|  |  |
| --- | --- |
| **To:** | The Finnish AIPPI group |
| **Date:** | 8 April 2020 |
| **Subject:** | AIPPI 2020 - Study Question - Rights in Data (Finland) |

# Current law and practice

*Please answer all questions in Part I on the basis of your Group's current law.*

# A. Protection of mere data

### 1) Can mere data (in general or some specific mere data) be subject to a property right / IP right? If yes, please answer the following sub-questions:

Yes.

**a) What type of property right / IP right would this be?**

Mere data can be subject to trade secret protection if it meets the requirements for protection set forth in the Finnish Trade Secrets Act (595/2018). We note, however, that the classification of trade secrets as an IP right or property right is not unambiguous.

Should mere data be aggregated or arranged in a way that it meets the requirement for protection as a catalogue or database, the answers below for questions I B apply.

**b) What are the requirements for such protection?**

In order for mere data to receive protection as a trade secret, it must meet the legal definition of a trade secret. Under Finnish law, a trade secret is defined as information a) which is not, as a body or in the precise configuration and assembly of its components, generally known among or readily accessible to persons who normally deal with the kind of information in question; b) which has financial value in business activities owing to a characteristic referred to in subparagraph a; and c) the lawful holder of which has taken reasonable steps to protect. Whether the above criteria are fulfilled in an individual case must be assessed on a case-by-case basis.

(Section 2 of the [Finnish Trade Secrets Act](https://www.finlex.fi/fi/laki/ajantasa/2018/20180595) (595/2018), Finnish and Swedish translations available only)

**c) Who is the owner of this property right?**

The trade secret holder is any natural or legal person lawfully controlling the trade secret. This allows not only the original proprietor of a trade secret but also *e.g.* licensees to defend a trade secret. Whoever is lawfully controlling a trade secret should be assessed on a case-by-case basis, for example, under licensing agreements or agreements on the use and disclosure of trade secrets.

(Section 2 of the [Finnish Trade Secrets Act](https://www.finlex.fi/fi/laki/ajantasa/2018/20180595) (595/2018), Finnish and Swedish translations available only)

**d) What acts are prohibited for third parties to avoid infringement?**

A trade secret may not be unlawfully acquired or attempted to be acquired. This includes acquisitions carried out by a) unauthorised appropriation; b) unauthorised copying, reproduction, observation or other processing of documents or other sources containing trade secrets (or from which such can be deduced); or c) other conduct contrary to honest commercial practices. An acquisition is also unlawful if a person, at the time when acquiring the trade secret, either knew or ought to have known that the trade secret was obtained directly or indirectly from a person who was using or disclosing it unlawfully. There are also specific provisions outlining what is not deemed as an unlawful acquisition (*e.g.* reverse engineering).

A trade secret may also not be unlawfully used or disclosed by a person having acquired the trade secret unlawfully (as outlined above) or by a person who has obtained information about the trade secret a) when acting in specific roles of an entity or foundation; b) in connection with enterprise restructuring proceedings; c) when performing a task for another person or otherwise in a confidential business relationship; or d) in another manner if bound by an agreement or obligation restricting the right to use or disclose the trade secret. Information obtained while being employed may not be unlawfully used or disclosed during the term of employment. Lastly, a trade secret may not be unlawfully used or disclosed by a person who knows or ought to know that the trade secret was obtained directly or indirectly from a person who was using or disclosing the trade secret unlawfully.

(Sections 3 and 4 of the [Finnish Trade Secrets Act](https://www.finlex.fi/fi/laki/ajantasa/2018/20180595) (595/2018), Finnish and Swedish translations available only)

**e) Is this right marketable? If so, are specific rules in contract law applicable?**

Yes. A trade secret may be transferred (i.e. sold or licensed), and general contract law principles apply. Also, competition law restrictions should be taken into account.

**f) Does your legislation/case law contain specific exceptions to this protection (e.g. access right for data mining, scientific research, etc.)?**

Yes. Exceptions include acquisition, use or disclosure for the purpose of protecting the general public interest to reveal misconduct or illegal activity (i.e. whistleblowing), or where it does not exceed what can be regarded as acceptable exercise of freedom of expression. Trade secrets may also be disclosed by an employee to certain employee representatives where the disclosure is necessary for the performance of the representative’s duties under law or a collective agreement.

(Sections 5 and 6 of the [Finnish Trade Secrets Act](https://www.finlex.fi/fi/laki/ajantasa/2018/20180595) (595/2018), Finnish and Swedish translations available only)

### 2) Is mere data protected by provisions other than a property right / IP right? If yes, please answer the following sub-questions:

Yes.

**a) What type of protection is available?**

Ownership of and right to use mere data may be created also through contractual provisions. The extent and nature of the protection depends on the contract between the parties.

Trade secrets are also protected by criminal law provisions. The Finnish Criminal Code (39/1889) regulates trade secret related crimes such as business espionage, violation of a business secret and misuse of a business secret.

Further, the Finnish Criminal Code provides for indirect protection of mere data by criminalising unauthorised access to data by way of hacking and other similar acts.

(Chapter 38, Sections 8 and 8a of the [Finnish Criminal Code](https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001) (39/1889, as amended))

(Chapter 30, Sections 4-6 of the [Finnish Criminal Code](https://www.finlex.fi/fi/laki/ajantasa/1889/18890039001) (39/1889, as amended))

**b) What are the requirements for such protection?**

Contractual protection: Please see the answer above to question I A 2) a).

Criminal law provisions for trade secrets: Please see the answer above to question I A1) b).

**c) Who is the person entitled?**

Contractual protection: Please see the answer above to question I A 2) a).

Criminal law provisions for trade secrets: Please see the answer above to question I A 1) c).

**d) What acts are prohibited for third parties to avoid infringement?**

Contractual protection: Please see the answer above to question I A 2) a).

Criminal law provisions for trade secrets: Business espionage covers acts of a) entering an area closed to unauthorised persons or accessing an information system protected against unauthorised persons; b) gaining possession of or copying a document or other record; or c) using a special technical device; with the intention of unlawfully revealing or utilising the trade secret. Violation of a business secret covers acts of unlawfully disclosing a trade secret of another or unlawfully utilising such, having gained knowledge of the secret in a specific position (*e.g.* while in the service of another, while acting in a specific role of a company, while performing a duty for another or while in a fiduciary business relationship, or during company restructuring proceedings) in order to obtain financial benefit for oneself or another or to injure another. Lastly, misuse of a business secret covers acts of using a trade secret which has been obtained or revealed through an act punishable under the Criminal Code in business activities or revealing a trade secret in order to obtain financial benefit for oneself.

Criminal law provisions prohibiting computer-based break-in: The Finnish Criminal Code prohibits any unauthorised access to data. The Code prohibits both: (i) acts which attempt to gain unauthorised access to an information system in which data is stored (including both the use of unauthorised user credentials as well as exploitation of security vulnerabilities); and (ii) attempts, through means of technical circumvention or security exploitation, to read or otherwise observe the data from outside of the information system.

**e) Are mere data marketable? If so, are specific rules in contract law applicable?**

Contractual protection: Yes. Normal contract law principles apply. General competition law restrictions should be taken into account.

**f) Does your legislation/case law contain specific exceptions to this protection (e.g. access right for data mining, scientist research, etc.)?**

No.

# B. Protection of databases

### 3) Can a database be subject to a property right / IP right? If yes, please answer the following sub-questions:

Yes.

**a) What type of property right / IP right would this be?**

Copyright, sui generis database right, catalogue protection or trade secret protection.

**b) What are the requirements for such protection?**

Sui generis database right: The *obtaining*, *verification* or *presentation* of a database has required substantial investment. This may mean a substantial investment in time, money or efforts. The investment should be directed *e.g.* at collecting or presenting the database and any investment in solely *creating* the content is irrelevant for the sui generis database protection.

Catalogue protection: A large number of information is compiled in a catalogue, table, program or another product. The main requirement for protection relates to quantitative and not qualitative criteria.

Copyright: A database can be protected by copyright in case it fulfils the requirements for copyright protection that is, it must be a sufficiently original and independent piece of work.

Trade secret: Please see the answers above to questions I A 1). This also applies to all subquestions below.

(Sections 1 and 49 of the [Finnish Copyright Act](https://www.finlex.fi/fi/laki/ajantasa/1961/19610404) (404/1961, as amended))

**c) Who is the owner of this property right?**

Sui generis database right and catalogue protection: The maker of the database or catalogue which also may be an entity that has financed or ordered the compilation of the database or catalogue. Further, the right to a database or catalogue that has been created in an employment relationship within the scope of the employee's duties shall automatically pass to the employer.

Copyright: The author of the database.

(Sections 1, 40b, and 49 of the [Finnish Copyright Act](https://www.finlex.fi/fi/laki/ajantasa/1961/19610404) (404/1961, as amended))

**d) What acts are prohibited for third parties to avoid infringement?**

Sui generis database right and catalogue protection: Third parties are prohibited to make copies or make available to the public the whole or, in qualitative or quantitative terms, a substantial part of the database or catalogue. The protection for databases and catalogues is available for 15 years from the year in which the product was completed or, if the product was made available to the public before the end of that time, until 15 years have elapsed from the year in which the product was made available to the public for the first time.

Copyright: Third parties are prohibited to make the protected work or a part of it available to the public or to reproduce it, including transferring it to another device. The protection is available until 70 years have elapsed from the year of the author's death.

**e) Does your legislation/case law contain specific exceptions to this protection (e.g. access right for data mining, scientist research, etc.)**

Yes. Under the Finnish Copyright Act, largely similar exceptions apply to the protection by copyright, sui generis database right and catalogue protection. With respect to published databases, such statutory exceptions include *e.g.* a right to quote, a right to reproduce for use in educational activities or in scientific research and a right to make single copies for a private use. However, the right to make single copies for private use does not permit to make a computer-readable copy of a computer-readable database. Furthermore, there are for instance certain exceptions that are applicable to certain archives, libraries and museums with respect to protected works included in their own collections.

The sui generis database right and catalogue protection only protect the database or catalogue in whole or in their substantial parts. Therefore, unsubstantial parts of a database or a catalogue are not similarly protected.

### 4) Are databases protected by any provision other than a property right / IP right? If yes, please answer the following sub-questions:

Please see the answers above to questions I A 2).

**a) What type of protection is available?**

Please see the answer above to question I A 2) a).

**b) What are the requirements for such protection?**

Please see the answer above to question I A 2) b).

**c) Who is the person or entity entitled to this protection?**

Please see the answer above to question I A 2) c).

**d) What acts are prohibited for third parties to avoid infringement?**

Please see the answer above to question I A 2) d).

**e) Does your legislation/case law contain specific exceptions to this protection (e.g. access right for data mining scientist research, etc.)**

Please see the answer above to question I A 2) f).

# C. Public Sector Information (PSI)

### 5) Does your legislation contain regulation/case law regarding PSI? If YES, please explain.

Yes. The topic is regulated in the Act on Openness of Government Activities (621/1999, as amended), under which official documents shall be public, unless otherwise regulated. A “document” is defined as a written or visual presentation, but also as a message relating to a given topic or subject-matter and consisting of signs which due to their use are meant to be taken as a whole, but are decipherable only by means of a computer, an audio or video recorder or some other technical device. Official documents also include *e.g.* documents delivered to or commissioned by an authority.

The Act regulates *e.g.* when a document enters the public domain, how access is granted to a document, and secrecy restrictions. The Act also includes a general duty of authorities to promote access, including that authorities shall promote the openness of their activities and, where necessary, produce inter alia guides, statistics and other publications on their services and practices. When requested to do so, an authority may compile and deliver a set of data, if the delivery is not contrary to document secrecy and the protection of personal data.

In addition, questions relating to *e.g.* information management, data security, production of datasets, electronic disclosure and interoperability of information systems are regulated in the Act on Information Management in Public Administration (906/2019).

An example of regulation regarding PSI is the regulation on spatial information, which in Finland is included in the Act on Infrastructure for Spatial Information (421/2009, as amended) and its specifying Decree (725/2009, as amended), implementing the European Union (EU) -level INSPIRE Directive. The purpose of the Act is to improve the availability and use of spatial data held by public authorities by creating a unified infrastructure for spatial information and making its services publicly available.

(Sections 1, 5, 20 and 21 of the [Act on Openness of Government Activities](https://www.finlex.fi/fi/laki/ajantasa/1999/19990621) (621/1999, as amended), the [Act on Information Management in Public Administration](https://www.finlex.fi/fi/laki/ajantasa/2019/20190906) (906/2019), the [Act on Infrastructure for Spatial Information](https://www.finlex.fi/fi/laki/ajantasa/2009/20090421) (421/2009, as amended), the [Decree on Infrastructure for Spatial Information](https://www.finlex.fi/fi/laki/alkup/2009/20090725) (725/2009, as amended))

### 6) Is there an access right to such PSI?

Yes. The Act on Openness of Government Activities contains provisions on the right of access to official documents in the public domain. Everyone has the right of access to an official document in the public domain, and access to documents not yet in the public domain is granted at the discretion of the authority. Access to secret documents is granted only in the situations specifically set forth in the Act.

The access right is facilitated by the avoindata.fi -service (available in English on https://www.opendata.fi/en), publishing public sector open data produced by the Finnish administration with the aim of promoting administrative transparency and facilitating access to public sector data for research and business development.

(Sections 9 and 10 of the [Act on Openness of Government Activities](https://www.finlex.fi/fi/laki/ajantasa/1999/19990621) (621/1999, as amended)).

The EU directives concerning re-use of PSI have been implemented and new legislation is currently under preparation in the EU. The Finnish Government has had an open data strategy and a program since 2012 for gradually opening public sector data resources and interfaces for the use of private persons and entities. The authorities have given decisions and orders that require offices, public companies and other public entities to open their information resources and data for more efficient use and wider dissemination, and the target is to proceed systematically and swiftly towards more open use of public sector information, data and interfaces. There are currently 1724 datasets from 791 publishers available at [https://www.opendata.fi/en.](https://www.opendata.fi/en)

# D. Health data

### 7) Does your legislation contain regulation/case law regarding health data? If YES, please explain.

Yes, especially given the nature of health data as sensitive personal data.

There are general rules for accessing data in the Act on Openness of Government Activities (621/1999, as amended), and more specific regulation regarding health data in the recently enacted Act Regarding Secondary Usage of Social and Health Information (552/2019, as amended). In addition, as a member of the EU, Finland applies the General Data Protection Regulation (GDPR, 2016/679). On a national level, there are some specifications to the GDPR in the Finnish Data Protection Act (1050/2018).

Many national laws in Finland contain specific provisions regarding the processing and use of health data, *e.g.* laws concerning patient records, customer data in social care and healthcare services and its electronic processing, and occupational healthcare.

### 8) Is there a right to access such information?

Yes.

According to the Act on Openness of Government Activities, everyone has the right of access to a public and official document, and access to documents not yet in the public domain is granted at the discretion of the authority. However, health data is categorised as secret information under the Act, and can be accessed only if the right to access has been regulated in another law or if the person whose health data is being used gives his consent to the access. According to the Act Regarding Secondary Usage of Social and Health Information, the Finnish authority may grant access to health data for a specific reason such as scientific research, gathering aggregated statistics, and education. The application for access to such information has to comply with the GDPR and other national legislation.

Also, the GDPR allows, under appropriate safeguards, the processing of special categories of personal data (including health data) for specific purposes, such as *e.g.* archiving purposes in the public interest, for scientific research, or for statistical purposes. Further situations where the prohibition of processing of special categories of personal data (including health data) does not apply are set forth in the Finnish Data Protection Act.

(Section 26 of the [Act on Openness of Government Activities](https://www.finlex.fi/fi/laki/ajantasa/2019/20190906) (621/1999), the General Data Protection Regulation (2016/679), the [Finnish Data Protection Act](https://www.finlex.fi/fi/laki/ajantasa/2018/20181050) (1050/2018)).

# Policy considerations and proposals for improvements of your Group's current law

**Could any of the following aspects of your Group's current law or practice relating to rights in data be improved? If YES, please explain and answer each of the sub-questions.**

### 9) Protection of mere data?

**a) Requirements for such protection(s)**

We consider that mere data should not be protected sui generis *e.g.*, by data producer right, i.e. there is no need for a new exclusive IP right.

As regards the protection of aggregated raw data and possible adjustments to current database right, please see question 10 below.

However, as discussed below under question 14, possibly some other type of protection instead of an IP type of exclusive right could be considered, *e.g.* in the form of limited protection against unauthorised access to mere data. The possible scope and content of such protection should be carefully analysed before any legislative action, and it should not lead to protecting mere data as such by law as an exclusive right. Therefore, we consider that the requirements for additional protection (if any) should be rather based on *the use* of mere data than its generation or existence.

If such new protection would be created, in order to gain protection, the mere data should have at least economic value in commercial activities and steps should have been taken to protect the mere data, similarly to what is required for trade secret protection. Mere data without any economic value in commercial activities should not be subject to protection.

**b) Ownership of the right(s)?**

We consider that the “ownership” of mere data (if any) should not be exclusive. As discussed above, a lawful non-exclusive control of mere data instead of exclusive ownership typical for IPRs could be considered. Protection against unauthorised access would be more relevant than ownership. Similarly to trade secret legislation, the possible new legislation (if any) should provide guidance regarding who is to be considered the holder of such right.

**c) Scope of the protection?**

Determining an appropriate term for the protection of such new protection (if any) is difficult as data typically has a very short life span. In this sense, there is necessarily no need for protection term of several years or even months. In any case, the term of protection should be much shorter than the term of protection of copyright and database.

Protection (if any) should concern commercial activities only. If anything, the right holder should have remedies against actions with economic benefit, circumvention of technical protection and perhaps access without authorisation.

**d) Exceptions to this protection?**

We are not supporting the creation of any exclusive right to protect data, but exceptions for this type of right (if any) should protect the public good and significant societal values such as science and education, environmental purposes, health and safety etc. Such exceptions should prescribe who is the beneficiary of such exception.

### 10) Protection of databases?

**a) Requirements for such protection(s)?**

As discussed above, in Finland databases currently enjoy protection under the Finnish Copyright Act Section 49, which governs both so called (1) catalogues and (2) databases (as amended in 1995 when the country entered the EU). The rights are partially parallel.

As for databases, substantial investment in the *obtaining*, *verification* or *presentation* of a database is required for protection. However, in order to be protected under the *catalogue* protection, it is only required that the material contains a substantial amount of information items.

Although database right and catalogue right are already available under Finnish law as neighbouring rights, it is currently unclear whether aggregated raw data that is not arranged in a systematic or methodical ways can be subject to the said rights and if yes, under what circumstances. This aspect could be further clarified, as discussed below:

In particular, improvement and clarification of legal provisions would be welcome regarding secondary use of databases and the question whether the requirement of "substantial investment" can be fulfilled with respect to data that has been automatically gathered or generated by machines (*e.g.* IoT devices).

In particular, it should be considered and clarified whether the threshold of "substantial investment" can be reached, if there has been a substantial investment in a complex machinery / system, which automatically gathers large amounts of data, without the data gathering being the exclusive or primary purpose of such system. In such case, we would suggest that obtaining database protection for the resulting material would, in addition to a substantial investment, also require that the data thus gathered is actually used and has commercial value.

Furthermore, we note that as to the Finnish situation, the existence of a national right (i.e. the right in catalogues), which essentially overlaps with the database protection, but seems however to be subject to a lower threshold, may cause confusion. Although there have so far not been significant problems in the coexistence of these two parallel rights, it should be analysed, whether such parallel rights should continue to coexist.

**b) Ownership of the right(s)?**

Currently, a “person who has made a database”, i.e. a natural person *or* a judicial person (*e.g.* a company) can be the (original) right holder. In the view of the Finnish group, this should continue to be the case.

However, we note that there may be need for further clarification in the future concerning the ownership with regard to *e.g.* complex IoT environments, where there may potentially be multiple parties who could be considered as the makers of the database, i.e. investors of time, money and efforts, and who are responsible for the acts and/or for the outcome of the compiling, verification and presentation.

**c) Scope of the protection?**

At present, the database right is an exclusive right to control the exploitation of the whole or in qualitative or quantitative terms, substantial part of a database by making copies (reproducing) of it and by making it available to the public in whatever manner.

As a point of departure, we consider the current requirements to be still valid, i.e. the right should cover the exploitation of the whole or in qualitative or quantitative terms substantial part of a database, but not the extraction of an individual information item. All in all, in the view of the Finnish group, the currently existing Finnish database right, which lies between traditional copyright and unfair competition, generally strikes a fair balance and represents a functioning implementation of the European directive on databases.

However, systematic unauthorised exploitation of individual items of data should also be within the scope of protection especially in cases where the target of the searches and extracts constitute a substantial part of the database, and there may be need for further clarification in this area. This issue is elaborated further under question 23.

**d) Exceptions to this protection?**

There are currently several exceptions to the database right, including the right of private copying (within certain limits discussed above), copying by certain cultural and educational institutions, as well as the citation right. These exceptions are found in Chapter 2 of the Finnish Copyright Act. We consider that clearly defined exceptions to database right will be needed in the future too.

As to the future, we find that an exception regarding so called data mining should be included (along the lines of the EU DSM Directive Articles 3 and 4 (text and data mining in scientific work and general provision on text and data mining)). Such exception should cover at least non-commercial data mining, and possibly also - within limited parameters - commercial data mining.

### 11) Rules on contract law, e.g. prohibition of contractual override, etc.?

Please see below our answers under questions 20 and 25.

**12) Are there any other policy considerations and/or proposals for improvement to your Group's current law falling within the scope of this Study Question?**

No.

# Proposals for harmonisation

**13)** In your opinion, should the protection of mere data and/or database be harmonized? For what reasons?

**If YES, please respond to the following questions without regard to your Group's current law or practice.**

**Even if NO, please address the following questions to the extent your Group considers your Group's current law or practice could be improved.**

Yes.

With regard to *mere data*: We support the idea of harmonisation that would prevent member states from passing laws or regulations that could result in monopolisation of information in any manner.

With regard to *databases*, currently, the regulation of rights to databases is internationally fragmented and the protection similar materials enjoy in different countries varies (*e.g.* the situation between EU and US differs significantly).

The existing regulation on databases, where such exists, may also be partially outdated and in need of updates: the currently existing EU database directive has been created during a time when databases were compiled, created and used locally through downloadable software. Currently, however, the compilation of databases differs significantly from the situation contemplated in the 1990s when the EU database directive was enacted: By way of example, databases may be compiled from data collected by networked IoT devices and software programs can search and access various information sources which can be located in different remote platforms geographically, and databases may be produced, held and accessed in multiple locations at the same time.

Consequently, the need for geographical harmonisation of protection of databases has in our view increased, and we also see a need to update the currently existing regulation (where such exists) as regards the object and scope of protection. This could happen mainly with an international agreement.

***Protection of mere data***

**14) Should mere data be subject to a specific protection, e.g. an IP right or other type of right?**

As discussed above under question 9, it is possible that there would be certain benefits in protecting mere data, but in the view of the Finnish group, some other type of protection instead of an IP type of exclusive right would serve better. We are concerned that granting exclusive rights to mere data involves the risk of monopolisation of information.

Consequently, we are not in support of the idea of protection of mere data in and of itself by a new exclusive IP right. However, we do support the idea of exploring further a limited protection against unauthorised access to mere data as long as such protection could be provided by regulation which would be specific and restricted in scope.

**15) If yes, what should be the requirements for such protection?**

It is difficult to define an exhaustive list of requirements that should be taken into consideration, if such limited protection against unauthorised access as discussed above under questions 9 and 14 would be created. At least, mere data that does not have economic value in commercial activities should not be protected. Additionally, active protection measures should be a requirement for protection, i.e. steps should be taken for protecting mere data in order to gain protection.

**16) Who should be the owner of this right / IP right?**

In the view of the Finnish group, it is difficult to define a single type of instance or entity which should be the “owner” of mere data, and as noted above, we do not support the creation of a new exclusive right for mere data as such. There are several instances with interest to own mere data, such as manufacturers, insurance companies and governments. Instances with interest solely to the output of mere data *e.g.*, applications, but not to mere data as such, should not be considered as potential “owners” of mere data.

Consequently, there should not be an “owner” per se for mere data and as noted above, if any new protection would be created, it should rather be focused on providing protection against unauthorised access to mere data. Furthermore, a controller of a set of mere data should only be protected against unauthorised access, if such controller has taken steps to qualify for the scope of protection, *e.g.* contractual steps to protect the data sets concerned. For the avoidance of doubt, no protection should be granted on the basis of mere generation or storing of data. Regulating the use of data should be more relevant than regulating its “ownership”.

**17) What acts should be prohibited to third parties to avoid infringement?**

If anything, unauthorised actions with economic benefit concerning a substantial part of the dataset should be prohibited. Also, right holders should have remedies against the circumvention of technical protection and possibly also other access without authorisation.

**18) Which exceptions, if any, should apply to this protection (e.g. access right for data mining, etc.)?**

Controllers of mere data should not have the right to restrict access to data where the requested access and related subsequent use serves general public interest or vital societal interest such as social, health or environmental interest. Also, mandatory access on the grounds similar to obligations stemming from dominant market position (under competition law) and significant market power (telecoms regulation) should be considered.

**19) What role should contract law play (e.g., prohibition of contractual override)?**

Generally speaking, we do not support restrictions on the freedom of contract. However, exceptions listed above should generally be mandatory and should therefore override contractual provisions.

***Protection of databases***

### 20) Should databases be subject to a specific protection, e.g. an IP right or other type of right?

Yes, they should. We consider that there is a need for an IP right protecting the investment made in creating compilations of data, and the sui generis database protection currently available under EU database directive seems an appropriate tool for this.

As regards aggregated data, we find possible clarifications and adjustments to the current database right a much better option than creating an entirely new IP right for mere data.

As discussed under question 10, there is a need for further clarification regarding the applicability and requirements of the currently existing database right vis-à-vis (aggregated) mere data. Furthermore, we wish to emphasise that the database right should continue to be inapplicable with regard to the individual data items, and the right should not be used to monopolise information.

### 21) If yes, what should be the requirements for such protection?

Please see above: the requirements should be linked to the substantial investment - either financial or other - made in order to create the database. However, as discussed above under question 10, there is a need for further clarity in this respect.

### 22) Who should be the owner of this right / IP right?

The maker of the database, i.e. the party that has made the financial or other investment necessary for making the database. It should be clear that this right may vest initially with a legal person. Please see question 10 b above.

### 23) What acts should be prohibited to third parties to avoid infringement?

Unauthorised exploitation (see above) of the whole database or substantial parts of it.

One point where clarification would be welcome is the concept of "substantial" part in the context of databases. Please see our answer to question 10 c above for further information.

Moreover, as discussed above under question 10 c, the question of unauthorised use of non-substantial extracts from a database should be analysed further, and possibly clarified. In the view of the Finnish group, there is a need to protect the right holders also in these cases: This could be the case *e.g.* where such use is systematic and continuous, or if the user knows or should have known that the taking of non-substantial extracts is prohibited in the licence agreement governing the database.

Furthermore, provision of unauthorised access to a database and the circumvention of technical protection measures protecting the database should be subject to further assessment. In this area, criminal law, in addition to IP legislation, may be an appropriate tool to give protection to the right holders.

### 24) Which exception should apply to this protection (e.g. access right for data mining, etc.)?

Please see our answer under question 10 d above.

### 25) What role should contract law play (e.g. prohibition of contractual override)?

Prohibition of contractual override has a role to play in situations where certain clearly defined user rights are deemed necessary for the public good and in order to avoid over-extending the scope of the protection. It should, however, be used with caution and a balance should be sought between the protection of the database maker's investment and public interest. The legislator has, for example, identified certain limited cases, where data mining should always be allowed, and the matter is solved by prohibition of contractual override.

Moreover, the Finnish group considers voluntary measures to encourage the use and agreeing on use of data generally desirable. One example of such measures is the encouragement of open data and availability of shared databases, especially in relation to data created in the public sector and/or using public funds.

***Specific regimes***

**26) Should Public Sector Information (PSI) be subject to a specific regime, e.g. regarding the control and access to such data/databases?**

We do not support any specific regime for PSI as regards control or access to such data/databases other than it is stated in our current legislation regarding PSI and the new Open Data and Public Sector Information Directive ((EU) 2019/1024).

### 27) Should health data be subject to a specific regime, e.g. regarding the control and access to such data/databases? If YES, please explain the desirable regime.

Yes. In particular, the data protection and privacy aspects must be carefully considered in this respect.

By way of example, Finland has recently started to promote secondary use of health and social data. A new Health and Social Data Permit Authority, Findata, started its operations in the beginning of 2020 with a task of facilitating data permit processing and improving data protection for individuals. The office also conducts anonymisation of data on behalf of controllers of health information. The gathering and utilising of information in this sector offers significant businesses and scientific possibilities, but at the same time poses big challenges in other sectors in particular in relation to privacy. Therefore, this sector needs particular attention from regulatory perspective, and any regulation in this sector should strike a careful balance between the economic interests and privacy.

Furthermore, instead of using data relating to an identified or identifiable natural person, the use of anonymous / aggregated health data could be incentivised.

***General***

### 28) Please comment on any additional issues concerning any additional aspect of Rights in Data you consider relevant to this Study Question.

N/A

### 29) Please indicate industry sector views provided by in-house counsel are included in you Group's answers to Part III.

Marketing and information services.

\* \* \*