SWEDEN – COUNTRY REPORT

Background

This report outlines the main laws which provide law enforcement and intelligence agencies with legal powers in relation to lawful interception assistance, the disclosure of communications data, certain activities undertaken for reasons of national security or in times of emergency, and censorship of communications under Swedish law.

1. PROVISION OF REAL-TIME INTERCEPTION ASSISTANCE

1.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

According to chapter 6, section 17, it is prohibited to intercept content data or monitor metadata associated with an electronic message.

However, under chapter 6, sections 19 and 21, network operators and service providers are obligated to:

(a) conduct their business and adapt and construct their network in a manner that enables the execution of court orders for the secret interception of electronic communications messages; and

(b) conduct their business in a manner that enables the execution of such court orders for secret interception without disclosure of such interceptions.

The content of an intercepted message must be made available in a form that can be easily processed by the government agency requesting the interception.

Chapter 6, section 19(a) requires network operators and service providers that own cables through which electronic signals are transmitted over the Swedish border, to transmit such signals to certain interaction points chosen by the network operator or service provider. The network operator or service provider must notify the National Defence Radio Establishment (Försvarets radioanstalt) (the "NDRE") of the location of these selected interaction points. Obligation with this requirement allows the Inspection of Defence Intelligence (the "IDI") to gain technical access to the electronic signals at the interaction points in accordance with the Defence Signals Intelligence Act (2008:717) (lag (2008:717) om signalspaning i försvarsunderrättelseverksamhet) (the "DSIA"). The IDI is then able to transmit some of the signals on to the NDRE, in accordance with their obligations under the DSIA.

In accordance with sections 5, 5(a) and 12 DSIA, the NDRE must present a court order from the Defence Intelligence Court mandating the monitoring of the electronic signals in question. The IDI does not however need to present a court order to require access to all the electronic signals passing through the interaction points. Consequently, the relevant network operator or service provider is obliged to give the IDI access to the cable-based electronic signals that pass through an interaction point, without the need for a court order or warrant.

The NDRE is responsible for the actual construction of the interaction point, for securing technical access to the signals at the interaction point and for further transmitting them to its own systems. While the network operator or service provider is obliged to bear the costs associated with the transmission of the signals to the interaction point, the NDRE bears the costs associated with the operation of the interaction point.

These requirements fall under the remit of defence intelligence conducted to support the Swedish foreign, security and defence policies and for mapping external threats to the country.

Chapter 6, section 19(a) also obliges any network operator or service provider that carries signals over the Swedish borders through cables to disclose to the NDRE any information in its possession that makes it easier for the NDRE to manage and intercept the signals accessed at an interaction point, for example, the title, architecture, bandwidth, or direction of the connections and the type of signalling. The obligation applies to all network operators or service providers that carry

cross-border signals i.e. not only to the network operators and service providers that own the cables.

1.2 Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")

Pursuant to chapter 27, section 21, the general obligation for network operators and service providers to provide interception assistance is qualified by the requirement that the requesting government agency first obtains a court approval authorising the interception. The request must be submitted to the competent court by a public prosecutor. According to chapter 27, section 18, a request for interception may only be granted in investigations relating to certain serious crimes. In this context, "serious crimes" include crimes for which the prescribed minimum penalty is imprisonment for two years or more and offences such as sabotage, arson, espionage, and terrorism.

In addition, a court approval will only be granted if the conditions set out in chapter 27, section 20 are fulfilled. Section 20 states that the use of interception must be of exceptional importance for the purpose of facilitating the criminal investigation in question. The court approval may only concern a particular number, address or the electronic communications equipment possessed by an individual who can reasonably be suspected of committing the crime under investigation. It may also concern another individual but only if there are particular reasons to believe that they will be contacted by the suspect.

According to chapter 27, section 21(a), if the public prosecutor responsible for the investigation deems that awaiting the court approval would result in a delay of material importance to the investigation, the public prosecutor may himself, without first obtaining a court approval, authorise an interim order for the secret interception. In such cases, the public prosecutor should inform the court of its decision, following which the court must promptly evaluate the interim order. If the court does not find reasons to support the decision, it must revoke the earlier decision, in which case no information collected under the interim order may be used in the investigation, if such information is detrimental to the person concerned.

Under chapter 27, section 22, it is prohibited to intercept communications involving information entrusted to certain individuals in their professional capacity. Such individuals are those who, according to chapter 36, section 5, are prohibited from disclosing information mentioned in the conversation. Examples of such individuals include advocates, physicians and freelance journalists (in relation to their sources).

2. DISCLOSURE OF COMMUNICATIONS DATA

2.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

According to chapter 6, section 20, all data relating to customer communications, including metadata and content data, are confidential and may not be disclosed to anyone other than the participants of the relevant communication.

However, according to chapter 6, section 22, confidentiality does not apply in the following situations, where the network operator or service provider must disclose:

- customer subscription details, upon request from any government agency, where they are needed for serving a person in accordance with the Service of Process Act (2010:1932) (delgivningslag (2010:1932)), if it could be expected that the person sought to be served is hiding or if there otherwise are exceptional reasons for such disclosure;
- customer subscription details, which relate to a suspected crime, upon request from the Public Prosecution Authority (Åklagarmyndigheten), the Police Authority (Polismyndigheten), the Swedish Security Service (Säkerhetspolisen) or any other government agency investigating a suspected crime;
- customer subscription details relating to a customer and other information relating to a specific electronic message, including information about the geographic area in which the relevant communication equipment is or has been situated, upon request from the Police Authority. The Police Authority can only make such a request to assist in the search for a person who has gone missing in circumstances which suggest their life is in danger or that they are at serious risk of harm;
- customer subscription details, upon request by the Enforcement Authority (Kronofogdemyndigheten), if needed in an enforcement process (meaning in the collection of debts or actions related to such enforcement) and the Enforcement Authority deems such information to be of material importance to the processing of a certain matter;
- customer subscription details, upon request by the Tax Agency (Skatteverket), in the event such information is of material importance to the processing of any matter relating to the calculation of tax owed, payment of tax-related charges or any matter relating to the correct registration of an address or domicile in accordance with the National Registration Act (1991:481) (folkbokföringslag (1991:481));
- customer subscription details, upon request from the Police Authority, if such information is needed for providing notification, obtaining information or identifying persons in relation to accidents or casualties, or when investigating such accidents or casualties, or when the Police Authority leave a person aged under 18 years old to the care of the social services in accordance with section 12 of the Police Act (1984:387) (polislag (1984:387));
- customer subscription details, upon request by the Police Authority or the Public Prosecution Authority, if such authority determines such information is necessary in order for the authority to be able to inform a guardian in accordance with Section 33, of the Act (1964:167) on Juvenile Criminals (lagen (1964:167) om särskilda bestämmelser om unga lagöverträdare); and

- customer subscription details and other information relating to a specific electronic message, upon request by a regional emergency service centre (regional alarmeringscentral) in accordance with the Act (1981:1104) on Regional Emergency Service Centres (lagen (1981:1104) om verksamheten hos vissa regionala alarmeringscentraler).

A request under section 22 ECA does not require a court approval or any particular decision by the relevant government agency.

Under chapter 6, section 16(c) ECA, a government agency may only request metadata retained by a network operator or service provider under chapter 6, section 16(a) in the following situations:

(a) where a network operator or service provider must, upon request from the Public Prosecution Authority, the Police Authority, the Swedish Security Service or any other government agency, in connection with an investigation of a crime, disclose customer subscription details pursuant to chapter 6, section 22;

(b) where, pursuant to a court order sought by a public prosecutor under chapter 27, section 21 CJP, network operators and service providers are, pursuant to chapter 27, section 19 CJP, required to disclose to the Police Authority, the Swedish Security Service or the Customs Agency (Tullverket) the following metadata (as detailed in the court order):

(i) information on messages which have been transmitted across an electronic telecommunications network or which have been transmitted to or from a telephone number or other address;

(ii) information on what electronic communication devices have been present within a certain geographic area; and

(iii) Information concerning in what geographic area a certain electronic communication device is or has been present.

(iv) According to chapter 6, sections 16(a) to 16(f), a network operator or service provider must retain customer subscription details and other information relating to a certain electronic message, which are necessary to track and identify:

(a) the source of the communication;

(a) the ultimate destination of the communication;

(a) the date, time and duration of the communication;

(a) the type of communication;

(a) the communication equipment; and

(a) the localisation of mobile communication equipment at the commencement and end of the communication.

Network operators and service providers are also obliged to retain data relating to failed calls or connections, in relation to which the network operator or service provider shall retain the data generated or processed.

The specific information which should be retained by a network operator or service provider is further clarified in sections 38 to 43, of the Ordinance (2003:396) on Electronic Communication (förordning (2003:396) om elektronisk kommunikation) (the "OEC"). In addition, under section 44 OEC, the Swedish Post and Telecommunication Authority (Sw. Post- och telestyrelsen) (the "PTA") may stipulate more detailed requirements relating to the storage of data.

The PTA, under exceptional circumstances, may also create exemptions from the obligation to retain data as per chapter 6, section 16(b) ECA. In such event, the PTA will consult with the Public Prosecution Authority, the Police Authority and the Swedish Security Service as obligated to do so by section 45 OEC.

According to chapter 6, section 16(d) ECA, data retained in accordance with chapter 6, section 16(a) ECA, must be retained for six months from the date the communication ended. After this period, the network operator or service provider must permanently delete the retained data.

It should be noted that chapter 6, sections 16(a) to 16(f), implement Directive 2006/24/EC of the European Parliament and of the Council (the "Data Retention Directive"), which on 8 April 2014 was declared invalid by the Court of Justice of the European Union (the "ECJ"). As a consequence, the validity of the data retention obligations of network operators and service providers described above was contested by certain network operators and service providers operating in Sweden. After the Administrative Court of Stockholm, on 13 October 2014, upheld the Swedish implementation of the Data Retention Directive as lawful, the case was appealed and subsequently referred to the ECJ.

On 21 December 2016 the ECJ delivered a judgement striking down chapter 6, sections 16(a) to 16(f) ECA as inconsistent with provisions of the Charter of Fundamental Rights of the European Union (joined Cases C-203/15 & C-698/15). In summary, the ECJ concluded that the Charter of Fundamental Rights precluded such legislation as it provides for general and indiscriminate retention of all traffic and location data of all subscribers and registered users relating to all means of electronic communication. However, according to the ECJ, EU Member States are allowed to adopt laws to retain traffic and location data so long as the purpose of the legislation is to fight serious crimes, and the retention of the data is proportionately limited with respect to the categories of data to be retained, the means of communication affected, the persons concerned and the retention period. Accordingly, what has been set out above regarding chapter 6, section 16(a) to 16 (f) ECA must be considered with some caution.

The Swedish legislator has not yet reacted to this ECJ judgment and thus the state of the law in this area is uncertain. Moreover, it is important to note that the ECJ judgment may also affect other legislative acts and the legal position should therefore be reevaluated accordingly.

2.2 Act (2012:278) on Collection of Data in Electronic Communication in the Crime Combatting Authorities' Intelligence Services (lag (2012:278) om inhämtning av uppgifter om elektronisk kommunikation i de brottsbekämpande myndigheternas underrättelseverksamhet) (the "IEUK")

Following a decision from the Police Authority, the Swedish Security Service or the Customs Agency, made by a duly authorized representative (meaning the head of the agency or a person to which the head of the agency has delegated the right), a network operator or service provider must, in accordance with section 1, disclose the metadata outlined under chapter 27 CJP summarised in paragraph 2.1(b) of this report above.

According to section 2, information may only be collected if:

(a) the collection is of particular importance in order to prevent or discover criminal activities, which involves any crime that is punishable with no less than two years imprisonment; and

(a) the reasons for the collection outweigh the interests of the person in relation to which the measure is targeted.

A court order will be required in accordance with chapter 27, section 21 CJP (as described above).

In this context, please note the information regarding the ECJ judgement delivered in December 2016 set out under section 2.1 on this report above.

3. NATIONAL SECURITY AND EMERGENCY POWERS

3.1 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

Under chapter 7, section 8 if a network operator or service provider does not fulfil its obligations under the ECA, and such breach severely threatens the public order, national security or public health or could otherwise be deemed to cause severe economic or operational problems for a supplier or user of an electronic communication network or service, the Swedish Post and Telecommunication Authority (the "PTA") may, with immediate effect, order an injunction against the relevant network operator or service provider.

A PTA decision of this nature is valid for a maximum of three months. If no corrective measures are taken by the network operator or service provider in breach, the period may be extended by a further three months.

The PTA may also revoke a network operator's or service provider's authorisation to use a certain radio transmitter or to use radio transmitters within certain radio frequencies in its business. The PTA may further change the terms and conditions of such authorisations.

In accordance with chapter 1, section 8, if Sweden is (or has recently been) at war or under the threat of war, or if there are extraordinary conditions that are caused by a war outside of Sweden, the government may issue regulations governing electronic communications networks and associated facilities and services, and other radio usage as necessary for the purposes of national defence or security in general. This may result in additional emergency powers for the relevant authorities.

3.2 Proposed Swedish Government Official Report (SOU 2013:33 – en myndighet för alarmering) (the "Report")

The Report provides that certain government agencies will be able to send text messages alerting citizens to emergency situations. The Report defines which government agencies hold this right and who is responsible for the costs that exercising this right entails.

3.3 Further legislative discussion

There have been theoretical discussions held that indicate that the government, under exceptional circumstances (for instance severe threats against national security), would have the right to invoke a constitutional privilege of self-defence (konstitutionell nödrätt) which may entail a wider scope of governmental power than otherwise described in this report. In accordance with page 95 of the preparatory works (SOU 2003:32 – Vår beredskap efter den 11 september: betänkande), the right to act in emergency situations is covered by Chapter 1-12 of the Swedish Form of Government (Regeringsformen (1974:152)), where Parliament's functions are delegated to the government. In situations where delegation powers under the aforementioned chapters do not exist, one option is to act through the constitutional privilege of self-defence.

The constitutional privilege of self-defence has never been exercised, thus making it difficult to properly assess its scope in this context. It is however not unlikely that the government may take control of a network operator's or service provider's network if this is necessary to uphold national security.

4. CENSORSHIP

4.1 Freedom of Press Regulation (tryckfrihetsförordning (1949:105)) and the Freedom of Speech Constitution (yttrandefrihetsgrundlag (1991:1469))

Under the Freedom of Press Regulation and the Freedom of Speech Constitution, there is a prohibition against censorship. The right to express an opinion, without it being censored, is thus a constitutional right in Sweden.

4.2 Code (1942:740) of Judicial Procedure (Rättegångsbalk (1942:740) (the "CJP")

As described above, under chapter 27, section 19, data may be secretly intercepted via real-time interception of electronic communications.

Government agencies have the right to prevent the customer communications (described above) from reaching its recipient where there is an on-going investigation relating to the discovery of offences which may include hacking, child pornography and drug crimes.

Government agencies also have the right to switch off a phone number in critical situations to prevent a suspect from contacting his or her accomplices or receiving warning calls.

4.3 Electronic Communications Act 2003 (2003:389) (lag (2003:389) om elektronisk kommunikation) (the "ECA")

Under chapter 7, section 9a, the Consumer Ombudsman (Konsumentombudsmannen) may order a network operator or service provider to prevent user access to a number whose digit structure lacks a geographical sense, if the marketing of the number or the service related to it is improper or if material information is omitted in the marketing material. This means that it may become impossible for users to reach the number or service in question.

Certain Internet Service Providers have entered into voluntary cooperation agreements with the Police Authority to block DNS that contain child pornography material. The content and scope of such agreements are confidential.

Moreover, in a recent judgement delivered by the Swedish Patent and Market Court of Appeal on February 13 2017, the court declared that an internet service provider that acts as an intermediary can be ordered to block access to websites that infringe intellectual property rights. As a consequence, the court issued an injunction, combined with a conditional fine, that required the internet service provider Bredbandsbolaget (Telenor) to block subscribers from accessing illegal streaming and piracy websites, The Pirate Bay and Swefilmer.

4.4 Other legislation on obligation to disclose subscriber data

The Tax Agency has far reaching powers which enable it to request information from network operators on the use of electronic communications of tax subjects (cf. what is set out above under paragraph 2.1). For example, the Tax Agency may use general tax legislation such as the Law on Taxation Procedures (2011:1244) (skatteförfarandelag (2011:1244)) to request information on subscribers and their use of electronic communications. Such order can be combined with a conditional fine amounting to several million SEK. There are no court approvals prior to the Tax Agency making its decision regarding the obligation to disclose subscriber data upon a conditional fine. However, if the network operators abstains from or objects to complying with the obligation, the obligation will be subject to a court proceeding.

Professional sellers or lessors active in the retail business are by law obliged to disclose information on the purchase of equipment that allows for reception of TV services to Radiotjänst i Kiruna AB. The professional sellers or lessors shall provide Radiotjänst i Kiruna AB with such information about the subscriber that is necessary in order for them to determine the appropriate TV license fee.

According to the Copyright Act (1960:729) (lag (1960:729) om upphovsrätt till litterära och konstnärliga verk) a rights holder can apply for an injunction, subject to a conditional fine, requesting an electronic communications service provider to disclose information regarding the origin and distribution network (i.e. the name and IP address) of the suspected.

5. OVERSIGHT OF THE USE OF POWERS

5.1 Judicial Oversight

Where court approval is provided for an interception or the collection of information pursuant to chapter 27, section 21 CJP, the competent court and the relevant public prosecutor have a supervisory role in the use of the measures that are used.

5.2 The Swedish Post and Telecommunication Authority (Post- och telestyrelsen) (the "PTA")

The PTA generally supervises network operators' and service providers' compliance with their respective obligations. According to chapter 7 of the ECA, the PTA is entitled to order a network operator or service provider to disclose information and documentation needed in order to ensure that the network operator or service provider complies with its obligations. Such order may be combined with a conditional fine. The PTA is also entitled to gain access to any facilities (excluding residences) where a network operator or service provider's business is conducted in order to perform an audit of the business in question.

If the PTA deems that a network operator or service provider has breached its obligations, it may order the network operator or service provider to rectify its breach. Such order may be combined with a conditional fine.

5.3 Inspection of Defence Intelligence (the "IDI")

The IDI supervises the secret defence intelligence activities performed by the National Defence Radio Establishment (the "NDRE"). It may do this, for example, by only permitting the NDRE to intercept signals transmitted in cables which are covered by a court order from the Defence Intelligence Court (Försvarsunderrättelsedomstolen).

5.4 Commission on Security and Integrity Protection (Säkerhets- och integritetsskyddsnämnden) (the "SIN")

All decisions on the collection of data under the Act on Collection of Data in Electronic Communication in the crime combatting Authorities Intelligence Services ("IEUK") shall be communicated to SIN, which supervises the relevant government agencies' compliance with the IEUK.

6. PUBLICATION OF AGGREGATE DATA RELATING TO USE OF GOVERNMENT POWERS

Restrictions on network operators and service providers

6.1 Publicity and Secrecy Act (offentlighets- och sekretesslagen (2009:400)) (the "PSA")

Under the PSA, the government has the legal authority to prevent a network operator or service provider from publishing aggregate data relating to intercept requests or acquisitions of metadata when, for example, secrecy under a current investigation applies to the aggregate data and any publication of the information may jeopardise or impair the investigation. Confidentiality will apply to activities such as those which aim to prevent, detect, investigate or prosecute crime, conducted by prosecutors, the police and the Swedish Security Service.

Neither the public prosecutor nor the Police Authority need to obtain any authority or court order before the information is to be considered confidential.

Confidentiality may also apply to data relating to preliminary investigations in criminal cases or a matter relating to the use of coercive measures, if the purpose of the measures is undermined by disclosure, or if future operations may be damaged by disclosure.

The government does not have the legal authority to prevent a network operator or service provider from publishing descriptions of, or information relating to, the laws described in this report.

Aggregate data published by government agencies.

The Public Prosecution Authority annually publishes a report of the use of secret surveillance-related laws. The report for 2015 is available at: https://www.aklagare.se/globalassets/dokument/rapporter/ovriga-rapporter/redovisning-av-anvandningen-av-vissa-hemliga-tvangsmedel-under-2015.pdf. The report does not include the details of any interception or surveillance initiated by the secret police.

7. CYBERSECURITY

7.1 Electronic Communications Act (2003:389) (Sw. Lag om elektronisk kommunikation) ("the ECA") and the Personal Data Act (1998:204) (Sw. Personuppgiftslagen) ("the PDA")

Under chapter 5, section 6A ECA (which implements the EU legislative package on electronic communications, e.g. Directive 2009/136/EC and Directive 2009/140/EC), a telecommunications network operator or service provider must take appropriate technical and organisational measures (including cybersecurity measures) to appropriately manage any risks posed to the security of networks and services. In particular, such measures have to provide safeguards to prevent and minimise the impact of security incidents on users and interconnected networks.

In the context of personal data protection, the ECA and PDA, which implement Directive 95/46/EC and contain regulations pertaining to cybersecurity in the context of personal data processing, stipulate that a data controller or processor (e.g. a telecommunications service provider) has to take appropriate cybersecurity measures to protect personal data. These measures must provide for an appropriate level of security based on (i) the technical possibilities available; (ii) the costs of the intended measures; (iii) the specific risks linked to the processing of the personal data; and (iv) the sensitivity of the personal data.

Pursuant to the ECA and the PDA, the regulator can use several supervisory measures to ensure compliance with the legislation (which includes requirements related to the protection against cybersecurity). In summary, the PTA:

(a) is entitled to receive any information and documentation required to conduct its supervision and can require access to the premises and infrastructure of the telecommunications operator, including any premises where personal data is processed; and

(b) has the power to issue injunctions and prohibitions to ensure compliance with the legislation and regulations issued pursuant to an Act (for example the PTA Regulation on Information Security (PTSFS 2012:4) (Sw. Post och Telestyrelsens Föreskrifter om krav på driftsäkerhet).

Note however that under current Swedish legislation, there is no general incident reporting obligation owed to the regulator (for example if a service company's database is hacked). Despite this, certain sector-specific regulation pertaining to data breaches in the telecommunications sector should be noted.

One such example is the specific breach notification regime for registered telecommunications operators, as set out in the Commission Regulation (611/2013) and PTSFS 2012:1, This requires that any such notification of a personal data breach by a registered operator is addressed to (i) the regulator and (ii) the individual (or "subscriber") unless the data has been securely encrypted and rendered unintelligible to any person who is not authorised to access it.

The information to be included in the notification to the regulator and the individual affected is specified in the annex to the Commission Regulation and includes:

(a) the service provider's identity and relevant contact details;

(b) the timing and circumstances of the breach;

(c) the nature and content of the data;

(d) the remedies contemplated;

(e) the likely consequences of the breach; and

(f) the technical or organisational measures taken to address the breach.

It is important to note that a notification addressed to the regulator may become publicly available, at least in part, under the Swedish Public Access to Information and Secrecy Act (2009:400) (Offentlighets- och sekretesslagen).

A further example is chapter 5 section 6C ECA which provides that a network operator or service provider must notify the regulator of any IT security breach that has had a significant impact on the operation of their networks or services (for example an attack that has led to a complete shutdown of the operator's critical systems).

It should also be noted that the Swedish legislator is currently in the process of implementing Directive 2016/1148/EU (the "NIS Directive"). This NIS Directive aims to ensure a high common level of network and information security across the EU but does not extend to public telecommunication service providers. Note however, that it is not yet clear how the Swedish legislator will implement the NIS Directive. Accordingly, this information should (for the time being) be treated with caution until the NIS Directive has been fully implemented.

The forthcoming General Data Protection Regulation 2016/679/EU (the "GDPR"), which enters into force in 2018 will define the requirements with regard to cybersecurity for personal data and will further require data controllers and data processors to implement a general personal data breach notification regime (which will include keeping a register of any data breaches).

The Swedish Post and Telecom Authority (Sw. Post och Telestyrelsen) ("the PTA") is the supervisory authority responsible for the administration of the ECA and the PDA in the telecommunications sector. The Swedish Data Protection Authority (Sw. Datainspektionen) ("the DIA") may also supervise compliance with the PDA in cases where personal data processing falls outside of the scope of providing network and telecommunication services.

As referred to above, under chapter 1 section 8 ECA, if Sweden is (or has recently been) at war or under the threat of war, or if there are extraordinary conditions that are caused by a war outside of Sweden, the government holds the right to issue new regulations governing electronic communications networks and any associated facilities and services necessary to providing national defence or security. This may result in additional emergency powers for the regulator and consequently, limitations on the rights of Swedish individuals in regards to their right to property, privacy, a fair trial and freedom of expression.

Chapter 7 section 8 ECA stipulates that if a network operator or service provider does not fulfil its obligations under the law (e.g. their cybersecurity requirements) and this breach severely threatens public order, national security or public health or could otherwise be deemed to cause severe financial or operational problems for the supplier or the users of the electronic communication networks or services, the regulator may, with immediate effect, order an injunction against the relevant network operator or service provider (which effectively acts as a conditional cease operations order).

Note that under the ECA and the PDA, the regulator can in fact combine such injunctions with a conditional fine. Moreover, under the PDA a data controller is liable to pay damages to a data subject for any damage and violation of their personal privacy caused by the processing of personal data in contravention of the PDA, for example by not implementing sufficient cybersecurity measures.

An individual can also be subject to a fine or imprisonment of up to two years, in addition to being liable to pay damages, if he or she intentionally or by gross negligence, processes personal data in contravention of the provisions of the PDA. In practice, the courts more usually impose penalties in the form of fines and damages with custodial sentences being rare. The few custodial sentences that have been handed down by the Swedish courts have generally been in cases involving further offences, such as defamation.

The decisions of the PTA and the DIA can be appealed in the first instance to the Stockholm County Administrative Court (the "County Court"). To appeal a decision of the County Court, leave to appeal must be obtained which then permits the Stockholm Administrative Court of Appeal and if necessary the Supreme Administrative Court, to retry the case.

8. CYBERCRIME

8.1 The Penal Code (1962:700) (Sw. Brottsbalken) (the "PC")

The following acts of cybercrime are punishable under Swedish law:

SECTION	Offence	Penalty
Chapter 4 section 9c,	Illegal access, also referred to 'intrusion' or 'hacking' Defined as "intentionally, and without permission, accessing information aimed to be processed through an automated process". It also includes the illicit alteration, deletion, insertion, blocking or disruption of such data (including Denial of Service Attacks). This cybercrime further includes situations where a perpetrator may be able to illicitly gain access to information (even if he or she did in fact not do so). Note that the term "illegal access" encompasses all forms of data that can be processed by a computer, and includes data permanently stored on a computer (e.g. on a hard drive), temporarily stored for processing (e.g. ones and zeros in the random access memory of a computer) or actual programs processing the previously mentioned forms of data. In this context, it should also be noted that interception of a message conveyed by a telecommunications company may be categorised as the separate offence "illicit access" under chapter 4 sections 8-9 PC.	Fines or imprisonment for up to two years. In cases of gross illegal access (for example in aggravating circumstances such as when material damages have been caused) the penalty is imprisonment for a minimum of six months and a maximum of six years.
Chapter 9 section 2 PC	Computer-related fraud Defined as the act of providing inaccurate or incomplete information by altering a computer program or recording, or otherwise illicitly affecting the outcome of an automated information process or a similar automated process, so that the offender benefits to the detriment of someone else. This provision therefore encompasses computer system or data manipulation which is carried out for financial profit i.e. the copying of magnetic strips on credit cards ('skimming') and 'phishing' attacks where, for example, copies of banks' web pages would be set up in order to steal the bank's customers' login details.	Fines or imprisonment for up to six months. Under aggravating circumstances the offender may be sentenced to imprisonment for a minimum of six months and a maximum of six years.

Additionally, if any of the criminal acts described above cause loss, this may lead to criminal liability for damages.

The authorities responsible for the administration of cybercrime legislation are the Swedish Ministry of Justice and the National Police Authority.

Chapter 2 section 4 PC stipulates that the legislation on cybercrime has extraterritorial reach, provided that the criminal act in question is directed towards Swedish data or Swedish IT-systems (e.g. non-nationals engaged in hacking activities in the jurisdiction).

Criminal cases pertaining to cybercrime are adjudicated by the general courts, i.e. the district courts, the Court of Appeal and the Supreme Court. If an offender has been sentenced to a fine in the district court and wishes to appeal this, a leave of appeal is necessary. Leave of appeal is also necessary should an appeal to the Supreme Court be sought by a defendant.

Law stated as at 17 February 2017.