REPORTS OF THE MINISTRY OF THE ENVIRONMENT 18en | 2018

How does the protection of personal data restrict the use of spatial data?

Päivi Korpisaari

MINISTRY OF THE ENVIRONMENT

Reports of the Ministry of the Environment 18en/2018

How does the protection of personal data restrict the use of spatial data?

Päivi Korpisaari

The article appeared in Liikejuridiikka 1/2018, p. 34-65, a magazine published by the Chamber of Commerce of Finland (Kauppakamari)

Ministry of the Environment, Helsinki 2018

Ministry of the Environment

ISBN: 978-952-11-4804-0

Layout: Government Administration Unit, Publications

Helsinki 2018

Description sheet

Published by	Ministry of the Environment		July 2018
Authors	Päivi Korpisaari		
Title of publication	How does the protection of personal data restrict the use of spatial data?*		
Series and publication number	Reports of the Ministry of the Environment 18en/2018		
ISBN PDF	978-952-11-4804-0	**ISSN (PDF)**	1796-170X
Website address (URN)	http://urn.fi/URN:ISBN:978-952-11-4804-0		
Pages	42	**Language**	English
Keywords	personal data, environmental data, geospatial data, publishing geospatial data, General Data Protection Regulation, concept of personal data, access to personal data, Personal Data Act, Act on the Openness of Government Activities, legislation		

Abstract

Public authorities possess a lot of geospatial data acquired by means of public funds or provided to them, including maps, cadastral and building data and environmental data. There is a growing interest in using such data for commercial purposes. Geospatial data published as open data in a readily accessible form would enable to develop applications and other services, such as those used in mobile phones. The broad scope of the concept of personal data means that geospatial data is often also to be considered personal data because it can be linked e.g. to a person who owns the land or occupies a certain property. In such cases geospatial data forms a personal data register, which means that the legislation on personal data protection imposes restrictions on its use.

The restriction on access to public personal data laid down in section 16, subsection 3 of the Act on the Openness of Government Activities also restricts the granting of access to geospatial data that may contain elements to be considered personal data by nature. This restriction on access also caused the European Commission to launch infringement proceedings against Finland in respect of forest data.

This article analyses to what extent geospatial data is to be considered personal data and what are the restrictions on the use of data that arise from the elements of geospatial data that are to be considered personal data by nature. The article suggests that making use of geospatial data could be facilitated through legislation that would make it easier to grant access to and otherwise process a geospatial data register that contains indirect personal data.[1]

* The article appeared in Liikejuridiikka 1/2018, p. 34-65, a magazine published by the Chamber of Commerce of Finland (Kauppakamari)

[1.] The article is partly based on a study on geospatial data and personal data protection by the same author, commissioned by the Ministry of the Environment. The article was also used to contribute to the MyGeoTrust research project funded by the Finnish Funding Agency for Technology and Innovation Tekes, aimed to enable a way that respects privacy to collect and use spatial data from mobile devices.

Publisher	Ministry of the Environment
Distributed by/ publication sales	Online version: julkaisut.valtioneuvosto.fi Publication sales: julkaisutilaukset.valtioneuvosto.fi

Kuvailulehti

Julkaisija	Ympäristöministeriö		Heinäkuu 2018
Tekijät	Päivi Korpisaari		
Julkaisun nimi	How does the protection of personal data restrict the use of spatial data? (Miten henkilötietojen suoja rajoittaa paikkatietojen käyttämistä?*)		
Julkaisusarjan nimi ja numero	Ympäristöministeriön raportteja 18en/2018		
ISBN PDF	978-952-11-4804-0	**ISSN PDF**	1796-170X
URN-osoite	http://urn.fi/URN:ISBN:978-952-11-4804-0		
Sivumäärä	42	**Kieli**	Englanti
Asiasanat	henkilötieto, ympäristötieto, paikkatieto, paikkatiedon julkaiseminen, tietosuoja-asetus, henkilötiedon käsite, henkilötiedon luovuttaminen, henkilötietolaki, julkisuuslaki, lainsäädäntö		

Tiivistelmä

Viranomaisten hallussa on paljon julkisin varoin hankittua tai niille toimitettua paikkatietoa, kuten karttoja, kiinteistöjä rakennustietoja sekä ympäristötietoja. Niiden kaupalliseen hyödyntämiseen on kasvavaa kiinnostusta. Jos paikkatietoja julkaistaisiin avoimena datana helposti hyödynnettävässä muodossa, niiden pohjalta tai avulla voitaisiin kehittää esimerkiksi matkapuhelimissa käytettäviä sovelluksia ja muita palveluita. Henkilötiedon laajasta käsitteestä johtuu, että paikkatiedot ovat usein myös henkilötietoja, koska paikkaa koskeva tieto voidaan yhdistää esimerkiksi maan omistavaan tai tietyssä rakennuksessa asuvaan henkilöön. Tällaisessa tilanteessa paikkatiedot muodostavat henkilörekisterin, jolloin henkilötietojen suojaa koskeva lainsäädäntö asettaa rajoituksia tietojen käyttämiselle. Julkisuuslain 16 §:n 3 momentissa säädetty julkisten henkilötietojen luovutusrajoitus puolestaan vaikeuttaa henkilötietoluonteisten paikkatietojen luovuttamista. Luovutusrajoitus on johtanut myös EU:n komission käynnistämään rikkomusmenettelyn Suomea vastaan metsätietojen osalta.

Tässä kirjoituksessa selvitetään, milloin paikkatieto on henkilötietoa, ja mitä rajoituksia paikkatietojen henkilötietoluoneesta seuraa niiden hyödyntämiselle. Artikkelissa esitetään, että paikkatietojen hyödyntämistä voisi edesauttaa lainsäädännöllä, joka mahdollistaisi välillisiä henkilötietoja sisältävän paikkatietorekisterin luovuttamisen ja muun käsittelyn nykyistä helpommin.[1]

* Artikkelin alkuperäisjulkaisun lähteenä on Kauppakamarin kustantama Liikejuridiikkalehti.

[1] Artikkeli perustuu osin allekirjoittaneen ympäristöministeriölle laatimaan paikkatietoja ja henkilötietojen suojaa koskevaan tutkimukseen. Artikkeli on myös kontribuutio TEKESin rahoittamaan MyGeoTrust -tutkimushankkeeseen, jonka tarkoituksena on mm. mahdollistaa yksityisyyttä kunnioittava tapa kerätä ja hyödyntää mobiililaitteista kerättyjä paikkatietoja.

Kustantaja	Ympäristöministeriö
Julkaisun jakaja/myynti	Sähköinen versio: julkaisut.valtioneuvosto.fi Julkaisumyynti: julkaisutilaukset.valtioneuvosto.fi

Presentationsblad

Utgivare	Miljöministeriet		Juli 2018
Författare	Päivi Korpisaari		
Publikationens titel	How does the protection of personal data restrict the use of spatial data? (På vilket sätt begränsar skyddet av personuppgifter användningen av geografisk information? *)		
Publikationsseriens namn och nummer	Miljöministeriets rapporter 18en/2018		
ISBN PDF	978-952-11-4804-0	**ISSN PDF**	1796-170X
URN-adress	http://urn.fi/URN:ISBN:978-952-11-4804-0		
Sidantal	42	**Språk**	English
Nyckelord	personuppgift, miljöinformation, geografisk information, offentliggörande av geografisk information, dataskyddsförordningen, begreppet personuppgift, utlämnande av personuppgifter, personuppgiftslagen, offentlighetslagen, lagstiftning		

Referat

Myndigheterna förvaltar mycket geografisk information som de förvärvat med offentliga medel eller som skickats till dem, t.ex. kartor, uppgifter om fastigheter och byggnader samt miljöinformation. Det finns ett växande intresse att använda dessa kommersiellt. Om geografisk information offentliggörs i lättillgänglig form som öppna data kunde man utifrån den, eller med hjälp av den, utveckla t.ex. program och andra tjänster för mobiltelefoner. Personuppgift är ett omfattande begrepp. Geografisk information utgör ofta också personuppgifter, eftersom den information som gäller en plats exempelvis kan kopplas till en person som äger marken i området eller bor i en viss byggnad. I sådana fall utgör den geografiska informationen ett personregister, vilket också innebär att den lagstiftning som skyddar personuppgifter sätter upp vissa begränsningar för hur uppgifterna kan användas. Den begränsning av utlämnande av personuppgifter som anges i 16 § 3 mom. i lagen om offentlighet i myndigheternas verksamhet (den s.k. offentlighetslagen) försvårar för sin del utlämnande av geografisk information som innehåller uppgifter som har karaktären av personuppgifter. Begränsningen av utlämnandet av uppgifter har också lett till att Europeiska kommissionen inlett ett överträdelseförfarande mot Finland som gäller skoglig information. I den här artikeln utreds när geografisk information betraktas som personuppgifter och vilka begränsningar som gäller för användningen till följd av att den geografiska informationen är av personuppgiftskaraktär.

I artikeln föreslås att nyttjandet av geografisk information kunde underlättas genom lagstiftning som i högre grad än i dag möjliggör utlämnande och annan hantering av register för geografisk information som innehåller direkta personuppgifter.[1]

* Artikeln har ursprungligen publicerats i tidskriften Liikejuridiikka, nr 1/2018, s. 34-65 utgiven av Kauppakamari.

[1.] Artikeln baserar sig delvis på en undersökning som undertecknad gjort för miljöministeriet och som gäller geografisk information och skydd av personuppgifter. Artikeln är också ett bidrag till forskningsprojektet MyGeoTrust som finansieras av Tekes och vars syfte är att bl.a åstadkomma ett sätt att samla in och utnyttja geografisk information via mobila apparater på ett sätt som respekterar integriteten.

Förläggare	Miljöministeriet
Distribution/ beställningar	Elektronisk version: julkaisut.valtioneuvosto.fi Beställningar: julkaisutilaukset.valtioneuvosto.fi

Contents

Päivi Korpisaari

HOW DOES THE PROTECTION OF PERSONAL DATA RESTRICT THE USE OF SPATIAL DATA?

How does the protection of personal data restrict the use of spatial data?

The authorities possess of a lot of spatial data obtained with public funds or submitted to the authorities. The data include maps, real property and building data, and environmental information. There is growing interest in the commercial exploitation of these data. Publishing spatial data as open data in a format lending itself to easy utilisation could allow using them for purposes such as the basis or help for developing mobile phone applications and other services.

Due to the broadness of the concept of personal data, spatial data is often also considered a form of personal data as data on a geographic location can be linked to the person who owns the land or lives in a certain building, for instance. In this situation, the spatial data will constitute a personal data filing system, and as a result, the legislation on the protection of personal data will impose limitations to the use of the data. The restriction to granting access to public personal data issued under Section 16(3) of the Act on the Openness of Government Activities further complicates the disclosure of spatial data with characteristics of personal data. This restriction to the disclosure of data has also resulted in an infringement procedure launched by the European Commission against Finland. The case concerns forest data.

This article investigates when spatial data is considered personal data and which limitations are caused to the utilisation of data if spatial data has the characteristics of personal data. The article proposes that the utilisation of spatial data could be promoted with legislation that would facilitate easier disclosure and other processing of a spatial data filing system that contains indirect personal data.[1]

1 The article is partly based on a study on the protection of spatial data and personal data prepared to the Ministry of the Environment by the present author. The article is also a contribution to the MyGeoTrust research project funded by the Finnish Funding Agency for Technology and Innovation (TEKES). Among other issues, the project aims to facilitate an approach for compiling and utilising spatial data collected from mobile devices that respects privacy.

1 Introduction and research question

1.1 The need for utilising the data possessed by the authorities

The authorities hold a lot of spatial data obtained with public funds. These data can be perceived as a resource available for the authorities as well as joint capital of society that must be stored in a cost-effective manner. Access to the data must be provided as openly as possible for the purposes of the general public, companies and other operators.[2] There is growing interest in the utilisation of the spatial data held by the public sector, including statistics, map data, real property and building information, and company and population data.[3] An improved exploitability of data facilitated by technological development would help generate new business and improve effectiveness, competitiveness and wellbeing. In addition to business interests, the better exploitability of data could also serve civic activity, education and science as well as enhance the effectiveness of administration.[4]

2 *Kauhanen-Simanainen, Anne – Rissanen, Olli-Pekka*: Suomi tarvitsee tietopolitiikkaa. [Finland needs an information policy.] Ministry of Finance publication 39/2017 October 2017 p. 14–15.

3 *Jaatinen, Tanja*: Muokkaako avoin data kansallista julkisuusperiaatetta? [Will open data change the national principle of openness?] In Päivi Korpisaari (ed.) Viestintäoikeus nyt – Viestintäoikeuden vuosikirja 2014 p 17–49, p 17. See also *Koski, Heli*: Avoimen tiedon vaikuttavuus – esitutkimus. [The effectiveness of open data – a preliminary study.] The Research Institute of the Finnish Economy 29 January 2015; Ministry of Finance publications 15a/2015 p. 1. "Open public data is any data (resource) that are produced or governed by a public organisation and are available in computer language for anyone to use, modify and share free or charge for both private and commercial purposes."

4 Ministry of Finance publication – 31/2015: Avoimesta datasta innovatiiviseen tiedon hyödyntä- miseen; Avoimen tiedon ohjelman 2013–2015 loppuraportti, p. 16. [From open data to the utilisation of innovative information; The final report of the Finnish Open Data Programme 2013–2015.] For more information on open data, also see *Poikola, Antti – Kola, Petri – Hintikka, Kari A.*: Julkinen data. Johdatus tietovarantojen avaamiseen. [Public data. Introduction to providing public access to data resources.] Publications of the Ministry of Transport and Communications 2010. Available at: https://www.lvm.fi/documents/20181/815557/Julkinen+data/467e-7da9-3038-46a1-b47e-994d7cd102d2?version=1.0, accessed 25 November 2017.

The utilisation of the data possessed by the authorities is inhibited by issues such as the fragmented and disjointed nature of the available data and the legislative or effective limitations concerning the disclosure or exploitation of data. The problem is not as much caused by a lack of data but rather by the fact that the available data may be stored in several different places and in a format that makes the data difficult to exploit.[5] In order to make it as easy as possible to utilise data collected with public funds and other means, it is important that the data maintained by society and the opportunities for using databases correspond to the needs of users. For instance, this means the provision of e-services instead of providing paper copies or printouts of the data. It would also be good if, for instance, all spatial data materials and services maintained by public administration would be compatible and described in a metadata service. Their usability would also be improved if all spatial data were made easily available in one place.[6]

Data are a good resource as they are not worn down or reduced with each use; instead, sharing them can generate new data or increase their value through refinement.[7] The use of data may also improve their quality if the users give feedback on or recycle the data they have processed.

However, obtaining, recording, storing and organising and other processing of data by the authorities with related obligations concerning information security, log data and other issues does not come for free. Data management requires both direct financial resources and take up employees' working hours. Storing and processing the same data by a number of different authorities is not financially efficient. It may also cause problems from the perspectives of the correctness, timeliness and relevance of data. Making data resources openly available also causes costs and losses of income to government agencies. On the other hand, open data often reduce the need for counselling and requests for information as well as the human resources required by these.[8]

5 For more on this topic, see Public sector information: a key resource for Europe. Green Paper on public sector information in the information society. COM (1998) 585 p. 1. Utilisation of data is difficult, for instance, when the data are dispersed or stored in the workstation of local authorities, ibid. 3.

6 Draft report on a policy on spatial data, version 0.8/22 September 2017 p. 6–7, 9–10 and 12.

7 The Ministry of Finance publication 39/2017 referred to above in footnote 2, p. 10.

8 The Ministry of Finance report 31/2015 referred to above in footnote 3, p. 16.

Under section 2, subsection 1(1) of the Act on Spatial Data Infrastructure in Finland (421/2009;), spatial data refers to the kind of data in an electronic format on the region of Finland that contains as a feature of data objects the location of the object as a direct or indirect reference to a place or geographic area. Therefore, spatial data is information attached to a location.[9]

The reference to spatial data may be direct, as is the case with coordinates, or indirect, as is the case with addresses, codes or names that refer to a certain location or region.[10] Spatial data include information concerning, for instance, terrain, land ownership and use, real property and buildings, establishments, municipalities, nature reserves, climate, weather, crimes, accidents or even radio reception, geographic information of a mobile phone, statistical data and data on traffic connections attached to a location.[11] Spatial data are used for purposes such as navigation applications, environmental plans, use of natural resources and planning of traffic connections.[12] On the other hand, location data indicates the location of a target using an address, real property code or coordinates, for instance.[13] Location data can be used to combine different data concerning the same target.

The spatial data possessed by the public sector is valuable not only to the planning activities of the public sector and citizens, but also to companies, which can use the data in the decision-making concerning their operational plans by combining the data with other information, such as consumer study data, environmental regulation and arrangements for public transport. Spatial data can also be processed to create services based on information,

---

9 Spatial Data Platform, http://esrifinland.maps.arcgis.com/apps/Cascade/index.html?appid=a5c3ae26cc bd429c-917496f9b9f67b90, accessed on 13 November 2017. Currently, the spatial data resources of central government are stored in over 90 map services or portals. The purpose of the spatial data platform established online is to provide cohesive spatial data maintained by different authorities that can be accessed via a single platform by anyone needing the data for different purposes. However, the data continue to be collected and maintained separately by different agents and functions. On the concept of spatial data and a draft report on a policy on spatial data, version 0.8 / 22.9.2017, p. 5, author not mentioned; was submitted for comments on the website of the Ministry of Agriculture and Forestry at: http://mmm.fi/ptps/selonteon-luonnoksen- commenting, accessed on 27 November 2017. See also *Rainio, Antti – Navinova Oy*: Paikkatietopoliittinen selonteko. Julkishallintoa koskeva taustaselvitys [A report on spatial data policy. A preparatory study on public administration] , 28 November 2017 p. 5. Available at: http://mmm.fi/documents/1410837/4108574/PTP_J_Selvitysraportti_20170423_Lopullinen/45faaf16-e85d- 49a1-be82-03e0a0bcbe0c, accessed on 29 September 2017, which notes that a preliminary survey on spatial data policy alone identified over 300 spatial data sets of the central government (on p. 6).

10 *Rainio* 2017 p. 10.

11 Draft report on a policy on spatial data, version 0.8/22 September 2017 p. 5 and, *Rainio* 2017 p. 10. As mentioned in the draft, "a map is a visual presentation of spatial data created for a specific purpose"

12 Draft report on a policy on spatial data, version 0.8 / 22 September 2017 p. 5.

13 Draft report on a policy on spatial data, version 0.8 / 22 September 2017 p. 5. Location data can refer to several different things depending on the context, and it is important to determine what is meant by the term in each situation. Under section 3(18) of the Information Society Code (917/2014), location data means "data which is available from a communications network or terminal device, shows the geographic location of a subscriber connection or terminal device, and is used for a purpose other than the delivery of a communication". The data protection principles presented in the present article are also applicable to the location data referred to in the Information Society Code. The name of the Information Society Code will be changed to the Act on Electronic Communications Services with the amendment 68/2018, which will enter into force on 1 June 2018.

including navigation, weather data, environmental reports and real property services.[14] According to the Director of Information Management of the Ministry of Agriculture and Forestry Antti Vertanen, as much as 80% of the data of public administration are spatial data.[15] A draft report on a policy on spatial data also notes that "[t]he majority of the data produced and maintained by public administration are spatial data".[16]

At the same time as the national and European spatial data infrastructure have developed as more compatible service entities, awareness of the opportunities for exploiting spatial data in the provision of services has also increased. The increasing demand for services has also led to a willingness of service providers to offer different view and download services. Private spatial data providers also have better opportunities for changing their processes to be compatible with the data sets of the authorities through interface services.[17]

The importance of spatial data in modern society is illustrated by the fact that, between 2015 and 2020, the total volume of ongoing, soon-to-be launched or completed projects on spatial data has amounted to over EUR 50 million.[18]

In addition to the aforementioned technical and practical aspects, the processing and particularly the disclosure of spatial data, as well as other data possessed by the authorities, is restricted by the fact that spatial data containing personal data may only be processed (including disclosed) if the conditions laid down in legislation concerning personal data are met and in the extent permitted by the law. As a result, the full potential of the data resources cannot be utilised for business purposes, for instance. Therefore, the purpose of this article is to determine

- how the concept of personal data is defined and when spatial data is perceived as personal data, and
- under which conditions can spatial data in the public domain classified as personal data be processed and disclosed for purposes other than private use, and
- how the usability of spatial data with characteristics of personal data could be improved.

---

14 *Janssen, Kathleen*: The Availability of Spatial and Environmental Data in the European Union. At the Crossroads between Public and Economic Interests. Wolters Kluwer Law & Business 2010 p. 3

15 A news article by the Ministry of Agriculture and Forestry: The digitalisation of public administration is supported with the Spatial Data Platform project http://mmm.fi/artikkeli/-/asset_publisher/julkisen-hallinnon-digitalisaatiota-tuetaan-paikkatietoalusta-hankkeella, accessed on 2 December 2017. According to a survey on spatial data infrastructure, spatial data constitutes around 80% of all of the data collected by our society (probably means the data collected in society); see *Muhli, Panu – Koskinen, Jarkko – Heinonen, Sirkka – Ruotsalainen, Juho – Parkkinen, Marjukka*: Selvitys paikkatietopoliittista selontekoa varten. Teknisen kehityksen vaikutukset Suomen paikkatietoinfrastruktuuriin. [A survey for the report on spatial data policy. The impacts of technological development on Finland's spatial data infrastructure.] 12 June 2017 p. 51.

16 Draft report on a policy on spatial data, version 0.8 / 22 September 2017 p. 5.

17 Government proposal to the Parliament for an act amending the Act on Spatial Data Infrastructure in Finland, HE 83/2015 vp p. 5 and 11.

18 *Rainio* 2017 p. 5.

The limitation concerning purposes other than private use is based on the fact that private use has been largely excluded from the scope of the Personal Data Act and the forthcoming General Data Protection Regulation of the European Union (later also referred to as GDPR)[19] as well as the data protection act which is currently under preparation. This article is mostly focused on examining the legal situation in light of the General Data Protection Regulation of the European Union, which will enter into force on 25 May 2018. To the extent afforded by its scope, this article will also take into account the valid regulation and the currently prepared national data protection act, on which a government proposal had not yet been completed at the time of writing this article.

1.2 The EU's data protection reform

The EU's General Data Protection Regulation is directly applicable and repeals the Data Protection Directive issued in 1995. It will enter into force on 25 May 2018. On 17 February 2016, the Ministry of Justice appointed a working group to investigate the need for national legislative measures required by the EU's General Data Protection Regulation and to prepare the necessary amendments. A working group on data protection known as the TATTI working group submitted their interim report on 21 June 2017. The working group proposed repealing the valid Personal Data Act and enacting a new general act on the protection of personal data that specifies and complements the General Data Protection Regulation to the extent permitted by flexibility at the national level. In addition to the new act on the protection of personal data, the working group proposed certain amendments to the Criminal Code of Finland and the Enforcement of Fines Act. Based on the proposal, the legislative amendments would enter into force on the date of application of the GDPR, i.e. on 25 May 2018.[20] In total, over 100 comments were submitted on the report. The final report is set to be completed on 16 February 2018. The aim is to submit the government proposal on the data protection act to the Parliament before this, in January 2018.

19 Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation).

20 Report by the working group on the implementation of the EU's General Data Protection Regulation (TATTI), Ministry of Justice reports and statements 35/2017.

1.3 Premises and basic concepts

Under Article 4 (1a) of the General Data Protection Regulation, 'personal data' means any information relating to an identified or identifiable natural person. A person can be identified directly or indirectly. The concept of personal data is examined in further detail in section 5.

Under the EU's General Data Protection Regulation, the processing of personal data means "any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction". The definition is extensive as is also the case with the current definition.

Article 4 (6) of the General Data Protection Regulation makes reference to a "filing system" instead of a personal data filing system. It refers to "any structured set of personal data which are accessible according to specific criteria, whether centralised, decentralised or dispersed on a functional or geographical basis". This definition is also extensive and similar as in the currently valid regulation. For example, in the preliminary ruling by the European Court of Justice C-212/13 (11 December 2014), image recording was considered to constitute a personal data filing system in a situation where an individual, in an effort to catch vandals, had installed under an overhang a continuously recording camera system that recorded image over old material and had been using the monitoring system for around six months.[21]

Under Article 4 (7) of the General Data Protection Regulation, a 'controller' "means the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data". The controller may also be provided for by law. Under both new and old legislation, a processor is the body which processes personal data on behalf of the controller. A personal data filing system may have one or more controllers if the register has been established for the joint use of the controllers. A key factor in determining which person or body is the controller is the effective control concerning the use of the personal data filing system. Among other issues, the controller determines which data are collected, where they are stored and processed, for which purpose they are used and how they are actually used.[22]

---

21 There was no monitor in the recording device, as a result of which the image could not be viewed in real time. The resident of the building who installed the camera was the only person with access to the system and its data. For more information on an image recording as a personal data file, see the Decision by the Data Protection Board 1/2002 (25 February 2002).

22 Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries, p. 10, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/inter- national_transfers_faq.pdf, accessed on 22 December 2017. See also Article 2 (d) of the Data Protection Directive and the opinion by the Data Protection Working Party 1/2010 on the concepts of controller and processor, 00264/10/FI, WP 169, 16 February 2010, p. 8–9. Effective control is the deciding factor; not whether the data processing has been legal or illegal.

2 Protection of private life and personal data

Article 8 of the European Convention on Human Rights safeguards everyone's right to respect for his private and family

life, his home and his correspondence.[23] Similarly, Article 7 of the Charter of Fundamental Rights of the European Union enshrines the right to respect for one's private and family life, home and communications. Protection of personal data is safeguarded separately from respect for private life under Article 8 of the Charter of Fundamental Rights of the European Union. The right to privacy and the protection of personal data are also laid down in section 10 of the Constitution of Finland.

The premise for the protection of private life is the right of an individual to live his or her life without arbitrary or unnecessary interference in the person's private life by the authorities or other third parties. Private life includes issues such as the rights of the individual to form and maintain relationships with other people and the environment, and the right to make decisions on one's person and body. A private life also includes the right of an individual not to disclose matters pertaining to his or her private life to anyone or only to one's loved ones to a certain extent.[24] In addition to that laid down in section 7 of the Constitution of Finland (the right to life, personal liberty and integrity), the protection of private life can also be considered to safeguard a person's right of self-determination.[25]

---

23 On the protection of private life as a human right protected under the European Convention on Human Rights *Pellonpää, Matti – Gullans, Monica – Pölönen, Pasi – Tapanila, Antti*: Euroopan ihmisoikeussopimus. [European Convention on Human Rights] Talentum 2012 p. 652–696.

24 Government proposal to the Parliament on amending the provisions on fundamental rights in Constitutions HE 309/1993 vp p. 52–53 and a report by the Perusoikeuskomitea [Fundamental rights commission], KM 1992:3 p. 292.

25 See HE 309/1993 vp p. 46 and *Korja, Juhan*i: Biometrinen tunnistaminen ja henkilötietojen suoja: tutkimus biometristen tunnisteiden lainsäädännöllisestä asemasta. [Biometric identification and the protection of personal data: a study on the legislative status of biometric identifier.] Rovaniemi 2016 p. 90–99. Of Finnish researcher in jurisprudence, Ahti Saarenpää in particular has studied the right of self-determination as a legal construction.

The concept of 'private life' is also broad in the practice of the Court of Justice of the European Union. It encompasses physical, mental and moral integrity. It also includes the right to create and maintain relationships with other people. Private life can also be considered to include a person's professional and business activities.[26] The right to a private life also protects the reputation[27] and honour[28] of an individual if a violation thereof fulfils a certain degree of severity.[29]

Individuals are not protected against a loss of reputation that is a predictable outcome of their personal actions. Committing an offence can be mentioned as an example of this.[30]

Under section 10(1) of the Constitution of Finland, "[e]veryone's private life, honour and the sanctity of the home are guaranteed." More detailed provisions on the protection of personal data are laid down by an Act."[31] The Personal Data Act (523/1999) is the most significant act for the protection of personal data. Furthermore, around 800 separate acts lay down provisions on the processing of personal data.[32] The generous regulation is partly based on the requirement for laying down provisions in an Act of the Constitution of Finland and the related interpretation practice by the Constitutional Law Committee.

The Constitutional Law Committee has set high standards for the accuracy of the regulation and considered that the regulation must be comprehensive and detailed.[33] In addition to the legal protection of data subjects, importance has also been given to

---

26 *von Hannover v. Germany* No. 2 (GC, 7 February 2012) section 95 and *Niemi etz v. Germany* (16 December 1992) section 29.

27 *Chauvy and Others v. France* (29 June 2004) section 70, *Abeberry v. France* (decision, 21 September 2004), *Leempoel & S.A. ED. Ciné Revue v. Belgium* (9 November 2006) section 67, *White v. Sweden* (19 September 2006) section 26, *Pfeifer v. Austria* (25 February 1992) section 35 and *Fürst-Pfeifer v. Austria* (17 March 2016) section 35.

28 *Radio France and others v. France* (30 March 2004), *Cumpănă and Mazăre v. Romania* (GC; 17 December 2004), *Sanchez Cardenas v. Norway* (4 October 2007) and *A v. Norway* (9 April 2009) section 64.

29 *Sidabras and Džiautas v. Lithuania* (27 July 2004) section 49 and *Axel Springer AG v. Germany* (GC, 7 February 2012) section 83.

30 *Sidabras and Džiautas v. Lithuania* (27 July2004) section 49 and *Axel Springer AG v. Germany* (GC, 7 February 2012) section 83.

31 For more on the protection of private life, see HE 309/1993 vp p. 52-53, KM 1992:3 p. 297, *Tiilikka, Päivi*: Sananvapaus ja yksilön suoja. Lehtiartikkelin aiheuttaman kärsimyksen korvaaminen. [Freedom of expression and the protection of the individual. Compensation for suffering caused by a newspaper article.] WSOYpro 2007 p. 136–142 and *Viljanen, Veli-Pekka*: Yksityiselämän suoja. [Protection of private life.] In *Hallberg, Pekka – Kara- puu, Heikki – Ojanen, Tuomas – Scheinin, Martin – Tuori, Kaarlo – Viljanen, Veli-Pekka*: Perusoikeudet. [Fundamental rights.] Alma Talent Fokus jakso III/6

32 See *Pitkänen, Olli* (ed.): Need to change national data protection statutes, Publications of the Government's analysis, assessment and research activities 41/2017, June 2017 and *Pitkänen, Olli Pekka – Ruuska, Petra*: Tietosuojalainsäädännön aiheuttama verolainsäädännön muutostarve. [Need for changing tax legislation as a result of data protection legislation.] IPR University Center 2017.

33 E.g. Constitutional Law Committee statement PeVL 5/2017 vp: Government proposal to the Parliament on the adoption of an agreement on fishing on the waterways of the river Tana concluded with Norway and for acts on bringing into force and application of the provisions contained by the legislation concerning the agreement, and an amendment to the Fishing Act, HE 239/2016 p. 9. See also PeVL 18/2012 vp; Government proposal to the Parliament for acts amending the Act on the Processing of Personal Data by the Police and the Act on the Processing of Personal Data by the Border Guard and amendments to certain related acts, HE 66/2012 vp p. 2.

the goals of data collection, the contents of the personal data on data subjects and the permitted purposes of use, and the duration of storing the data and their transferability.[34] Flexibility is restricted by the fact that the protection of personal data is also partly included in the protection of private life protected under the same provision.[35] According to the Constitutional Law Committee, the requirements for comprehensiveness, accuracy and definiteness of the regulation related to the protection of personal data can also be met to some extent with an EU regulation or a general act contained by the national law.[36]

The protection of private life and personal data can be restricted in order to protect other rights. Human rights conventions make reference to the conditions for restricting the rights that they protect.[37] The necessity of the restriction and imposing the restriction in order to safeguard an acceptable outcome is key. In its committee report 25/1994, the Constitutional Law Committee of the Parliament considered that imposing restrictions to basic rights is only possible when said restrictions are set forth by law, are precise and unequivocal, and acceptable and proportionate to a legitimate purpose for restriction (the principle of proportionality). A regular act may also not be used to issue restrictions that extend to the core area of fundamental rights. There may also not be a conflict between the restrictions and Finland's international human rights obligations. Ensuring sufficient arrangements for legal protection is a further requirement.[38]

The protection of private life and the protection of personal data are not fully overlapping; instead, the objects of protection only overlap in part. This is due to the fact that some data related to individuals that are not concerned with the person's private life are protected as personal data.[39] The concept of personal data is examined in further detail in section 5 of the present article.

---

34 PeVL 71/2014 vp; Government proposal to the Parliament for the Act on the Processing of Personal Data by the Customs and certain related acts, HE 71/2014 vp p. 2 and PeVL 19/2012 vp; Government proposal to the Parliament for legislation concerning the processing of personal data by the Criminal Sanctions Agency, HE 2/2012 vp p. 2.

35 PeVL 18/2012 vp p. 2.

36 PeVL 5/2017 vp s. 9 ja PeVL 38/2016 vp; Government proposal to the Parliament for acts amending the Rescue Act and the Act on Emergency Response Centre Operations, HE 100/2016 vp p. 4.

37 See. Article 8(2) of the ECHR and Article 8(2) of the CFR. In turn, the scope of the protection of personal data is regulated under article 52(1) of the CFR. On restricting the protection of personal data *Wallin, Anna-Riitta*: Tiedonsaanti asiakirjoista ja henkilötietojen suoja EU:n perusoikeuskirjassa tunnustettuina perusoikeuksina. [Access to information in documents and the protection of personal data as fundamental rights recognised by the Charter of Fundamental Rights of the European Union.] In *Nieminen, Liisa* (ed.): Perusoikeudet EU:ssa. [Fundamental rights in the EU.] Lakimiesliiton kustannus. Helsinki 2001 p. 351–386, p. 374 and *González Fuster, Gloria – Gutwirth*, Serge: Opening up personal data protection: A conceptual controversy. Computer Law & Security Review 2013 Vol. 29 Iss. 5 p. 531–539, p. 532–536.

38 For more information on the preconditions for restricting fundamental rights, see *Viljanen, Veli-Pekka*: Perusoikeuksien rajoitusedellytykset. [The conditions for restricting fundamental rights.] WSOY lakitieto 2001.

39 This is already apparent in the definition of the concept of personal data. See also the decision by the Court of Justice of the European Union (CJEU) on a case concerning public access to documents and protection of personal data, *ClientEarth, Pesticide Action Network Europe (PAN Europe) v. European Food Safety Authority (EFSA) and the European Commission*, for which the CJEU stated that "the concepts of 'personal data', within the meaning of Article 2(a) of Regulation No 45/2001, and of 'data relating to private life' are not to be confused". Cf. KHO 2012:88 and on the criticism of the case see *Pitkänen, Olli – Tiilikka, Eija – Warma, Päivi:* Henkilötietojen suoja. [Protection of personal data.] Vantaa 2013 p. 43–44.

3 Freedom of expression and right of access to information

Freedom of expression is protected under section 12 of the Constitution of Finland and Article 10 of the European Convention on Human Rights. In turn, Article 11 of the Charter of Fundamental Rights of the European Union protects the right to freedom of expression and freedom to impart information. The scope of application of the provision on the freedom of expression includes political, societal, religious, entertaining, commercial and artistic forms of expression. The provision on the freedom of expression protects the right of individuals to express information, opinions and other messages as well as the right of recipients to receive these.[40]

Freedom of expression is a right of individuals while at the same time promoting common good, or democracy, and pluralistic public debate that is as reliable as possible and inherent to a democracy.[41] Freedom of expression includes different forms of creative activities, self-expression and commercial communications.[42]

Public access of the activities by the authorities is an essential part of the freedom of expression. The Act on the Openness of Government Activities lays down further provisions on the pubic availability of documents (621/1999; Act on the Openness of Government Activities). Under section 1 (1) of the Act, official documents shall be in the public domain, unless specifically provided otherwise in the Act or another Act. According to section 9(1) of the Act on the Openness of Government Activities "[e]veryone has the right of access to an official document in the public domain.". Section 24 of the Act on the Openness of Government Activities and numerous special acts issue exceptions to the public availability of documents.

---

40 On freedom of expression as a fundamental right and the principles of interpretation of the European Court of Human Rights in cases concerning freedom of expression *Tiilikka 2007* p. 120–135 and 169–235.

41 See *Petäjä, Ulf*: Varför yttrandefrihet? Om rättfärdigandet av yttrandefrihet med utgångspunkt från fem centrala argument i den demokratiska idétraditionen. Växjö Universitet Växjö 2006 p. 184–185.

42 HE 309/1993 p. 56.

The purpose of the principle of openness is to improve the opportunities for the social engagement of citizens, and to monitor the use of authority and activities by the authorities.[43] From an international viewpoint, the principle of openness in Finland is rather extensive. A person requesting information is not required to give justifications for requesting the information and his or her identity is not disclosed.[44] The Principle of openness also includes the right to the commercial use of the data obtained from the authorities.

Directive 2003/98/EC of the European Parliament and of the Council of 17 November 2003 on the re-use of public sector information of 17 November 2003 and the Directive 2013/37/EU of the European Parliament and of the Council of 26 June 2013 amending Directive 2003/98/EC on the re-use of public sector information also aim at public access to information and the better utilisation of information in the public domain. According to section 6 of the introduction of Directive 2013/37/EU, open data policies which encourage the wide availability and re-use of public sector information for private or commercial purposes can play an important role in kick-starting the development of new services based on novel ways to combine and make use of such information, stimulate economic growth and promote social engagement. However, this development requires a level playing field at Union level in terms of whether or not the re-use of documents is authorised in the Member States.

The public access to environmental information and spatial data is also regulated with, for instance, the directive on public access to environmental information[45], the INSPIRE directive[46] and the Act on Spatial Information Infrastructure (421/2009). As part of the preliminary work for the amendment to the Act on Spatial Information Infrastructure, it was decided that the spatial information infrastructure safeguards the right of everyone to access to public documents and recordings protected under section 12 of the Constitution of Finland and the right of everyone to the possibility to influence the decisions that concern their own living environment protected under section 20 of the Constitution of Finland. The benefits brought to citizens were considered mostly indirect, i.e. it was considered that they would be realised through better transparency of the administration and opportunities for influence and involvement.[47] A further aim of public access to environmental information is promoting the health and wellbeing of current and future

43 HE 309/1993 vp; justifications of section 10 of the Constitution of Finland valid at the time.

44 Exceptions include parties' right of access and the disclosure of information in situations in accordance with section 16(3) of the Act on the Openness of Government Activities (disclosure of personal data filing system).

45 Directive 2003/4/EC of the European Parliament and of the Council of 28 January 2000 on public access to environmental information and repealing Council Directive 90/313/EEC.

46 Directive 2007/2/EC of the European Parliament and of the Council of 14 March 2007 establishing an Infrastructure for Spatial Information in the European Community (INSPIRE).

47 Government proposal for an act on spatial data infrastructure, HE 18/2009 vp p. 18 and HE 83/2015 vp p. 11.

generations, improving the quality of decision-making concerning the environment and enhancing the implementation of decisions, gaining the citizens' acceptance of decision-making concerning the environment, and fostering democracy.[48]

As such, the provision on the freedom of expression of the European Convention on Human Rights does not guarantee a right to access documents and recordings in the possession of the authorities; however, in the case-law of the European Court of Human Rights, this right has been derived from certain other human rights on an individual basis. For instance, the right to life may entitle the family members of a person who has been killed to gain access to the records concerning the pre-trial investigation of the killing. Similarly, the right to a fair trial entitles a person to have access to material submitted to the courts by the respondent on appeal regardless of whether the material has significance to solving the case. The right to respect for private and family life can entitle a person taken into custody as a child to obtain records from the authorities concerning his or her childhood, for instance, while the freedom of expression may sometimes require the disclosure of documents possessed by the authorities to an organisation promoting public access requesting access to the materials.[49]

48 *Kumpula, Anne*: Ympäristö oikeutena. [The environment as a right.] Jyväskylä 2004 p. 79 ja HE 18/2009 vp p. 18.

49 In *Tiilikka, Päivi:* Access to Information as a Human Right in the Case Law of the European Court of Human Rights. Journal of Media Law 2013 Vol. 5 Iss. 1 p. 79–103.

4 Other fundamental rights with relevance to the topic

Section 2(2) of the Constitution of Finland guarantees the right of the individual to participate in and influence the development of society and his or her living conditions. According to section 14(3) of the Constitution of Finland, "[t]he public authorities shall promote the opportunities for the individual to participate in societal activity and to influence the decisions that concern him or her". Section 20 of the Constitution lays down provisions on the responsibility for the environment. According to the section, nature and its biodiversity, the environment and the national heritage are the responsibility of everyone. Moreover, the public authorities must "endeavour to guarantee for everyone the right to a healthy environment and for everyone the possibility to influence decisions that concern their own living environment". According to legal literature, the values and obligations expressed in section 20(1) of the Constitution of Finland must be considered equal to other fundamental rights such as the protection of property and the freedom to engage in commercial activity.[50] Moreover, section 20(2) of the Constitution includes a so-called duty to protect, which may influence the obligation to produce and share information concerning the environment. These fundamental rights are also in favour of the right to access spatial data and environmental information.

50 *Kumpula, Anne – Määttä, Tapio – Similä, Jukka – Suvantola, Leila*: Näkökulmia monitieteiseen ympäristöoikeuteen. [Perspectives on multidisciplinary environmental law.] Turku 2014 p. 127. See also KHO 2002:86 and KHO 2006:58. On the connections between environmental law and fundamental rights, see Kuusiniemi, Kari: Perusoikeudet ja ympäristö. [Fundamental rights and the environment] In *Kuusiniemi, Kari – Ekroos, Ari – Kumpula, Anne – Vihervuori, Pekka*: Ympäristöoikeus. [Environmental law.] Alma Talent online publication chapter I 4. The section indicates that the connections between environmental law and fundamental rights are largely related to the protection of property.

5 When can data be considered personal data?

The preconditions to the concept of personal data are imposed by the Data Protection Directive and, beginning on 25 May 2018, the General Data Protection Regulation, i.e. EU law. Finland cannot lay down provisions on its own national definition for personal data more concise than the concept of personal data in accordance with the legislation of the European Union without violating the Directive or Regulation. Personal data means any information relating to a natural person. This means people and, as a rule, only living individuals. While protection has been granted to deceased persons in certain individual cases, we do not have comprehensive data protection for the deceased.[51] Indeed, according to Article 27 of the GDPR, the "Regulation does not apply to the personal data of deceased persons". While Member States may provide national exceptions to this, the working group on data protection appointed by the Ministry of Justice did not propose introducing special regulation on deceased persons in its interim report.

51 The question of the protection of the personal data of deceased persons is fairly complex, and the scope of the present article does not permit further consideration of the issue. More on the topic in Pitkänen – Tiilikka – Warma 2013 p. 48–51 and Forss, Marko: Kuolemanjälkeinen kunnia ja yksityiselämä – mitä tietoja kansalainen saa julkaista kuolleesta henkilöstä erityisesti sosiaalisessa mediassa? [Honour and private life after death – what information may citizens publish on a deceased person, particularly on social media?] In Korpisaari, Päivi (ed.): Viestinnän muuttuva sääntely [The changing regulation of communications], Viestintäoikeuden vuosikirja 2016 p. 171–211. According to the EU's Data Protection Working Party, deceased persons are no longer natural persons in civil law as referred to in the Data Protection Directive; Opinion 4/2007 on the concept of personal data of the Data Protection Working Party, 01248/07/EN, WP 136, 20 September 2007 (WP 136 opinion 4/2007) p. 22.

Information on the concept of personal data during the current and future legal situation has been compiled in the below table.

CONCEPT OF PERSONAL DATA

Currently applied legislation		*Legislation applied from 25 May 2018*
The EU's Data Protection Directive	**Personal Data Act**	**GDPR**
Any information concerning an identified or identifiable natural person. An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity. *Introduction*: to determine whether a person is identifiable, account should be taken of all the means likely reasonably to be used either by the controller or by any other person to identify the said person; whereas the principles of protection shall not apply to data rendered anonymous in such a way that the data subject is no longer identifiable.	Any information on a private individual and any information on his/her personal characteristics or personal circumstances, where these are identifiable as concerning him/her or the members of his/her family or household.	Any information relating to an identified or identifiable natural person. An identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. *Recital*: To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly. To ascertain whether means are reasonably likely to be used to identify the natural person, account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments.

In short, 'personal data' therefore refers to any information related to an identified or identifiable natural persons. Whether the information is concerned with the person's private activities or his or her activities as a self-employed person or a private trader or in public life is insignificant in assessing the issue.[52] The reference to any information aims at a wide scope of application of the legislation concerning personal data.[53]

52 Compare with the Personal Data File Act, which was interpreted to mean that the data concerning a natural person in capacities other than as private individuals – including as a self-employed person, a private trader or in public life – fell outside of the scope of application of the Personal Data File Act (Government proposal to the Parliament for a Personal Data Act and certain related acts, HE 96/1998 vp p. 34–35).

53 Frequently Asked Questions Relating to Transfers of Personal Data from the EU/EEA to Third Countries p. 9, http://ec.europa.eu/justice/policies/privacy/docs/international_transfers_faq/ international_transfers_faq.pdf, accessed on 22 December 2017. However, see and cf. KHO 2012:88.

"Personal data" need not be accurate or verified, but may also include erroneous data. For example, this is indicated in the provisions concerning the right of access by the data subject and the rectification and supplementation of erroneous, incomplete or obsolete data (sections 26–29 of the Personal Data Act and Articles 15 and 16 of the GDPR). The concept of personal data includes both factual claims, and subjective opinions and value judgements. Personal data may concern a person's private and family life or his or her professional or social activities or economic status. For instance, medical prescription information is personal data that concern both the physician and the patient.[54]

According to section 26 or the recital of the GDPR, personal data which have undergone pseudonymisation, which could be attributed to a natural person by the use of additional information should be considered to be personal data. To determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used either by the controller or by another person to identify the natural person directly or indirectly. Account should be taken of all objective factors, such as the costs of and the amount of time required for identification, taking into consideration the available technology at the time of the processing and technological developments. The principles of data protection should not apply to anonymous information, namely information which does not relate to an identified or identifiable natural person or to personal data rendered anonymous in such a manner that the data subject is not or no longer identifiable.

The concept of personal data is broad. According to the definitions presented above, details such as a real estate code or an address are personal data as they can be "attributed to a natural person by the use of additional information" and the means to identify a natural person are reasonably likely to be used. Therefore, spatial data is often considered personal data and a list of spatial data will constitute a personal data filing system.[55]

A person is often directly identifiable based on his or her name and date of birth. A person can be identified indirectly when the available identifiers do not, as a rule, enable the identification of the person, but when combining data with other information (which the controller may or may not possess) makes it possible to single out the person. In some cases, combining individual information at the group level (such as an age group or region of birth) makes it possible to identify a person fairly reliably, particularly if

54 WP 136 opinion 4/2007 p. 7.

55 For information on photographs as personal data, see the Decision by the Data Protection Board 1/2002 (25 February 2002) and the Office of the Data Protection Ombudsman: Valokuva ja yksityisyydensuoja henkilötietolain kannalta [Photographs and the protection of privacy from the perspective of the Personal Data Act], updated on 27 July 2010; for information on an IP address as personal data see Article 29 Data Protection Working Party (WP 29) Working Document: Privacy on the Internet - An integrated EU Approach to On-line Data Protection, 5063/00/EN/ final., WP 37. For information on an IP address as personal data, see *Scarlet Extended SA v. Société belge des auteurs, compositeurs et éditeurs SCRL (SABAM) (C-70/10) and Patrick Breyer v Bundesrepublik Deutschland (C-582/14)*.

some kind of additional information is available.[56] In the decision of 19 October 2016 on Patrick Breyer v Bundesrepublik Deutschland (C-582/14), the European Court of Justice ruled that a dynamic IP address constitutes personal data in accordance with the Data Protection Directive if the online media services provider has the means which may likely reasonably be used in order to identify the data subject with additional data which the internet service provider has about that person. This decision is concerned with dynamic IP addresses, i.e. temporary addresses that internet service providers allocate to individual internet connections and which change each time there is a new connection to the internet. Therefore, a dynamic IP address did not in itself constitute information relating to an identified natural person, but it became personal data once it enabled identifying a natural person when combined with additional data.

The predominant level of technology and related development opportunities during data processing also contribute to this. If the intention is to store the data for a long period, the controller must take into account the possibility that the data may be identified at a later stage of the storage period, resulting in the data being considered as personal data.[57]

However, a mere hypothetical possibility to single out a person from a certain group does not in itself make a person identifiable. It there are no means reasonably likely to be used to identify the person or the likelihood for identifying the person is negligible, the person is not considered identifiable and the data are not considered personal data.[58]

56 WP 136 opinion 4/2007 p. 13–14. According to the Working Party, " it seems therefore justified to consider" that, for instance, information published about a criminal case in a newspaper without identifiers is information about identifiable persons and as such 'personal data' if one can find out who committed the crime or who was the person concerned by looking up different newspaper articles from the relevant time period.

57 WP 136 opinion 4/2007 p. 15.

58 WP 136 opinion 4/2007 p. 15.

6 Disclosure of personal data in the public domain

First, the utilisation of data possessed by the authorities is restricted by the secrecy criteria laid down in section 24 of the Act on the Openness of Government Activities, which may be connected to public interest or the protection of an individual.[59] Second, in addition to the secrecy criteria, the means of obtaining – or, more accurately, disclosing – data is also restricted by section 16 (3) of the Act on the Openness of Government Activities, which is as follows:

> "Access may be granted to a personal data filing system controlled by an authority in the form of a copy or a printout, or an electronic-format copy of the contents of the system, unless specifically otherwise provided in an Act, if the person requesting access has the right to record and use such data according to the legislation on the protection of personal data. However, access to personal data for purposes of direct marketing, polls or market research shall not be granted unless specifically provided otherwise or unless the data subject has consented to the same."

As a result of this subsection, in the context of granting access to many personal data contents (=a personal data filing system), the authority must verify that the data recipient is entitled to process personal data under legislation on personal data. For instance, case KHO 2016:161 of the Supreme Administrative Court concerned the method of granting access to a personal data filing system. A law firm had requested the National Supervisory Authority for Welfare and Health (Valvira) to provide public information on the names of the authority's medical officers and their medical specialities. As this was a matter of granting access to the personal data in a personal data filing system of an authority, a prerequisite for the disclosure of data in accordance with the modes of access laid down in section 16(3) of the Act on the Openness of Government Activities, namely a copy

59 For information about these kinds of situations, see *Mäenpää, Olli*: Julkisuusperiaate. [The principle of openness] 3rd renewed edition. Helsinki 2016 p. 211–227.

or a printout, or an electronic-format copy of the contents, was the right of the party requesting access to record and use the requested data under the provisions on the protection of personal data. According to the Supreme Administrative Court, the data were not generally available data as referred to in section 8(1) of the Personal Data Act and the law firm had no right to process the personal data it had requested and was therefore also not entitled to obtain the data in the form of a copy or a printout, or an electronic-format copy. However, the law firm was entitled to get access to the data through other modes. The Supreme Administrative Court left open the question on how access should be granted to the data and left this for the data provider to decide.

In turn, if the recipient of the data is entitled to process the data, as is the case of journalists pursuant to the so-called journalistic exemption, the authority (the party granting access to the personal data) is in any case obligated to determine that the processing of personal data is conducted in compliance with section 32 of the Personal Data Act concerning data security.[60] The Data Protection Ombudsman has ruled that the information should be requested in writing in a document that presents an acceptable explanation on the lawful use of the data to ensure the lawfulness of processing. The appropriate protection of the data must also be verified in this context.[61] Article 86 of the General Data Protection Regulation issues provisions on granting access to personal data in the public domain in that "personal data in official documents held by a public authority or a public body or a private body for the performance of a task carried out in the public interest may be disclosed by the authority or body in accordance with Union or Member State law to which the public authority or body is subject in order to reconcile public access to official documents with the right to the protection of personal data pursuant to this Regulation". Therefore, the provision leaves room for special regulation at the national level. In Finland, this is represented by section 16(3) of the Act on the Openness of Government Activities and the provisions of special acts.

60 See KHO 2012:55 in which the Supreme Administrative Court noted, in response to a request by a journalist to information on the wages of professors, that "the university was responsible for ensuring that the processing of personal data was conducted in accordance with section 32(1) of the Personal Data Act. For this purpose, a newspaper had to provide the controller with appropriate reports and commitments according to section 32(2) of the Personal Data Act and other adequate guarantees of the security of the data as provided in section 32(1) of the Personal Data Act." See also KHO 2015:44, which allowed the disclosure of the names of recently deceased persons by the Population Register Centre to a newspaper for journalistic purposes.

61 See the brochure by the Office of the Data Protection Ombudsman Henkilötietojen luovuttaminen viranomaisten henkilörekistereistä [Disclosure of personal data from the personal data filing systems of the authorities; in Finnish] (updated on 27 July 2010) and the brochure by the Office of the Data Protection Ombudsman Miten toimit, jos tietoja pyydetään salassa pidettäviä tietoja sisältävistä henkilörekisteristä [How to act if data are requested from personal data filing systems containing secret information; in Finnish], http://www.tietosuoja.fi/7614.htm. Accessed on 30 July 2017. According to the Data Protection Ombudsman, the authority that grants access to data, i.e. the controller, is responsible for the lawfulness of the disclosure of data (1179/41/2016; 21.4.2016).

As presented above, section 16(3) of the Act on the Openness of Government Activities imposes restrictions on providing access to publicly available personal data, or rather the modes of access. The subsection aims at preventing situations where granting extensive access to personal data under the Act on the Openness of Government Activities would result in illegal processing of personal data.[62]

At the same time, it makes it more difficult to utilise the data as, instead of gaining access to the filing system, a person requesting access has to receive the data in such small batches that these will not constitute a personal data filing system.

The provision is a general provision which is only applied if not otherwise provided elsewhere in the act.[63] A special act may therefore lay down provisions on more extensive access to data. The principle of purpose limitation also restricts the disclosure of personal data.[64]

The so-called TATTI working group making preparations for the implementation of the General Data Protection Regulation was unanimous about a need for assessing whether the provision on the disclosure of data of the Act on the Openness of Government Activities should be amended in light of both the GDPR as well as the current development in IT and society. However, the working group failed to reach consensus on how to coordinate the protection of personal data in line with the GDPR and the public availability of general documents. As a result, the interim report of the working group did not include a proposal for amending the Act on the Openness of Government Activities despite the fact that it deemed it necessary to re-evaluate the provision.[65] Therefore, the legal situation will remain unchanged after the entry into force of the General Data Protection Regulation: while access to individual data in the public domain may be granted without the restrictions in accordance with section 16 (3) of the Act on the Openness of Government Activities. However, the authority must verify that the data recipient has grounds for processing the personal data for which access has been granted when providing access to the personal data filing system or its part.

62 Government proposal to the Parliament on an Act on the Openness of Government Activities and related acts, HE 30/1998 vp p. 74. Also *Mäenpää* 2016 p. 204–205.

63 HE 30/1998 p. 73.

64 For more on this, see Article 5, paragraph 1(b) and Article 6, paragraph 3(2) of the GDPR. See also section 8(2) of the Personal Data Act.

65 Report by the working group on the implementation of the EU's General Data Protection Regulation (TATTI), Ministry of Justice reports and statements 35/2017 p. 37. See also the proposal for a draft on the amendment of the Act on the Openness of Government Activities by the members of the group Nurmi (chair), Talus and Walkila p. 209–212.

In practice, publishing personal data included in a personal data filing system in an open data network entails creating a technical user connection. While the concept of technical user connection has not been defined in legislation, it means that a person provided with a technical user connection gains access to the personal data filing system of the controller and is able to search for data in the filing system of the controller using his or her own search parameters. Based on a ruling by the Constitutional Law Committee, an act must lay down provisions on technical user connections as it enables extensive and rapid data transfer.[66]

In its decision 2015:41, the Supreme Administrative Court ruled that due to the fact that section 16(3) of the Act on the Openness of Government Activities makes no reference to disclosing data via a technical user connection, public tax records concerning a natural person could not be disclosed to a company engaged in financial activities by providing a technical user connection to a personal data filing system maintained by the Tax Administration in the absence of an explicit legal provision.[67] Providing a technical user connection would have granted the applicant with unlimited access to all public records on the income taxes of taxable persons even though, under the Personal Data Act, the applicant was only entitled to process the data of its clients. As the Act on the Openness of Government Activities, the Personal Data Act and the Act on the public disclosure and confidentiality of tax information included no general provisions which could have been used as the basis for granting access to data via a technical user connection, the user connection could not be granted.

Under section 29(3) of the Act on the Openness of Government Activities, an authority may grant technical user connection to the data in its personal data filing system to some other authority, if the other authority needs to take the information into account in its decision-making under an obligation separately laid down in legislation. However, in the context of secret information, the technical user connection may only be used for searching for information about the persons who have given their consent to do so unless separately explicitly otherwise provided on the disclosure of secret information. The provision is only suitable for the exchange of information between the authorities; in other words, it may not be used to provide a company with a technical user connection to a personal data filing system of a public authority. Based on the practice of the Constitutional Law Committee and the decision by the Supreme Administrative Court as well as a Government proposal on amending the Forest Data Act 170/2017, which is currently under consideration by the Parliament, it can be inferred that separate legislation would be required to facilitate more extensive disclosure, and thus better utilisation, of spatial data, including for the use of private companies.

66 Constitutional Law Committee statement PeVL 12/2002 vp on the Government proposal for an act amending the Enforcement Act and certain related acts and the Constitutional Law Committee statement PeVL 14/2002 vp on the Government proposal for amending the provisions concerning obtaining and disclosing the data on the social welfare assistance implemented by the Social Insurance Institution of Finland

67 Section 29 (3) of the Act on the Openness of Government Activities and sections 12 and 20 of the Act on the public disclosure and confidentiality of tax information lay down provisions on which data can be granted access to via a technical user connection. The case presented here did not concern a situation referred to in the legal provisions.

7 Spatial data sets as personal data filing systems

Spatial data sets maintained by the authorities that include personal data are personal data filing systems. In addition to other legislation, the norms concerning the processing of personal data are applied in this context. The quality of the processed data is insignificant in assessing whether or not it comprises personal data. Before granting access to spatial data considered personal data, the authorities must ensure that[68]

- the data are disclosed only based on a legal right
- the disclosed data are accurate
- in accordance with the purpose limitation principle, the data are compatible with the purpose for which they are requested
- a written record is produced of the disclosure of personal data, and the purpose of use of the data and the person requesting the data
- information security is ensured during data storage and transfer
- unnecessary data are archived and/or destroyed
- the disclosure and use of data is monitored and instructed, and any misuse is interfered with

As the list indicates, access to information considered personal data in the public domain has been relatively strongly restricted. The restrictions have created a need for facilitating the disclosure of environmental information in situations where there is a general and acceptable need for the data and where these can for example be disclosed separately from owner information that directly reveals the person's identity (although the data are still considered personal data) and where there is fairly low risk of overly extensive interference with privacy due to the quality of the data.

68 Here, the statement of the Data Protection Ombudsman 1179/41/2016 was adapted as a source.

According to section 10 of the Constitution of Finland, provisions on the protection of personal data are laid down by an Act. Therefore, special regulation is also possible from the perspective of the Constitution as long as the restriction fulfils the general prerequisites for the restriction of fundamental rights.[69] For example, the Government proposal to the Parliament for an act on the abolition of separate alluvial plains as real property and certain related acts (HE 102/2015 vp) noted that providing access to the real estate code information in a real property data system and property boundary information does not weaken the protection of personal data as the disclosure of other real property data and ownership information via a technical user connection requires a separately issued permit with purpose limitation.[70] The Data Protection Ombudsman also considered that this kind of regulation did not cause a problem to the protection of personal data.[71] In the legislative phase, a solution has been made to find a balance between public availability and public interest on one hand and the protection of personal data on the other.

In recent times, the relationship between location-specific data and the protection of personal data has also been reflected in the context of the Act on the Forest Information System of the Finnish Forest Centre (419/2011). The information concerning forest ownership and quality is considered personal data. However, it has been proposed that the disclosure of these data should be made easier compared to the currently valid Personal Data Act and section 16(3) of the Act on the Openness of Government Activities, as the Government of Finland received a formal notice issued by the European Commission on the implementation of Directive 2003/4/EC on public access to environmental information on 25 September 2015. According to the Commission, Finland had not fulfilled all of its obligations laid down in Article 3(1) and Article 4(2) of the Directive as the access to data on forest reserves was restricted under personal data legislation and the restrictions to granting access to data laid down in section 16(3) of the Act on the Openness of Government Activities and as the aforementioned subsection required for the person requesting access to data to provide reasons for the request. As a result of the notice, the relationship between the public access to environmental information and the protection of personal data has been evaluated in a draft Government proposal for acts amending the Act on the Forest Information System of the Finnish Forest Centre as well as in a Government proposal to the Parliament for acts amending the Act on the Forest Information System of the Finnish Forest Centre drafted after the former (HE 170/2017). In addition to responding to the infringement procedure, the aim of the amendment is to

69 PeVM 25/1994 vp: regulation in an act, precision and accuracy the acceptability of the grounds for restriction, the integrity of the core area, the principle of proportionality, arrangements for legal protection, compliance with human rights obligations.

70 See e.g. what has been said of the disclosure of real property data in the Government proposal HE 102/2015 vp p. 20 and 32.

71 Statement by the Office of the Data Protection Ombudsman Dnro 2319/03/2015 (18 September 2015). 72 HE 170/2017 p. 3.

implement the goal set in the Programme of Prime Minister Sipilä's Government regarding more efficient utilisation of forest resources data, improving the quality of the forest resources data sets, and enhancing the electronic processing of the data.[72]

The provision of the Act on the Openness of Government Activities concerning restrictions to granting access to data has also been applied to the disclosure of forest resources data that does not include the names and contact details of land owners.

This is due to the fact that the broadness of the concept of personal data results in perceiving forest resources data as personal data in cases where it is easy to find out the person connected to the data.[73] Therefore, the amendments proposed to the Act on the Forest Information System of the Finnish Forest Centre would ensure that current data disclosure procedures related to the protection of personal data would no longer apply to the disclosure of public environmental information in the future. However, for the purpose of protecting personal data, a request for accessing forest resources data could not be made based on names of natural persons.[74]

The topic is considered in the Government proposal 170/2017 as follows:

> "The provisions of the Directive on public access to environmental information regarding the grounds for the disclosure of environmental information are special provisions in relation to the Data Protection Directive. While the right of access to information contained by the Act on the Openness of Government Activities are primarily more extensive than those of the Directive on public access to environmental information, the Act restricts the disclosure of data more strictly than the Directive in cases where the environmental information is part of the personal data filing system of a public authority. According to the Act on the Forest Information System of the Finnish Forest Centre, a copy or a printout a copy or a printout, or an electronic-format copy of contents including personal data may be provided if the conditions laid down in section 16(3) of the Act on the Openness of Government Activities are met. The requirements of the Directive on public access to environmental information would be taken into account by including a special provision in the Act, which would derive from section 16(3) of the Act on the Openness of Government Activities in the context of the disclosure of environmental information."[75]

72 HE 170/2017 p. 3.

73 See Draft 7 November 2016 Ministry of Agriculture and Forestry; Natural Resources Department; Government proposal for acts amending the Act on the Forest Information System of the Finnish Forest Centre, https://api.hankeikkuna.fi/asiakirjat/f5bac47c-e23d-4e01-8db0-d968d683c95e/f3f3f0a1-989e-432a-aea7-d5c8846fbd47/ MUIS-TIO_20161125102931.pdf, accessed on 19 October 2017, p. 13.

74 Ibid. 13–14 and HE 170/2017 vp p. 13 and p. 9.

75 HE 170/2017 p. 13. Also in the draft Government proposal.

However, it is not possible to interfere with the core of the protection of personal data merely based on the fact that the Directive on public access to environmental information is a special provision in relation to the Data Protection Directive. If the fact that this law is a form of special legislation would entitle doing this, the legislation of a number of areas of expertise could undermine the protection of personal data. It must also be taken into consideration that, as a newer set of legal standards, the new General Data Protection Regulation has more weight as a source of legislation in the context of the protection of personal data than the older Directive on public access to environmental information. As a legal instrument, the Regulation can also be interpreted to have more influence as a provision than the Directive. Instead of providing mechanical interpretation arguments, the right to environmental information and the protection of personal data must be coordinated in a manner that allows safeguarding the core contents of both rights. There are certain difficulties in this, as "personal data" has been defined as a relatively extensive concept in both the Data Protection Directive and the General Data Protection Directive. A solution must be sought in the interpretation concerning the grounds for processing the data (as well as the provisions on the environment and data protection), and by also taking into account whether the data in question is direct or indirect personal data in the more precise regulation of the grounds for the processing. Article 86 of the GDPR also mentions reconciling the protection of personal data with public access to documents.

The amendment to the Act on the Forest Information System of the Finnish Forest Centre would make public forest resources data available for everyone in the future. However, the proposed provision would not apply to the disclosure of the name, address and other contact details or personal identity codes of the landowners; the restrictions concerning the protection of personal data would continue to apply to the disclosure of these data. The act also proposes laying down provisions requiring the Finnish Forest Centre to remind those granted access to environmental information on the obligations concerning the protection of personal data when providing access to the information.[76] Moreover, the disclosure of the name and contact information of land owners as well as forest resources data via a technical user connection would be possible in the extent allowed by the purpose limitation or under some other grounds possibly laid down in another act .[77]

The entry into force of the proposed amendment to the Act on the Forest Information System of the Finnish Forest Centre would not mean that forest resources data separated from ownership information were not treated as personal data. Instead, the amendment proposes an exception to the general restriction of the disclosure of personal data. It remains to be seen whether the bill will be submitted for assessment by the Constitutional Law Committee, and whether the Committee considers it proportionate, for instance. At

76 HE 170/2017 vp p. 16.

77 HE 170/2017 vp p. 16.

least the restriction to a fundamental right appears to be precise and unequivocal. The disclosure of forest resources data separately from ownership information and without a possibility for the disclosure of data on the basis of names of owners is also not likely to involve significant interference with the protection of personal data or private life. This restriction to the protection of personal data is also used to safeguard another acceptable aim, namely environmental protection and utilisation of valuable forests in as good and sensible manner as possible. This is a question of a legal solution aiming to find a balance between the public interest and the protection of the private life of land owners.

8 The conditions for processing spatial data with characteristics of personal data in accordance with the GDPR

According to section 40 of the introduction of the General Data Protection Regulation, in order for processing to be lawful, personal data should be processed on the basis of the consent of the data subject concerned or some other legitimate basis, laid down by law. In this context, law refers to a law issued under the General Data Protection Regulation of the European Union or in other Union or Member State law as referred to in the Regulation. Processing is also lawful where it is necessary in the context of a contract or the intention to enter into a contract.[78]

The national implementation of the General Data Protection Regulation is only possible for the parts for which the Regulation provides a direct mandate. Therefore, the processing of personal data is carried out directly under the General Data Protection Regulation for the purposes of the consent of the data subject, the performance of a contract, protection of the vital interest of the data subject or another natural person or carrying out the legitimate interest of the data subject or a third party. Laying down a national law supplementing the General Data Protection Regulation has been deemed necessary and possible only for the parts where processing is carried out in accordance with a legal obligation to which the controller is subject or where processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority.[79]

In practice, the grounds for the processing of personal data have been determined so comprehensively in the Personal Data Act and special acts that situations where there is a rational need for the processing of personal data but no grounds for the processing

78 Section 44 on the introduction of the GDPR.

79 Ibid. and a table on flexibility in the report by the working group on the implementation of the EU's General Data Protection Regulation (TATTI), p. 48–67.

exist under legislation are relatively rare. However, the opportunities introduced by new technology may bring along new kinds of situations to which no grounds for processing in accordance with the law will apply. In such situations, it has often been possible to apply the permission issued by the Data Protection Board as provided in section 43(1) of the Personal Data Act in accordance with section 8, subsection 1(9) of the Personal Data Act. However, this authorisation procedure will be abolished with the entry into force of the General Data Protection Regulation and the new data protection act.[80]

As the new Regulation and data protection act enter into force, the aim is that the lawful grounds for the processing of personal data are included in the General Data Protection Regulation or the data protection act[81] or in special legislation. Section 1(e) of Article 6 of the General Data Protection Regulation, which is applicable to the authorities, and its national implementation (processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller) and section 1(f) of said Article, which is applicable to parties other than the authorities (processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party) will often provide a basis for the processing of personal data corresponding to the cases solved by the Data Protection Board.

The controller is obligated to indicate the existence of a lawful basis for the processing. An administrative fine referred to in Article 83 of the GDPR may be imposed as a result of a lack of lawful grounds for processing after the adoption of the General Data Protection Regulation.

The conditions for the processing of personal data are laid down in the long Article 6. Its first paragraph lays down provisions on the processing of personal data as follows:

Lawfulness of processing

1. Processing shall be lawful only if and to the extent that at least one of the following applies:

   a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;

   b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;

80 For information on the conditions for processing of personal data under the Personal Data Act, see *Pitkänen – Tiilikka – Warma* 2013 p. 71–110. See. e.g decisions by the Data Protection Board 14 July 2011 3/2011 and 3 December 2010 4/2010 on Google's right to process street view data and the restrictions imposed on Google in permit conditions.

81 Only points (c) and (e) allow flexibility at the national level concerning the basis for the processing of personal data.

c) processing is necessary for compliance with a legal obligation to which the controller is subject;

d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;

e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.

Points (c) and (e), i.e. compliance with a *legal obligation* to which the controller is subject or performance of a task carried out *in the public interest or exercise of official authority* vested in the controller, are the most common grounds for the processing of personal data applicable to the activities by the authorities. The activities by the authorities fairly infrequently concern consent and contract as the grounds for processing of personal data. Nonetheless, as such, they are possible and lawful grounds.

According to the working group on data protection appointed by the Ministry of Justice, the processing of personal data in the public sector should as a rule be based on points (c) or (e) of paragraph 1 of Article 6, i.e. the compliance with a legal obligation, the public interest or the exercise of official authority.[82] In the context of spatial data, point (c) is primarily applicable, i.e. compliance with a legal obligation to which the controller is subject. The exercise of official authority vested in the controller in accordance with point (e) may also apply occasionally, although recording activities are not as such exercise of official authority but rather involve entering data on a previously implemented measure to a register controlled system. By contrast, a topographical survey or similar carried out for the purpose of recording data is a form of exercise of official authority. The public availability of environmental information also serves public interest. From the perspective of the authorities, the grounds for processing data can be summarised as follows:

82 Report by the working group on the implementation of the EU's General Data Protection Regulation (TATTI), Ministry of Justice reports and statements 35/2017 p. 101.

GROUNDS FOR THE PROCESSING OF PERSONAL DATA IN ACTIVITIES BY THE AUTHORITIES ACCORDING TO THE GDPR

Most common	Possible	Not possible
Legal obligation	Consent	Interests pursued by the controller or by a third party
A task carried out in the public interest OR in the exercise of official authority	Contract	
	Vital interest	

In its interim report, the working group on data protection appointed by the Ministry of Justice proposed that a new data protection act should be used to supplement the legal basis for the processing in the context of the authorities. A lot of feedback was given on the regulation that the working group proposed in its report (incl. repetition of point (e) of the General Data Protection Regulation in the act), and the final proposal may therefore be changed. For this reason, the contents proposed in the interim report, which are currently uncertain from the perspective of law enactment, will not be further discussed in this article.

According to the General Data Protection Regulation, the legitimate interests pursued by the controller or by a third party (Article 6, paragraph 1 (f)) cannot be used as the legal basis for processing carried out by the public sector.[83] The processing of spatial data with the characteristics of personal data cannot therefore be justified based on the legitimate interests pursued by the controller or by a third party; instead it must be based on a legal obligation of the authority or third party acting as the controller or the performance of duties in the public interest or in the exercise of official authority, or, in the context of private controllers, the purposes of the legitimate interests in accordance with point (f), for instance.

For a commercial company processing spatial data, the processing is likely to be based on either a contract or point (f) of paragraph 1, Article 6 of the GDPR on legitimate interests. In this case, the company serving as the controller must be prepared to provide documents on the consideration of the legitimate interest as well as the interests, fundamental rights and freedoms of the data subject. According to point 47 of the introduction of Regulation, this consideration must include the reasonable expectations of data subjects based on their relationship with the controller.

Such legitimate interest could exist, for instance, where the data subject is a client or in the service of the controller. In this assessment, it is important to consider whether a

83 This is also noted in the report by the working group on the implementation of the EU's General Data Protection Regulation (TATTI), Ministry of Justice reports and statements 35/2017 p. 50.

data subject can reasonably expect at the time and in the context of the collection of the personal data that processing for that purpose may take place. The interests and fundamental rights of the data subject could override the interest of the data controller where personal data are processed in circumstances where data subjects do not reasonably expect further processing. For instance, the processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned. It is also noted that the processing of personal data for direct marketing purposes may also be regarded as carried out for a legitimate interest.[84]

The transition of the consideration for the grounds for processing to the controller as a result of the entry into force of the General Data Protection Regulation is a major change. In this context, attention must also be paid to the purpose limitation principle and the right of the data subject to object to the processing of his or her personal data in cases of processing based on the data subject's consent (see point 50 of the introduction). Moreover, in accordance with Article 13, paragraph 1(d) of the GDPR, the data subject must be informed about the processing of his or her personal data if the data have been collected based on the person's consent[85] and Article 14, paragraph 2(b) if personal data have not been obtained from the data subject.[86]

The EUs' Data Protection Working Party WP29 has interpreted the presence of a legitimate interest in the context of the Data Protection Directive. Where applicable, these principles may also be utilised in the interpretation of the General Data Protection Regulation as the wording of the Regulation is largely compliant with that of the Directive. According to the Data Protection Working Party, the legitimate interest must be fairly concrete and something expected at least in the near future so that it can be weighed against the interests of the data subject. Interests that are too vague or speculative will not be sufficient. The nature of the interests may be beneficial to society at large, (such as the interest of the press to publish information about government corruption or the interest in carrying out scientific research) or be purely based on the economic interest of a company to target its marketing, which is less pressing for society as a whole and may even be controversial.[87]

---

84 Section 47 of the introduction of the Regulation. For information on legitimate interests under the Data Protection Directive, see the extensive 75-page opinion by WP29 844/14/EN WP 217: Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC. Adopted on 9 April 2014.

85 See also sections 2–4 of said Article.

86 See in particular point (b) of Article 14(2) based on which the controller must provide the data subject with information on the legitimate interests pursued by the controller or by a third party if the processing is based on point (f) of Article 6(1).

87 Opinion 06/2014 on the notion of legitimate interests of the data controller under Article 7 of Directive 95/46/EC; 844/14/EN; WP 217; 9 April 2014 p. 26. E.g. establishing a Google street view service similar to the one referred to above could be permitted on the basis of legitimate interests if boundary condition concerning data protection principles, including information security, data minimisation, were taken into account.

The application of a legitimate interest "calls for a balancing test: what is necessary for the legitimate interests of the controller (or third parties) must be balanced against the interests or fundamental rights and freedoms of the data subject. The outcome of the balancing test determines whether Article 7(f) may be relied upon as a legal ground for processing. ".[88] The balancing test will naturally not be carried out if no legitimate interests are present.[89]

88 WP 217 p. 25. The opinion has been issued based on the Data Protection Directive.

89 WP 217 p. 26.

9 Summary and conclusions: how can public access to spatial data be reconciled with the protection of personal data

Spatial data can include, for instance, place names, administrative units, addresses, real property, transportation networks, hydrography and protected areas, vertical positions, land cover, geology, buildings, production and industrial facilities, population distribution, geographic characteristics of climate, biogeographical regions, living environments and biotopes, the distribution of a species, energy reserves and mineral resources related to certain area or place when these are stored in an electronic format.

As a rule, spatial data are not personal data. However, these will become personal data if they can be connected to an identified or identifiable natural person. It is possible to identify a person if, for instance, the owner of a property concerning spatial information can be determined based on a phone call or an email. Spatial data will also be considered personal data when the authority or company receiving the data combines these with the data already at its disposal, and when the combined data allow identifying the data as concerning a natural person.

The concept of personal data in accordance with the General Data Protection Regulation is by far not more concise than the concept of personal data defined in currently valid legislation. The data currently considered personal data will also continue to be personal data after the entry into force of the General Data Protection Regulation and the new data protection act. Location-specific data separated from data concerning individuals is also considered personal data if it is easy to determine who owns or holds a property, for instance. In this case, the applied legislation concerning personal data as well as the restrictions concerning granting access to data laid down in the Act on the Openness of

Government Activities set limitations to the disclosure of data in the public domain as a personal data filing system or via a technical user connection.[90]

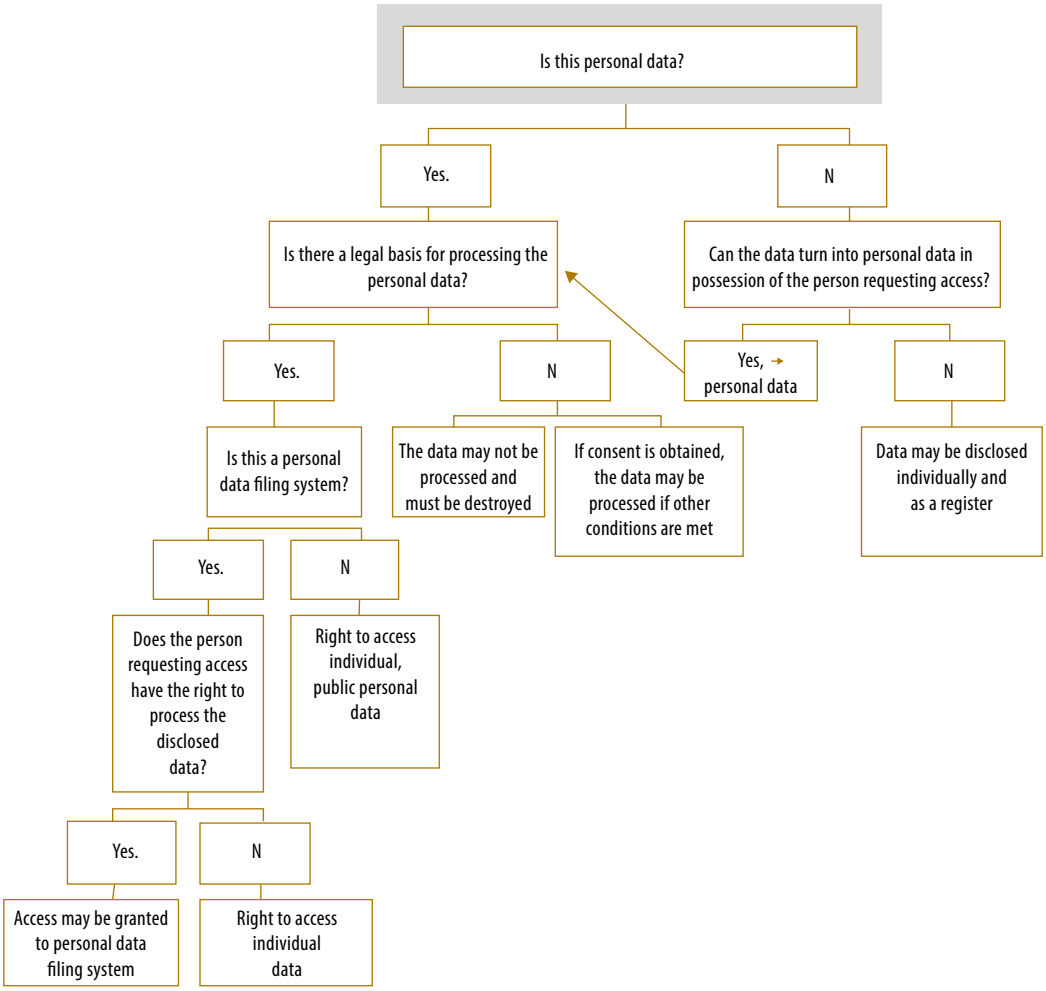
After the entry into force of the General Data Protection Regulation, it must be determined to what extend spatial data and/or environmental information can be processed and disclosed based on point (c) (legal obligation), (e) (performance of a task carried out in the public interest or in the exercise of official authority) or (f) (legitimate interests pursued by private parties) of Article 6. If the disclosure of spatial data or environmental information is ruled to concern the performance of a task carried out in the public interest as referred to point (e) of Article 6 of the General Data Protection Regulation, the processing will have a lawful basis under the new Regulation. However, according to the Regulation, provisions on the grounds based on points (c) and (e) of Article 6 must be laid down in the Union or the Member State law. Therefore, the processing (incl. disclosure) cannot be merely based on a general norm of the General Data Protection Regulation.

In the internal activities of the authorities, the extensive concept of personal data and the requirement for a lawful basis do not typically cause any problems, as the authorities have the statutory competence required for processing different spatial data and environmental information. In turn, private operators will find it more difficult to utilise spatial data as, for example property owners or residents ("data subjects") may not (at least currently) have a customer, commissioning or contractual relationship with a commercial agent.

Providing public access to databases would require an exception to the provision of section 16(3) of the Act on the Openness of Government Activities, according to which access may be granted to a personal data filing system controlled by an authority in the form of a copy or a printout, or an electronic-format copy of the contents of the system only if the person requesting access has the right to record and use such data according to the legislation on the protection of personal data. Exceptions similar to those in the Act on the Forest Information System of the Finnish Forest Centre may be issued to the disclosure procedures if required by compelling reasons and as long as the protection of the privacy of data subjects is not violated. In other words, the exception requires weighing the legitimate interests of controllers and/or third parties against the interests of the data subjects. If, on one hand, the regulation is precise and unequivocal and the possible harm caused to the data subjects is very insignificant, and, on the other, providing access to the databases would produce significant benefits, it may be possible under a special act. This is easiest to accomplish when persons can be only indirectly identified from personal data filing systems and when the data in the personal data filing system is in the public domain or otherwise easy to detect (e.g. buildings visible in Google street view) and users cannot search the data directly using the names of persons.

90 See HE 18/2009 vp p. 5 and HE 83/2015 vp p. 5.

The current process for the disclosure of spatial data can be described as follows:



All in all, the opportunities for more efficient utilisation of spatial data would be improved if the issue was considered as a whole and a special act was used for laying down provisions on the disclosure and other processing of spatial data with conditions that would be easier to implement than currently. At the moment, several different ministries are carrying out various projects concerning spatial data. It would be worth investigating the opportunities for increasing cooperation between the ministries. A further aim should be to ensure that the spatial data services of public administration would conform to the key general needs of the parties that need the data and that the services would be arranged in the manner most efficient to society.

ISBN 978-952-11-4804-0 (PDF)
ISSN 1796-170X (PDF)