Nordic GDPR working group Report

Preliminary findings and suggested work

Contents

1 Executive summary

The GDPR Working Group has explored the legal and practical issues of dissemination of geospatial data, such as addresses, buildings and oblique images, in regards to the GDPR.

The wide definition of personal data in the directive, and the particular challenges of the public sector, creates a somewhat complex and still not clear picture of the legal situation. The GDPR Working Group has tried to describe these issues in chapter 3, 4 and 5, with particular focus on the geodata issues. There are grey areas in this picture where the lawyers cannot provide clear-cut answers.

In particular, we find it difficult to say with certainty what appropriate technical and organisational measures according to GDPR Art. 32, that is required in any given circumstances. This is particularly challenging the view of the demand on public bodies to make public information as widely accessible as possible. It needs to be considered on a case-by-case basis, and national circumstances will have important influences on the solutions.

Nevertheless, the GDPR Working Group has experienced how knowledge sharing can be beneficial in order to translate the very general articles under the GDPR into something meaningful. When the Nordic agencies distribute the same type of data in the same manner, they will benefit from sharing knowledge on how the GDPR has been interpreted more specifically. What we have learned from our discussions, is also that the handling of these challenges requires input not just from the legal personnel, but also from IT personnel and other experts.

The GDPR Working Group suggests that its members will continue to update each other on relevant matters, with inclusion of other experts from the organizations when required. This could be done by setting up a resource group whose mandate will be to hold either in-person or virtual meetings once or twice a year. The Resource Group could also propose initiatives for more in-depth discussions on a Nordic or European basis.

2 Introduction

2.1 Mandate

The Directors Generals have acknowledged that the General Data Protection Regulation (EU) 2016/679 ("GDPR") poses common challenges in the Nordic countries in relation to geospatial data and their classification.

The NIC Working Group was asked at "Store Chef Meeting" in Tórshavn to come up with a proposal to move forward with exchanging knowledge and challenges in respect of the GDPR in the Nordic countries.

A group of GDPR experts from the Nordic NMCAs discussed this and made a proposal in connection to the Nordic IT and Development Working Group meeting in Helsinki on 23 and 24 January 2019.

The Director Generals agreed at "Lille Chef meeting" in Copenhagen on 3 April 2019, that the GDPR Experts will continue their work based on this proposal, which includes focusing on this scenario:

How to handle dissemination of geospatial data such as addresses, buildings and oblique images, taking into account different methods of providing the data as a service and conditions for access.

2.2 Overview of work

The GDPR Working Group has explored the legal and practical issues of this scenario pursuant to the GDPR and produced this report. We have had a number of Skype meetings and one meeting in Copenhagen 23-24 January 2020.

This final report shall be presented at "Lille Chef Meeting" in March 2020.

3 Legal framework

3.1 Summary of the GDPR issues

The principles of processing personal data are laid down in the GDPR Art. 5, while Art. 6-11 regulates the lawfulness of the processing, chiefly how it can be based on either consent or law. Art. 12-23 describe the right of the individual (data subject) that the controller needs to deal with. Art. 24-43 describe the rules that apply to a controller (or processor) on how this processing should be carried out. The 'processing rules' for a data controller will therefore be a combination of the principles and data subjects rights with the adequate measures that each product and situation requires.

Art. 4 no. 1 defines 'personal data' as *any information relating to an identified* or *identifiable natural person*. An identifiable natural person (or 'data subject') is defined as 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.

According to section 26 of the recital, in order to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used to identify the natural person directly or indirectly. 'Reasonable' refers to factors such as the costs and amount of time required for identification.

The EU legislator has chosen a broad definition of personal data, meant to be dealt with on a case by case basis, rather than prescriptive rules, i.e. a list of what is considered personal data. This approach was also used in the former Directive, and has to some extent been criticised in the academic world.[1]

According to Art. 32, the controller shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk to the rights and freedoms of the natural persons. According to Art 24, these measures shall be reviewed and updated where necessary. This indicates that there could be situations where the risks to the natural persons are so insignificant that no particular measures are required. This was also the case with the earlier directive that applied the same broad definition of personal data.

This is supported by an opinion of the Article 29 Data Protection Working Party[2] on the "concept of personal data". In Opinion 4/2007, page 25 it states: "These rules were therefore designed to apply to situations where the rights of individuals could be at risk and hence in need of protection. The scope of the data protection rules should not be overstretched, but unduly restricting the concept of personal data should also be avoided. The legislation has defined its scope, excluding a number of activities, and allows flexibility in the application of rules to activities that are within its scope. Data protection authorities play an essential role in finding an appropriate balance in this application."

The use of the term "situations" seems to indicate that the opinion's talk about the practical side of the processing rules; as "adequate administrative and technical measures" will depend on the situation. This is different from the data that is not considered personal data at all. For example, the GDPR allows archiving under national law in some situations, making the right to erasure no longer applicable. These data are clearly still personal data, but some of the processing rules do not apply. However, you could also argue that in certain situations the data is no longer personal data, because the "reattachment" as described above is no longer reasonably possible, and that this becomes the basis for omitting the use of processing rules. Whether making this distinction have any practical application is another matter. We will return to this discussion during the considerations of the various geodata products.

You can also have situations where the need of protection is no longer there. This can be the case where the data that used to be personal data are anonymised which is common for statistical data. Other examples are when data are pseudonymised, and the "reattachment" is unavailable (encrypted or otherwise restricted), or when data are pseudonymised and the "reattachment" is controlled by the data subject.

You can also have situations where data collected as non-personal data becomes personal data through processing, such as weather data or aerial photography.

Deciding when a certain processing do not require any special measures, does create more of a challenge for the public sector than the private sector, since public data is often supposed to be freely and widely available, preferably online.[3] This is particularly the case with geodata that is a part of the national

[1] An example of the academic criticism:
"As a result [of this broad definition], European data protection law is facing a risk of becoming 'the law of everything', meant to deliver the highest legal protection under all circumstances, but in practice impossible to comply with and hence ignored or discredited as conducive to abuse of rights and unreasonable."
(from the article The law of everything. Broad concept of personal data and future of EU data protection law by Nadezhda Purtova, Tilburg Institute for Law).

[2] Article 29 Data Protection Working Party was an independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018. Their opinions on issues that have not been significantly changed in GDPR, such as the definition of personal data, are still valid.

[3] According to Danish professor, Peter Blume the GDPR is and should mainly be a private sector project. He argues that the EU legislator should have chosen separate rules for the public and private sector because of the very different relationship to the data subjects. In his opinion, the one size fits all approach can't ensure fully harmonised rules across both sectors and the 28 Member States. To exemplify the differences, he writes 'The tasks, resources and regulatory context relevant to local authority in Bratislava and the conditions under which Google and other multinational corporations operate are simply not comparable.'

infrastructure, both as a support for physical infrastructure and as a vital component in the information society.

One solution to this problem is regulate in law that no measures are required, according to Chapter IX in the GDPR, for example under Article 86, Processing and public access to official documents. Here one can set national rules for such access based on national circumstances, type of document etc. National circumstances justifying that no particular measures are taken, could for example be the national traditions for openness of public data.

The following extracts from the GDPR recitals summarises the guidelines that should be adhered to when interpreting what the correct processing rules are:

> 2: …respect their fundamental rights and freedoms, in particular their right to the protection of personal data…. strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
>
> 4: …The right to the protection of personal data is not an absolute right; it must be considered in relation to its function in society and be balanced against other fundamental rights, in accordance with the principle of proportionality.
>
> 9: Differences in ... processing of personal data in the Member States may prevent the free flow of personal data … may therefore constitute an obstacle to the pursuit of economic activities at the level of the Union, distort competition and impede authorities in the discharge of their responsibilities under Union law.
>
> 18: … does not apply to the processing of personal data by a natural person in the course of a purely personal or household activity … could include correspondence and the holding of addresses, or social networking and online activity undertaken within the context of such activities. However, this Regulation applies to controllers or processors which provide the means for processing personal data for such personal or household activities.
>
> 26: …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 information on an identifiable natural person. …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…. The principles of data protection should therefore not apply to anonymous information...
>
> 28: The application of pseudonymisation to personal data can reduce the risks to the data subjects concerned and help controllers and processors to meet their data-protection obligations.
>
> 154: … Personal data in documents held by a public authority or a public body should be able to be publicly disclosed by that authority or body if the disclosure is provided for by Union or Member State law to which the public authority or public body is subject….

3.2 Legal sources on geodata as personal data

There is little source material for geodata and personal data issues in the Nordic countries, as well as on the European level.

When Google started to release Street View, there was a number of processes around the legality of this, also in Europe. Google has taken several precautions, more or less voluntarily, including blurring of persons and license plates. It has opened for individuals to ask that breaches of privacy are rectified, something that the GDPR has strengthened.

This will also apply to public bodies publishing aerial photography or oblique images, and we have indeed in the group discussed one such case in Denmark. The conclusion seems to be that publishing is fine, but we must be prepared to deal with claims for erasure.

Professor Päivi Korpisaari from University of Helsinki has made a report on the subject "How does the Protection of Personal Data Restrict the Use of Spatial Data" for the Finnish Ministry of the Environment in 2018.[4] In this report, it is stated that geospatial data are as a rule not personal data. However, according to the report it should be noticed that personal data refers to any information related to an identified or identifiable natural person. The reference to any information aims at a wide scope of application of the legislation concerning personal data. Because of this, according to the report, geospatial data will become personal data if it can be connected to an identified or identifiable natural person.

According to the aforementioned report it is possible to identify a person, if, for instance, the owner of a property concerning geospatial information can be determined based on a phone call or an e-mail. Geospatial 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. Therefore, details such as a real estate code or an address of a building have been considered 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 (page 23 and 40).

Respectively, "place-bound" data, such as but not limited to addresses or data concerning environmental factors, living conditions, buildings or yards related to a specific real estate, have been considered personal data relating to the owner of real estate, if the owner is a natural person. Building information can also be considered personal data of a tenant, if the receiver of such data easily and without excessive costs can identify who lives in the building. If data relating to the conditions of a specific area concerns for example all the real estates placed in the respective postal code zone, the data is considered personal data of the real estate owners in the respective area, because it is relatively easy to define whom the data concerns.

However, it is stated in the aforementioned report that maps have not in practice been considered personal data, although an address or real estate number can be established based on the map and a building in which a natural person lives, or a real estate owned by such a person can be established based on the map. According to Päivi Korpisaari, it seems to this extent like the usefulness and necessity of the data, the long-term common use of the data and the fact that the data is indirect personal data (identification requires additional measures), have passed the literal interpretation of the data protection legislation (page 40).

3.3 Aggregation of data by others

An issue that we are confronted with on occasion is natural persons complaining to us about what a third party receiving our data has done. The third party is a controller under personal data law and are responsible for their own processing under GDPR, but from a political point of view this can be a complicated issue. One precaution we tend to take is to inform receivers of data of their obligations under the GDPR. It has been discussed as a potential source for undermining the trust in the public registers.

3.4 Transfer to third country

Chapter V in the GDPR regulates any transfer of personal data to a country outside EU/EEA. The need for a legal basis for the transfer itself will be triggered no matter how the distribution is regulated in national or European law, and no matter if the data is publicly available or merely available for natural and legal persons claiming to have a specific interest in receiving these data.

Nevertheless, public authorities are entitled to make data publicly available without appropriate safeguards as mentioned in article 46. This derogation only applies for registers from which the national or EU legislator has decided that certain information shall be open for consultation, either by the general public or by any person who can demonstrate a legitimate interest. Sometimes the legislator has set up certain requirements for allowing consultation of these data, thus letting the distribution depend on the specific matter. An example is the exception for physical property information in the Norwegian Cadastre Act, see Chapter 5.2.2.

[4] See prof. Päivi Korpisaari, How does the Protection of Personal Data Restrict the Use of Spatial Data, Reports of the Ministry of the Environment 18/2018, Helsinki, http://julkaisut.valtioneuvosto.fi/handle/10024/160974.

If the derogation does not apply, it is necessary to apply appropriate safeguards for the personal data either not to be transferred or to comply with the transfer rules. For Norwegian Cadastre data that is not covered by the exception in the law, access is only possible if you have a Norwegian digital identity, or if you have a direct agreement with Kartverket that grants you access. This is to avoid dealing with the transfer rules.

4 Geodata as personal data

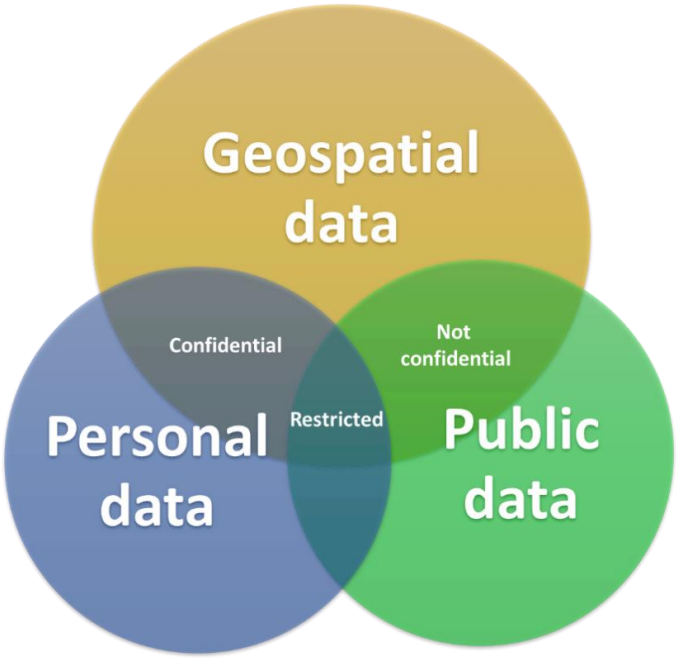
According to our mandate, the GDPR Working Group should focus on "addresses, buildings and oblique images". We have expanded this scope to other physical cadastre data as well as aerial images. Land registry data (ownership etc.) have been discussed but omitted, as it is raising a number of additional issues that could be explored with more success in a separate report.

Public bodies need to handle various more or less harmonious rules on how we can handle our data, particularly how to disseminate them. The diagram below illustrates the various categories. As we are only interested in geospatial data, only these overlaps are commented.

Confidential: Generally not distributed. *Example*: protected addresses.

Not confidential: Available without restrictions. *Example*: address database.

Restricted: available to certain users or user groups. *Example*: cadastre data.



Geodata is by nature connected to a place, and the place can be connected to a person or data object as discussed above. The table shows who are the possible data subjects for each of them.

Type of data	Categories of data subjects
Addresses	People who live at the address or real estate owners
Building information	People who live in the buildings or real estate owners
Cadastral data	People who are registered in the cadastre as (right) owners
Images from oblique angles	People who live in buildings shown on the image or owners thereof
Aerial images	People who live in buildings shown on the image or owners thereof

Therefore, the crucial point in determining whether geodata is personal data lies in the element "relating to" in the definition of personal data.

The Article 29 Data Protection Working Party[5] concludes in Opinion 4/2007: "The second element – "relating to" – has so far often been overlooked, but plays a crucial role in determining the substantive scope of the concept, especially in relation to objects and new technologies."

According to the Opinion 4/2007, there are three alternatives for how the data can relate to a person:

1. The *content* is about that person, or
2. The data is used or likely to be used, taking into account the circumstances, with the *purpose to evaluate, threat or influence a person* in a certain way, or
3. The use of the data is likely to have an *impact* on a person's rights and interests.

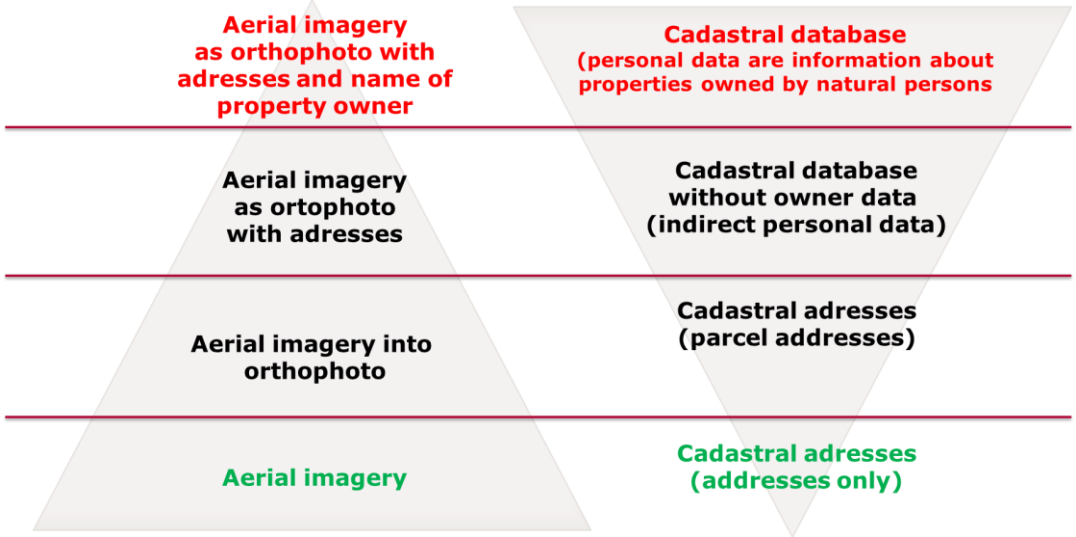
Using addresses as an example, it does however raise several questions that are not easily answered:

1. An address describes an object, not a person. However, a description of an object can in a certain context be a description of a person. The opinion mentions value of a property. However, is a coordinate a description of an object, which can be a description of a person? Of course, if you can be connected to it as your property or abode, but unlike the value that becomes a description of what you own, the coordinate cannot be permanently attached to your person, and it will not describe you unless other information is connected.
2. Is an address with coordinates used or likely to be used to evaluate, to threat or to influence a person?
3. Is the use of an address with coordinates likely to have an impact on a person's rights and interests?

However, addresses connected to coordinates fulfil important functions in today's information society. It is important in many situations to be able to verify that such an address exists, for example if a customer provides an address to a webshop or a citizen to a public institution. As such, the interest in verifying the addresses will at least to some extent outweigh the somewhat remote likeliness of these data being used in a way detrimental to persons. In the Nordic countries, such lists are available with varying grades of openness, from completely open to a more restricted access, depending on national policies.

The Working Group have also arrived to such and other conclusions on how to disseminate geodata using different reasoning, but without finding a common ground because we see the GDPR rules differently. Mainly it is a question of having different national starting points, such as whether there are national legislation pertaining to this, what traditions we have for openness, and how the national DPA has dealt with these issues in the past. The Regulation opens for national differences based on such considerations, if the data subjects still receive an adequate protection.

The following illustration shows how datasets in green (non-personal data) can come from or go towards red (personal data) depending on the processing of the data set.



[5] Article 29 Data Protection Working Party was an independent European working party that dealt with issues relating to the protection of privacy and personal data until 25 May 2018. Their opinions on issues that have not been significantly changed in GDPR, such as the definition of personal data, are still valid.

The black datasets are more uncertain, as it will depend on the situation and the existence of national law on these matters. This is a grey area where many lawyers of the Nordic contries can't give clearcut answers on what measures are needed, as it will depend om the circumstances.

5 National products and practices

5.1 General dissemination policies

5.1.1 Denmark

SDFE (Agency for Data Supply and Efficiency) distributes addresses, information on buildings and oblique images in the exercise of official authority. These official tasks are laid down in national law to which the organization or another public authority is subject.

The aim of efficient work processes for both public authorities and private companies has been a crucial driver in the opening of standardized geospatial data about Denmark and its citizens.

In accordance with recent guidance from the national DPA, we do not consider the address register, our topographic maps and registered building information as personal data. To elaborate this further, the national DPA confirmed that specific geospatial data only can be defined as 'personal data' when it in a given processing situation directly deals with an individual, is of significance to the individual or intends to create a relation between the individual and the specific data.[6] Thus, as a general rule geospatial data as basic data regarding an object will fall outside the material scope of the GDPR.

Due to the lack of case law and interpretations in this area, SDFE has made a specific assessment regarding the organiation's processing of geospatial data, in connection with the Danish Address Register (DAR) and SDFE's topographic maps, as a processing of personal data.

To this end, it must be stated that the purpose of DAR is to gather all of Denmark's addresses in a single register. This helps to greatly reduce the number of errors in the public administration, due to the fact that the authorities can use the same address information for different contexts. Thus, the purpose of DAR is not to identify individuals and the address registration is unlikely to have an impact on a particular individual's status, course of action, rights or duties. Consequently, the basic address information cannot be seen as personal data as defined in the GDPR.

However, third-party users of SDFE's basic address registrations still have to make their own assessments to determine whether their use of data falls within the scope of the GDPR.

Nevertheless, it will be fair to say that some oblique images show one or more actual natural person/s and therefore fall under the term 'personal data,' taking all measures for identification into account. A Danish law professor has even stated that one person can be identifiable under the GDPR if another person can make *reasonable assumptions* about his or hers identity from the information held in the photo (e.g. location, date and specific objects belonging to that person).

Despite this, GDPR does not put limits on our ability to freely distribute all our geodata to the public.

A large number of geospatial datasets are made publicly available under a free and open data license.

[6] The national DPA refers to page 9-10 of the Article 29 Data Protection Working Party's opinion 4/2007 on the concept of personal data. The WP establishes that in some situations, information conveyed by data concerns objects, and not individuals. This information does not "relate to" an individual directly, which is a requirement according to the GDPR for the information to be considered personal data and thus within the scope of the regulation.
The WP shows this with an example: The value of particular house is information about an object. Data protection rules will not apply, as it solely illustrates real estate prices in a given area. However, this information can be considered personal information under some circumstances; the house is an asset of the owner, which will determine the extent of the person's obligation to pay some taxes. The example shows that the data controller will have to make a specific assessment to determine whether or not the data is solely about an object, or if it's somehow indirectly "relating to" an individual due to the specific use of the data.

They include:

- Topographic data in various formats and scales, including themes such as road networks, buildings, forests, built-up areas etc.;
- Location-based addresses;
- Topographic data in various formats and scales, including themes such as road networks, buildings, forests, built-up areas etc. and
- Orthophotos (geometrically corrected aerial photography).

Put in other words, SDFE is responsible for making a lot of geodata public available, but the distribution of cadastral information and parcels is not part of SDFE's statutory tasks. These data are instead processed by the sister agency called GST (Geodatastyrelsen). GST deals indisputably with personal data e.g. cadastral information in relation to real estate owners. Therefore, the organization has implemented a dissemination policy that enables them to respect the GDPR, especially the principle of data minimization.

5.1.2 Norway

Our dissemination policy for geodata can be categorised like this:
1. Open, free of charge geodata;
2. Open, but not free of charge geodata; and
3. Restricted and not free of charge geodata.

Most of our topographic data and physical property information belong to no. 1. Some of the cadastral and land registry data and aearial images belong to no. 2, and the rest of the cadastral and land registry data belong to no. 3.

Besides this, the INSPIRE directive is implemented through the Geodata law, which regulates accessibility of geodata and the sharing of such data between public bodies.

According to the Public Administration Act, documents, records and similar registers for the authority are open for inspection unless otherwise covered by regulation.

5.1.3 Finland

National Land Survey of Finland collects topographic data, i.e. aerial images, topographic maps and laser scanning data, from the entire country. The datasets include for instance:

- place names
- roads
- buildings
- waterways
- fields
- topographic features and elevations
- cadastral boundaries
- administrative boundaries

The topographic data is open data (since 2012). The legal basis for processing the topographic data is the Finnish Act on the National Land Survey of Finland (1025/2018, section 2 (3))

Open data by National Land Survey of Finland is licensed under a Creative Commons Attribution 4.0 International License. Based on the licence the data may be freely copied, distributed and published. It may be processed and utilised for commercial purposes and used as part of applications or services. There is an exception for security graded data pursuant to the Finnish Territorial Surveillance Act 755/2000 section 14.

The Finnish Land Information System comprises Cadastre and Land Register data. The Finnish Land Information System is regulated by the Act on the Land Information System and Related Information Service 453/2002. Except for cadastral boundaries and real estate numbers, the aforementioned topographic data is not part of the Finnish Land Information System.

Data in the Finnish Land Information System can be disseminated in accordance with section 6 of the Act on the Land Information System and Related Information Service. The National Land Survey of Finland is obliged to provide a free public access to the data included in the Land Information System and the possibility to take notes of the data at the Land Survey Office. Extracts, certificates and other documents are subject to charge, or these can be obtained through a technical user interface (the technical user interface can be used by authorities or private entities, that have been granted a license for obtaining data through the technical user interface). Unless otherwise provided on special grounds, electronic copies of the data may be given subject to charge.

In addition, a natural person can get access to data of pieces of real estate owned or possessed by the person in question through an e-service portal maintained by the National Land Survey of Finland.

Dissemination

According to article 86 of the GDPR, 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 the GDPR.

According to section 28 of the Finnish Data Protection Act (1050/2018), the provisions on the openness of government activities apply to the right of access to data and to other disclosure of personal data from a filing system of a public authority.

The Finnish Act on the Openness of Government Activities (621/1999) contains provisions on the right of access to official documents in the public domain, officials' duty of non-disclosure, document secrecy and any other restrictions of access that have been considered necessary for the protection of public and private interests, as well as on the duties of the authorities for the achievement of the objectives of the said act. According to section 1 (1) of the said act official documents shall be in the public domain, unless specifically provided otherwise in the said act or another act.

The disclosure of personal data in the public domain is restricted by 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, 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 section, in the context of granting access to many personal data contents (personal data filing system), the authority must verify that the data recipient is entitled to process personal data under legislation on personal data i.e. GDPR and the Finnish Personal Data Act. This section 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.

However, it should be noticed that section 16 (3) of the Act on the Openness of Government Activities is a general provision which is only applied if not otherwise provided elsewhere in the Act or another Act. A special act, such as for instance the Act on the Land Information System and Related Information Service, may therefore lay down provisions on more extensive access to data (see section 6 above). *However, in Finland there are no special provisions on granting access to for instance addresses of buildings or pieces of real estate or to oblique images.* In addition, it should be noticed that based on a ruling by the Finnish Constitutional Law Committee, an act must lay down provisions on technical user connections as it enables extensive and rapid data transfer. 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.[7]

[7] Same source as footnote 4, p. 28.

Providing public access to databases containing geospatial data considered personal data would require an exception to the provision of section 16 (3) 3 of the Act on the Openness of Government Activities. It has been stated in legal literature that 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.[8]

5.1.4 Sweden

Official documents are, with the exception of those considered secret, available to the public according to chapter 2 of the Freedom of the Press Act (Tryckfrihetsförordningen). The definition of official documents is broad and covers most of the information that Lantmäteriet distributes including images, registers, maps etc. Because of this, addresses, building information and oblique images can be accessed by the public through a request based on the Freedom of the Press Act filed with the agency that is responsible for storing the information in question. The right to access official documents includes viewing the document for free at the agency and/or receiving a copy of the document that may be subject to a charge. The right to access official documents does not extend to digital access to the information. Digital access is instead regulated in various acts regulating specific registers. Information of a smaller extent can sometimes be sent digitally to the public as part of a general obligation of service.

5.2 Addresses and buildings information (cadastre)

5.2.1 Denmark

The distribution of address data is regulated in the Danish Address Act (adresseloven).

Article 16(1), (2) and (3) states:

(1) The Minister for Climate, Energy and Utilities shall ensure that information in the Danish Address Register about road names and addresses, cf. section 14(2) and (3), and information about supplementary town names and postcodes, cf. section 14(4), is made freely available digitally and that it is made available as common basic data for everyone.

(2) Public-sector basic data registers on people, businesses, properties and buildings shall, in connection with registrations which include a road name or an address, use the Danish Address Register as the authoritative source of information on existing road names and addresses in Denmark.

(3) Public authorities and institutions shall, when establishing new IT systems, organise the system so that registrations which include a road name or an address, use the Danish Address Register as the authoritative source of information on existing road names and addresses in Denmark.

With reference to the Act on Spatial Information (lov om stedbestemt information) the organization is responsible for providing easy access to the Agency's geospatial data through The Map Supply (Kortforsyningen.dk), Geodatainfo.dk, aws.dk and the Agency's map guide. All of these platforms are accessible for the public.

The Minister for Climate, Energy and Utilities has the right to decide whether geospatial data should be open or not. Article 13(1) states:

(1) The Minister for Climate, Energy and Utilities shall make decision on which geospatial data from registers, maps etc., falling under the scope of this Act, that will be open to other public authorities,

[8] Same source as footnote 4, p. 41-42.

businesses and citizens. The Minister also makes decision on how these data, registers and maps should be available.

The INSPIRE Directive is transposed into Danish legislation through The Act on Infrastructure for Geographic Information, which came into force in May 2009.

Everyone can get access to the Agency's geospatial data through the Map Supply (Kortforsyningen.dk), the Open Geography Portal (Geodatainfo.dk), the Address Web Services (aws.dk) and the Agency's map guide (https://sdfekort.dk/spatialmap).

In addition, SDFE distributes basic data on behalf of a variety of public entities via the distribution platform Datafordeleren. One example worth mentioning is the transfer of data from the GST's property formation register (Ejerfortegnelsen) to different categories of users. Some of them being public and private authorities who are entitled to access the register unlimited in order to fulfill their legal obligations.

Ejerfortegnelsen is divided into 3 levels by which access to the Register is granted either fully or partially. Level 2 and 3 contain confidential personal data, such as national identification numbers and addresses, in combination with names that are not to be disclosed to the public, except for users who have the needed legal basis for collecting that data (e.g. personal information covered by an address confidentiality program).

Whenever GST is met with such a request, the user must demonstrate the existence of a lawful basis, as set out in Article 6 of the GDPR.

It is clearly stated in relation to the distribution platform that any collecting public or private authority should consider its obligations under the GDPR when receiving the data, thus becoming data controller for the proceeding processing which might include aggregation of data.

5.2.2 Norway

The complete addresses and building information is available through the Cadastre (Matrikkelen) and access is restricted according to Section 30 of the Cadastre Act:

Cadastral data may be provided for use related to:

a. public planning, administrative procedure and administration,
b. purposes pursuant to this Act, the Planning and Building Act, or Condominium Unit Act,
c. applications for public licences, or
d. dealing with other interests related to possession of cadastral parcels or their use.

Cadastral data may be provided for other purposes if the person to whom the information is to be provided shall ensure a legitimate interest, and consideration for the personal information protection of those registered does not outweigh this interest.

Cadastral data that does not contain personal data, or only includes data that identifies, maps, or specifies types of cadastral parcels, buildings or addresses, may be provided for all types of use.

The last paragraph reflects the discussion during the adaptation of the Act, where one was consolidating traditional openness for property data in Norway with the considerations in the Personal Data Act. There was a strong political interest in preserving this openness for the benefit of society.

We concluded that the physical information about properties could not be said to not be personal data, considering the aforementioned wide definition. Furthermore, we concluded that this meant that the Personal Data Directive (like the GDPR) required us to make specific exceptions in the Act. The result was "*data that identifies, maps, or specifies types of cadastral parcels, buildings or addresses*".

Based on this, the following products are freely available for download and use:

1. Addresses
    - "Matrikkelen – Adresse" is the official addresses of a building, parcel or other physical object. Today it can be a street address (street name and number) or a parcel address (kommunenummer/gårdsnummer/bruksnummer/festenummer/seksjonsnummer). In the future, the official address register is going to include only street addresses.
    - "Matrikkelen – Adresse Leilighetsnivå" is the official addresses with addresses for units inside the buildings (apartments) as well.
    - These are also available with varying specifications and content, such as WMS/WFS, street addresses only, etc.
2. Buildings and property map

    "Norgeskart.no" gives open access to the property map of Norway, with addresses and information on the buildings, limited to type of building and whether it is a listed building or not.

5.2.3 Finland

In Finland, the municipalities have a duty to register and maintain the addresses of buildings and addresses databases even though there is no comprehensive mandatory legislation concerning the registration and maintenance of addresses or addresses databases. However, there are still some areas and buildings without addresses.

Municipalities disseminate address data of buildings among other recipients to the Population Register Centre of Finland and to the National Land Survey of Finland. Population Register Centre of Finland maintains the Population Information System, which is one of the most central databases in Finland.

The National Land Survey of Finland maintains a topographic database. This database contains for example all Finnish road and street information. There is no special legislation concerning the topographic database, for instance on dissemination of data from the topographic database, such as the special legislation on the Finnish Cadastre and Land Register.

5.2.4 Sweden

Digital access to personal data in the cadaster and land register and the apartment register, which includes building information and addresses, is regulated in its own acts: act on the cadastre and land register (lag (2000:224) om fastighetsregister) and act on the apartment register (lag (2006:378) om lägenhetsregister).

Article 2 in the Act on the cadastre and land register contains a list of legitimate purposes for which personal data in the register may be disseminated. For an interested party to get access to personal data an application must be made to Lantmäteriet. The applicant will be granted access if the intended processing corresponds with the purposes listed in article 2.

In a similar manner article 5 in the Act on the apartment register statues the purposes for which the data the register contains may be processed. In article 18 it is stated that municipalities are granted direct digital access to data in the apartment register concerning information about residential apartments located in the municipality in question. Article 17 gives the government the mandate to stipulate ordinances with additional rules on digital access to the apartment register. The government has done so in the ordinance on the apartment register (förordning (2007:108) om lägenhetsregister). Article 6 of the ordinance stipulates that the Swedish Tax Agency may have direct digital access to the apartment register. In addition, article 7 states that requested selections of data from the register may be provided digitally to the Swedish Tax agency, Statistics Sweden, the municipality where the apartment in question is located and to the owner of the property in question.

The primary purpose of the cadastre and land register is to make the information in the register available to the public whilst the primary purpose of the apartment registry is to ensure the production of qualitative national accommodation and household statistics. In a broader perspective the aim of the dissemination of the data from both registers can be described as to actualize the value of the information in society.

Lantmäteriet has concluded that although addresses and building information contains personal data, they are harmless to distribute. The Act on cadastre and land register does not differentiate between harmless and non-harmless personal data. Whether dissemination of personal data in the register is allowed or not depends solely on the presence of a legitimate purpose. According to article 2 (1) one such legitimate purpose is if the data are required to fulfil tasks that the state or a municipality is legally obligated to perform. Lantmäteriet has a general task, regulated in the ordinance with instructions for Lantmäteriet (förordning (2009:946) med instruktion för Lantmäteriet), to sufficiently provide society with certain geodata. The agency has concluded that this task corresponds with the legitimate purpose mentioned above and issued an internal decision to that effect. This lets Lantmäteriet distribute addresses and building information openly.

The reason that dissemination of data from the apartment register is more restricted compared to the cadastre and land register is on one hand that the former register has a the somewhat narrower purpose of ensuring the production of statistics. Furthermore, the concern was raised by the legislator that the apartment register can be cross-checked with the population register. Since the register contains information on every residential apartment in Sweden, the possibility of cross-checking led to the conclusion that the data in the apartment register is sensitive from a privacy perspective.

5.3 Images (aerial, orthophoto and oblique angles)

5.3.1 Denmark

In reference to article 4 (1) in the Act on Spatial Information (lov om stedbestemt information) the organization is responsible for mapping the land of Danmark, Faroe Islands and Greenland as well as establishing, providing and developing the related data, registers and maps.

By visiting skraafoto.kortforsyningen.dk it is possible to freely access and download SDFE's aerial imagery from oblique angles.

5.3.2 Norway

Aerial images (historic and current) are freely available for viewing as orthophoto from norgeibilder.no. If you want a copy of an original aerial image, you can buy it from us.

5.3.3 Finland

See chapter 5.1.3.

5.3.4 Sweden

The legal ground for the dissemination of oblique images and aerial photos can be found in the ordinance with instructions for Lantmäteriet. According to article 3 (2) of the ordinance one of Lantmäteriet's main tasks is to provide certain geodata to the public to the extent that it meets society's needs. This is the basis for disseminating oblique images and aerial images.

Oblique images are available for purchase but are not actively marketed or published since the supply is limited and only covers the years 1976-2005. Historical orthophotos can be accessed as open data on www.lantmateriet.se. As for other aerial photos these are not open data in the sense that they are not free of charge, but they are available for purchase without legal restrictions like those present in the before mentioned register acts.

6 Conclusions and the way forward

The GDPR does not restrict the distribution of open geospatial data if it is personal data and there is a legal basis for the distribution, e.g. the task is subject to national or EU legislation. However, it creates a number of practical questions as to how this distribution should be handled.

The GDPR contains more detailed regulations on processing rules than the preceding Directive. However, it still gives leeway for interpretation, in particular for exceptions under national law and to what extent the controller should apply the described measures. The GDPR makes the weighing of interests mandatory when deciding upon these practical solutions. Nevertheless, it leaves a national room for respecting existing laws and traditions on the handling of open data.

The broad definition of personal data forces the Nordic Mapping and Cadastral Agencies to take the GDPR into account when distributing a number of different types of geospatial data. The GDPR leaves it up to the public organizations to translate this legal standard into prescriptive rules, applicable to the organizations' exercise of official authority.

The EU legislator assumes throughout the articles of the GDPR that the distribution of personal data is regulated in national law. In the future, the national legislator therefore has to define more clearly the statutory task in order to ensure transparency and compliance for the public authority's processing of personal geospatial data.

In addition, the comparable processing of geospatial data will probably lead to the identification of the same consequences for the data subjects. With reference to recital 75 in the preamble of the GDPR these could be identity theft or fraud, financial loss, damage to the reputation, loss of confidentiality of personal data protected by professional secrecy, unauthorised reversal of pseudonymisation, or any other significant economic or social disadvantage. The likelihood of the specific consequences should be concretized by carrying out an Article 32-assessment.

The Nordic countries deal differently with many similar geodata products. However, we think this is largely a result of both national traditions and legislation from the time where the European Data Protection Directive and not the GDPR was applicable, as well as the existing cases from the national DPAs. We have a similar understanding of the GDPR and differences simply exploit the leeway that the GDPR gives to national law.

The GDPR Working Group has found that the scenario in the mandate has the right focus when pointing out which datasets to look at as practical examples of the Mapping Authorities challenges.

The GDPR Working Group has experienced how knowledge sharing can be beneficial in order to translate the very general articles under the GDPR into something meaningful. When the Nordic agencies distribute the same type of data in the same manner, they will benefit from sharing knowledge on how the GDPR has been interpreted more specifically.

There are also important issues that we have not explored in depth. This includes questions of what processing rules apply when making geospatial data available to third countries, how we deal with certain GDPR requirements when it comes to Risk Analysis (DPIA), privacy by default, and how to handle complaints and issues when other parties are aggregating our data.

What we have learned from our discussions, is also that the handling of these challenges requires input not just from the legal personnel, but also from IT personnel and other experts on our activities.

The GDPR Working Group suggests that its members will continue update each other on relevant matters, with inclusion of other experts from the organizations when required.

This could be done by setting up a resource group whose mandate will be to hold either in-person or virtual meetings once or twice a year.

The Resource Group could also propose initiatives for more in-depth discussions on a Nordic or European basis.