DATATILSYNET

Odense Kommune
Flakhaven 2
5000 Odense C

Sent to: odense@odense.dk and
aps@odense.dk

3 February 2011

The Danish Data
Protection Agency
Borgergade 28, 5.
DK-1300 Copenhagen K

Phone +45 3319 3200
Fax +45 3319 3218

E-mail
dt@datatilsynet.dk
www.datatilsynet.dk

J.no. 2010-52-0138
Ref.
Kristian Gyde Poulsen
Direct +45 3319 3215

Regarding processing of confidential and sensitive personal data in connection with use of Google Apps online office suit

1. The Danish Data Protection Agency hereby resumes the case regarding Odense Municipality's use of Google Apps online office suite with calendar and document processing features.

Via the Danish Data Protection Agency's notification system on 12 February 2010, Odense Municipality requested an advance opinion from the Danish Data Protection Agency regarding the municipality's planned use of the aforementioned cloud solution.

Odense Municipality wants teachers to use the solution when registering information about lesson planning and assessments of lesson plans and individual students' educational development. In addition, the teachers take notes on the classes and the students' cooperation and prepare letters to parents regarding their children. They also wish to use the solution for planning and sending invitations to meetings and distributing information about school-related activities.

According to Odense Municipality, this involves sensitive information including: data concerning health, serious social problems and other purely private matters.

In letters dated 4 October and 15 November 2010, Odense Municipality provided supplementary information.

2. The Danish Data Protection Agency discussed the matter in a meeting of the Data Protection Council and, on this basis, provides the following opinion:

2.1. When commencing the processing of personal data, the controller authority or company is responsible for structuring the processing of personal data to ensure compliance with the Act on Processing of Personal Data and the Executive Order on Security. As the controller authority, Odense Municipality's responsibilities include ensuring that the data about citizens processed by the municipality is at all times protected by the necessary security measures.

The Danish Data Protection Agency has not previously issued opinions on the use of a cloud solution in a specific area. The case presented involves sensitive personal data. Therefore, the Danish Data Protection Agency finds that there is a need to thoroughly consider whether the described cloud solution will meet the requirements that apply when a Danish administrative authority processes such data about citizens.

As the case is presented, the Danish Data Protection Agency sees problems in a number of areas, as described below, in relation to the requirements of the Act on Processing of Personal Data[1] and the Executive Order on Security[2]. Thus, the Danish Data Protection Agency does not concur with Odense Municipality's assessment that confidential and sensitive data about students and parents can be processed in Google Apps.

The Danish Data Protection Agency is willing to reconsider the case for a revised statement if Odense Municipality continues work on the case and seeks solutions to the identified issues.

In relation to some issues, it will be necessary to apply for a formal authorisation from the Danish Data Protection Agency for the proposed processing of sensitive personal data, cf. section 3.3 below.

In light of the case's principle character and potentially far-reaching consequences for the citizens of Odense Municipality, the Danish Data Protection Agency's view is that the decision of whether to use a solution of this kind in this area should be subject to an assessment by the municipality's political bodies.

2.2. The purposes of the Act on Processing of Personal Data's are threefold: Firstly, it aims to secure a continued high level of protection for individual citizens. Secondly, the law is intended to be flexible and provide the option of processing personal data with use of modern technologies. And lastly, a purpose of the law is to implement the EU's directive on the protection of personal data[3].

In line with these purposes, the Danish Data Protection Agency has a generally positive view of the use of new technologies, including, in principle, cloud computing. Meanwhile, the Danish Data Protection Agency also views one of its most important tasks as highlighting the fact that technological developments can represent increased risks to people's right to privacy and data protection.

---

[1] Act no. 429 of 31 May 2000 on Processing of Personal Data, with subsequent revisions

[2] The Danish Ministry of Justice's executive order no. 528 of 15 June 2000, as revised by executive order no. 201 of 22 March 2001, on security measures for the protection of personal data that is processed for public administration

[3] Directive 95/46/EEC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data

The level of data protection, which in Denmark is stipulated by the Act on Processing of Personal Data and the Executive Order on Security, must naturally be observed as a minimum. In regard to the specific plans presented by Odense Municipality, a number of questions arise in relation to this legislation. In short, these questions refer to five issues:

1) Any transmission of data to data centres located in other non-secure third countries than the USA requires a legal basis for such transmission, the existence of an agreement based on the EU Commission's standard contractual clauses and an application for authorisation from the Danish Data Protection Agency, for example.
2) The risk assessment conducted by Odense Municipality is, in the view of the Danish Data Protection Agency, inadequate. The Danish Data Protection Agency recommends the use of ENISA's checklist.
3) The processor agreement, which is planned to solely comprise of elements from Google's standard terms and conditions, does not meet the Act on Processing of Personal Data's requirement that Odense Municipality must secure that Google may only act on instructions from the municipality; nor does the processor agreement state that the Executive Order on Security applies to the data processing by Google.
4) The Danish Data Protection Agency questions whether Odense Municipality can meet the Act on Processing of Personal Data's requirements for control to ensure that the security measures are upheld by the processor, given that the municipality does not know where the data are physically located.
5) It is not indicated, or cannot be deemed adequately established based on the materials presented, how the Executive Order on Security's and the Act on Processing of Personal Data's requirements will be met in a number of areas, including:

    a. Deletion of data so that it cannot be recreated.
    b. Transmission and login. It is not indicated whether there is encryption between Google in Ireland and Google Inc.'s various data centres. With regard to login via internet with access to sensitive personal data, the Danish Data Protection Agency recommends the use of a solution with several factors, digital signature, for example.
    c. Control of rejected attempts to access data. There is no information regarding automatic rejection of attempts to access data by circumventing Odense Municipality's login server.
    d. With regard to the logging requirement under Section 19 of the Executive Order on Security, no information is provided about what data are logged or how long the log is stored.

Sections 3-9 below contain the Danish Data Protection Agency's assessments regarding the various issues in relation to the Act on Processing of Personal Data and the Executive Order on Security.

3. Transmission of data to third countries

3.1. Odense Municipality has stated that Google Ireland Limited is the processor in connection with the municipality's use of Google Apps.

Odense Municipality has furthermore stated that the data are physically located at Google Inc.'s data centres. According to Odense Municipality, Google has provided the following information about these data centres:

> "*Google applications run in a multi-tenant, distributed environment. Rather than segregating each customer's data onto a single machine or set of machines, Google Apps data from all Google customers (consumers, business, and even Google's own data) is distributed amongst a shared infrastructure composed of Google's many homogeneous machines and located across Google's many data centers.*"

Odense Municipality has stated that Google's data centres are located in the USA and Europe and that users in Europe and Denmark primarily get their data from data centres in Europe.

Odense Municipality has also stated that Google subscribes to the Safe Harbor programme and thus is obliged to cooperate with and comply with the data protection authorities in the EU, and that Odense Municipality, on this basis, considered the company to be the equivalent of a secure third country.[4]

Odense Municipality has lastly stated that the data centres in the USA and Europe in which the data are stored are owned by Google Inc.

According to the American Department of Commerce's website, Google Inc. has subscribed to the Safe Harbor Principles and that Google Inc. is subject to the powers of the Federal Trade Commission.[5]

In connection with processing this case, the Danish Data Protection Agency has obtained supplementary information via telephone from the American Department of Commerce, which stated that all companies in the Google Inc. group are subject to Google Inc.'s subscribing to the Safe Harbor Principles.

3.2. Section 27 of the Act on Processing of Personal Data contains special rules about transfer of personal data to countries outside of the EU (third countries).

3.3. Odense Municipality's transmission of data to the processor Google Ireland Limited in Ireland does not constitute a third country transmission subject to Section 27 of the Act on Processing of Personal Data, as Ireland is an EU member country.

---

[4] In connection with this, Odense Municipality refers to Google Apps' Security and Privacy documentation: http://www.google.com/support/a/bin/answer.py?hl=en&answer=60762

[5] http://safeharbor.export.gov/companyinfo.aspx?id=10543

Nor does the transmission of data to data centres located in EU member countries or EEA countries constitute a third country transmission subject to Section 27 of the Act on Processing of Personal Data.

However, the transmission of data to data centres in the USA and certain countries in Europe would constitute a third country transmission subject to Section 27.[6] As it has been stated that the personal data are physically located in Google's data centres, which are located in the USA and Europe, the Danish Data Protection Agency must take the view that the transmission of data to third countries will occur. These transmissions of data must comply with Section 27 of the Act on Processing of Personal Data.

The Danish Data Protection Agency's view is that, based on the information presented in the case, **Google Inc.'s data centres in the USA** are covered by Google Inc.'s subscribing to the Safe Harbor Principles and thus, as Google Inc., are subject to the powers of the Federal Trade Commission. Thus, it must be assumed that the data centres in the USA, in accordance with the EU Commission's decision of 26 July 2000, must be presumed to have an adequate level of protection. The transmission of personal data to these data centres will thus be permitted pursuant to Section 27(1) of the Act on Processing of Personal Data.

The transmission of data to **data centres located in other insecure third countries than the USA**, may only occur if the conditions in Section 27(3) or Section 27(4) of the Act on Processing of Personal Data are met. It has not been stated whether all of Google Inc.'s data centres in Europe are located within the EU/EEA.

Based on the information presented, it must be assumed that there is not the necessary compliance with Section 27(3) to transfer data to such data centres.

Furthermore, based on the information presented, it must be assumed that Odense Municipality has not entered into an agreement based on the EU Commission's standard contractual clauses with these data centres, nor has granted Google Ireland Limited a clear mandate to enter into agreements, in Odense Municipality's name and on behalf of Odense Municipality, based on the EU Commission's standard contractual clauses with such data centres. Thus, based on the information presented, the transmission cannot take place based on Section 27(4) of the Act on Processing of Personal Data either.

If data centres in Europe – but outside of the EU/EEA – are to be used, Odense Municipality and the individual data centres may enter into an agreement based on the EU Commission's standard contractual clauses, or Odense Municipality may grant Google Ireland Limited a clear mandate to enter into agreements, in Odense Municipality's name and on behalf of Odense Municipality, based on the EU Commission's standard contractual clauses with the

[6] This would be the case if the data centre is located in a European country that is not an EU member country or an EEA country.

individual data centres. In addition, it would be necessary to apply for authorisation from the Danish Data Protection Agency pursuant to Section 27(4) of the Act on Processing of Personal Data.

For further information on the area of application of the rules, refer to the Article 29 Working Party's document no. 176[7], which states that transmission of data from a processor in the EU to a sub-processor in a third country may occur 1) in cases where an agreement is entered into based on the EU Commission's standard contractual clauses directly between the controller in the EU and the sub-processor in the third country, and 2) in cases where the processor in the EU is granted a clear mandate to enter into agreements, in the processor's name and on its behalf, based on the EU Commission's standard contractual clauses with sub-processors in third countries.

4. General information on processing security in connection with Odense Municipality's use of Google Apps

4.1.1. As the controller, Odense Municipality must ensure that the necessary security measures are taken, cf. Section 41(3) of the Act on Processing of Personal Data.

Section 14 of the Executive Order on Security states that external communication connections may only be established if special measures are taken to ensure that unauthorised parties cannot gain access to personal data through these connections.

In the Danish Data Protection Agency's Guidance to the Executive Order on Security,[8] an explanation is provided regarding Section 14 of the Executive Order on Security that special security measures must be taken according to the authority's assessment of security risks in the specific situation, including with consideration of the nature of the data being processed. To determine the security level, it is necessary for the controller to conduct a comprehensive risk assessment including all elements of the communication connection.

To meet the Act on Processing of Personal Data's security requirements, in the view of the Danish Data Protection Agency, the controller must conduct a risk assessment in relation to the various aspects of a potential cloud solution, which is planned to be used for processing of sensitive personal data.

4.1.2. Odense Municipality has stated that the municipality has conducted a risk assessment. The municipality has attached this as an attachment to the municipality's e-mail of 4 October ("Risk assessment re. Google Apps – Summary"). The following is stated in the risk assessment:

---

[7] FAQs in order to address some issues raised by the entry into force of the EU Commission Decision 2010/87/EU of 5 February 2010 on standard contractual clauses for the transfer of personal data to processors established in third countries under Directive 95/46/EC

[8] Danish Data Protection Agency's guidance no. 37 of 2 April 2001 to executive order no. 528 of 15 June 2000 on security measures for the protection of personal data that is processed for public administration

> "The risk assessment was conducted in accordance with the principles for risk assessment described in the DS484 standard; the method does not comply slavishly with DS-484, but has minor modifications as described below."

Odense Municipality has further stated that the municipality's assessment of risk in relation to the tasks Google Apps is to be used for is a "medium" risk of loss of confidentiality when creating documents and "medium" risk of loss of integrity when sharing documents, while all other areas are assessed to have "low" risk.

In regard to the SAS 70 Type II Certification cited in the case, Odense Municipality has referred, in the e-mail of 4 October 2010, to the attached document "Google SAS70 Audit in relation to Odense's use of Google Apps", which contains the following conclusion:

> "The execution of an SAS70 Type II Audit at Google means that independent auditors have controlled and verified Google security practice within the areas of Google Apps for which Google, as the supplier to Odense Municipality, is responsible. On this basis, Odense Municipality finds that Google's security practice is adequate in relation to the Act on Processing of Personal Data's requirements on storage and deletion of data."

Odense Municipality has further stated that the municipality has had insight into Google's control targets, control policies, control processes and implemented controls, as well as into the cited SAS 70 Type II report. Odense Municipality has further stated that the auditor personally chooses which data centres it wishes to visit. Each year, the auditor has audited at least one data centre in the USA and one data centre in the EU. In the following year, they visit new/other data centres. The goal is that all data centres in which Google Apps data are located must be audited within three years of the original SAS 70 Type II certification in 2008.

Lastly, in the e-mail of 4 October 2010, Odense Municipality sent the document, "*Security Backgrounder – Google Apps Messaging and Collaboration Products*" to the Danish Data Protection Agency. This document states the following in regard to data stored in Google Apps (p. 6):

> "*Encryption is a commonly accepted way to protect data and Google regularly considers encryption for each of its applications. However, while encryption secures data, it also negatively impacts the speed of search and collaboration. For this reason, Google consciously decided not to encrypt Google Apps data at rest on its systems. The data is, however, 'obfuscated' or masked using proprietary algorithms. This makes the data very difficult to read, because access to Google's proprietary tools is required to unscramble the masked data. In combination with the company's restricted access policy and use of strong authentication mechanisms, the masking of data at rest maintains both the usability and privacy of data.*"

4.2. Based on the information provided, the Danish Data Protection Agency takes the view that Odense Municipality has conducted a risk assessment

based on the principles of DS 484; i.e., the risk assessment does not fully follow DS 484, but has minor modifications. The Danish Data Protection Agency also assumes that Odense Municipality has not conducted a risk assessment that considers the specific context in which the data from the municipality will be processed at Google.

Odense Municipality has further acknowledged that the municipality did not assess the technology used in the cloud solution in question from Google.

According to the document cited in section 4.1.2, "*Security Backgrounder – Google Apps Messaging and Collaboration Products*", "*Google consciously [has] decided not to encrypt Google Apps data at rest on its systems.*" Therefore, the Danish Data Protection Agency assumes that data stored at Google Ireland Limited and Google Inc.'s data centres are not encrypted.

Odense Municipality has not, in the materials submitted, conducted an assessment of the risks connected to the lack of encryption at Google Ireland Limited and Google Inc.'s data centres. This is an example of an area in which Odense Municipality, in the view of the Danish Data Protection Agency, is willing to run an unclear risk.

Taking the generally increased risk into account that, in the view of the Danish Data Protection Agency, must be assumed with cloud computing, the Danish Data Protection Agency's overall assessment is that Odense Municipality *has not* conducted an adequate risk assessment and that the municipality thus has not complied with Section 41(3) of the Act on Processing of Personal Data.

The Danish Data Protection Agency recommends that Odense Municipality utilise the approach outlined by ENISA in the publication, "*Cloud computing – Benefits, risks and recommendations for information security*", including the checklist found on pp. 71-82 in ENISA's publication.

5. The regulations of the Act on Processing of Personal Data regarding data protection requirements when using an external processor

5.1. Based on the information provided, Odense Municipality will use Google Ireland Limited as the processor in connection with Google Apps.

With regard to the requirement on a processor agreement, Odense Municipality has stated that the processor agreement between Odense Municipality and Google Ireland Limited is stated in sections 1.4 and 1.5 of "Google Apps General Terms".

Sections 1.4 and 1.5 of "Google Apps General Terms" are as follows:

> "*1.4 Privacy Policies. Customer acknowledges that it has chosen to have its End Users personal data processed by Google as part of the Services within the scope of the Services' capabilities, which are reflected in the Google Privacy Policies. Customer therefore instructs Google to provide the Services and*

process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same. The Google Privacy Policies are hereby incorporated by reference into this Agreement. Customer agrees to protect the privacy of End Users by complying with a policy communicated to End Users which is no less protective than the Google Privacy Policies.

1.5 Data Protection. In Section 1.4 and Section 1,5, the terms "personal data", "processing", "data controller" and "data processor" shall have the meanings ascribed to them in the EU Directive. For the purposes of this Agreement and in respect of the personal data of End Users, the parties agree that Customer shall be the data controller and Google shall be a data processor. Google shall take and implement appropriate technical and organisational measures to protect such personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorised disclosure or access."

5.2. Public authorities' use of a processor must comply with the requirements in the Act on Processing of Personal Data and the Executive Order on Security.

5.3.1. *The Act on Processing of Personal Data's requirements on instructions and processor agreement*
Section 41(1) of the Act on Processing of Personal Data requires that individuals, companies, etc. that perform work for the controller or the processor and who have access to data may process these only on instructions from the controller.

In addition, Section 42(2) of the Act on Processing of Personal Data also requires, among other things, that the processor agreement must clearly state that the processor may solely act on the instructions of the controller.

If the general requirements cited by Odense Municipality are to solely comprise the processor agreement, this requirement would be described as follows: "*Customer … instructs Google to provide the Services and process End User personal data in accordance with the Google Privacy Policies and Google agrees to do the same.*" (cf. section 1.4 of "Google Apps General Terms").

In the view of the Danish Data Protection Agency, this solely obliges Google Ireland Limited to process the personal data in accordance with Google Inc.'s own Privacy Policy. Thus, Odense Municipality solely instructs Google Ireland Limited to process data in accordance with the Google Inc. group's own guidelines. The Danish Data Protection Agency finds that such instructions must be deemed devoid of content, in purely material terms.

In addition, it does not appear to be out of question that Google Ireland Limited can unilaterally change the agreement terms in the company's general terms and conditions, nor is there anything in the processor agreement that prevents Google Inc. from unilaterally changing the company's Privacy Policy. On this basis, the Danish Data Protection Agency's view is that Odense

Municipality, in reality, has no control of how the data will be processed. The agency therefore assumes that Google Ireland Limited – and Google Inc. – decide how the data will be processed.

On this basis, the Danish Data Protection Agency does not agree that a processor agreement comprised solely of the two sections (1.4 and 1.5) of "Google Apps General Terms" meet the requirement of Section 42(2) of the Act on Processing of Personal Data that the processor agreement must clearly state that the processor may solely act on the instructions of the controller. Nor does the agency agree that an agreement with this content adequately ensures that Google Ireland Limited processes the data only on instructions from Odense Municipality, cf. also Section 41(1) of the Act on Processing of Personal Data.

Section 7 of the Executive Order on Security further requires that the processor agreement states that the rules of the Executive Order on Security also apply to the processing by the processor. If the processor is established in another member country, the agreement must further state that the provisions on security measures stipulated in the legislation of the member country where the processor is established also applies to the processor. Thus, the processor must both comply with the Danish security requirements and the requirements in the processor's home country.

To meet the security requirements of the Act on Processing of Personal Data, Odense Municipality's processor agreement with Google Ireland Limited must further state that the rules of the Danish Executive Order on Security apply for the data processing that Google Ireland Limited performs as the processor for Odense Municipality. The Danish Data Protection Agency is unable to find that this requirement is met.

5.3.2. *The Act on Processing of Personal Data's requirements on control of the processor*

When a controller hands over processing of data to a processor, the controller must ensure that the processor can take the technical and organisational security measures cited in Section 41(3)-(5) and ensure that this happens. This is stipulated by Section 42(1) of the Act on Processing of Personal Data.

Further, the Guidance to the Executive Order on Security states that the controller must *actively* ensure that the processor abides by the required security measures and that, in this regard, it may be relevant to obtain an annual auditor's statement from an independent third party.

Regarding this issue, Odense Municipality has stated that the municipality will ask Google to confirm that the IT security audit includes a control that the required security measures stipulated by the Executive Order on Security are upheld by Google.

Regarding the question of where the data are physically located, Odense Municipality has stated that the data are located in the supplier Google's data centres and that these are located in the USA and Europe.

Thus, the Danish Data Protection Agency assumes that Odense Municipality is unaware of where the data are physically located. On this basis, the Danish Data Protection Agency questions whether Odense Municipality will be able to actively ensure that the required security measures are upheld at the data centres. On the existing basis, the agency's view is that the requirements in Section 42(1) of the Act on Processing of Personal Data on control of processors cannot be considered as being met.

6. Deletion of personal data

6.1. Odense Municipality has stated that the overall solution uses data media located on Google's premises, as well as in the login solution, which is located on Odense Municipality's premises.

Regarding the data media in Odense Municipality's login solution, the municipality has stated that it has an agreement on the destruction of IT material (hard disks) with an external company, on whose premises the destruction takes place, making it impossible to recreate data.

Regarding Google's data media, Odense Municipality has stated that Google states the following regarding ensuring that personal data are deleted after the completion of processing and regarding the discarding of data media:

> *"Deleted Data*
> *After a Google Apps user or Google Apps administrator deletes a message, account, user, or domain, and confirms deletion of that item (e.g., empties the Trash), the data in question is removed and no longer accessible from that user's Google Apps interface.*
> *The data is then deleted from Google's active servers and replication servers. Pointers to the data on Google's active and replication servers are removed. Dereferenced data will be overwritten with other customer data over time.*
> *Media Disposal*
> *When retired from Google's systems, disks containing customer information are subject to a data destruction process before leaving Google's premises. First, policy requires the disk to be logically wiped by authorized individuals. The erasure consists of a full write of the drive with all zeroes (0x00) followed by a full read of the drive to ensure that the drive is blank.*
> *Then, another authorized individual is required to perform a second inspection to confirm that the disk has been successfully wiped. These erase results are logged by the drive's serial number for tracking.*
> *Finally, the erased drive is released to inventory for reuse and redeployment. If the drive cannot be erased due to hardware failure, it must be securely stored until it can be destroyed. Each facility is audited on a weekly basis to monitor compliance with the disk erase policy."*

Lastly, Odense Municipality has stated that, via the attached SAS 70 Type II report produced by an independent auditor, the municipality feels certain that all personal data are deleted at Google Inc. after the completion of processing.

6.2. Regarding the deletion of data media, the Danish Data Protection Agency's guidance to Section 9 of the Executive Order on Security states:

> "When discarding storage media and equipment that contains personal data, the storage media should be destroyed or demagnetised so that it is no longer possible to read the contents. If the controller, rather than destroying the storage media, transfers these for the purpose of reuse, the stored data must be deleted effectively through overwriting.
>
> For the overwriting of data media, the Danish Data Protection Agency recommends the use of a special program that overwrites data multiple times in accordance with a recognised specification (e.g., DOD 5220.22-M).
>
> In case of the repair of equipment, stored data must be deleted prior to repair as far as possible."

Furthermore, Section 5(5) of the Act on Processing of Personal Data states that the data collected may not be kept in a form which makes it possible to identify the data subject for a longer period than is necessary for the purposes for which the data are processed.

6.3. Regarding data media at Google Ireland Limited and Google Inc.'s data centres, the sent materials indicate that data on disks that are to be reused are overwritten and that a control is then conducted of whether the data have been overwritten. It is further stated that media that cannot be reused are stored until they are destroyed. It is not indicated how these disks will be destroyed.

The Danish Data Protection Agency's view is that, based on the information provided in this case, it is impossible to assess whether the deletion of data media at Google Ireland Limited's and Google Inc.'s data centres is adequate. Further, the Danish Data Protection Agency finds it to be unclear whether the data are deleted in such a way that they cannot possibly be recreated from Google's servers. On this basis, the agency finds it difficult to deem the requirements for deletion in Section 9 of Executive Order on Security and Section 5 of the Act on Processing of Personal Data as being met.

7. Transmission and login

7.1. In connection with the planned processing of personal data, data will be transmitted from Odense Municipality's servers to Google Apps. Further, data will be transmitted internally between Google Ireland Limited and Google Inc.'s various data centres.

Odense Municipality has stated that in Google Apps it is possible to ensure that all processing of data occurs in encrypted form via Secure Sockets Layer (SSL)/Transport Layer Security (TLS) session encryption. Odense Municipal-

ity has further stated that the municipality utilises this encryption, and that the encryption level is 128bit RC4.

7.2. The information presented in the case does not indicate whether encryption is used for the transmission of data internally between Google Ireland Limited and Google Inc.'s various data centres.

7.3. The attachment to the e-mail of 4 October 2010 sent by Odense Municipality, "Exchanging login and user data between Odense Municipality's user catalogue and Google Apps' school solution", contains a description of how user login involves a validation of the user's authorisation on Odense Municipality's login server.

Further, this attachment states that users of Google Apps may be physically located outside of Odense Municipality (on the internet). Thus, the Danish Data Protection Agency must assume that employee's connection to Odense Municipality's servers can occur via internet.

According to the provided information, sensitive personal data subject to Sections 7 and 8 of the Act on Processing of Personal Data are involved in the planned processing of data and that the data can be accessed via internet.

As access to sensitive personal data via internet requires an especially high level of security in the view of the Danish Data Protection Agency, the agency recommends the use of digital signature or another solution with multiple factors in such cases.

8. Control of rejected attempts to access data

8.1. Odense Municipality has stated that all login attempts are registered in a log on the municipality's login server, that the log file is inspected monthly by an administrator and that follow-up is conducted for accounts with more than five failed logins during the period. The account is then closed and the user is contacted.

In an answer to a question from the Danish Data Protection Agency, Odense Municipality stated in an e-mail of 15 November 2010 that only the administrator account can be accessed directly from outside of the Odense server. This account is used solely for configuration of the system and does not have access to the individual users' accounts.

8.2. Section 18 of the Executive Order on Security states that all failed login attempts must be registered. If, within a determined period, a predetermined number of consecutive failed login attempts are registered from the same workstation or with the same user identification, further login attempts must be blocked. Follow up must be conducted on an ongoing basis by the authority.

8.3. Odense Municipality has not provided information about how the municipality will ensure control of failed login attempts in cases where someone

attempts to access Odense Municipality's accounts in Google Apps without entering into Odense Municipality's login server. Nor has Odense Municipality provided information about how the municipality will ensure that the system's automatic rejection of further attempts to gain access will come to the attention of the relevant person in cases where someone attempts to access Odense Municipality's accounts in Google Apps without entering into Odense Municipality's login server.

As the case stands, the Danish Data Protection Agency does not find that Odense Municipality has substantiated that the requirement on control of rejected attempts to gain access stipulated by Section 18 of the Executive Order on Security can be upheld if somebody attempts to access data without entering into the municipality's login servers.

9. Logging

9.1. In a letter of 25 June 2010, the Danish Data Protection Agency asked Odense Municipality how Section 19 of the Executive Order on Security on logging will be observed.

In an e-mail of 4 October 2010, Odense Municipality replied that Google Apps performs the necessary logging and that Google Apps Premium customers can request a copy of the log via Google's support function.

9.2. According to Section 19(1) of the Executive Order on Security, mechanical registration (logging) of all uses of personal data must be carried out. The registration must at least contain information about the time, user, type of use and an indication of the person the utilised data referred to, or the search criteria used. The log must be stored for six months, after which time it must be deleted. Authorities with a special need may store the log for up to five years.

Section 19(2)-(5) of the Executive Order on Security lists a number of exceptions to this provision.

9.3. It has not be stated whether Google Ireland Limited and Google Inc.'s data centres perform logging of uses of personal data, what information is logged, or how long the log is stored. As the case stands, the Danish Data Protection Agency does not find it to be substantiated that the municipality will be able to comply with the logging requirements in Section 19 of the Executive Order on Security.

10. As stated in the introduction, the Danish Data Protection Agency sees problems in a number of areas in relation to the requirements of the Act on Processing of Personal Data and the Executive Order on Security. Thus, the Danish Data Protection Agency does not concur with Odense Municipality's assessment that confidential and sensitive data about students and parents can be processed in Google Apps.

As mentioned previously, the Danish Data Protection Agency is willing to reconsider the case for a revised statement if Odense Municipality continues work on the case and seeks solutions to the identified issues.

It is also the view of the Danish Data Protection Agency that the decision of whether to use a solution of this kind in this area should be subject to an assessment by the municipality's political bodies.

On the existing basis, the Danish Data Protection Agency will take no further action in the case.

Best regards,

Henrik Waaben
Chairman of the Data Protection Council

Janni Christoffersen
Director