Nordic GDPR working group Report

Preliminary findings and suggested work

1 Executive summary

The Director Generals agreed at "Lille Chef meeting" in Copenhagen on 3 April 2019, that a group of GDPR Experts will carry out work according to a mandate described in chapter 2.1. The GDPR experts (hereafter called the GDPR Working Group) has explored and discussed the legal and practical issues of the scenario described in the mandate pursuant to GDPR.

The discussion focused on the following datasets:

- Addresses
- Building information
- Cadastral data
- Land registry data
- Satellite images
- Images from oblique angles
- Aerial images

We have discussed in length the definition of personal data, the concept of pseudonymisation and how this pertains to the geospatial data. There are still further sources to explore before this discussion can be brought to a satisfactory conclusion (chapter 2.3).

In chapter 4 to 9 of the report, we has collated information from all countries about the following issues:

- Who are the recipients of the data?
- What and how are we transferring to third country?
- Have we carried out any risk analysis or DPIA (Data Protection Impact Assessment) for the distributing we are doing?
- What other technical and administrative measures are we applying?
- To what extent do we consider aggregation by others, i.e. that the recipients combine our data with other data in a lawful or unlawful manner, and lastly
- What are the legal grounds for each of us for dissemination personal geospatial data?

There is still scope for comparing and discussing this information, as it was only completed in early August.

In Chapter 10, we relate the findings so far. We find that GDPR creates a number of legal and practical questions for dissemination of geospatial data, and that knowledge sharing and discussion greatly assist us in seeking solutions. Handling 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 thinks there are two alternatives for further work, see Chapter 11:

1. Continue to discuss on a fairly high level with a relatively low use of resources; or
2. Identify and focus on more detailed work requiring more resources.

We do not feel that we have had sufficient time to discuss these matters, to be able to conclude with one or the other alternative.

The GDPR Working Group would therefore like to propose to the "Store Chef meeting" that we continue until we fell ready to clearly recommend and describe one of the alternatives.

Contents

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 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 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 GDPR and produced this report. The work has been carried out by Skype meetings.

Each GDPR expert has described their organization's processing of geospatial data in the exercise of official authority by filling out a questionnaire. If the organization has a made a record according to Article 30 for this process, the record is the basis of the answers to the questionnaire. The GDPR Working Group has discussed the common issues, Chapter 2, and agreed on exploring certain types of data and legal issues, Chapter 3.

The GDPR Working Group has made some preliminary conclusions and proposed further work, see chapter 10 and 11.

This final report shall be presented at "Store Chef Meeting" in September 2019.

2.3 Legal framework

2.3.1 What is personal data?

According to the GDPR definition, 'personal data' means *any information relating to an identified* or *identifiable natural person* ('data subject').

An identifiable natural person 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 of the GDPR; 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 processing and technological developments.

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]

The approach is understandable in view of the rapid developments in society. It is important that possible future incarnations of personal data are not inadvertently excluded as it could be with a prescriptive rule. As the lawmakers have stated, there will in future be a constant need for putting boundaries on society's exploding generation and aggregation of data, as well as advances in data analytics.

In order for the approach to be practical, it needs to be limited by an interpretation which takes into consideration the concerns and goals of the personal data regulations.

There is a general agreement that there is a "threshold", beneath which the risks of processing data are so insignificant that processing rules under the GDPR can be fully or partly omitted. This was also the case with the earlier directive that applied the same broad definition of personal data.

Indeed such a threshold is necessary for the broad definition to work in practice. This is also supported by an opinion of the Article 29 Data Protection Working Party[2] on the "concept of personal data". In Opinion 4/2007 it states on page 25:

"As a general consideration it has been noted that the European lawmaker intended to adopt a broad notion of personal data, but this notion is not unlimited. It should always be kept in mind that the objective of the rules contained in the Directive is to protect the fundamental rights and freedoms of individuals, in particular their right to privacy, with regard to the processing of personal data. 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 Directive 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."

[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.

This threshold can be reached by implementing technical and administrative measures, such as pseudonymisation, which creates a dataset that do not need further processing rules to be applied, or decryption, see Article 25. It can also be set in law, for example under Article 86, and then it is a matter of interpreting the law for the various settings as use of data is constantly changing. It is fair to say that the existence of this threshold creates a particular problem for the public sector, which does not apply to the private sector.[3]

Where that threshold is will depend on the dataset and the circumstances around its dissemination. This is an issue that we need to dig into, more than we have had time for so far.

2.3.2 Personal data concept as applied to geodata

To begin with, the GDPR Working Group needed to examine differences and similarities in their interpretation of 'personal data' when handling geospatial data in the exercise of official authority. Furthermore, the GDPR Working Group has examined which types of personal geospatial data that are wholly or partly exempted from the GDPR processing rules under national law.

These discussions have led to the conclusion that the following types of data are both relevant to the scenario and will include personal data.

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
Land registry data	People who are registered in the land registry as (right) owners
Satellite images	People who live in buildings shown on the image or owners thereof
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

Addresses or buildings with coordinates are available as stand-alone datasets in all Nordic countries, without the information about who lives there. These stand-alone datasets are by all members of the GDPR Working Group considered to be exempted from the processing rules in the regulation, as they are pseudonymised data, sometimes called indirect personal data.

According to Article 4(5) of the GDPR 'pseudonymisation' means the processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person. In other words, pseudonymised data is data actively made not attributable to a specific data subject.

When data is pseudonymised in this way, it is easier to mitigate any related risks to the data subjects concerned and meet the GDPR obligations. Addresses and buildings in a database that also provides the context of the persons living there, such as the cadastre and land registry, are more vulnerable from a personal data point of view and therefore generally more strictly treated.

[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.'

The GDPR Working Group has understood pseudonymisation as described above to be a privacy-by-default measure, and it does not change the status of the data as personal data, as stated in Recital 26 of the GDPR. It merely exempts the particular dataset from some or all of the processing rules in the Regulation. In other word, it falls below the threshold described above.

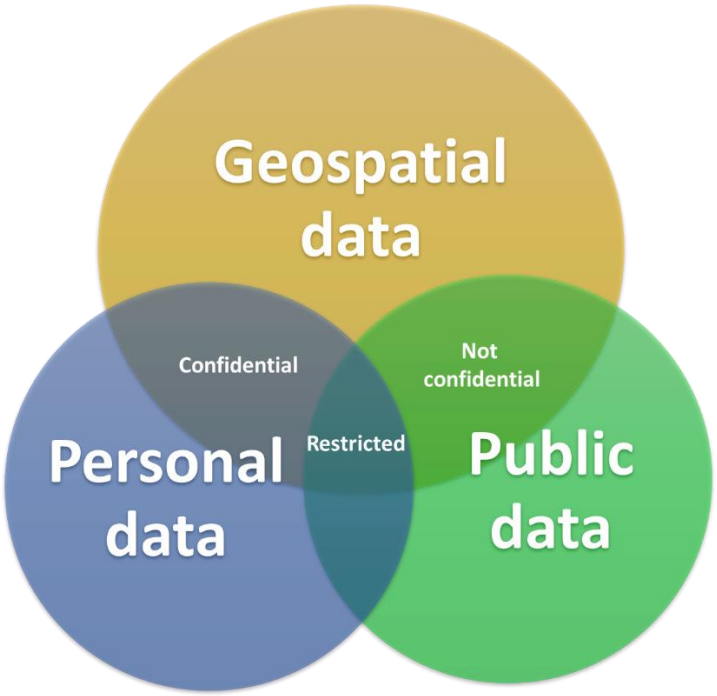
It would be useful to explore this matter further, as it could provide guidance for similar existing issues and future developments of our products and services. In July 2019 one of the Danish Mapping Agencies has received relevant guidance from the Danish Data Protection Agency (Datatilsynet) on the application of the GDPR in relations to specific geospatial datasets. Unfortunately, it is not possible to deduce if the distribution of basic geospatial data in general falls "outside the scope of the Regulation" as the guidance only covers some very specific cases. The GDPR Working Group has agreed on the need to ask for further clarification on what is meant by falling outside, as well as exploring under what other circumstances the dataset may not fall outside the Regulation, see the discussion on "threshold" above.

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.



3 Issues for consideration

Once you have categorised a dataset as personal data, you need to establish a record of processing activities according to GDPR Article 30. This needs to include, besides contact information and general information about your basis for the processing, a description of the following:

- Categories of data subjects;
- Categories of personal data;
- The categories of recipients;
- Where applicable, transfers of personal data to a third country or an international organisation,;
- Where possible, the envisaged time limits for erasure; and
- Where possible, a general description of the technical and organisational security measures.

Since this report focus on dissemination of geospatial data, the fact finding in the various countries as described in chapter 4 – 9 focus on the following issues:

- Who are the recipients of the data?
- What and how are we transferring to third country?
- Have we carried out any risk analysis or DPIA (Data Protection Impact Assessment) for the distributing we are doing?
- What other technical and administrative measures are we applying?
- To what extent do we consider aggregation by others, i.e. that the recipients combine our data with other data in a lawful or unlawful manner, and lastly
- What are the legal grounds for each of us for dissemination personal geospatial data?

4 The recipients of the data

By 'recipients' the legislator means a natural or legal person, public authority, agency or another body, to which the personal data are disclosed, whether a third party or not.

A third party is defined as the legal or natural person *other than the data subject, controller or processor* who, under the direct authority of the controller or processor, are authorised to process personal data.

Public sector should distinguish between processing of personal data within the public sector and dissemination of personal data outside the public sector. GDPR applies as such to processing within the public sector but article 86 of the GDPR enables national or EU legislation to make it possible for the public sector to disseminate personal data in order to reconcile public access to official documents and information with the right to the protection of personal data pursuant to the GDPR.

4.1 Denmark

4.1.1 Addresses

The Danish Address Register is the basic data register for addresses in Denmark. Every address is enriched with a geographical coordinate and has a unique key that makes the register easy to use across public and private IT systems. The Address Web Services enable such distribution between systems. Besides the professional use, anyone with access to internet can locate addresses by visiting http://danmarksadresser.dk/adresser-i-danmark/.

Whereas each municipality is obligated to keep the Danish Address Register according to the regulations laid down by the Minister for Climate, Energy and Utilities, the system as such is operated, maintained and developed by SDFE (the Danish Agency for Data Supply and Efficiency). In order to ensure the data quality SDFE is also obligated to supervise the municipalities and hear appeals against their decisions.

4.1.2 Other open geospatial data

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 citizen.

A large number of geospatial datasets are made publicly available under a free and open data license. 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.;
- Orthophotos (geometrically corrected aerial photography); and
- Cadastral information and parcels.

4.1.3 Information on buildings

GeoDanmark is a collaboration between SDFE and the municipalities that ensures the distribution of building information used for the public administration of buildings, roads and watercourses. GeoDanmarks' database contains authoritative data such as topographic maps with building polygons and links to other relevant geospatial data from the tax authorities' Central Register of Buildings and Dwellings (Bygnings- og Boligregistret).

On https://bbr.dk/forside every real estate owner can check the registered building information and via an authentication solution report changes and errors to the data. Even though everyone with access to the internet can look any building up on this page, the responsible authority for the register has inserted a disclaimer making it clear that only the real estate owner can disclose the information to others.

4.1.4 Oblige images

On https://skraafoto.kortforsyningen.dk anyone can freely access and download SDFE's aerial images from oblique angles.

4.1.5 Addresses in combination with data on real estate owners

In addition, the organization 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 Geodata Agency's Property Formation Register (Ejerfortegnelsen) to different categories of users. The majority of these users are found in the public and financial sector where specific groups of professionals are entitled to access the register unlimited in order to fulfill specific legal obligations.

4.2 Finland

4.2.1 General access to geospatial data

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.

According to Finnish legal literature 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 Finnish legal literature, it seems to this extent like the usefulness and necessity of the data and 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.[4]

4.2.2 Addresses and information on buildings

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.

4.3 Norway

4.3.1 Addresses

Addresses with coordinates are freely available for viewing and printing from our web services. The addresses database can also be downloaded from geonorge.no.

The addresses database is the official addresses for Norway, which is the complete address for a building, part of building, parcel or other object. Addresses inside a building (floor or apartment no.) is not included. The address is also connected to the property number and administrative units. It can be a road address or a cadastre address. There are still areas where road addresses do not exist.

4.3.2 Building information

See addresses and cadastral information.

4.3.3 Cadastral and land registry information

In the area of public versus private interests, there may be the need to weigh and explain balance and this may need input on a legal basis. There is an exemption rule in GDPR as well as older law on doing this balance, but public bodies need a specific law and processing grounds after GDPR.

[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, p. 40.

The addresses are distributed according to such an exemption in law. The same goes for all other types of physical information about the property, like the cadastral map.

Property information from the land registry and the cadastral registry that is not exempted as mentioned above, is restricted and published according to applicable laws.

The Land Registration Act and The Cadastral Register Act with associated regulations, regulate registration, processing and disclosure of information from the registers.

The personal data being processed is primarily name, address and personal ID number associated with the rights an individual has in property, or in connection with enterprises registered in the cadastral register. It is necessary to use the personal ID number in order to ensure the correct individual is registered. The personal ID number is processed according to Section 12 of the Personal Data Act.

Copies of the land registry registration for a property can be viewed online. It is not possible to do this anonymously, as we restrict it to people who have a Norwegian identity. This is done to avoid distribution to third countries. People who do not have this identity needs to order the copies.

These copies do not contain full personal ID number or any information about personal debts, such as mortgages. To access this information, you need a special access that is only given to certain groups according to the law (public bodies, lawyers, real estate agents, etc).

4.3.4 Aerial images

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.

4.4 Sweden

4.4.1 General access to geospatial data

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. As such addresses, building information and oblique images are all accessible by the public through a request filed with the agency that is responsible for storing the information. The right to access official documents includes the right to receive a copy of the documents in question. There is no fee for viewing the documents on site but for copies or print-outs a small amount is charged to cover the costs. Any member of the public is therefore a possible recipient of data.

Public access to official documents does not extend to digital information. Digital access is instead regulated in various laws that each govern specific registers. A lot of information is still sent to the public through e-mail and similar channels, but this is not an obligation. Rather we are able to choose that form of delivery in order to save time, resources and to meet expectations of availability from the public.

4.4.1 Addresses and building information

Digital access to personal data in the cadastral registry, which includes building information and addresses, is regulated in its own law, Fastighetsregisterlagen. The law sets up a list of legitimate purposes for which personal data in the registry can be distributed. It also designates Lantmäteriet as the data controller and establishes the right to charge users for the information. Personal data in the register is distributed if an applicants' intended processing corresponds with the uses for which the information may be released.

As we are not a supervisory authority, we do not investigate the actual use of data after access has been granted. What we consider in the application process is the legality of our distribution. However, our law on access to public information and secrecy (Offentlighet och sekretesslagen, kap. 21 § 7) states that personal data may not be distributed if there is reason to believe that the information will be processed in violation of the GDPR. Misuse of any kind is of course difficult to predict but depending on what we learn

about the prospective recipients plans, we can deny them access. At the same time, it should be noted that this legislation only rarely has hindered distribution of data.

Lantmäteriet has concluded that although addresses and building information contain personal data, they are harmless to distribute. The cadaster law, Fastighetsregisterlagen, does not distinguish between harmless and non-harmless personal data and so, regardless of such classification, dissemination is only allowed for legitimate purposes. One of these (§ 2 p. 1) concern the fulfilling of tasks that the state or a municipality is legally obligated to perform. Lantmäteriet has a general task to sufficiently provide society with certain geodata. The agency has concluded that this task corresponds with the legitimate purpose cited above and issued an internal decision to that effect. This lets us distribute addresses and building information openly.

4.4.1 Oblique images and aerial images

Lantmäteriet has a limited supply of oblique images, only covering the years 1976-2005. There are no current plans to update our existing stock. The pictures are not actively marketed or published. They are however available for purchase, but the requests are few and far between.

Historical orthophotos can be accessed as open data on our website www.lantmateriet.se. Other aerial images are available for purchase, in other words not open data but not limited by the procedures surrounding addresses or building information.

5 Legal grounds for disseminating personal geospatial data

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

5.2 Finland

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.[5]

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

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

detect (e.g. buildings visible in Google street view) and users cannot search the data directly using the names of persons[6].

5.3 Norway

The geospatial data that we distribute can be categorised like this:
1. Open, free of charge geospatial data;
2. Open, but not free of charge geospatial data; and
3. Restricted and not free of charge geospatial data.

The primary rule in the Public Administration Act is that case documents, records and similar registers for the authority are open for inspection unless otherwise covered by regulation.

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.

Registration, processing and disclosure of information from and about the cadastre and land registry is regulated by The Land Registration Act and The Cadastral Register Act with associated regulations.

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

5.4 Sweden

As outlined in section 4.4 there are two main paths that establishes legal grounds for disseminating geospatial geodata. In chapter two of the Freedom of the Press Act any member of the public is given the right view in-formation in official documents. With few exceptions, this also includes the right to a copy or printout of the document in question. After a request for information is processed, delivery is usually made through e-mail or similar technical solutions, even though the right of the public mostly extends to information on paper. What information can be accessed this way is limited by the law on public access to information and secrecy. However, personal geospatial data is generally not considered secret and is regularly sent out on these grounds.

Aside from the general right to view official documents Sweden has several laws governing content and access to different registers. As such, we have a law about the vehicle-registry, another about cadaster and land ownership, and so on. Most of our geodata dissemination has its legal grounds in these more specified acts. Lantmäteriet also has its own tasks, issued by the government, to ensure that society has the access it needs to certain geo-data. As legal grounds for dissemination, this generally applies to information that is not part of our registers, such as aerial images.

6 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 public 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 to consultation, either by the public in general or by any person who can demonstrate a legitimate interest. Sometimes the lawmaker has set up certain requirements for consultation of these data, thus letting the distribution depend on the specific matter.

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

In the Lindqvist preliminary ruling The Swedish Court of Appeal needed to know if an individual was breaking the rules on cross-border transfers of personal data outside the EU/EEA by posting information on the Internet about her co-workers. The European Court of Appeal answer to this was no. In the specific case, the posting was not construed as "transferring" personal data to a third country. The European Court supported the arguments made by Lindqvist, concluding that web site operators posting personal data online are not subject to the legal regime governing the transfer of personal data unless (i) they actually send the personal information to internet users who did not intentionally seek access to the web pages, or (ii) the server infrastructure is located outside the EU.

One could questioning if this ruling also applies to public authorities' transfers of open data to some extent. However, the Court's decision primarily relied on the fact that no person in a third country actually accessed any personal data made available on Mrs Lindqvist's site. When a public data distribution platform is intended for a broader use and by design actually facilitates third country visitor's access the reasoning in the ruling makes little sense.

6.1 Denmark

By reference to the derogation in article 49(1)(g), SDFE's distribution of open geospatial data complies with chapter V in the GDPR.

The hosting of other kinds of geospatial (confidential) data takes place inside the EU.

6.2 Finland

The topographic data is open data and can therefore be transferred to and used in third countries.

Data in the Finnish Land Information System is not transferred to any third countries. For instance access of natural persons is possible only if you are registered in the Finnish Population Information System and have bank codes or similar that enable strong electronic identification.

6.3 Norway

By reference to the derogation in article 49(1)(g), Kartverkets distribution of open geospatial data comply with chapter V in the GDPR. This applies also to address and building data in pseudonimised form.

The land registry and cadastre data is only accessible if you have a Norwegian digital ID, or order it through our online system. Access is given in accordance with the laws and regulations for access to land registry and cadastre data.

All are hosted in Norway, except for orthophoto, which is handled by Geodata AS and hosted on Amazon.

6.4 Sweden

Lantmäteriet does not consider publishing of open data a transfer to third countries, in accordance with the Lindqvist ruling cited above. When distributing data according to the process stipulated in Fastighetsregisterlagen, as described under 4.4.1, the applicant must answer questions about the intended storage of information so that we can make an informed decision with regards to this issue.

When considering the articles on third country transfers, particularly art. 49.1 g, the room for interpretation has resulted in a degree of uncertainty regarding the intent of the EU-legislature and consequent applicability of the article on some registers housed by Swedish authorities. This is likely to persist until such a time that the courts have ruled on the matter.

7 Risk analysis (DPIA)

7.1 Denmark

The distribution of basic geospatial data through 'Datafordeleren' has activated the obligation under the GDPR article 35 to ensure a DPIA. The reason for this is the distribution of Personal Identification numbers of all Danish citizens and all the administrative Personal Identification Numbers for non-citizens that primarily can use is for identification purposes in their communication with the tax authorities.

With reference to a newly published guide from the Danish Data Protection Agency every other processing of personal data (e.g. the distribution of buildings, addresses and aerial imagery) will be assessed by using the method from ENISA.

7.2 Finland

The topographic data is open data. No DPIA according to GDPR has yet been executed. Although another risk analysis has been done.

The National Land Survey of Finland is working to create a Geospatial Platform. The Geospatial Platform harmonises the spatial data of the state, regions and municipalities and makes them available for companies and communities. The goal of this project is to create a shared spatial data platform for the public administration, which will offer common specifications and services for public administration data producers, shared and coherent data sets for all data users, and common user services. Risk analysis will be implemented following among other things GDPR article 35.

7.3 Norway

When we made the Art. 30 records, everyone was obliged to enter if they had done risk analysis now or before. We are currently working through the records to see if something needs to be followed up.

7.4 Sweden

For the time being Lantmäteriet conducts these assessments on a case-by-case basis when need arises. A similar function was however put into place at an earlier stage in order to ensure that information processed by Lantmäteriet is paired with an appropriate level of security. The procedure (called "Informationsklassificering") reviews and categorizes information mainly from a data security standpoint but also includes listing and consid-ering what personal data is present and how it is to be processed. Though not equal to an impact assessment according to art. 35 there is a certain overlap between the two. Lantmäteriet is therefore considering expanding the existing procedure to include what is needed for it to also serve the purpose of impact assessment.

8 Measures

GDPR has a general requirement to have what is called "data protection by design and by default". This means that safeguards and other measures needs to be "built in" to the administrative and technical systems.

Art. 25 no. 2: *The controller shall implement appropriate technical and organisational measures for ensuring that, by default, only personal data which are necessary for each specific purpose of the processing are processed. That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage and their accessibility. In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.*

A lot of these measures will already be in place as ordinary security precautions that any public organisation will have to safeguard the integrity of their data. The challenge is to see how far GDPR makes additional requirements and how to meet this. A DPIA is meant as a tool to find out this.

As stated in art. 25 no. 3: *An approved certification mechanism pursuant to Article 42 may be used as an element to demonstrate compliance with the requirements…*

8.1 Denmark

SDFE has implemented every control under the ISO 27001 standard providing requirements for an information security management system (ISMS). The controls apply to nearly every processing of geospatial data that falls under the SDFE's responsibilities in the role of data controller and data processor.

8.2 Finland

The National Land Survey of Finland complies with GDPR and other legislation on the processing of personal data. As a controller National Land Survey of Finland has implemented many technical and organisational measures for ensuring compliance with the relevant regulations, such as but not limited to, accessibility and validity of the data.

8.3 Norway

Kartverket have implemented a number of measures to ensure the integrity and safety of our databases and services. These are also meant to safeguard personal data.

8.4 Sweden

Lantmäteriet has undertaken multiple measures to ensure that we live up to the standards set out in the GDPR. Considering the fast-paced nature of the field, we would also like to note that continuous commitment would be needed to ensure adequate levels of privacy and security.

9 Aggregation of data by others

9.1 Denmark

SDFE collect, store and distribute different geospatial data, but will seldom aggregate geospatial data that will lead to direct identification of a natural person. The basic geospatial datasets are used in many ways outside the organization. Other central governmental organs and municipalities collect for instance address data and building information in order to make decisions influencing the data subjects on legal matters. The assessment of property tax is one good example of how the economy of a specific group of data subjects is influenced by the aggregation of SDFE's basic geospatial data.

SDFE uses a disclaimer when the collection of the personal geospatial data takes place in order to ensure transparency of the consequences of aggregation. The users are informed that the aggregation of data might lead to identification of natural persons, and in that case, they are obliged to comply with the GDPR, unless one of the exemptions under article 2(2) applies.

9.2 Finland

The topographic data is considered open data and the further use of it by others is not considered a problem. Each recipient is obliged to comply with the GDPR (if as such applicable) and any relevant national legislation on the processing of personal data.

9.3 Norway

Kartverket have applied the point of view that where laws and regulations require us to distribute personal data, we can do that without considering the further use of it by others. They are responsible for their processing and possible aggregation. This is a general principle of the law that we do not think is changed with GDPR.

9.4 Sweden

In past projects Lantmäteriet has identified the aggregation of data to pose a potential security risk, albeit difficult to assess. Similarly, it poses a potential risk to data subject integrity. But to consider all information and processing possibilities available to a bad-faith actor remains a futile undertaking, and as such we haven't found a practical way of completely avoiding the risks involved when distributing personal data. Instead, we trust in the responsibilities of data controllers to adhere to the GDPR in their respective processing. However, in the face of increasing digitalization of government data and services, an awareness of these issues is to be recommended.

10 What have we learned so far?

GDPR does not hinder the distribution of open geospatial data if 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 broad definition of personal data forces the Nordic Mapping and Cadastral Agencies to take GDPR into account when distributing a number of different types of geospatial data. GDPR is leaving it up to the public organization to translate this legal standard into prescriptive rules applicable to the organizations' exercise of official authority.

This poses a major challenge for the GDPR experts in the organization. It can be hard, not to say impossible, to make a bulletproof statement when met with questions like "Are we obliged to delete oblique images when a police car is waiting outside a data subject's home?" "What level of security is appropriate knowing that the data is open?" The rights for the data subjects sometimes make little sense when the organization's legal basis is its task carried out as public authority in comparison with data controllers whose interests is related to their business and whose purposes can be delimited on their own advice.

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 the statutory task in order to ensure transparency and compliance for the public authority's processing of personal geospatial data. For now, some Nordic countries might need to make this basis clearer next time a review on the law shall take place.

In addition, the comparable processing of geospatial data will probably lead to the identification of the same consequence 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 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 same type of data in the same manner they will benefit from sharing knowledge on how the GDPR has been interpreted more specifically. An important conclusion is also that handling these challenges requires input not just from the legal personnel, but also from IT personnel and other experts on our activities.

11 Conclusions and the way forward

Implementing GDPR has been a major challenge for both public and private sector in Europe. However, it has clearly showed that public sector has some particular challenges, and the work of the GDPR Working Group has shown that public sector bodies dealing with geospatial data have some particular challenges of their own.

The Working Group will suggest that we continue to explore the issues we have highlighted in this report:

1. The definition of personal data; in which situations do and do not the GDPR apply to the handling of specific kinds of geospatial data?
2. If the geospatial data is personal, under what circumstances can some or all of the processing rules in the Regulation be omitted?
3. In particular, what processing rules applies for making geospatial data available to third countries, in particular when it is done in open on-line solutions? The use of cloud solutions is a part of this.
4. It can also be useful to look at 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 others are aggregating our data.

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.

A uniform and predictable interpretation of how geospatial data turns into personal data shall be the long-term goal in this work (as it should be also in the whole EU). The GDPR Working Group has concluded that if we want to achieve a clearer legal situation, working together in formulating inputs to the national Data Protection Agencies (DPAs) and the European Data Protection Board will be beneficial.

The work has therefore clearly demonstrated that there is an overlying legislative aspect of our common work, as well as a more practical aspect of comparing actual methods and experiences.

The GDPR Working Group think there are two alternatives here:

1. Continue to discuss on a fairly high level with a relatively low use of resources, and see if a more detailed work will be needed in the future; or
2. Identify and focus on more detailed work requiring more resources, e.g. more work for the involved legal professionals, as well as the participation of IT professionals from each organization.

The GDPR Working Group do not feel that we have had sufficient time to discuss these matters, to be able to conclude with one or the other alternative. In many ways, we are still in the middle of the discussions. The statements received from the Danish DPA also indicates a line of inquires towards our other national DPAs which may be crucial in the search of common grounds and recommendations. There is still scope for comparing and discussing the information in chapter 4-9, as it was only completed in early August.

A conclusion on no. 2 will also involve describing this work more detailed to enable a decision from the Directors.

The GDPR Working Group would therefore like to propose to the “Store Chef meeting” that we continue until we fell ready to clearly recommend and describe one of the alternatives. We would also propose that the work is concluded with a physical meeting.