DOCUMENT RETENTION: DATA STORAGE AND RETENTION PERIODS

Document retention is the storage of company and personal data in accordance with company policy and statutory obligations.

Every company and other organisation must deal with the growing amount of data created and collected by it and its employees. The exponential growth in electronic data has resulted in data storage costs becoming a substantial cost item. There is a need to limit data storage. Can data be destroyed after a certain period of time? This process has various legal aspects that must be taken into account.

Cost reductions can be achieved by limiting data storage without negatively affecting the company's statutory obligations and legal position.

In Dutch law, certain company data is subject to a minimum retention period, whereas personal data is subject to a maximum retention period. In addition, to protect the interests of the company, the validity periods and limitation periods applicable to agreements and compensation claims must, as much as possible, be taken into account when making decisions relating to the retention and destruction of data. Should a dispute arise, the company must have access to all the information needed to defend itself.

Litigation commenced in the United States, or an investigation commenced by a regulator or supervisory body, may involve an unexpectedly far-reaching document discovery process or a mandatory order for the production of documents. (See also the chapter entitled "e-Discovery and privacy: The eternal dilemma".) Because the destruction of data may directly conflict with obligations relating to this, a clear policy for data retention and data destruction is recommended. This helps achieve a reduction in costs relating to data storage, but without negatively affecting a company's ability to comply with its statutory obligations or to defend its legal position in a dispute

General obligation to retain company data

A Dutch legal entity (*rechtspersoon*) is required[1] to maintain records and retain the associated documents and data carriers in such a way that the rights and obligations of the legal entity can always be ascertained. In addition, information relevant to taxation must always be clear from the records.[2] Relevant documents and data carriers must be retained for a minimum period of seven years.[3]

Dutch law also explicitly identifies a limited number of documents that must be retained, e.g. the balance sheet and profit and loss account of a legal entity.[4] But the law is silent on the other documents that must be retained. It will depend on the type of organisation, but in any case the documents to be retained generally include agreements, permits and licences, staff records, accounting information (including about receivables and debts) and the associated relevant correspondence.

Other specific retention obligations may apply in certain business sectors. For example, the financial sector is subject to an obligation to retain all data obtained in the context of a customer due-diligence investigation for five years after the end of the business relationship[5] and an obligation to retain reports about unusual transactions for at least five years after this was reported.[6]

Maximum retention periods for personal data

If the documents and data retained contain personal data, the Dutch Data Protection Act (Act)[7] is applicable. The Act does not set specific minimum or maximum retention periods, but it does state that personal data cannot be retained longer than necessary for the purposes for which the data are collected or used.[8] The maximum retention period for personal data stated in the proposal published on 25 January 2012 for the EU's new privacy regulation ("proposed regulation")[9] is lower, and the proposal also states that the

Personal data may not be retained longer than necessary for the purposes for which the data are collected or used.

[1] Dutch Civil Code, art. 2:10(1). Article 3:15i states a similar obligation for the self-employed and professional practitioners.

[2] State Taxes Act, art. 52(1).

[3] Dutch Civil Code, art. 2:10(4); State Taxes Act, art. 52(4).

[4] Dutch Civil Code, art. 2:10(2).

[5] Prevention of Money Laundering and Terrorist Financing Act, art. 33; Decree relating to Prudential and Valuation Rules under the Financial Supervision Act, art. 14.

[6] Prevention of Money Laundering and Terrorist Financing Act, art. 34.

[7] Bulletin of Acts and Decrees 2000, 302.

[8] Data Protection Act, art. 10.

[9] Proposal for a Regulation of the European Parliament and of the Council on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation), 25/1/2012, COM(2012) 11 final. Found at http://ec.europa.eu/justice/data-protection/document/review2012/com_2012_11_en.pdf. ("proposed regulation")

storage period for personal data must be kept to "a strict minimum".[10]

The Act imposes a notification requirement on the processing of personal data. Under a law called the Data Protection Act Exemption Decree (DPAED),[11] exemptions are allowed in certain situations; however, these exemptions are effective only for certain time periods. If personal data is retained for longer than these time periods, the exemption no longer applies and the processing of the personal data must be reported. While these time periods relate to the exemptions, they may also be seen as an indication of the maximum period that lawmakers consider necessary for the retention of personal data in these situations.[12] The table below illustrates the indicative maximum retention periods relating to various types of personal data:

Type of personal data	Notification exemption period / Indication of maximum retention period	Statutory reference
Employee data	2 years after end of employment	DPAED, art. 7:5
Debtors / creditors	2 years after receivable paid	DPAED, art 12:6
Subscriptions	2 years after end of subscription	DPAED, art. 11:5
Job applicants	4 weeks after end of job application procedure, unless permission is obtained for a year	DAPED, art 5:6

Storage method

For the most part, a company may determine how it meets its retention obligations. The documents and data to be stored may be retained in digital form, as long as they are available during the full retention period and can be made legible within a reasonable period of time. Several documents are also subject to an additional requirement that they be retained in paper form, i.e. the balance sheet and profit and loss account.[13]

The Act requires a controller to take suitable technical and organisational measures to secure the personal data against loss or any form of wrongful processing.[14] The proposed regulation further elaborates and refines this obligation. Article 23 of the proposed regulation provides that, in determining the processing method and on conducting the process, a controller must implement technical and organisational measures and procedures so that the processing complies with the conditions of the proposed regulation and ensures that a data subject's rights are protected. Furthermore, technical measures must be taken to ensure that the collection or retention of data is limited to the amount and the period strictly necessary in view of the objectives. A company could potentially rely on a document retention policy as one way of carrying out the obligation to implement suitable technical and organisational measures and procedures.

In determining the fine after a security breach resulting from a violation of the proposed regulation, the extent to which the measures required by article 23 were implemented will be taken into account.[15] The lack of an internal policy, or the lack of suitable measures to comply with the proposed regulation (including the article 23 measures), can result in a fine of 2% of the annual worldwide turnover of a company in the case of an intentional or negligent act or omission.[16]

Retention obligations in practice–Document retention policy

Companies and institutions frequently retain many more documents and much more data than strictly necessary, and they do so for a period longer than required by law. Furthermore, the same documents are, in practice, often stored in different locations at the same time. This leads to an unnecessary burden on the company's storage capacity, particularly if a company does not have clear guidelines on what should or should not be stored and if there are no physical or digital limitations on the amount of data stored. Setting a maximum size for mailbox capacity and/or digital archive capacity can be helpful with this.

A document retention policy creates clarity about retaining and destroying documents.

To make this clearer, a company can introduce a "document retention policy" about retaining and destroying documents. A document retention policy would determine the following for each type of document: (i) how it must be stored, (ii) in what form, (ii) in which physical or digital location and (iv) who is responsible for it. Preparing such a policy document forces a company to actively consider how it wishes to deal with retaining and archiving documents. To limit the costs involved, the company should decide which documents are necessary and relevant, and how long they should be stored.

[10] Proposed regulation, consideration 30.

[11] Bulletin of Acts and Decrees 2001, 250.

[12] See also the information sheet published by the Dutch Data Protection Authority entitled "Retention periods for personal data in your hands", dated July 2012. Found at http://www.cbpweb.nl/Pages/inf_va_bewaartermijnen.aspx.

[13] Dutch Civil Code, art. 2:10(4).

[14] Data Protection Act, art. 13.

[15] Proposed regulation, art. 79:2.

[16] Proposed regulation, art. 79.6(e).

The following aspects must be taken into account:

1. the statutory retention periods;
2. data storage costs;
3. the need to have access to certain data as evidence in proceedings;
4. the obligation to submit data during a discovery or investigation process.

Providing evidence

Prior to signing a contract, the contract parties frequently have extensive e-mail contact. In some cases, many draft versions of contracts are exchanged. If and when a contract is finalised and signed, the relevance of the preparatory documentation decreases. Still, a situation could potentially arise in which it is useful to have this information, e.g. in a dispute over the interpretation of the contract according to the Haviltex criterion and later legal precedents.[17] If the agreement has expired, and all the obligations in the contract have been satisfied, the preparatory documentation will generally no longer be needed. The decision whether or not to retain such correspondence will involve a consideration of the risks involved in destroying it.

If a company is or may be involved in civil proceedings in the United States, or if the company is under investigation pursuant to regulatory legislation or foreign law, including the US Foreign Corrupt Practices Act (FCPA)[18] or the UK Bribery Act 2010,[19] the company may be required to make available all the relevant information under its control to the other party and/or the regulator. (For more detailed information about this, see also the chapter entitled "e-Discovery and privacy: The eternal dilemma"). If a company has destroyed this information, and there is evidence at that time or later that this information existed, in such civil proceedings the simple fact that the information has been destroyed will in most cases result in losing the case and the imposition of large punitive damages. In the event of regulatory and criminal proceedings, the consequences for the company would be high fines and restrictive measures. However, if relevant data is destroyed in accordance with a document retention policy that is based on objective criteria and consistently applied, this could serve as a legitimate defence on the part of the company.

[17] Supreme Court, 13 March 1981, NJ 1981, 635 (Ermes/Haviltex). See also Supreme Court, 19 January 2007, NJ 2007, 575 (Meijer/Pontmeyer).

[18] See "Foreign Corrupt Practices Act: An Overview". Retrieved 27 March 2013 from http://www.justice.gov/criminal/fraud/fcpa/.

[19] See UK *Bribery Act 2010*, 2010 Chapter 23. Retrieved 27 March 2013 from http://www.legislation.gov.uk/ukpga/2010/23.

4

Introducing a document retention policy

The success of a document retention policy depends on good communications about the intent and implementation of the policy, and its acceptance by the company. It is extremely important to make the employees aware of the importance of the document retention policy and its consistent implementation, both from a risk-control aspect (i.e. retaining the correct documents) and a cost-control aspect (i.e. not retaining documents unnecessarily). It may be helpful to share information with employees about the cost of unnecessary data storage.

The success of a document retention policy depends on good communication and the policy's implementation and acceptance by the company.

A document retention policy should cover not only the decision to retain documents and data, but also the decision to destroy certain documents after time has passed. For documents subject to a maximum statutory retention period, such as documents containing personal data, destruction is mandatory. The company must decide whether to destroy documents after the minimum statutory retention period in the Dutch Civil Code and tax legislation has passed. In the event of a discovery process or a criminal or other investigation, it will be in the company's benefit to be able to demonstrate that the document retention policy was implemented consistently.

Tips & Tricks

- Make a summary of the different types of information stored in the company.
- Determine which minimum or maximum retention periods apply for this information.
- With the approval of the works council or the employee representation body, establish a document retention policy that determines the following for each type of information and document:
  - how long it is to be stored;
  - in what form;
  - at which physical or digital location; and
  - who is responsible for it.
- Communicate the document retention policy internationally to existing and new employees.
- Provide regular information and training to create employee awareness of the policy.
- Distribute a short data retention guide listing the principles that must be observed when purging files and mailboxes.
- To encourage the timely deletion of non-relevant e-mails and data, set a maximum size for the e-mail inbox capacity and/or a maximum length for the retention period for e-mails.
- Ensure that employees store digital documents and other data only on company equipment, and not on their own personal devices.
- If the company permits "BYOD" (Bring Your Own Device), make sure the document retention policy is also implemented on these devices.
- Ensure that employees leaving the company purge their e-mail inbox and, where necessary, provide their colleagues with access to this.
- Inform employees about the costs of data storage.
- Emphasise the importance of using the data retention guide when purging e-mails and data.
- Ensure that stored documents are purged regularly. The need or desire to retain a particular document can decrease over time. Be sure to consider backups as well.
- Have a user panel and the IT department regularly evaluate the document retention policy.

The members of the Houthoff Buruma Privacy Team:

Wolter Wefers Bettink
Partner at Houthoff Buruma, Dutch lawyer specialising in IP and IT litigation, privacy and e-business
T +31(20)605 6167 | w.bettink@houthoff.com

Thomas de Weerd
Partner at Houthoff Buruma, Dutch lawyer specialising in IT law, outsourcing, privacy and e-business
T +31(20)605 6985 | t.de.weerd@houthoff.com

Copyright © 2013 Houthoff Buruma

All rights reserved. Short passages from this edition may be used in other publications, under the condition that the source is clearly cited. We prefer the use of the following form: "Privacy: Tips & Tricks for Companies, Houthoff Buruma".

Apart from this, no part of this publication may be reproduced, stored in an automated filing system, transmitted in any form or by any means, electronic, mechanical, photocopying, recording or otherwise, without the prior written permission of Houthoff Buruma. This publication is provided for informational purposes only and does not constitute legal advice. This publication has been compiled with the utmost care; nevertheless, Houthoff Buruma cannot be held liable for any errors or inaccuracies, nor any associated consequences.