DATA PRIVACY

THE NETHERLANDS
Houthoff Buruma

CONTACT INFORMATION
Thomas de Weerd
Houthoff Buruma
Gustav Mahlerplein 50
1082MA Amsterdam
The Netherlands
+31 20 605 6361
t.de.weerd@houthoff.com

1. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Personally Identifiable Information, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

In the Netherlands the processing of personally identifiable information (hereinafter "personal data") is governed primary by the Dutch Data Protection Act (hereinafter "DPA") (Wet bescherming persoonsgegevens). The DPA is an implementation of the European Privacy Directive 95/46/EC.

The DPA provides that personal data may be collected and processed for specific, explicitly defined and legitimate purposes. Any further processing of those data may - in
principle - only take place for purposes which are compatible with the purposes for which the personal data was initially collected.

The DPA requires the processing of personal data to be transparent, which implies that data subjects should be informed of the processing of their personal data.

An unofficial translation to English of the DPA can be found at: http://www.dutchdpa.nl/downloads_wetten/wbp.pdf

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

Administrative enforcement:
The Dutch Data Protection Authority (hereafter "Authority") has the power to conduct investigations regarding compliance with the DPA on its own initiative and on the requests of interested parties such as data subjects. In case the Authority is of the opinion that the DPA is violated, it can force compliance under forfeiture of an administrative penalty. In addition, the Authority can impose a fine of EUR 4,000 in case the data controller has violated his duty to notify to the Authority that he is processing personal data.

Civil enforcement:
In the event the personal data of a data subject are processed in violation of the DPA, the data subject can instigate civil proceedings against the party processes its data. The data subject can for instance request an injunction or claim compensation for its damages.

Criminal enforcement:
Criminal enforcement measures can be imposed for (i) the violation to notify the fully or partly automated processing of personal data pursuant to article 27 DPA, (ii) the transfer of personal data outside the EU to a country without an adequate level of protection (article 78 section 2 DPA) and (iii) the failure of a non-EU company which processes data within the scope of the DPA to appoint a representative in the Netherlands (article 4 section 3 DPA).

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

The Authority has been appointed as the supervisory authority with respect to the DPA.

d) Any additional information that is material?
In addition to the procedures referred to under 2, the Authority is entitled to start an investigation to establish compliance with the DPA at its discretion.

The Authority tends to publish the results of its investigation relating to violation of the DPA on its website (www.cpbweb.nl). The negative publicity which follows from such publication may result in reputational damages.

2. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Personal Health Information, and any material obligations.

   a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

   The DPA contains special rules relating to the processing of personal health information. Personal data concerning a person's health is considered to be so-called sensitive personal data. According to article 16 DPA it is prohibited to process special personal data except as otherwise provided in the articles 21 and 23 DPA.

   According to article 21 DPA a controller is only allowed to process personal data concerning a person's health in limited cases. For example, this is allowed if and to the extent that this is necessary for the execution of a health insurance agreement.

   If the legal exceptions as given by article 21 DPA do not apply, there are also general exceptions (article 23 DPA), such as explicit consent of the data subject, or the data concerned have been made public by the data subject in an evident manner. Furthermore, the prohibition of article 16 DPA also does not apply if the processing of personal data is necessary for the establishment, exercise or defense of a right in law, is necessary to comply with an obligation of international public law or is necessary with a view to an important public interest.

   b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

   Reference is made to the answer to question 1b.

   c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.
Reference is made to the answer to question 1c.

d) Any additional information that is material?

The processing of sensitive (health) data is subject to close scrutiny by the Authority. For instance, recently the Authority investigated the information security of a number of Dutch hospitals on its own initiative.

3. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that are applicable to Financial Information, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

In the Netherlands the processing of personal data included in financial information is governed by the DPA.

The processing of financial information is also governed by certain provisions from the Act on Financial Supervision (hereinafter "AFS") (Wet op het financieel toezicht), which is further specified in a number of decrees. Links to relevant legislation in English (unofficial) can be found at: http://www.minfin.nl/english/Subjects/Financial_markets/Financial_supervision/Publications

The AFS regulates the financial sector in the Netherlands in general, and is not particularly meant to address privacy obligations. It does however regulate the conduct of financial firms in general and covers the conduct with respect to handling of information, including personal data. The AFS contains a general obligation for financial firms to have a sound and controlled business organization and to operate its business in a sound and controlled way (article 4:11, 4:14 AFS). These general obligations may be used by supervisory authorities to ensure proper behavior with respect to data protection.

Section 1:89 AFS provides that the supervisory authorities must keep all information (including personal data) confidential, unless there is a statutory basis for disclosure of such information.

Section 20 of the Decree on Prudential Rules pursuant to the AFS and Section 31b of the Decree on the Supervision of the Conduct of Financial Enterprises ("Supervision
Decree”) pursuant to the AFS impose a specific duty on certain financial firms to have procedures and internal measures to safeguard the processing of automatically saved information, which may include personal data.

Sections 33 and 35 of the Supervision Decree provide for a duty for certain financial services firms to store data about their clients (which includes personal data) for at least 5 years.

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

For personal data included in financial information, reference is made to the answer to question 1b.

Furthermore, the AFS can be enforced through both administrative and criminal law. Most offences, however, are enforced with administrative sanctions. The most important administrative sanctions include an administrative fine and an order with or without a penalty for non-compliance. Fines may vary from EUR 10,000 to EUR 4,000,000 (or even more if the offender gains a larger amount with his offence), but will have to take into account the specific circumstances of the offence. A combination of criminal and administrative prosecution is generally not allowed.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

For personal data included in financial information, reference is made to the answer to question 1c.

Furthermore, the AFS is supervised and enforced by two administrative authorities, being the Dutch Central Bank (de Nederlandsche Bank) and the Authority for the Financial Markets (Autoriteit Financiële Markten). Criminal sanctions may be imposed for the violation of certain sections of the AFS. Criminal prosecution is a task of the public prosecutor (Openbaar Ministerie) and criminal sanctions are eventually imposed by judges. Criminal prosecution for violations of the AFS, however, does not appear very often.

d) Any additional information that is material?
Pursuant to article 25 DPA it is possible to specify the standards of the DPA in codes of conduct. If the rules contained in a certain code of conduct properly implement the DPA (or other legal provisions on the processing of personal data) the Authority gives its approval to that code of conduct. Acting in accordance with the approved code of conduct implies that the party concerned is acting in accordance with the DPA.

In the Netherlands financial institutions are bound by Code of Conduct for Processing Personal Data Financial Institutions (hereinafter "Code of Conduct") (Gedragscode Verwerking Persoonsgegevens Financiële Instellingen). The Code of Conduct is approved by the Authority.

If a party concerned has the opinion that a financial institution acts in breach of the Code of Conduct, it can turn itself to the Financial Services Complaints Board (Stichting Klachteninstituut Financiële Dienstverlening). In certain cases, dependent on the content of the complaint, the party concerned can also file a complaint directly to the Authority or with the competent court.

4. Provide a brief description of the subject matter of data privacy laws in your jurisdiction that is applicable to other sensitive data, and any material obligations.

a) What is the cite to such laws? Provide a link, if available, to an online copy of such law.

According to article 16 DPA it is prohibited to process personal data concerning a person's religion or philosophy of life, race, political persuasion, health and sexual life, or personal data concerning trade union membership, except as otherwise provided in the DPA. The exceptions to the abovementioned prohibition given by the DPA either apply to a specific category (for example just given for the category of personal data concerning a person's criminal behavior) or are general exceptions. The general exceptions (article 23 DPA) include explicit consent of the data subject, or when the data concerned have been made public by the data subject itself in an evident manner. Furthermore, the prohibition of article 16 DPA also does not apply if the processing of personal data is necessary for the establishment, exercise or defense of a right in law, is necessary to comply with an obligation of international public law or is necessary in view of an important public interest.

This prohibition also applies to personal data concerning a person's criminal behavior, or unlawful or objectionable conduct connected with a ban imposed with regard to such
conduct. If the legal exceptions given by the DPA do not apply, the processing of special personal data is a violation of the DPA.

b) What are the penalties imposed for a breach of such law? Any criminal sanctions?

Reference is made to the answer to question 1b.

c) Identity the applicable administrative authority with jurisdiction for enforcement of such laws.

Reference is made to the answer to question 1c.

d) Any additional information that is material?

Reference is made to the answer to question 2d.