Data Security Standard 10

Accountable suppliers

The bigger picture and how the standard fits in

2018
# Contents

## Overview

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Overview</td>
<td>3</td>
</tr>
</tbody>
</table>

## Know your suppliers

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Who they are</td>
<td>4</td>
</tr>
<tr>
<td>Supply chains</td>
<td>5</td>
</tr>
<tr>
<td>Cloud supplier</td>
<td>5</td>
</tr>
<tr>
<td>Contracts</td>
<td>6</td>
</tr>
<tr>
<td>When is a contract needed?</td>
<td>7</td>
</tr>
<tr>
<td>Why are contracts between controllers and processors important?</td>
<td>7</td>
</tr>
<tr>
<td>What needs to be included in the contract?</td>
<td>7</td>
</tr>
<tr>
<td>Can standard contracts clauses be used?</td>
<td>8</td>
</tr>
<tr>
<td>What responsibilities and liabilities do processors have in their own right?</td>
<td>8</td>
</tr>
</tbody>
</table>

## Due diligence

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Prior to starting a new contract</td>
<td>9</td>
</tr>
<tr>
<td>Organisations interaction’ with the ICO</td>
<td>9</td>
</tr>
<tr>
<td>Penalties and prosecution</td>
<td>9</td>
</tr>
<tr>
<td>Enforcement notices</td>
<td>10</td>
</tr>
<tr>
<td>Audits and advisory</td>
<td>10</td>
</tr>
<tr>
<td>Other sources of information</td>
<td>10</td>
</tr>
<tr>
<td>Specific GDPR compliance by suppliers</td>
<td>10</td>
</tr>
<tr>
<td>During a contract</td>
<td>11</td>
</tr>
<tr>
<td>Managing contract disputes</td>
<td>12</td>
</tr>
</tbody>
</table>

## Appendix 1

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Table of Data Security Level 10 Assertions</td>
<td>14</td>
</tr>
</tbody>
</table>

## Appendix 2

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Useful resources</td>
<td>15</td>
</tr>
</tbody>
</table>

## Appendix 3

<table>
<thead>
<tr>
<th>Section</th>
<th>Page</th>
</tr>
</thead>
<tbody>
<tr>
<td>Data security reports</td>
<td>17</td>
</tr>
</tbody>
</table>
Overview

The National Data Guardian’s (NDG) Data Security Standard 10 - Accountable suppliers, states that

“IT suppliers are held accountable via contracts for protecting the personal confidential data they process and meeting the National Data Guardian’s Data Security Standards.”

IT suppliers understand their obligations as data processors under the GDPR, and the necessity to educate and inform customers, working with them to combine security and usability in systems. IT suppliers typically service large numbers of similar organisations and as such represent a large proportion of the overall ‘attack surface’. Consequently, their duty to robust risk management is vital and should be built into contracts as a matter of course. It is incumbent on suppliers of all IT systems to ensure their software runs on supported operating systems and is compatible with supported internet browsers and plug-ins.
Know your suppliers

Who they are

You should know your suppliers of IT which handle personal information, IT services and your suppliers, which may not be primarily IT based, but have an IT element.

Dependent on the type of organisation, this may be an easy or a more complex task. For example, for small social care providers this should be relatively easy, whereas for larger organisations or groups this might be more challenging.

In Data Security Standard 2, there is a requirement to demonstrate that you know which systems hold personal confidential information. In that Standard you recorded both digital and paper-based information assets, but for this Standard you only need to record digital systems.

The information that should be recorded is the products and services they deliver, their contact details and the contract duration, as in the example below:

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Products</th>
<th>Services</th>
<th>Contract</th>
<th>Start and end date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Care Planning System</td>
<td>Care Planning Product</td>
<td>Cloud based care planning system</td>
<td>C:\Contract\IT\CPS</td>
<td>dd/mm/yyyy – dd/mm/yyyy</td>
</tr>
<tr>
<td>eRoster</td>
<td>eRoster Pro</td>
<td>Web based staff rostering system</td>
<td>\sharepoint\contract\IT\eRoster</td>
<td>dd/mm/yyyy – dd/mm/yyyy</td>
</tr>
<tr>
<td>Outsourced HR advice</td>
<td>HR advice</td>
<td>Service to provide HR advice and guidance</td>
<td>Manager’s filing cabinet</td>
<td>dd/mm/yyyy – dd/mm/yyyy</td>
</tr>
<tr>
<td>Outsourced Payroll Service</td>
<td>Payroll product name</td>
<td>Outsourced payroll service</td>
<td>Manager’s filing cabinet</td>
<td>dd/mm/yyyy – dd/mm/yyyy</td>
</tr>
</tbody>
</table>

The organisation can name its suppliers, the products and services they deliver and the contract durations.

Data Security Standard 10.1

Under the General Data Protection Regulation (GDPR), social care organisations are called “controllers”. Your suppliers are called “processors”. This is because you determine how and why your suppliers process the data or information you give them. “Processing” is any way in which data or information can be used, stored, collected, created, destroyed or organised.

As a controller, you are expected to know and provide direction to your suppliers. There is advice in Appendix 2 about this.
Supply chains

When it comes to identifying suppliers, it is easy to identify those whose primary business and contract relate to IT systems.

However, not every contract is readily identifiable as having an IT systems component and a supplier may subcontract for the IT systems element.

Looking at our example of the outsourced HR service, it might not be obvious that they use an IT system in which they store personal confidential information from your organisation as this is bundled into a broader contract for services.

It is better to double check with all of your suppliers to see if they have systems which store any of your organisation’s personal confidential information. If they do, you need to make a record of this (see Data Security Standard 1 and the information flows guidance) and make sure that it is covered in your contracts.

There is no simple answer, but with increasing digitisation, it is safer to assume that any sizeable contract will have an IT system within it that may contain personal confidential data.

Cloud supplier

Any sizeable cloud contract will invariably mean moving some personal confidential data into the cloud. A cloud contract with storage containing personal confidential data should be included as a system. As in our example of the cloud-based care planning system.

"Knowing your suppliers well is vitally important."

Darren Mort, NHS Digital

MANDATORY - The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.

Data Security Standard 10.1.1
Contracts

As well as knowing their nature and length, contracts should be reviewed to ensure GDPR compliance as stated in Article 28 of the GDPR. Under Article 28, controllers must only appoint processors who can provide “sufficient guarantees” to meet the requirements of the GDPR.

Many of the contractual obligations necessary to comply with GDPR were already required under the Data Protection Act (DPA) 1998 and/or NHS Standard Contracts (where applicable) - key components are set out in NDG Data Security Standard 1: Personal confidential data.

The GDPR introduces some key changes that must be incorporated within third party contracts to reflect the new obligations placed on data processors by Article 28. For example:

- the data processor's liabilities in respect of a breach of GDPR;
- the data processor's liability for a breach by one of their sub-contractors.

You should consider how you will:

- review third party contracts;
- update contracts to reflect new responsibilities;
- address non-compliance by your third-party contractors.

The GDPR makes written contracts between controllers and processors a general requirement, rather than just a way of demonstrating compliance with the seventh data protection principle (appropriate security measures) under the DPA.

These contracts must now include certain specific terms, as a minimum.

These terms are designed to ensure that processing carried out by a processor meets all the requirements of the GDPR (not just those related to keeping personal data secure).

The GDPR gives processors responsibilities and liabilities in their own right, and processors as well as controllers may now be liable to pay damages or be subject to fines or other penalties.
When is a contract needed?

Whenever a controller uses a processor (a third party who processes personal data on behalf of the controller), it needs to have a written contract in place. Similarly, if a processor employs another processor it needs to have a written contract in place.

Why are contracts between controllers and processors important?

Contracts between controllers and processors ensure that they both understand their obligations, responsibilities and liabilities. They help them to comply with the GDPR and help controllers to demonstrate their compliance with the GDPR. The use of contracts by controllers and processors may also increase peoples’ confidence in the handling of their personal data.

What needs to be included in the contract?

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

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- notify the controller without undue delay if it becomes aware of a breach of the personal data it is processing on behalf of the controller;
- delete or return all personal data to the 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 Article 28 obligations, and tell the controller immediately if it is asked to do something that would infringe the GDPR or other data protection law of the EU or a member state.
Can standard contracts clauses be used?

Where suppliers hold personal data on your behalf and they act as processors they may only process the data in accordance with your written instructions. This means that legally the processor must not disclose information to anyone else unless they have told you about the request beforehand and you have told them to comply with it (**you should consider making this requirement explicit in the contract**). Where the processor is required by law to disclose information, they still need to inform you but are not seeking your permission. The only exception to this is where the law also requires that your organisation (as controller) is not informed about the disclosure. Such a case might arise where access to information held by the processor is required by a court order, where the data controller is the subject of an investigation.

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

A processor must only act on the documented instructions of a controller. If a 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 controller and will have the same liability as a controller. In addition to its contractual obligations to the controller, under the GDPR, a processor also has the following direct responsibilities:

- not to use a sub-processor without the prior written authorisation of the data controller;
- to co-operate with supervisory authorities (such as the ICO);
- to ensure the security of its processing;
- to keep records of processing activities;
- to notify any personal data breaches to the data controller;
- to employ a data protection officer; and
- to appoint (in writing) a representative within the European Union if needed.

If a processor fails to meet any of these obligations or acts outside or against the instructions of the 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 processor uses a sub-processor then it will, as the original processor, remain directly liable to the controller for the performance of the sub-processor’s obligations.

Contracts with all third parties that handle personal information are compliant with GDPR.

Data Security Standard 10.1.2
Due diligence

Prior to starting a new contract

Due diligence involves researching organisations so that you can be assured of their compliance with data protection laws and the NDG Data Security Standards.

The Information Commissioner’s Office (ICO) provides many resources to check the status of any organisation.

Check the organisation’s registration details for GDPR. A link to the registration portal is in Appendix 2.

Organisation’s interaction with the ICO

Part of your due diligence can include looking at the organisation’s interactions with the ICO.

The ICO is the regulatory body for data protection in the UK. The ICO has three levels of interactions with organisations:

- Penalties and prosecution
- Enforcement Notices
- Audits & Advisory

Penalties and prosecution

The most serious action the ICO can take can involves monetary penalties or prosecution.

https://ico.org.uk/action-weve-taken/enforcement/
**Enforcement notices**

Deemed less serious than monetary penalties, an enforcement notice would lay out a course of action the organisation should do to correct a deficiency(s) in data protection. The enforcement notice actions are normally signed off by the chief executive of the organisation that requires improvement. Enforcement notices can lead to monetary penalties if the required actions specified in the enforcement are not undertaken.

https://search.ico.org.uk/ico/search/decisionnotice

**Audits and advisory**

Audits and advisory can be self-initiated and are seen as demonstrating how an organisation can improve its data protection compliance. They are not binding, like enforcement notices.


In looking at the action the ICO can take, it must be noted that such action represents a point in time. There are plenty of examples of organisations which have changed their business following interaction with the ICO. It should also be remembered that given the newness of GDPR, all the actions are likely to come from its predecessor, the Data Protection Act 1998.

**Other sources of information**

As part of your due diligence activities you can also look into the news and sector specific publications which may contain details of breaches that are still under investigation by the ICO (thus not published).

**Specific GDPR compliance by suppliers**

Given the newness of GDPR, it is difficult to see how any organisation can be completely compliant in the early stages. However, organisations can be prepared, and some will be better prepared than others.

A way of measuring preparedness for GDPR is to review the ICO checklist and the health and care GDPR checklist. The health and care GDPR checklist is best suited to suppliers who process patient / service user information and have been working with the previous IG Toolkit. The ICO checklist is more general and therefore could be used for suppliers who process non-health personal data, i.e. of their staff.
The Care Provider Alliance have also produced some sector specific material to support care providers in GDPR compliance.

Both checklists and the CPA website are linked in Appendix 2:

**During a contract**

Existing suppliers should be asked about their preparedness for GDPR. This can entail asking the supplier to complete the general ICO checklist or the health and care GDPR checklist for suppliers which process patient and service user information.

Alternatively, if a supplier supplies their own plans for GDPR preparedness, they should be checked against the ICO or health and care GDPR checklist to ensure completeness. This is especially important where you receive blanket assurances from suppliers, stating that they are fully compliant with GDPR in a relatively short time after it passes into law.

**MANDATORY - Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance.**

Data Security Standard 10.2.1
## Managing contract disputes

As well as the usual business contract monitoring process, any disputes with suppliers that have a data security or data protection implication should be recorded.

These include incidents that meet the threshold as being reportable / notifiable, as well as ones that are beneath that bar.

Remember under GDPR, processors can report incidents independently, including ones concerning the data controller.

An example of a list of disputes with supplier/controllers is shown below:

<table>
<thead>
<tr>
<th>Supplier</th>
<th>Products</th>
<th>Incident</th>
<th>Escalation</th>
<th>Start and end date</th>
</tr>
</thead>
<tbody>
<tr>
<td>Care Planning System</td>
<td>Care Planning Product</td>
<td>Supplier won’t encrypt its primary service user index. Although other modules are encrypted.</td>
<td>Escalated to supplier via admin. dd/mm/yy</td>
<td>dd/mm/yy – dd/mm/yy</td>
</tr>
<tr>
<td>eRoster</td>
<td>eRoster Pro</td>
<td>The rostering templates for another organisation (with different start / end times) was applied to our organisation causing confusion and problems at changeover. May have affected care.</td>
<td>Not a data loss but logged on SIRI Level 2 and subject to a full audit and outcomes.</td>
<td>dd/mm/yy – dd/mm/yy</td>
</tr>
<tr>
<td>Outsourced HR advice</td>
<td>HR advice</td>
<td>Their datacentre was hacked and data exfiltrated containing staff medical information.</td>
<td>Logged on SIRI tool level 2 &amp; reported to ICO and under investigation.</td>
<td>dd/mm/yy – dd/mm/yy</td>
</tr>
<tr>
<td>Outsourced Payroll Service</td>
<td>Payroll product name</td>
<td>Staff have received increased targeted phishing emails to the email they receive payslips to. Supplier denies any incident has occurred.</td>
<td>Under investigation</td>
<td>dd/mm/yy – dd/mm/yy</td>
</tr>
</tbody>
</table>
All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.

Data Security Standard 10.3
# Appendix 1 -
## Table of Data Security Level 10 Assertions

<table>
<thead>
<tr>
<th>Assertion</th>
<th>Mandator</th>
<th>Sub Assertion</th>
<th>Evidence</th>
</tr>
</thead>
<tbody>
<tr>
<td><strong>10.1 The organisation can name its suppliers, the products and services they deliver and the contract durations.</strong></td>
<td>Yes</td>
<td>10.1.1</td>
<td>The organisation has a list of its suppliers that handle personal information, the products and services they deliver, their contact details and the contract duration.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>10.1.2</td>
<td>Contracts with all third parties that handle personal information are compliant with GDPR.</td>
</tr>
<tr>
<td><strong>10.2 Basic due diligence has been undertaken against each supplier according to ICO and NHS Digital guidance.</strong></td>
<td>Yes</td>
<td>10.2.1</td>
<td>Basic due diligence has been undertaken against each supplier according to ICO guidance.</td>
</tr>
<tr>
<td></td>
<td>No</td>
<td>10.2.4</td>
<td>The person with overall responsibility for data security is assured that suppliers who are Data Processors are prepared for GDPR.</td>
</tr>
<tr>
<td><strong>10.3 All disputes between the organisation and its suppliers have been recorded and any risks posed to data security have been documented.</strong></td>
<td>No</td>
<td>10.3.1</td>
<td>List of data security incidents – past or present – with current suppliers.</td>
</tr>
</tbody>
</table>
Appendix 2 - Useful resources

Care Provider Alliance

Has an Introduction to Cyber Security for Social Care Organisations and also provides examples of third party contracts.


Cyber security risks in the supply chain: National Cyber Security Centre

An introduction to cyber security risks in supply chains and also provides examples to highlight the benefits of an inclusive approach.

https://www.ncsc.gov.uk/guidance/cyber-security-risks-supply-chain

Guide to GDPR accountability and governance contracts: Information Commissioner’s Office


GDPR Regulations: The European Parliament and the Council of the European Union

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).


GDPR guidance contracts and liabilities between controllers and processors: Information Commissioner’s Office

These pages sit alongside our overview of the GDPR and provide more detailed, practical guidance for UK organisations on contracts between controllers and processors under the GDPR.

GDPR checklist: Information Commissioner’s Office

Designed to help you, as a controller understand and assess your high-level compliance with data protection legislation. Includes the new requirements for data processors, the rights of individuals, data breaches, and designating a data protection officer, under the upcoming General Data Protection Regulation.


Health and care GDPR checklist: Information Governance Alliance

The objective is to provide guidance on the steps organisations should consider taking to build on the work they will already have completed when undertaking annual Toolkit assessments. The checklist provides guidance on:
• the new legal obligations;
• reviewing your existing data protection framework to identify gaps;
• implementing measures that are necessary to comply with GDPR.

https://digital.nhs.uk/information-governance-alliance/General-Data-Protection-Regulation-guidance
Appendix 3 –
Data security reports

The National Data Guardian review

Recommendations to improve security of health and care information and ensure people can make informed choices about how their data is used.

Review of Data Security, Consent and Opt-Outs

The government response

‘Your Data: Better Security, Better Choice, Better Care’ is the government’s response to:

- the National Data Guardian for Health and Care’s ‘Review of Data Security, Consent and Opt-Outs’;
- the public consultation on that review;
- the Care Quality Commission’s Review ‘Safe Data, Safe Care’.

It sets out that the government accepts the recommendations in both the National Data Guardian review and the Care Quality Commission review.

It also reflects on what we heard through consultation to set out immediate and longer-term action for implementation.

Your Data: Better Security, Better Choice, Better Care