Bloomberg BNA

Bloomberg Law®: Privacy & Data Security

Country Profile: SWEDEN

Erica Wiking Häger, Pernilla Book, and Martin Hallström of Mannheimer Swartling, Stockholm, provided expert review of the Sweden Country Profile and wrote the Risk Environment section. [Last updated July 2016. – Ed.]

I. Applicable Laws and Regulations

In 1973, Sweden became the first country to enact a data protection law. After Sweden joined the European Union, Sweden adopted EU Directive 95/46/EC. The adoption of the directive led Sweden to amend its data protection law into its present form as the Swedish Personal Data Act (*Sw. Personuppgiftslagen (SFS1998:204)*) (PDA) (in Swedish; in English). In addition, the PDA is supplemented by the Swedish Personal Data Ordinance (*Sw. Personuppgiftsförordningen (1998:1191)*) (PDO) (in Swedish; in English). Sweden has also passed other laws that address privacy in specific areas, including the Camera Surveillance Act (*Sw. Kameraövervakningslag (2013:460)*) (in Swedish); the Credit Information Act (*Sw. Kreditupplysningslagen (1973:1173)*) (in Swedish); the Collection Act (*Sw. Inkassolag (1974:182)*) (in Swedish); the Electronic Communications Act (*Sw. Lagen om elektronisk kommunikation (2003:389)*) (in Swedish); and the Patients' Personal Data Act (*Sw. Patientdatalag (2008:355)*) (in Swedish).

Under the PDA, personal data is defined as any type of information that directly or indirectly refers to a living person (a "data subject") (§ 3). Sensitive personal data is personal data that reveals race or ethnic origin, political opinions, religious or philosophical beliefs, trade union membership, or information that concerns health or sex life. Furthermore, Sweden recognizes a distinction between structured and unstructured data: unstructured data is subject to less strict rules, as many sections of the PDA do not apply to processing of unstructured data (§ 5a) so long as the processing is not a violation of the data subject's privacy.

Unstructured data is defined as personal data that is not part of or intended to be part of a collection of data that has been structured to manifestly facilitate searches or compilations of personal data. Typical examples are processing of personal data in running text, tape recordings (auditory or visual), and search functions in e-mail programs. The data controller's main obligations when processing unstructured data is to (i) notify the Data Inspection Board of such processing (see more about this obligation below) and (ii) take appropriate technical and organizational measures to protect the personal data from unauthorized access, theft, etc.

A controller of personal data, defined as a person who alone or with others decides the purpose and means of processing personal data, must ensure that personal data (i) is processed lawfully, in a correct manner, and in accordance with good practice; (ii) is processed for a specific, explicitly stated, and justified purpose; (iii) is processed in an adequate and relevant way in relation to the purpose for which it was collected and is not processed for any purpose inconsistent with the purpose for which it was collected; (iv) is only processed to the extent necessary to achieve the purpose for which it is collected; (v) is correct and, if necessary, current; (vi) is corrected, blocked, or erased if it is incorrect or incomplete; and (vii) is not kept longer than is necessary to accomplish the purpose (PDA § 9).

Generally, personal data may only be processed if the data subject has given consent, defined as a voluntary, specific, and unambiguous expression of will

by which the data subject, having received notice, accepts processing of his personal data (PDA § 3). Non-consensual processing is permitted if it is necessary:

- to enable the performance of a contract with the data subject or to enable measures that the data subject has requested to be taken before a contract is entered into;
- for the controller of personal data to be able to comply with a legal obligation;
- to protect the vital interests of the data subject;
- to perform a task that is in the public interest (i.e., research, archiving, public opinion polls);
- for the controller of personal data or a third party to whom the personal data is provided to be able to perform a work task in conjunction with the exercise of official authority; or
- for a purpose that concerns a legitimate interest of the controller of personal data, or of such third party to whom personal data is provided, to be satisfied, if this interest is of greater weight than the data subject's interest in protection against violation of his personal integrity (§ 10).

Section 13 of the PDA prohibits the processing of sensitive personal data, except in certain circumstances (§ 14). Sensitive personal data may be processed if:

- the data subject has given his consent to the processing or in a clear manner made the information publicly available (§ 15);
- the processing is necessary in order (i) for the data controller to perform its duties or exercise its rights under employment law, (ii) for the data subject's or a third party's vital interests to be protected when the data subject cannot provide consent, or (iii) for legal claims to be established, exercised, or defended (§ 16);
- the information is processed by a non-profit organization with political, philosophic, religious, or trade union goals, and the information concerns members of the organization or third parties that, because of the organization's goals, have regular contact with the organization (§ 17);
- the processing is for health and hospital care purposes and is necessary for preventative medicine and health care, medical diagnosis, care or treatments, or management of health and hospital care services (§ 18); or
- the processing is for research (where such processing is preapproved) or statistics purposes, and the societal interest is manifestly greater than the risk of violation of the personal integrity of the individual (§ 19).

A data subject may revoke consent at any time (PDA § 12).

If data is collected from the data subject, the controller must, in connection with the collection of the data, voluntarily provide the data subject with information about the processing of the data (PDA § 23). If the information has been collected from a source other than the data subject, the data subject should be informed of the collection either upon registration of the data or, if the data is collected with the intention of transferring/disclosing it to a third party, when the data is disclosed or transferred to the third party for the first time (§ 24). The information provided to the data subject should include information concerning the identity of the controller; the purpose of the processing; organizations with which the data may be shared (including types of organizations); the fact that the data subject, upon request and free of charge once every year, has the right to request an excerpt from the data controller's register to control what data is processed about him; and all other information necessary in order for the data subject to be able to exercise his rights (§ 25).

If the data is collected through a source other than the data subject, notification does not need to be provided if it would be impossible or would involve a disproportionate effort (PDA § 24).

When the controller of personal data is established in a third country, i.e., a country outside of the EU/EEA, but uses equipment situated in Sweden for the processing of the personal data, the controller must appoint a representative who is established in Sweden (PDA § 4).

II. Regulatory Authorities and Enforcement

The PDA is enforced by the Swedish Data Inspection Board (*Datainspektionen*). The main rule is that controllers of personal data need to notify the Data Inspection Board of any processing by filing a notification with the Board (§ 36). The notification to the Board should contain the following information:

- the data controller;
- the purpose of the processing;
- the categories of data subjects affected by the processing;
- the categories of personal data processed;
- the recipients of the personal data (i.e., if the personal data is disclosed or shared with third parties);
- whether the personal data will be transferred to a third country; and

- the safety measures taken to safeguard the processing.

However, if the controller of personal data appoints a personal data representative and notifies the Data Inspection Board of such appointment, the controller does not have to file a notification of the processing of personal data with the Board.

A person who intentionally or by negligence provides untrue information to data subjects or to the supervisory authority, processes sensitive personal data or personal data on criminal offenses in contravention of the PDA, transfers personal data to a third country in contravention of the PDA, or neglects to notify the Data Inspection Board, shall be sentenced to a fine or imprisonment of at most six months or, if the offense is grave, to imprisonment up to a maximum of two years (§ 49).

If the Data Inspection Board cannot obtain information sufficient to conclude that the processing of personal data is lawful, it may order a default fine (PDA § 44).

III. Risk Environment

The Swedish Data Inspection Board started 53 new supervisory matters during 2015. The most noteworthy matters were directed towards communities in Sweden and other Swedish authorities processing Swedish citizens' personal data.

The focus of the Data Inspection Board has been, and to a certain extent continues to be, cloud services and registration of ethnical data in the social services as well as on the residential market. The Board has also had a special focus on camera surveillance and has appealed and won many cases where camera surveillance permits had been granted by the county administrative board. The focus on camera surveillance also includes the use of drones for surveillance. The Board has acted to make the use of drones for public surveillance subject to approval by the county administrative board. The Administrative Court of Appeal in Sweden has recently concluded that the use of drones constitutes camera surveillance and is governed by the Camera Surveillance Act. In March 2016, the Administrative Supreme Court determined to grant leave of appeal and will hence try the relevant case.

The Data Inspection Board offers consultations on processing personal data in certain situations and provides education to data protection officers. The Board also acts in supervisory matters, generally by first giving a notice of correction to the company in question before any enforcement measures, such as conditional fine orders, are issued to enforce corrective measures. Supervisory matters may be initiated through site visits or inquiries to the company.

Awards of damages for breaches of privacy have regularly been low in Sweden, averaging SEK5000 per breach per individual. Higher amounts have been awarded in severe cases involving other criminal offenses. The Data Inspection Board's total budget for 2015 was around SEK44 million, none of which was derived from fines.

The largest risk posed to companies observing Swedish data protection law is the coming implementation of the General Data Protection Regulation within the EU, which changes the landscape for Swedish and European data processing. The new regulation will increase the compliance requirements for companies, combined with significantly higher sanctions for violations.

Both the new administrative procedures and the creation and monitoring of new internal processes will be a challenge for many companies. Many larger companies observing Swedish data protection law have already started working to implement new routines and measures in order to be able to meet the higher standards of the General Data Protection Regulation once implemented. The Swedish Government has recently initiated an investigation as to what measures need to be taken in national law as a consequence of the General Data Protection Regulation entering into force. The result of said investigation shall be presented in May 2017. The Data Inspection Board also published both a checklist (in Swedish) and an FAQ page (in Swedish) in order to help organizations comply with the GDPR.

In addition, the October 2015 judgment of the European Court of Justice (C-362/14) poses a risk to all companies transferring personal data from within the EU to companies authorized under the Safe Harbor regime in the United States. The judgment, which invalidated the EU Commission's decision to accept transfers of personal data to the United States under the Safe Harbor regime, gives the mandate to each supervisory authority within the EU to determine if a transfer of personal data to the United States is permitted. This poses a large risk for companies that previously relied on the Safe Harbor regime due to the current uncertainty regarding the legality of such transfers and to the fact that companies in certain cases will need to secure another legal ground for transferring personal data to the United States. Other legal grounds for transferring personal data to a third country could be consent from the data subject, the use of other legal exceptions in the PDA, the use of

the EU Commission's Model Contracts for the transfer of personal data to third counties, or (within the group of companies) by implementing so-called binding corporate rules that satisfy an adequate level of safety for the processing. In February 2016, the EU Commission disclosed that it had reached an agreement with the U.S. regarding the successor of the Safe Harbor regime, the "Privacy Shield" arrangement. Following criticism from the Article 29 Working Party, the European Parliament, and the European Data Protection Supervisor, the European Commission formally approved an amended version of the arrangement on July 12, 2016. From Aug. 1, 2016, U.S.-based companies are able to self-certify their framework compliance with the U.S. Department of Commerce and more easily transfer data. See "Privacy Shield EU-U.S. Data Transfer Pact Completed," *Privacy Law Watch* (July 13, 2016). Prior to implementation, the new arrangement will not have any effects specific for Sweden.

IV. Emerging Issues and Outlook

A. Data Retention Laws

In April 2014, the Court of Justice of the European Union struck down the EU Data Retention Directive 2006/24, finding that the law interfered with the fundamental right to privacy. As a result, the Swedish Post and Telecom Authority (PTS), which regulates electronic communications and postal services, informed Internet service providers that it did not intend to act on the basis of the data retention rules implemented in Sweden. On June 13, 2014, the special investigator, appointed by the Swedish Ministry of Justice, judged the Swedish law unaffected by the Directive, and the PTS instructed Internet service providers to resume storing data. A court ruling from the administrative court of Stockholm on Oct. 13, 2014, also found that the Swedish law still applies.

B. Household Waste

In July 2015, Sweden's Data Inspection Board found that a municipal waste company acted improperly when it instructed employees to visually inspect and record the contents of customer garbage cans. Following the inspections, the company sent letters to customers related to food waste disposal. According to the Board, the company lacked guidelines about information recording and failed to inform households about the data that would be retained. In such situations, companies should provide clear information about recording during waste removal, develop instructions on the type of information to be recorded, and ask households to opt in to such a service. According to the Board, although the Personal Data Act does not refer to personal waste specifically, processing it could be considered processing personal data. See "Sweden Finds Privacy in Household Waste," *Privacy Law Watch* (July 9, 2015).

C. Ambulance Video Plan

The Data Inspection Board is appealing a local court decision that will allow ambulances to transmit live pictures from accident scenes to hospitals. The Board does not oppose the scheme itself, which would allow hospital staff to prepare for patients before their arrivals. However, given the likelihood that patients will not be able to grant permission or prior consent, the Board recommends that the project's time span be reduced from two years to one and that limits be placed on the area where filming can take place. See "Swedish Agency Appeals Ambulance Video Plan," *Privacy Law Watch* (Sept. 21, 2015). The Administrative Court agreed with the Board and found that the time span should be limited to one year.

D. Right to Be Forgotten

On June 2, 2015, the Data Inspection Board announced that it will review a cross-section of right-to-be-forgotten requests denied by Google in order to examine Google's handling processes and assessments. In doing so, the Board will investigate various issues Google has had to address, such as what constitutes a public person. If the Board finds that Google has erred in refusing to remove any of the results, the Board will require Google to remove them. See "Swedish Privacy Regulator Will Review Google Right to Be Forgotten Decisions," *Privacy Law Watch* (June 18, 2015).