COUNTRY COMPARATIVE GUIDES 2022

The Legal 500 Country Comparative Guides

Sweden

TMT

Contributor

Hellström Law

Anna Fernqvist Svensson

Lawyer, Partner, Owner | anna.fernqvist@hellstromlaw.com

This country-specific Q&A provides an overview of tmt laws and regulations applicable in Sweden.

For a full list of jurisdictional Q&As visit **legal500.com/guides**

SWEDEN
TMT

1. What is the regulatory regime for technology?

Please see references to relevant legislation below.

2. Are communications networks or services regulated?

Communication networks and services are mainly regulated in the Electronic Communications Act (Sw. Lag om elektronisk kommunikation) and the GDPR. The Radio and TV Act (Sw. Radio- och tv-lag) and the Radio Equipment Act (Sw. Radioutrustningslag) also contain relevant legislation.

3. If so, what activities are covered and what licences or authorisations are required?

The Electronic Communications Act applies to electronic communication networks and services and their corresponding installations, services and other radio usage. The transmitted content itself does not fall within the scope of the act. According to the act, public communication networks that are normally provided in exchange for money, and publicly accessible communication services, may only be provided if the business has been reported to the Swedish Post and Telecom Authority (Sw. Post- och telestyrelsen).

4. Is there any specific regulator for the provisions of communications-related services?

The Swedish Post and Telecom Authority and the Swedish Authority for Privacy Protection, abbreviated IMY (Sw. Integritetsskyddsmyndigheten) are the main regulators of communication-related services.

5. Are they independent of the government control?

The Ministry of Infrastructure (Sw. Infrastrukturdepartementet) is responsible for the Post and Telecom Authority and the Ministry of Justice (Sw. Justitiedepartementet) is responsible for the Swedish Authority for Privacy Protection.

6. Are platform providers (social media, content sharing, information search engines) regulated?

Yes, the Bulletin Board System Act (Sw. Lag (1998:112) om ansvar för elektroniska anslagstavlor), the GDPR and the Electronic Communications Act are applicable. As a starting point, the person who publishes something in social media that is regarded as personal information is responsible for the personal information that the publication entails. The company that provides the platform may also be liable if the company has the ability to influence posts or determine which posts shall be published.

In some cases, a publication may be covered by the so-called private exemption in the GDPR. According to the private exemption, the GDPR shall not apply to the processing of personal data carried out by a natural person in the course of a purely personal or household activity. If a person publishes personal data for a wider audience, for example by publishing pictures or other things in social media, then it is not to be considered a matter of purely private nature. This means that the private exemption does not apply and the person who publishes becomes the data controller for the publication.

According to the Bulletin Board System Act the provider/administrator of an electronic bulletin board is required to provide information to anyone who uses the service about the provider's/administrator's identity and the extent to which incoming messages become available to other users. The provider/administrator

should also have such oversight of the service that is "reasonably required with regard to the scope and direction of the business". According to the law, the provider of an electronic bulletin board is also responsible for removing or otherwise preventing messages from spreading if:

- the content obviously means unlawful threat, unlawful violation of personal integrity, incitement, agitation against an ethnic group, child pornography offense or unlawful depiction of violence, or
- it is evident that the user has infringed the copyright or rights protected by the copyright law by submitting the message (eg attached copyrighted material).

If the provider/administrator is responsible for electronic message boards and a message is posted that contains, for example, material infringing copyright or racist statements, the provider/administrator is obliged to remove it as soon as possible. If the provider/administrator does not do so within "reasonable time", the provider/administrator may be held liable for violations of the Bulletin Board System Act, which may result in a fine or even imprisonment.

According to the new Swedish Electronic Communications Act (2022:482), which entered into force on 3 June 2022, providers of electronic communications are liable for their platforms and what is posted on them.

7. If so, does the reach of the regulator extend outside your jurisdiction?

The responsibility to comply with the Bulletin Board Act and Electronic Communications Act is imposed on the provider of the service itself and not on the provider of infrastructure or hardware for the service. This means that, regardless of the server's location, one can be held responsible if one is a Swedish citizen or resides in Sweden as a foreigner.

8. Does a telecoms operator need to be domiciled in the country?

There is no need to be domiciled in the country.

9. Are there any restrictions on foreign ownership of telecoms operators?

There are no restrictions on foreign ownership of telecom operators.

However, it shall be noted that in a ruling last year from the Administrative Court of Stockholm regarding the expansions of 5G networks, the court concluded that the Swedish Post and Telecom Authority was right in combining authorization to use radio transmitters with bans on Huawei products in central functions in Swedish 5G networks. Furthermore, the use of personnel or functions placed abroad should cease on 1 January 2025 and, if necessary, replaced with personnel and functions within Sweden. This was all decided due to the potential security risks to Swedish networks. The investigation largely consisted of assessments made by the Swedish Security Police and the Armed Forces.

10. Are there any regulations covering interconnection between operators?

In chapter 5 of the new Electronic Communications Act, the matter of interconnection between operators is covered. Operators of a public communication net are obliged to negotiate about interconnection with those who provide, or intend to provide, electronic communication services to the public. Such negotiations are subject to confidentiality.

According to chapter 5, sections 3-4 of the act, the Swedish Post and Telecom Authority may impose obligations on operators who control the end users´ access to interconnect, to take measures that enables the end users to connect with each other. As for operators with significant market power, they can be obliged to e.g. adopt non-discriminating terms and fulfil certain demands relating to the access and use of the net in question in accordance with chapter 5 sections 8-21 of the act.

11. If so are these different for operators with market power?

According to chapter 5, sections 3-4 of the act, the Swedish Post and Telecom Authority may impose operators who control the end users´ access to interconnect, to take measures that enables the end users to connect with each other. As for operators with significant market power, they can be obliged to e.g. adopt non-discriminating terms and fulfil certain demands relating to the access and use of the net in question in accordance with chapter 5 sections 8-21 of the act.

12. What are the principal consumer protection regulations that apply

specifically to telecoms services?

In chapter 5 of the Electronic Communications Act, the rights of consumers purchasing electronic communication services can be found. There are also provisions explaining the duties of the operators.

Operators that offer their services to consumers must have their prices and general terms accessible for the consumers. It is sufficient to have them uploaded to the website of the company. Furthermore, the agreement between the consumer and the operator must contain clear and easily accessible details about e.g. the lowest level of quality offered, the measures taken to measure and control the traffic with the purpose of avoiding overloads of the net and how the measures can affect the quality of the services, and delivery time. An agreement between a consumer and an operator may not have a longer curing period than 24 months.

After the curing period, an operator that has provided services in combination with terminal devices must, at the request of the consumer, remove operating locks without charge or delay.

13. What legal protections are offered in relation to the creators of computer software?

Computer software and their creators are protected through several acts, the most relevant being the Patent Act (Sw. Patentlagen), the Act on the Right to Employee´s Inventions (Sw. Lag om rätten till arbetstagaresuppfinningar), the Circuit Pattern Protection Act (Sw. Lag om skydd för kretsmönster för halvledarprodukter), the Industrial Secrets Protection Act (Sw. Lag om skydd för företagshemligheter), and the Copyright Act (Sw. Lag om upphovsrätt till litterära och konstnärliga verk).

Program codes per se are not eligible for patent registration in Sweden. A technical invention that is executed by software can however be patentable, thus resulting in an indirect protection of the software.

Software will obtain copyright protection if it is original in the sense that it is an intellectual creation of the creator.

14. Do you recognise specific intellectual property rights in respect of data/databases?

There is no specific recognition of intellectual property rights in respect of data/databases. It is nonetheless possible for databases to acquire copyright protection under section 49 of the Copyright Act, which implements Directive 96/9/EC. The article stipulates that a person who has created a catalogue, chart or similar, in which a great number of data have been compiled, or which is the result of a big investment, has the exclusive right to produce copies of the work and make it accessible for the public. The aforementioned right is valid until fifteen years after the year of creation of the work have passed. If the work has been made accessible for the public within fifteen years, the right becomes valid until fifteen years from the publication have passed.

15. What key protections exist for personal data?

The key protections are mainly laid out in the GDPR, together with some supplementary Swedish legislation. In summary, the following can be said about the protection.

Basic principles

Personal data shall be:

(a) processed lawfully, fairly and in a transparent manner in relation to the data subject (‘lawfulness, fairness and transparency’);

(b) collected for specified, explicit and legitimate purposes and not further processed in a manner that is incompatible with those purposes; further processing for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes shall, in accordance with Article 89(1) of the GDPR, not be considered to be incompatible with the initial purposes (‘purpose limitation’);

(c) adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed (‘data minimisation’);

(d) accurate and, where necessary, kept up to date; every reasonable step must be taken to ensure that personal data that are inaccurate, having regard to the purposes for which they are processed, are erased or rectified without delay (‘accuracy’);

(e) kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed; personal data may be stored for longer periods insofar as the personal data will be processed solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) of the GDPR subject to implementation of the appropriate technical and organisational measures

required by the GDPR in order to safeguard the rights and freedoms of the data subject ('storage limitation');

(f) processed in a manner that ensures appropriate security of the personal data, including protection against unauthorised or unlawful processing and against accidental loss, destruction or damage, using appropriate technical or organisational measures ('integrity and confidentiality').

Furthermore, data controllers are obliged to be able to demonstrate that, and how, they fulfil the obligations of the GDPR (accountability).

Legal basis

All processing of personal data has to rest on at least one of the six legal grounds set out in the GDPR. The six legal grounds are the following:

- Processing of personal data that emanates from consent from the data subject. The consent can cover one or several specific purposes.
- Processing of personal data that is necessary to fulfil a contract to which the data subject is a party or in order to take steps at the request of the data subject prior to entering into a contract.
- Processing of personal data that is necessary to fulfil a legal obligation.
- Processing of personal data that is necessary to protect vital interests of the data subject or other natural persons.
- Processing of personal data that is necessary to carry out a task that is of public interest, or in line with the exercise of official authority of the data controller.
- Processing of personal data that is necessary for purposes of legitimate interests pursued by the data controller or a third party. This does not apply when interests or fundamental rights and freedoms of the data subject require protection of the personal data, especially when the data subject is a child. The exclusion cannot be applied to processing executed by public authorities in the performance of their tasks.

Information duty

It must be clear for the data subjects how their personal data are processed. Accordingly, the data subjects must be made aware of the processing of personal data per se, why the data is being processed, and how it is used. Understandable information must be provided by the data controller about the processing and in a manner which makes it easy for the data subjects to find the information. If the data subjects are children, the language needs to be even clearer. See articles 13 and 14 of the GDPR.

Rights of the data subjects

Data subjects have a number of rights listed in the GDPR. These are mainly laid out in articles 15 up to and including 21 and comprise the following rights:

- Right to information and access by the data subject;
- Right to rectification;
- Right to erasure;
- Right to restriction of processing;
- Right to notification of erasure or restriction of processing;
- Right to data portability; and
- Right to object.

The data subjects have the right to receive the personal data provided to a data controller in a structured, commonly used and machine-readable format (Right to access). Upon request from the data subject, the personal data is under certain circumstances to be erased (Right to erasure). Moreover, the data subject has the right to transfer those data to another data controller without hindrance where (i) the processing is based on consent pursuant to point (a) of article 6(1) or point (a) of article 9(2) or on a contract pursuant to point (b) of article 6(1); and (ii) the processing is carried out by automated means (Right to data portability). When it is technically feasible, the data subject has the right to have personal data transmitted directly from one data controller to another.

It shall also be noted that more stringent rules apply to 'sensitive' personal data (e.g. personal data relating to health or trade union membership).

16. Are there restrictions on the transfer of personal data overseas?

There are no restrictions regarding transfer of data between states in the EEA.

The GDPR stipulates when transfers of personal data to an area outside of the EEA are allowed. In short, transfers are permitted when:

- there is a decision from the Commission stating that a third-party state ensures an adequate level of protection for personal data;
- the data controller has made suitable protection measures, such as Binding

Corporate Rules or Standard Contractual Clauses;
- special situations and single cases require it, such as e.g. when the data subject has explicitly consented to the proposed transfer, after having been informed of the possible risks of such transfers for the data subject due to the absence of an adequacy decision and appropriate safeguards; the transfer is necessary for the performance of a contract between the data subject and the data controller or the implementation of pre-contractual measures taken at the data subject's request; the transfer is necessary for the conclusion or performance of a contract concluded in the interest of the data subject between the data controller and another natural or legal person; the transfer is necessary for important reasons of public interest.

17. What is the maximum fine that can be applied for breach of data protection laws?

According to article 83 in the GDPR, the maximum fine that can be applied for a breach is EUR 20 million, or 4 % of the company´s annual turnover of the previous financial year, whichever is higher. According to the Swedish Data Protection Act (2018:18), a public authority can be fined with maximum MSEK 10.

18. What additional protections have been implemented, over and above the GDPR requirements?

The Data Protection Act (2018:218) and the Data Protection Ordinance (2018:19) (the "DPA") contain further regulations regarding data protection on aspects allowed by the GDPR. The DPA contains regulations regarding the processing of data concerning criminal offences and processing of social security number. The DPA also contains regulations that the GDPR is applicable outside its actual scope. However, the DPA is subsidiary in relation to other law or regulation, which allows for deviating provisions. Apart from the DPA there are a number of sector specific acts such as the Swedish Patient Data Act (2008:355), the Swedish Eletronic Communications Act (2022:482), the Swedish Marketing Act (2008:486), the Swedish Criminal Data Act (2018:1177) etc.

19. Are there any regulatory guidelines or legal restrictions applicable to cloud-based services?

Typically, a cloud service provider will qualify as a data processor according to the GDPR. In order for the processing of the data processing to be compliant with the GDPR there has to be a written contract between the data controller and the data processor. This contract is supposed to make sure that the data processor protects the personal data with all technical and organisational measures necessary to ensure the protection of the rights of the data subjects. Due to the Schrems II judgement of the European Court of Justice on 16 July 2020 the use of US based cloud services must be assessed by the customers using said services. The EU-US Privacy Shield was declared invalid by the court and therefore a verification of the data protection laws in the recipient country must be made and the risk assessment must be documented. Even if you use the SCCs or the new SCCs adopted by the European Commission on 4 June 2021 you have to take supplementary measures to make sure (to the extent possible) that the transfer of personal data to the US is safe. See also the proposal for a new NIS 2 directive in section 17.1 below. In accordance with Article 16 of Regulation (EU) No 1094/20101, EIOPA has issued guidelines which provides insurance and reinsurance companies with guidance on how the regulations on assignment agreements in Directive 2009/138/EC2 (Solvency II) and in Commission Delegated Regulation (EU) 2015/353 (the delegated regulation) shall apply for assignment agreements with cloud service providers (EIOPA-BoS-20-002).

The guidelines are addressed to the competent authorities and are intended to provide guidance on how insurance and reinsurance undertakings should apply the requirements for assignment agreements set out in the above acts in the context of outsourcing to cloud service providers.

The guidelines apply from 1 January 2021 for all assignment agreements on cloud services entered into or modified on or after this date.

20. Are there specific requirements for the validity of an electronic signature?

The general requirements for electronic signatures are set out in the eIDAS Regulation (EU 910/2014) and the Act on Supplementary Regulations to the eIDAS Regulation (Sw. Lag med kompletterande bestämmelser till EU:s förordning om elektronisk identifiering). Detailed provisions regarding the requirements are however not included in the aforementioned documents. Instead, the Commission has the authority to further specify the

standards required.

An electronic signature can be created in two ways.

Either directly, with the help of an electronic certificate that connects validation data for an electronic signature to a physical person, confirming at least the name or pseudonym of the person, or

Indirectly, in the sense that the user proves her/his identity so that a special signature certificate can be delivered by a third-party service and then used to produce the electronic signature.

In eIDAS, there are three levels of security relating to electronic signatures. These are: standard electronic signatures, advanced electronic signatures (AdES), and qualified electronic signatures (QES). Standard electronic signatures have the lowest level of trust, and can e.g. be in the shape of a scanned handwritten signature. A QES has the highest level of trust. It is the only type of signature that has the same legal value as a handwritten signature. For an electronic signature to become a QES, it requires that the signatory uses a certificate based digital ID that has been issued by a Trust Service Provider (TSP), together with a qualified signature creating device (QSCD). The QSCD can be in the shape of a smart card, a USB token or an application that creates a disposable password.

Different levels of security are needed depending on what the signatory wants to do.

21. In the event of an outsourcing of IT services, would any employees, assets or third party contracts transfer automatically to the outsourcing supplier?

No, not automatically. However, if an asset of a business according to section 6 b of the Swedish Employment Protection Act (Sw. Lag om anställningsskydd), e.g. an IT service, which is deemed to be an “autonomous economic entity”, is being transferred, an employee working in that department might be transferred to the outsourcing supplier, unless he or she refuses. In practice, this is not an issue, since it tends to be solved by the involved parties.

As for assets and third-party contracts, no transfer to the outsourcing supplier will occur.

22. If a software program which purports to be a form of A.I. malfunctions, who is liable?

The question of A.I. malfunction liability would, for the time being, probably have to be resolved with the help of provisions concerning product liability and classical principles of liability. If this would result in a fair result remains to be seen.

23. What key laws exist in terms of: (a) obligations as to the maintenance of cybersecurity; (b) and the criminality of hacking/DDOS attacks?

(a) obligations as to the maintenance of cybersecurity; and

The GDPR contains some provisions regarding the maintenance of cybersecurity. They are however mostly concentrated on the protection of personal data.

When it comes to the protection of technical infrastructure, the NIS directive (EU 2016/1148) has been implemented in Swedish law via the Swedish Act on IT Protection for Socially Important and Digital Services Act (Sw. lag om informationssäkerhet för samhällsviktiga och digitala tjänster) 1 August 2018. This act serves as the main framework. The purpose of the directive is to achieve a high level of security in networks and information systems that belong to:

1. services crucial to society within the sectors of
    - energy,
    - transport,
    - banking,
    - infrastructure of the finance market,
    - healthcare,
    - delivery and distribution of drinking water,
    - digital infrastructure, and
2. digital services in general.

Different rules apply for services that belong to categories 1 and 2.

The European Commission presented on 20 December 2020 a proposal for an update of the NIS directive, the so called NIS 2. The proposal contains inter alia extended and strengthened supervisory possibilities, fines when in breach of the rules on risk management and incident reporting, an EU network with representatives from national crisis management authorities which shall inter alia lead to a coordinated handling of cyber incidents and crisis with cross-border

impact, extended sharing of information, extended and more detailed obligations on entities covered by the NIS directive, extended number of sectors to be considered such as the postal service, waste water, public administration, critical industry production such as production of pharmaceuticals, med tech and chemicals and cloud based services.

According to the Swedish Act on Protection Security (Sw. säkerhetsskyddslagen (2018:585)), parties that conduct business or manage operations of importance to Swedish security interest as well as of Swedish international commitments, shall implement security safeguards. On 29 April 2021 the Swedish Government proposed a new act on supplementary rules to the EU Cybersecurity Act. The proposed act entered into force on 28 June 2021. The government has given the Defence Materiel Administration the task to act as authority for cyber security certification in Sweden. Two units at the Defence Materiel Administration will administer the function, partly the newly created Inspectorate for Cyber Security Certification (*Sw. Inspektionen för cybersäkerhetscertifiering*) and partly the Swedish IT Security Certification Body (*Sw. Sveriges Certifieringsorgan för IT-säkerhet*), previously organized within the Defence Materiel Administration. The function is divided into an inspection regarding cyber security certification and a body for certification of IT-security. This division is made to ensure requirements on independence.

(b) the criminality of hacking/DDOS attacks?

Chapter 4, section 9 c of the Penal Code (Sw. Brottsbalken) stipulates the illegality of DDOS attacks and hacking. The punishment is a fine or imprisonment for up to two years. If the DDOS attack or hacking can be considered severe, the punishment is imprisonment for up to six years.

24. What technology development will create the most legal change in your jurisdiction?

It is plausible that the swift development of A.I. and self-controlling vehicles will result in the biggest legal change in the near future. However, one should not underestimate the legal and economic consequences that could occur if crypto currencies and blockchain technologies are allowed to further develop.

25. Which current legal provision/regime creates the greatest impediment to economic development/ commerce?

As a member state of the EU, Sweden implements and applies all EU legislation. National Swedish laws, not emanating from the EU, do not create any major impediments to economic development.

Some legislation regarding taxation, employment protection and permits for the construction of buildings could be seen as hindering. Long processing times with the authorities is also an impediment to economic development that is difficult to contradict.

26. Do you believe your legal system specifically encourages or hinders digital services?

Digital services are ruled in essence by EU legislation. The provisions set out in Swedish legislation are often of a general character, with supplementary information in the preparatory works. Sweden strives for being in the forefront when it comes to digital services and the legislation is not hindering this development.

The Swedish tech-market has been seen continuous and rapid development for a long time. In 2017 Forbes ranked Sweden as the best country in the world for business and Sweden still enjoys a solid position at the top of the table. The technology friendly system has enabled many Swedish tech-companies to flourish. In addition to this, Sweden is widely considered to be one of the leading countries in Europe when it comes to technology start-ups. In May 2021 the investment company GP Bullhound reported that Sweden holds the number one position for the most valuable tech companies in Europe. Thanks to substantial value appreciations from Swedish companies such as Klarna, Spotify and Evolution Gaming the total value of the Swedish tech companies has reached 151 billion US dollars. Many fast growing tech companies have been established by persons previously working for the Swedish companies, Spotify, Skype, iZettle et al. Sweden had 21 unicorns by December 2021.

As for legislative measures that encourages digital services and development, it should be mentioned that it is possible to apply for generous tax deductions for employees working with R&D.

27. To what extent is your legal system ready to deal with the legal issues associated with artificial intelligence?

The Swedish legal system is not yet completely ready to

deal specifically with legal issues associated with A.I. Since Sweden is far from alone in the EU in this regard, it is not unlikely that this will be resolved within the EU. In Sweden work is being performed in this regarding pointing out the importance of guidelines and standards and the cooperation within the EU in this field.[1] On 19 February 2020, the European Commission published a White Paper aiming to foster a European ecosystem of excellence and trust in Artificial Intelligence[2] and Report on the safety and liability aspects of AI.[3] The White Paper proposes:

- Measures that will streamline research, foster collaboration between Member States and increase investment into AI development and deployment;
- Policy options for a future EU regulatory framework that would determine the types of legal requirements that would apply relevant actors, with a particular focus on high-risk applications.

On 21 April 2021, the EU Commission presented its proposal for a regulation on harmonized rules for artificial intelligence in the framework of Digital Europe Strategy COM(2021)206. The Swedish Government has commented on the proposal and is positive to it and sees the importance in the continued work concerning artificial intelligence. Thus, the adaptation to artificial intelligence is a work in progress and we expect many developments of the legal system in the coming years.

[1] See e.g. the report of the Swedish Ministry of Enterprise and Innovation National direction for artificial intelligence (Sw. Nationell inriktning för artificiell intelligens), N2018.14, in which it is stipulated inter alia that Sweden shall be the best country in the world using the possibilities of digitalization and Sweden is in the very forefront compared with other countries around the globe. The aim of the document is to point out general direction of the A.I. work in Sweden and to lay the basis for future priorities.

[2] White Paper on Artificial Intelligence – A European approach to excellence and trust, COM(2020) 65 final.

[3] Report on the safety and liability implications of Artificial Intelligence, the Internet of Things and robotics, COM(2020) 64 final.

Contributors

Anna Fernqvist Svensson
Lawyer, Partner, Owner

anna.fernqvist@hellstromlaw.com