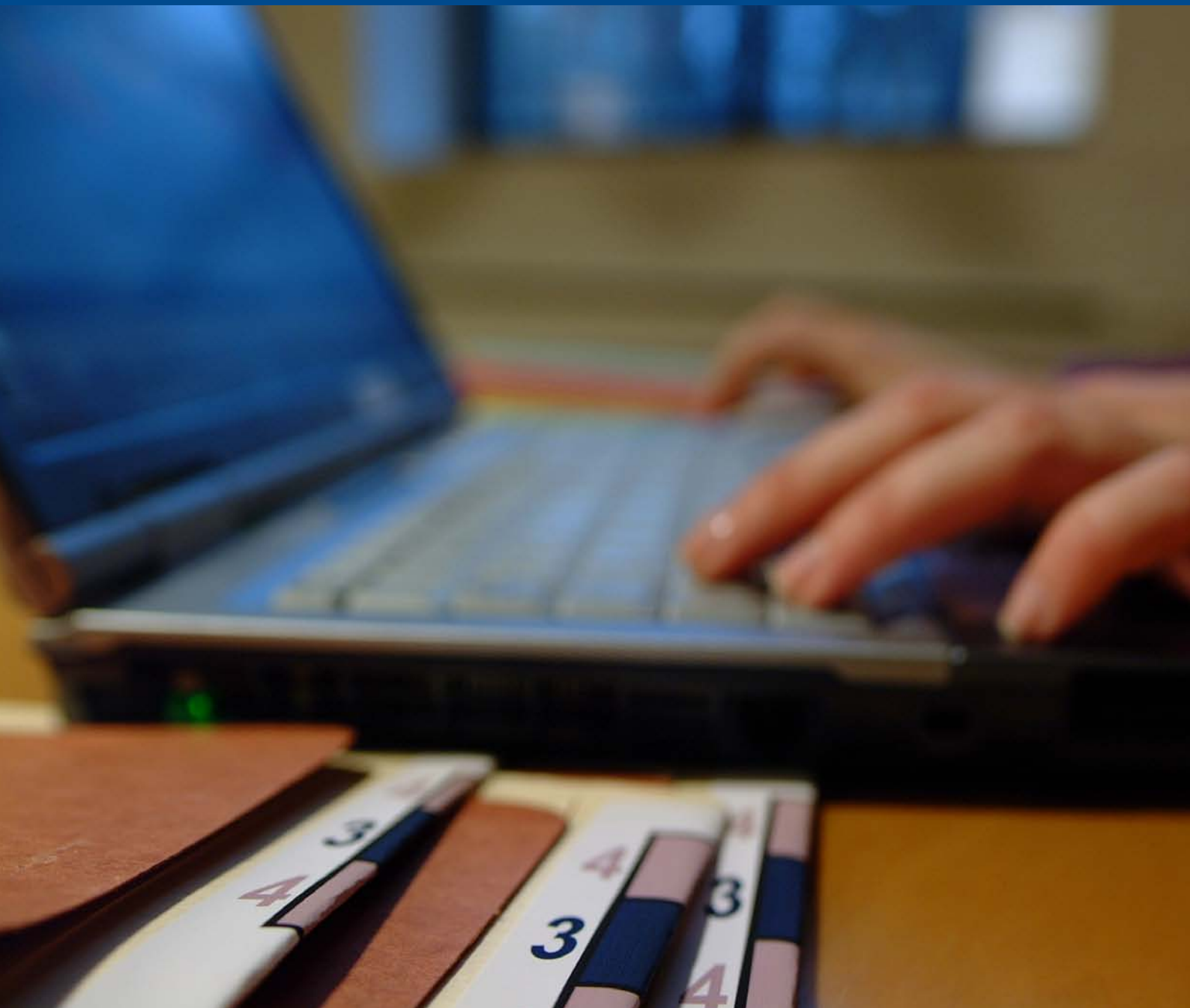
Datatilsynet

Data processor agreements

pursuant to the Personal Data Act and the Personal Health Data Filing System Act

Guide

October 2012



List of contents

PART 1

DATA PROCESSOR AGREEMENTS - GUIDE

This Guide outlines on data processor agreement. This Guide should be read in parallel with the draft agreement. The attachment contains a draft agreement pursuant to the Personal Data Act and Attachment B a draft agreement pursuant to the Personal Health Data Filing System Act.

We did not think it would be helpful to prepare an exhaustive template or list of what a data processor agreement should include. The potential contractual parties are too different for this to be practical, and the drafts would have been unmanageable to most people.

Nevertheless, with this brief Guide and the proposal for data processor agreement pursuant to the Personal Data Act, we have attempted to outline what the main elements should be.

If the data controller is uncertain whether the agreement will be sufficiently specific, the undertaking may seek advice from The Norwegian Data Protection Authority. We would prefer the undertaking to prepare a draft agreement before seeking guidance. In this way, we will be able to work more efficiently together and it will be easier for the Data Inspectorate to say whether it considers the agreement to be sufficiently connected to what it is intended to regulate.

The Norwegian Data Protection Authority

Assumptions and clarifications

Some undertakings choose to outsource the processing of personal data wholly or partly to other enterprises, so-called data processors. The relations between a data controller and a data processor must be regulated by an agreement – a data processor agreement, see section 13 and 15 of the Personal Data Act.

A data processor agreement may be a separate agreement between the parties or an integral part of a system of contracts.

According to section 15 of the Personal Data Act, no data processor may process personal data in any other way than that which is agreed in writing with the data controller.

The data controller must ensure that the data processor has an adequate security level, see section 15 of the Personal Data Act. For further information, see the pages on Internal Control and Data Security.

Data controller:

- The person who determines the purpose and means of the processing of personal data; see section 2 no. 4 of the Personal Data Act.

- He is responsible for ensuring that data are processed in accordance with the requirements listed in the Personal Data Act.

Processing personal data means any use of personal data, such as collection, recording, alignment, storage and disclosure or a combination of such uses.

Data processor:

- The person who processes personal data on behalf of the controller; see section 2 no. 5 of the Personal Data Act.
- He has an independent responsibility to ensure satisfactory information security to protect the personal data processed on behalf of the controller; see section 13 of the Personal Data Act.
- He can only process personal data pursuant to an agreement with the data controller.

The person acting as data processor will have an independent responsibility for the personal data processed on his own behalf, for example data about his own employees.

The processing of sensitive personal data will probably require a more detailed agreement than an agreement about isolated invoicing assignments. Furthermore, the degree of detail will vary from quite fundamental requirements to quite specific measures regarding data security for example.

Minimum requirements

Together with this template, the items below constitute the minimum requirements for what should be included in a data processor agreement. The data controller may establish more stringent requirements than those mentioned in the Personal Data Act, but may not propose terms and conditions that are in conflict with the minimum requirements of the Personal Data Act.

1 State the purpose

The agreement must clearly state the purpose of the processing of personal data. The processor may only process the data in accordance with the purpose defined by the controller.

Typical examples of data processor assignments include the shredding of paper documents, IT operations, invoicing, camera surveillance and the processing of personal data such as payment of wages.

2 Describe how the personal data are to be processed

The agreement must state clearly what the processor is to do with the personal data.

Are they only to be stored for future use (archival authority) or are they to be processed in some way. The agreement must also regulate or clarify whether there is to be other processing, such as linkage to other personal data/registers.

2.1 Specific procedures for use of the personal data

The data processor does not have a right of disposition of the personal data and cannot therefore process them for their own purposes.

2.2 Rules for the disclosure of personal data

The data processor must act accordingly to the agreement. If he is to disclose personal data to other external parties, this must be clearly stated in the data processor agreement. The agreement must include provisions indicating the party to whom personal data may be surrendered and the conditions for such use.

3 Regulate any use of subcontractors in the agreement

If the data processor makes use of subcontractors for the provision of services, this must be clearly indicted in the agreement between the data processor and the data controller. Section 2-15 of the Personal Data Regulations prescribes security requirements for other undertakings - the contracting party.

4 Protect the rights of the data subject

The agreement may specify the division of work between the controller and the processor, for example who is to handle and process inquiries from the data subjects. A typical example is that the controller receives an inquiry, forwards it to the processor who then answers the data subject's inquiry. This could for example be questions concerning

- Access; see section 18 of the Personal Data Act,
- Rectification and deletion; see sections 27 and 28 of the Personal Data Act,

5 The agreement must require the data processor to have satisfactory information security

The requirements for satisfactory information security are laid down in section 13 of the Personal Data Act. The agreement must clarify what the data processor needs to have in place regarding security measures to safeguard confidentiality, integrity and accessibility in connection with the processing of personal data; see chapter 2 of the Personal Data Regulations.

What must be done to safeguard:
Confidentiality: make sure that data are only available to the persons who are to have access to them.
Integrity: prevent unauthorised or inadvertent change to personal data.
Accessibility: ensuring access to personal data where accessibility is necessary.

The agreement should include provisions on:

- Data Breach notification; see section 2-6 of the Regulations.
- Clarification of who is liable for giving notice of the discrepancy to the Data Protection Authority if the discrepancy has resulted in the unauthorised disclosure of personal data.
- Access control and adequate control mechanisms, for example log-keeping.
- Other requirements resulting from chapter 2 of the Regulations:
    - Confidentiality
    - Security audits
    - Physical security measures
    - Documentation of procedures etc.
    - Persons that are to have access to the personal data

Both parties have an independent responsibility under section 13 of the Personal Data Act, see chapter 2 of the Personal Data Regulations, and the agreement may regulate each contractual partners responsibilities.

6 Term of agreement

The agreement must include:

- Information about the term of agreement
- What is to be done with the data after expiry of the agreement – whether the data are to be restored or deleted and whether back-up copies are to be restored or deleted.
- How often a security audit is to be made.

7 Transfer to other countries

If the personal data are to be transferred to other countries, this must be regulated in the agreement. Reference is made to sections 29 and 30 of the Personal Data Act. For further information about this, see the Data Inspectorate's website.