Contracts between data controllers and data processors

At a glance

- Whenever a data controller uses a data processor it needs to have a written contract in place.
- The contract is important so that both parties understand their responsibilities and liabilities.
- Data controllers remain liable for their compliance with the DPL even if the processing of personal data is delegated.

Data processors must only act on the documented instructions of a controller. Data processors which breach their contractual obligations may be liable for damages to the affected data controller. The Ombudsman has certain investigatory powers, non-compliance with which may lead to prosecution.

Checklist

Contracts must include the following mandatory terms:

- the data processor must only act on the written instructions of the data controller (unless required by law to act without such instructions);
- the data processor must take appropriate measures to ensure the security of processing.

Contracts should, as a matter of good practice, include the following details:

- the subject matter and duration of the processing;
- the nature and purpose of the processing;
- the type of personal data and categories of data subject; and
- the obligations and rights of the controller.

Contracts should include the following terms:

- the data processor must ensure that people processing the data are subject to a duty of confidence;
- the data processor must only engage a sub-processor with the prior consent of the data controller and a written contract;
- the data processor must assist the data controller in providing subject access and allowing data subjects to exercise their rights under the DPL;

- the data processor must assist the data controller in meeting its DPL obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- the data processor must delete or return all personal data to the controller as requested at the end of the contract; and
- the data processor must submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their legal obligations, and tell the controller immediately if it is asked to do something infringing the DPL.

As a matter of good practice, our contracts:

- state that nothing within the contract relieves the data processor of its own direct responsibilities and liabilities under the DPL; and
- reflect any indemnity that has been agreed.

Checklist

In addition to the obligations set out in the checklist above, a data processor should practice the following best practices. The data processor must:

- co-operate with the Ombudsman in accordance with Part 6 of the DPL;
- ensure the security of its processing in accordance the seventh data protection principle; and
- notify any personal data breaches to the controller in accordance with section 16 of the DPL.

A data processor should also be aware that:

- it may be subject to investigative and corrective powers of the Office of the Ombudsman under Part 6 of the DPL;
- if it fails to meet its obligations, the data controller may be subject to an administrative fine under section 55 of the DPL.

In brief

When is a contract needed?

Whenever a data controller uses a data processor (a recipient who processes personal data on behalf of the controller) it should have a written contract in place. Similarly, if a data processor employs another sub-data processor, it needs to have a written contract in place, as it will be a data controller towards that data processor.

Appropriate contractual measures will be an important aspect of assessing your compliance with the seventh data protection principle (security – integrity and security).

This obligation may overlap with your obligations under the eighth data protection principle (international transfers) where you transfer personal data outside the Cayman Islands.

What needs to be included in the contract?

Contracts must include as a minimum the following terms, requiring the processor to:

- only act on the written instructions of the data controller;
- take appropriate measures to ensure the security of processing.

Where the data processor has a limited need to use personal data for its own purposes (e.g. to comply with legal/regulatory requirements that apply to the data processor), this should be noted as an exception to the general rule that the data processor should only act on the data controller's instruction. In this case, the data processor will be a data controller in its own right, with all rights and obligations pursuant to the DPL.

Additionally, depending on the nature and scope of processing undertaken by the data processor and the risk posed, it might be appropriate to include additional requirements, for example those requiring the data processor to:

- ensure that all staff processing the data are subject to a duty of confidence;
- only engage sub-processors with the prior approval of the data controller and under a written contract;
- assist the data controller in providing subject access and allowing data subjects to exercise their rights under the DPL;
- assist the data controller in meeting its DPL obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the data controller as requested at the end of the contract; and
- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their obligations under the DPL, and tell the data controller

immediately if it is asked to do something infringing the DPL or other data protection law.

Where the processing undertaken by the data processor is particularly complex, or affects many different types of data subjects and/or personal data, it might be desirable for the contract to explain the specific context in which processing is performed, for example by specifying the subject matter and duration of the processing, the nature and purpose of the processing, and the type of personal data and categories of data subject.

We are aware that it may be difficult for some local data controllers to get larger organizations to amend their standard DPAs that reference EU law. The requirements under the DPL are also found in EU law. An EU compliant DPA will consequently also be compliant under the Cayman DPL.

What responsibilities and liabilities do data processors have in their own right?

A data processor must only act on the documented instructions of the data controller. If a data processor determines the purpose and means of processing (rather than acting only on the instructions of the controller) then it will be considered to be a data controller and will have the same liability as any data controller.

In addition to its contractual obligations to the data controller, a data processor must also comply with the seventh data protection principle (security – integrity and security), by ensuring that equivalent obligations as those imposed on the data controller are observed.

The data processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorization of the data controller;
- to co-operate with the Office of the Ombudsman;
- to ensure the security of its processing;
- to document their processing activities; and
- to notify any personal data breaches to the data controller without delay.

If a data processor fails to meet any of these obligations or acts outside or against the instructions of the data controller, then it may be liable to pay damages in legal proceedings or be subject to fines or other penalties or corrective measures.

If a data processor uses a sub-processor then it will, as the original data processor, remain directly liable to the data controller for the performance of the sub-processor's obligations.

Relevant provisions

Data Protection Law, 2017

Schedule 1, Part 2, para 3: Processing contract to ensure reliability

Part 6: Enforcement