WGIC POLICY REPORT: 2020-01

Geospatial Information and Privacy: Policy Perspectives and Imperatives for the Geospatial Industry

ARNOUT DESMET

MESSAGE FROM CHAIR

Over the last few years, we have experienced a growing awareness and sensitivity in society related to data privacy and personal data protection. There are different perspectives amongst geographies and user groups but the trend is clear. As a result, policy-makers are putting data privacy higher on the agenda and are taking various legislative initiatives across the globe. At the same time, location-based technology, applications and services in the public and private domain are increasingly diverse, accurate and pervasive. The amount of data collected by today's smartphones packed with GNSS chips, gyro, barometric-pressure sensors, accelerometers, high-resolution cameras, etc., is exploding and almost always location-referenced. Evolutions in the Earth Observation and Terrestrial LiDAR industry accelerate the prevalence, resolution and capturing frequency of satellite, aerial and terrestrial imagery data. And the automotive, telematics and logistics industry drives the deployment of a multitude of sophisticated sensors in commercial and private vehicles. This location-based data explosion in turn triggered the emergence of a wide variety of business models based on digital profiling, location-based advertising and monetization of user data in various shapes and forms.

The Policy Committee was established by the WGIC Executive Board to discuss various policy issues impacting the geospatial industry and to engage with multiple stakeholders in private and public sectors around these themes. As an industry, dealing with location-based data in various aspects, we prioritized Geospatial Information and Privacy as the focus for the Policy Committee in 2019. We also established a Special Interest Group (SIG) to help the Policy Committee with the assessment of current and upcoming regulations and policies in different territories and markets and the impact on the geospatial industry. The SIG analysis serves as the basis for this paper, representing a high-level analysis of current legislation and policies in key markets across the world and its impact on the geospatial industry. This paper also provides recommendations to the WGIC membership and the geospatial industry at large on how to proactively address the privacy concerns in society in full compliance with data protection legislation in our day-to-day business.

With the publication of this paper, the Policy Committee hopes to inform the WGIC members and the geospatial industry on the policy perspectives and related obligations related to geospatial information and privacy. We also want to stimulate a broader and well-informed debate with all stakeholders in the public and private sectors and we welcome all feedback and suggestions for further research and collaboration around this theme.

I would like to thank in particular all SIG contributors, the Considerati consultants, the WGIC secretariat and my fellow members of the Policy Committee for their invaluable support in realizing this policy paper.

Enjoy the reading.

Arnout Desmet
Chair WGIC Policy Committee

BARBARA RYAN

MESSAGE FROM POLICY ADVISOR

Having spent most of my professional career in the public sector, I have been pleasantly surprised, in fact, really impressed with how seriously the Members of the World Geospatial Industry Council (WGIC) have advanced the study of personal privacy protection. The Council is comprised of companies representing the entire ecosystem of the geospatial industry, and in that regard understands the importance of the protection of personal privacy information. This report, undertaken by the WGIC Policy Committee, presents an overview of the personal privacy legislative environments in selected countries around the world, and to the best of my knowledge, is the first of its kind.

As indicated by the Chair of the WGIC Policy Committee, we established a Strategic Implementation Team (SIG) who were able to report on existing, and in some instances, planned privacy regulations and legislation in twelve countries. While this was unique, in and of itself, we needed to expand these geographies to include other major markets (e.g. China and the Russian Federation) where WGIC Members conduct business. We then turned to Considerati (https://www.considerati.com) a legal and public affairs consultancy for the digital world located in the Netherlands. Not only did they review and validate the work of our SIG volunteers, they expanded our global view, described the logic of data protection legislation, including definitions of geospatial data, personal data, and their interaction, articulated impacts on the industry, and provided a flow chart that helps all users (controllers and processors) better understand this complicated subject.

Clearly the value of this report will be determined by its use and uptake. I am optimistic that those in both the private and public sectors will find it to be one of the most easily read publications, potentially a primer, on the important and relevant topic of personal privacy protection in the geospatial arena.

Barbara J. Ryan
WGIC Policy Advisor

Contents

1 Introduction

Data protection and privacy laws around the world are evolving as lawmakers and regulators are moving away from protecting a selected set of personally identifiable information towards regulating the collection, use, and dissemination of information that could directly or indirectly identify an individual. At the same time, due to the power of location, technologies that collect, analyze, visualize, store, and distribute geolocation and other types of geospatial information are being used more often in government, industry, academia and by citizens. These two trends are converging, as the privacy community is recognizing the power of location information – often aggregated with other types of information - to either identify a specific individual or make critical decisions based upon his or her movements, activities, associations, and relationships. Due to the inherent versatility of geospatial information which allows one data set to be used for a variety of applications, it is difficult to develop laws and regulations that protect the privacy, and the misuse of data while still allowing the collection and use of geospatial information for a wide range of important applications. The challenge will become even greater as the quality of the data (accuracy, precision, timeliness, etc.) increases, and the scope of data (radar, infrared, hyperspectral, etc.) grows.

The World Geospatial Industry Council (WGIC) (https://wgicouncil.org) is a global association of companies representing the geospatial ecosystem. Among its objectives are to represent business interests, share perspectives of the geospatial industry, and undertake policy advocacy and dialogue with public authorities, multilateral agencies, and other relevant bodies. In that regard, the WGIC has recently undertaken an effort to look more closely at data privacy, as it relates to location.

This document will focus mainly on the following two questions:

1 How does data protection and privacy legislation relate to the geospatial information sector?

2 What are the requirements under data protection and privacy legislation throughout the world, and how do they impact the members of the WGIC and the geospatial industry at large?

1.1 Scope and methodology

To help WGIC understand the implications and/or impact of privacy and data protection laws in relevant markets and geographies, a Special Interest Group (SIG) comprised of subject matter experts from around the world was convened. These experts described their respective legislative and regulatory environment, and to the extent possible, the impacts of these environments on the geospatial community. Furthermore, desk research was conducted to assess privacy and data protection legislation in selected jurisdictions.

As a baseline for comparison, the requirements from the European Union General Data Protection Regulation (GDPR) were used. The GDPR was chosen as a baseline for the comparison, as the WGIC regards the GDPR as the most comprehensive and demanding privacy and data protection framework in the world. For the selected jurisdictions the main privacy and data protection laws were assessed using the GDPR requirements. On the basis of this, a level of alignment with GDPR was established.

It is important to note that only a high-level scan could be performed for each jurisdiction, focusing on the main privacy and data protection laws. As such, country-specific requirements for geospatial information privacy outside of these privacy / data protection laws, may not have been fully covered in this quick scan.

For a full overview of the laws that were assessed please consult the following document: Data Protection Obligations - High-level Overview. (https://docs.zoho.com/file/060gd2a12b0d0d69744909c0030eee69a7e45)

2. Privacy, data protection and geospatial information

2.1 The right to privacy and data protection

The right to privacy is generally recognized throughout the world. At a global level, the right to privacy is enshrined in the Universal Declaration of Human Rights (UDHR) and the International Covenant on Civil Rights and Political Rights (ICCPR). The UDHR states that:

> "No one shall be subjected to arbitrary interference with his privacy, family, home or correspondence, nor to attacks upon his honour and reputation. Everyone has the right to protection of the law against such interference or attacks."

The right to privacy also extends to personal information. This form of privacy protection is generally called informational privacy or data protection.

2.2 Data protection legislation

Data protection legislation has two main goals: the first goal is to protect the rights and freedoms of individuals, the second goal is to provide clear rules on the use of personal data in order to facilitate its use.

Data protection legislation has its origins in the early seventies of the twentieth century. In 1970 the first data protection law was drafted in the German state of Hessen.[1] Ever since, Europe has been a frontrunner in data protection legislation, culminating in 2018 with the General Data Protection Regulation (GDPR). The GDPR is considered by many as the most robust and mature data protection legislation in the world, and more and more countries are adopting rules and regulations that are similar to the GDPR. Therefore, we take the GDPR as our main point of reference when discussing the impact of data protection legislation for the geospatial industry.

Next to the GDPR there are other important treaties and regulations in the area of data protection, such as the Council of Europe Convention for the Protection of Individuals with regard to Automatic Processing of Personal Data (Convention 108), the Organization for Economic Cooperation and Development (OECD) Guidelines on the Protection of Privacy and Transborder Flows of Personal Data, the APEC privacy framework, and standards such as the International Organization for Standardization/International Electrotechnical Commission (ISO/IEC) 29100. While different from the GDPR, these instruments share the logic of the GDPR and have similar rules and requirements.

The following principles are the most important elements of data protection:

1. Personal data processing must be legitimate, fair and transparent (lawfulness, fairness and transparency);
2. Personal data may only be processed for specified purposes (purpose limitation);
3. Only those data that are necessary for the purpose should be processed (data minimisation);

[1] Hesschisches Datenschutzgesetz, 7 October 1970 (GVBl. I S. 625)

4. Personal data must be accurate (accuracy);
5. Personal data must be kept no longer than necessary (data retention and storage limitation);
6. Personal data must be kept secure (integrity, confidentiality and availability); and
7. Where personal data are processed, it must be demonstrated that such processing is in line with the principles above (accountability).

2.3 Geospatial data and personal data

For providers of geospatial information it is important to determine when data protection legislation applies to them. To answer this question we first need to determine whether geospatial data qualifies as personal data.

2.3.1 Geospatial data

Geospatial data refers to data about "objects, events, or phenomena that have a location on the surface of the earth. The location may be static in the short-term (e.g., the location of a road, an earthquake event, children living in poverty), or dynamic (e.g., a moving vehicle or pedestrian, the spread of an infectious disease). Geospatial data combines location information (usually coordinates on the earth), attribute information (the characteristics of the object, event, or phenomena concerned), and often also temporal information (the time or life span at which the location and attributes exist).[2]

2.3.2 Personal data

Personal data is defined in the GDPR as:

> "any information relating to an identified or identifiable natural person (the data subject).[3]

A natural person can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person. Recital 26 of the GDPR states that:

> "to determine whether a natural person is identifiable, account should be taken of all the means reasonably likely to be used, such as singling out, either by the controller or by another person to identify the natural person directly or indirectly."

A theoretical possibility that information can be linked to an individual is therefore not enough, it must be reasonably likely that this can be done in practice. So, in practical terms, when you are able to single out an

2 Kristin Stock and Hans Guesgen, 'Geospatial Reasoning with Open Data', Automating Open Source Intelligence, 2016, p.1.
3 Other jurisdictions may use different definitions such as 'personal identifiable information (PII)'. We shall use the definitions from the GDPR in this report.

individual based on available data, the data should be considered personal data. It is not always necessary to know a persons' name, when you are able to uniquely distinguish them from others, then data protection legislation will generally apply.

2.3.3 Understanding geospatial data as personal data

Geospatial data or geographic information systems do not always relate back to, or provide the possibility to identify, individuals. Therefore, geospatial information will generally not fall within the scope of privacy and data protection legislation. If the information attributed to the geospatial information is about individuals however, or it allows individuals to be identified, the geospatial information automatically becomes personal data, and data protection legislation applies. The GDPR also specifically mentions 'location data' as a possible identifier through which an individual can be identified.

So, whether geospatial data should be considered personal data is very much dependent on the circumstances of the case. A geographical map of a country for instance would not qualify as personal data in and of itself. However, when the map is used in conjunction with GPS data to show the real-time movement of individuals, the geospatial information should be considered personal data. This means that the concrete use case for geospatial information is of critical importance in determining whether or not data protection legislation applies, and if so, what rules apply.

2.4 Conclusion

Privacy and data protection laws have been enacted throughout the world. Although data protection legislation is generally enacted on a country to country basis, the overarching logic and contents are comparable, in part because of international instruments such as the Council of Europe Convention 108 and the OECD Guidelines. The European Union General Data Protection Regulation (GDPR) is generally regarded as the most robust and mature data protection framework in the world.

Data protection legislation is only relevant for the geospatial industry if data regarding individuals is being processed (i.e., personal data). If an organisation processes geospatial data that cannot be attributed to an individual, then that data will generally not qualify as personal data. Processing these data will, therefore, not be subject to privacy and data protection legislation.

When geospatial information is linked to an individual and/or can be used to identify an individual, privacy and data protection legislation applies. So, whether geospatial information must be considered personal data is very much dependent on the information that is attributed to the geospatial information. If these data are about, or can be linked to an individual, then data protection legislation applies.

3. The logic of data protection legislation

3.1 To whom does data protection legislation apply?

Data protection legislation applies to the natural or legal person taking the initiative to process personal data: the data controller. The data controller determines the purposes for the processing and the means to do so. Data controllers are responsible for ensuring that they comply with all obligations set out under data protection and privacy legislation.

The controller may enlist a third party to process data on their behalf. This third party is called the data processor. Data processors only process personal data under the instructions of the data controller, they are not allowed to use the personal data for their own purposes; if they do, they become data controllers. The GDPR sets requirements for data processors, for instance regarding data security. Furthermore they are bound by a data processing agreement.

So, in order to determine the impact of privacy and data protection legislation on the geospatial industry, we first need to establish which of these roles the provider of geospatial information takes on.

Here there are multiple possibilities, depending on the business model of the geospatial information provider:

- A first option is that a third-party requests geospatial information (e.g. coordinates) form a geospatial information provider. When the geospatial information provider provides these 'raw data' to a third party and that third party adds information which renders the geospatial information personal data, or uses it for a purpose which allows for the identification of an individual, then that third party should be considered the data controller for that purpose. An example of this could be an earth-observation satellite provider licensing high-resolution imagery to a cadastral taxation agency.
- A second option is that the geospatial information provider itself creates geospatial information that is considered personal data. These data may be subsequently be used by the provider for its own services, or sold to others. In both case the provider should be considered the data controller. An example of this could be a manufacturer of connected turn-by-turn navigation equipment, collecting GNSS trace data of its users.
- A third option is that the geospatial information company is hired by an organisation to perform services (e.g. build a GIS, generate specific geospatial information at the request of the organisation) which entails the processing of personal data. In this case the geospatial information company will generally be the data processor. An example of this could be a geospatial services provider generating household analytics for government agencies by combining object extraction from Earth Observation data with cadastral data.
- A fourth option is that a geospatial information provider works closely with a third party to create an application or service through which personal data is processed. In that scenario the provider and the third party may be joint controllers, sharing responsibility from a data protection perspective. An example of this could be a joint R&D project where parties mutually decide on the goals of the project, the personal data to be processed and they in which the data is processed.
- A final option is that the provider of geospatial information is merely a supplier of non-personal data. This would generally mean that the provider does not fall within the scope of privacy legislation (such as the GDPR) and therefore does not have any legal obligations stemming therefrom when processing non-personal data. An example of this could be a geospatial information provider which processes earth-observation data but does not have the ability to reference this data to another dataset through which individuals may be identified or become identifiable.

The important question any geospatial information provider should ask themselves is:

"Who determines the purpose for which (my) geospatial information is used: is that me, a third party or both of us?"

This translates to the following flowchart[4]

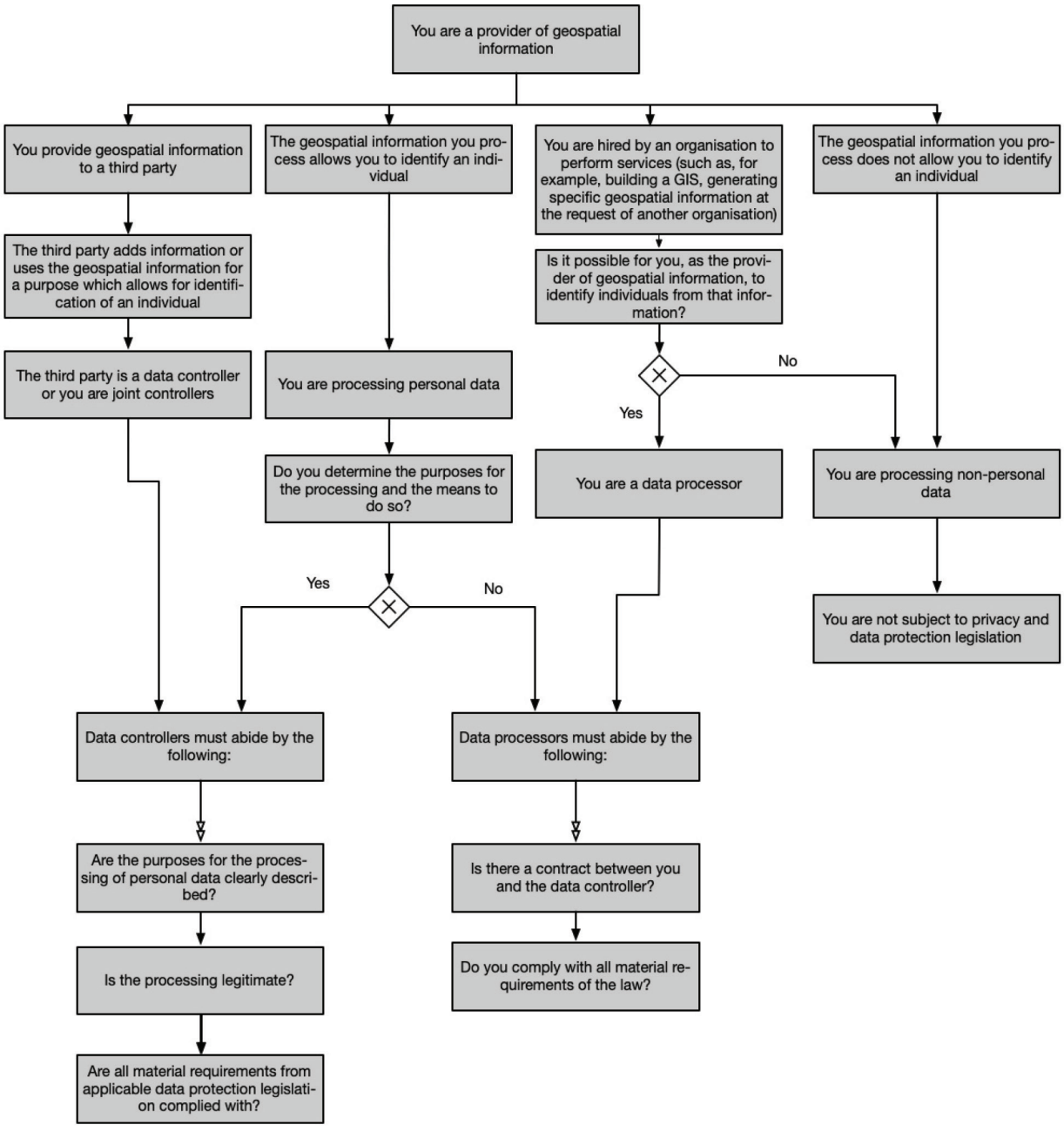

Figure 1: Flowchart for determining controller / processor relations

[4] Note that a geospatial information provider may offer multiple services. As such, the provider may be considered a data controller for one service, but a data processor for a different service.

3.2 When is processing of personal data allowed?

In those cases where the geospatial information provider is a (joint) data controller, the provider needs to determine whether his or her processing activity is legitimate under data protection legislation. In order to determine whether processing is legitimate, data protection legislation generally uses the following logic:

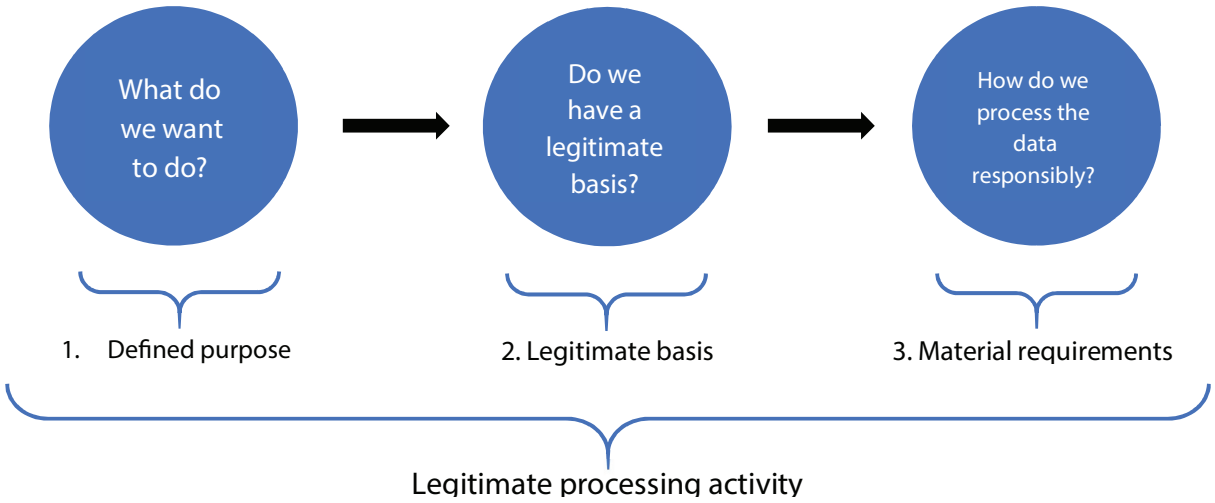

Figure 2: The logic of data protection legislation

3.2.1 Defined purpose

The first step to processing personal data is to establish a clear goal for processing the data. Personal data may only be collected for specified, explicit and legitimate purposes (purpose specification) and not further processed in a manner that is incompatible with those purposes (purpose limitation). Therefore, the first step is to determine why personal data are actually collected and further processed.

3.2.2 Legitimate basis

The second step is to determine whether the purpose defined in Step 1 is legitimate. The GDPR sets out six legal grounds which provide a legal basis for any processing of personal data. The legitimate grounds for processing are:

1. Where consent is given by the individual for the processing;
2. Where the processing is necessary for the performance of a contract to which the individual is a party;
3. Where the processing is necessary for compliance with a legal obligation;
4. Where the processing is necessary in order to protect the vital interests of an individual;
5. Where the processing is necessary for the performance of a task carried out in the public interest; and
6. Where the processing is necessary for the purpose of a legitimate interest, except where those interests are overridden by the interests or fundamental rights of the data subject.

In addition to the above, which applies to the processing of personal data in general, the GDPR sets out different rules for the processing of 'special categories of personal data'. This applies to the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a person's sex life or sexual orientation. When processing location data, it is often possible to denote special categories of personal

data when following the movements of a certain individual. Organizations need to consider risks to privacy when processing such data. Think for example of location data which provides insight into the movements of a certain individual indicating that that individual often visits a certain church or other location which may reveal religious beliefs. The processing of this kind of personal data is prohibited unless any of the exemptions under article 9(2) GDPR apply.

3.3 Material requirements

Once it has been established that the processing is for a legitimate purpose, the processing is allowed. But only on the condition that processing is done in a responsible manner. To ensure responsible processing, data protection legislation generally sets out specific compliance and accountability requirements. Under GDPR the most relevant requirements are: informing the data subject of the said processing, setting up a register of data processing activities, fulfilling data subject rights, managing processor relations, conduct Data Protection Impact Assessments (DPIAs) where appropriate, provide adequate security, notify the authorities and subjects of data breach notifications and ensure privacy by design and by default

4. Privacy and data protection requirements per jurisdiction

4.1 WGIC survey and research

In the previous chapter we have outlined the logic of data protection legislation and briefly discussed the overall requirements, using the GDPR as a baseline. But while the overall logic of data protection is fairly similar throughout the world, there are of course differences in the actual national laws, which may have a significant impact on the geospatial information providers depending on which country they are active in.

In this chapter we explore data protection legislation from various parts of the world in order to give a more detailed assessment of how personal data processing is governed throughout the world. To this end, desk research was done for all listed countries. Furthermore, a survey prepared by representatives from the European Commission Joint Research Centre (JRC), European Commission External Consultants, and the WGIC Policy Committee was distributed to representatives of a Special Interest Group (SIG) with representatives from: Australia, Canada, European Union, India, Malaysia, Mexico, Singapore, South Africa and the United States of America. For the full list of representatives, please consult Annex I.

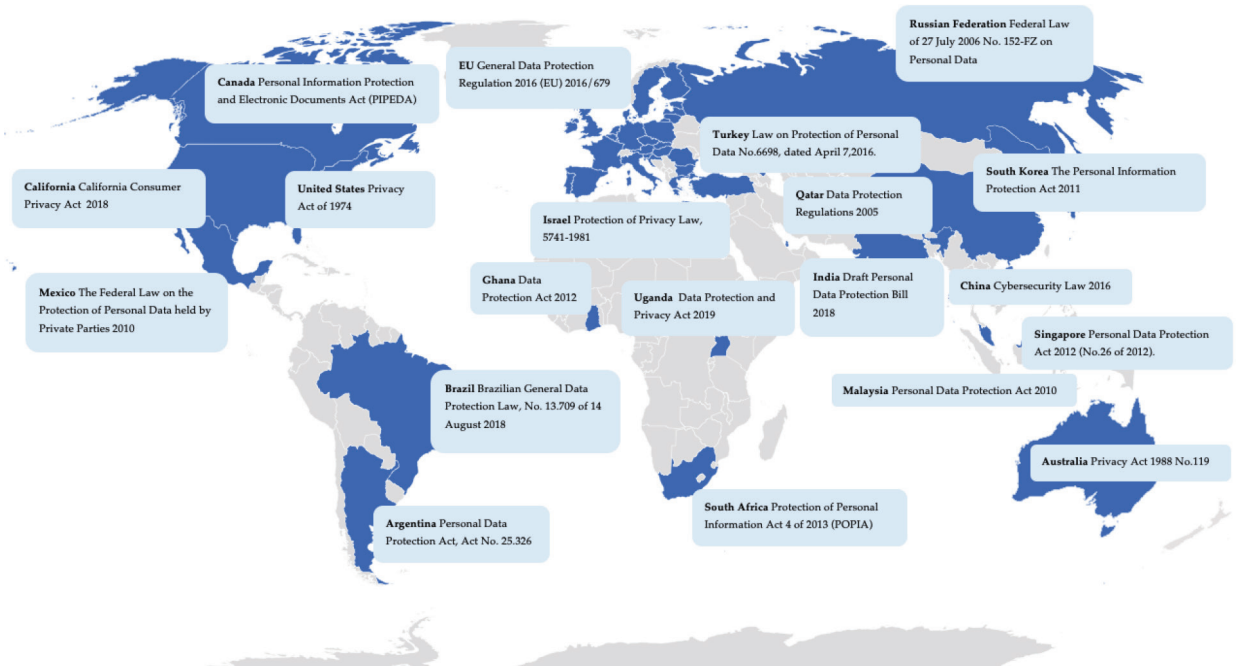

Figure 3: An overview of reviewed data protection regimes throughout the world

The survey discusses the different regulations from these representative jurisdictions and compares the provisions and obligations of these regulations (concerning location privacy) to the EU's GDPR. The GDPR has been applied as the benchmarking reference as we believe it is the most comprehensive and demanding legislation related to data privacy protection to date. It also impacts a large cross-section of the geospatial community and WGIC membership and is now being used as a template for emerging data protection regimes throughout the world.

4.2 Overview of data protection obligations

In order to compare and contrast countries, the SIG determined key data protection obligations, using GDPR as a benchmark. The selected countries were assessed against this benchmark and the level of alignment of local data protection legislation with the GDPR established. The answers have been represented in tabular form with green ( ) representing large alignment with the GDPR obligations or provisions, yellow ( ) representing some form of alignment albeit in a different form and red ( ) indicating that no obligation is reflected or no information is available. For the full overview of answers and references to the various laws and regulations and corresponding articles please consult the full overview associated with this report. This document includes more information on the assessed legislation and corresponding articles per country.

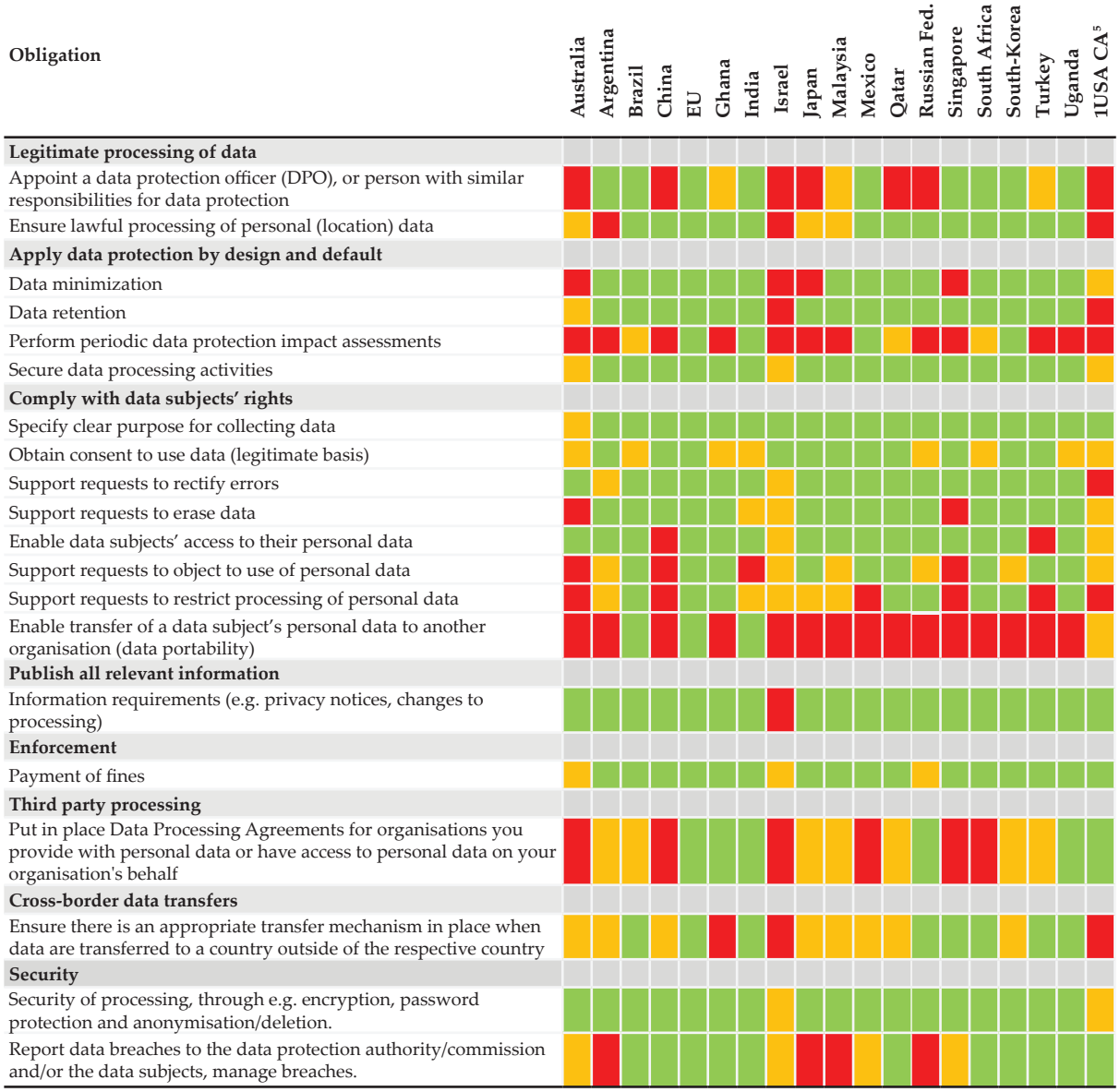

Figure 4: Overview of alignment with GDPR requirements per jurisdiction

[5] In the United States privacy is regulated at both the federal and state level. For this report we have assessed California. In the full country breakdown, the federal level is also included.

Based on Figure 4 we can see the following alignment with GDPR per country:

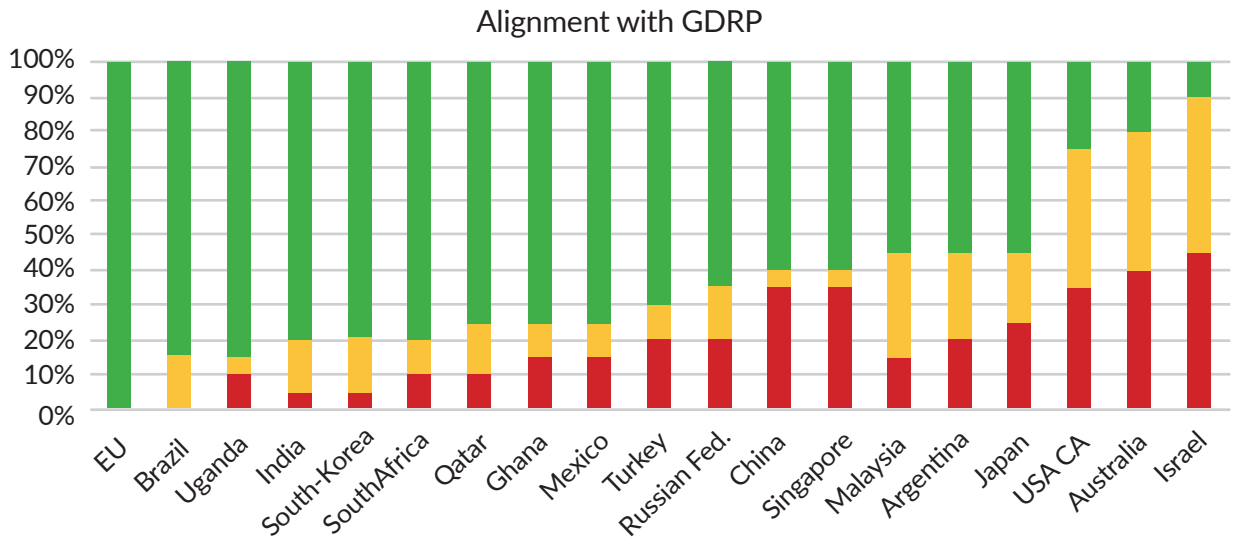

Figure 5: Ranking of alignment with GDPR requirements per jurisdiction

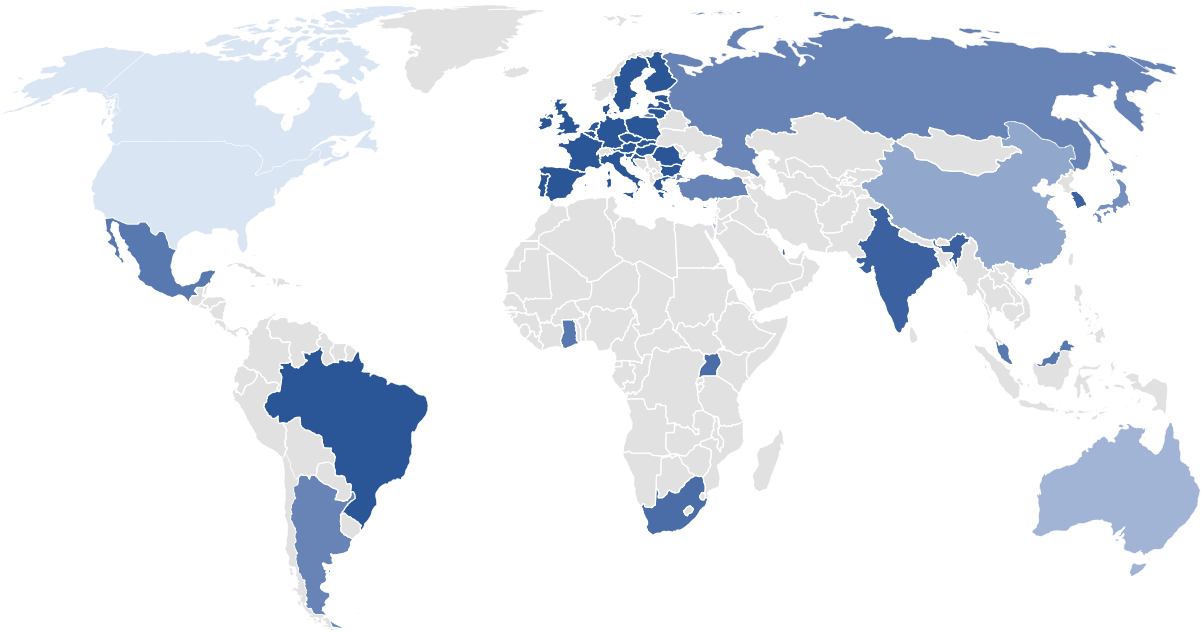

Figure 6: Map representing highest (dark blue) to lowest (light blue) level of alignment with EU's GDPR

Based on our survey we see significant differences in terms of alignment with the GDPR. While low alignment with the GDPR requirements may indicate a lower level of privacy and data protection, differences in alignment may be explained in several other ways.

Some jurisdictions have relatively new data protection laws that were inspired by the GDPR. As such, these countries show a high level of alignment with the GDPR. On the other hand, some countries have a rich tradition in privacy and data protection, but do not have a singular data protection law (such as for instance the United States). Given the limitations of our quick scan (see methodology), requirements stemming from other regulations may not have been included in the comparison.

Given the above, a high or low level of alignment with GDPR does not necessarily correspond with a high or low level of privacy and data protection. Furthermore, the level of alignment with the GDPR, while a good indicator for robust data protection legislation, may not say anything about the actual level of protection and enforcement of that legislation.

Finally, it is important to note that in various jurisdictions, new data privacy regulations are in various legislative stages. The approach taken by the SIG was to assume the latest available draft or proposal of the subject regulation will be passed in its entirety, and it was that version that was compared to GDPR. This was particularly the case in India and Malaysia.

5. Impact on the geospatial industry

The geospatial industry impact of the above described obligations varies per country and per application. To determine possible impact, geospatial information providers should first study their local data protection legislation and determine the scope and impact of that legislation.

When judging the impact for the geospatial industry, however, it is also important to know which data protection law actually applies. For example, the scope of legislation which is in force in the EU may also have an impact in the US. This is due to the extra-territorial scope of the GDPR. The GDPR is applicable to entities outside of the EU, when they target the EU market with goods or services, or when they monitor the behavior of data subjects in the EU as far as their behavior takes place within the EU. So, in judging the impact of the legal regime in question, geospatial information providers should not only look at the country where they are established, but also in which countries their activities are taking place, as it might very well be the case that they (also) fall under the jurisdiction of the country they are targeting with their services.

Concerning applications, impact levels may also vary per country. The common perception though is that data and data privacy impact all industries. Examples of applications with high data privacy impact are listed below:

- Land ownership;
- Location traceability from mobile devices;
- Fleet monitoring;
- Route monitoring/traffic modeling;
- In-car navigation/mobile navigation;
- Site analysis/geo marketing analysis;
- GIS in health-related analysis;
- GIS in crime hotspot analysis; and
- GIS in risk assessment.

As stipulated in Chapter 2, data protection legislation is applicable (and thus may have an impact on the geospatial industry) when personal data are processed.

The scope of data protection legislation from other regions or countries may vary widely. For example, the Brazilian General Data Protection Law maintains roughly the same material and territorial scope as the EU GDPR, whereas the material scope of Argentina's Personal Data Protection Act[6] is potentially much broader.

Across all regulations, a common concern was the linking of location-based data with other data, and there was a consensus that methods used to address this concern should be employed. The representatives of the SIG are in support of not linking said data at all as compared to including risk-aversion provisions. In case this linking cannot be avoided, then anonymizing and/or pseudonymizing should be considered. It was also indicated that:

[6] The Personal Data Protection Act 2000 will be repealed by the Protection of Personal Information Act (POPIA) once approved. The Argentinian data protection authority ('AAIP') announced, on 20 September 2018, that the President of the Argentine Republic, had sent the draft data protection bill to the National Congress of Argentina for consideration.

"as a result of the GDPR, location privacy awareness is improving within the geospatial community. In terms of recognition, we are seeing companies making decisions on where and/or how, they want to be seen respecting the privacy of end users."

Within the sample space, the company preparedness of privacy laws is highest in the EU, according to the survey, with a reported medium level of adoption. All other countries indicated a low level of company preparedness. Many representatives believed that preparedness and comparison to other industries are not possible at this stage because of the novelty of the regulations on the whole.

6. Compliance and accountability: best practices

Organizations that are subject to data protection and privacy legislation will have to fulfil a number of material requirements in order to process personal data legitimately. By looking at data protection and privacy legislation in force from jurisdictions worldwide, the vast number of these material requirements can be categorized under the following ten topics.

6.1 Privacy policy and governance

Organizations are generally required (in any case for GDPR) to have effective measures in place in order to demonstrate compliance with each of the principles and requirements as set out in the data protection and privacy legislation. This is to be done through data protection and privacy policies and processes designed to embed privacy compliance within the organization.

In addition, organizations should implement solid risk management. The requirement to do Data Protection Impact Assessments (DPIAs) forms an important element of such a risk management framework.

6.2 Accountability and demonstration of compliance

Organizations must be able to demonstrate that personal data are processed according to the rules and principles set out under data protection and privacy legislation. This requirement stems from the principle of accountability. Organizations must be able to demonstrate that they have taken appropriate measures in order to ensure that they are working in line with data protection obligations.

6.3 Processing in relation to third parties

When organizations process personal data together with third parties, the relationship between the parties needs to be defined, and the necessary agreements need to be concluded.

Joint controllers have to determine and document, in a transparent manner, their respective responsibilities in terms of compliance with data protection and privacy legislation.

When an organization engages a third party to process personal data on their behalf and based on their instructions, this third party will generally be regarded as the data processor. In such cases, the organization needs to conclude agreements with such processors to ensure and guarantee that the personal data processing is in compliance with all legal requirements.

It is also possible that an organization interacts with other parties that are data controllers on their own, meaning that these other parties decide their own purposes and means of processing personal data. In such a scenario, both parties are responsible for ensuring compliance with data protection and privacy legislation for their respective activities.

6.4 Data transfers

Organizations must pay close attention to transferring personal data to countries outside of the jurisdiction of applicable data protection and privacy legislation. It is often required, that in order for such data transfers to be legitimate, that organizations put in place appropriate safeguards. There are a number of legally recognized safeguards, such as contractual agreements or Binding Corporate Rules (BCRs).

6.5 Privacy by design & by default / Full life cycle and data protection

Organizations must take into account the principles of 'Privacy by design' and 'Privacy by default'. Privacy by design means that organizations need to take into account privacy and data protection into the design of their products and services. Privacy by default entails that organizations need to take technical and organizational measures to ensure that only those personal data elements are processed which are necessary for the purpose of the processing. This means that by default, the most privacy-friendly settings need to be set.

Full life cycle data protection means that privacy and data protection should be taken into account throughout the full life cycle of a product or service. In particular when changes are made to the product or service, it should be assessed whether the existing technical and organizational measures to protect the personal data are still sufficient.

When an organization wants to perform a new high-risk processing activity or when there is a change in the risk of an existing processing activity, a Data Protection Impact Assessment (DPIA) needs to be conducted. A DPIA consists of an assessment of the risks of the processing activity to the rights and freedoms of the individuals involved. A DPIA also includes mitigating measures which can be taken in order to reduce the identified risk. By performing a DPIA, organizations can ensure that necessary measures are taken.

6.6 Security of processing

Personal data must be processed in a manner that guarantees the confidentiality, integrity and availability of that data. Organizations must ensure that personal data are protected from unauthorized access and use, but also from accidental loss, destruction or damage. This can be done, for example, through pseudonymization and/or encryption of personal data, access control, password policies, firewalls and intrusion detection systems. Furthermore, security awareness for employees is of the utmost importance.

As part of its security policy, an organization must set up procedures in case a data breach occurs. In the event of a data breach, every employee must know who to contact to initiate the procedure in order to assess the (potential) data breach and, where necessary, report it to the data protection authority and possibly any individuals involved.

6.7 Data subject rights

Data subject rights are part of various data protection and privacy laws and are intended to give individuals control over their personal data. For example, such rights may give individuals the right to request an overview of all their personal data that is processed by the organization and obtain a copy thereof. Or they may be able to request to rectify or erase their personal data and they can, for example, obtain human intervention in cases of automated decision-making. It is important that organizations address these rights and know how to respond and fulfill to these kinds of requests.

6.8 Transparency

Organizations must inform individuals about the processing of their personal data. It is important that individuals are informed about the processing of their personal data in its entirety. Data protection and privacy legislation mostly aims to put the control over personal data in the hands of the individuals to whom such personal data belongs. Individuals can only take such control if they are aware of how their personal data are processed and by whom. The information provided by organizations should therefore be given in a

concise, transparent, intelligible and easily accessible form. Doing so will allow organizations to give individuals the choice to make informed decisions with regard to the processing of their personal data.

6.9 Monitoring and enforcement

Monitoring and enforcement of data protection and privacy policies within the organization is important to ensure that measures taken are effective and applied in a correct and uniform manner. Cases of non-compliance should be detected and remedied.

6.10 Awareness

It is important to create awareness within an organization with regard to data protection and privacy in order to ensure privacy compliance. It is the task of an organization to seek ways through which to create such awareness among employees, for instance by sending out regular information bulletins, organizing training sessions for employees and work instructions to work in line with applicable policies.

To illustrate how these best practices are related to legislation, the below matrix shows, for various jurisdictions, whether such practices are actually mandated by law.

Best Practices	Australia	Brazil	EU	India	Malaysia	Mexico	South Africa	USA (California)
Set up a governance structure for (location) data protection								
Set up a (location) data management program								
Develop personal data protection risk strategy								
Develop personal data protection policy								
Put in place Data Protection Agreements for organisations you provide with personal data or have access to personal data on your behalf								
Ensure awareness raising and training in place for all staff								
Implement traceability								
Audit trail of policy documents and changes								
Customer records (consent, requests, complaints etc.)								
Audit trail on access to data, use of data, and transfer to other organizations (to support data requests, breach investigations)								
Security								
Encryption								
Password protections								
Monitoring								
Compliance with a data protection policy								
Customer perception								
Effectiveness of data handling and security controls								

Figure 8: Best practices and their relation to legal requirements

7. Summary and conclusion

- Privacy and data protection legislation are highly relevant to the geospatial industry, and may have a significant impact on geospatial information providers throughout the world. Geospatial information providers should determine, based on their business model and service offerings, what their exposure to data protection legislation is. Based on this assessment, the provider can take the necessary steps to become compliant.

- Data protection legislation is only relevant for the geospatial industry if data regarding individuals is being processed (i.e., 'personal data'). When geospatial data cannot be attributed to an individual it will not be considered 'personal data'. As such, it will generally not be subject to privacy and data protection legislation.

- Whether geospatial data should be considered personal data is very much dependent on the circumstances of the case. If the information attributed to the geospatial information is about individuals, or if the geospatial data itself allows individuals to be identified, the geospatial information automatically becomes personal data, and data protection legislation applies.

- Geospatial information providers may use geospatial data in a number of ways. The actual use will determine whether data protection legislation applies and if so, which rules the geospatial information provider should follow.

- When processing personal data, geospatial information providers qualify either as 'data controllers' or 'data processors'. A data controller determines the purposes and means for the processing, while a data processor acts on the instructions of the data controller. The data controller is the main norm addressee of data protection legislation.

- Personal data may only be processed for legitimate purposes. When processing personal data in the capacity of a data controller, geospatial information providers should specify a clear goal for the processing and determine its legitimacy.

- Privacy and data protection legislation has been enacted throughout the world. The jurisdictions reviewed for this report show varying levels of alignment with the EU General Data Protection Regulation (GDPR). Requirements seen throughout the world are data security, purpose specification, and notification. Requirements that are less common are the need to do data protection impact assessments, providing data portability and rules on third party processing.

- Geospatial information providers, especially those acting as data controllers, should implement technical and organisational measures to enable compliance. These include implementing privacy policies and governance, security measures, agreements with third parties (processors), privacy by design, data subject rights, and awareness raising.

8. ANNEX I – Contributors acknowledgement

Africa:

Derek Clark (South Africa), WGIC

Asia Pacific:

Glenn Cockerton (Australia), Spatial Vision

Dr. Siva Kumar (India), IIC Technologies

Ir. Mazura Nor Zulkifli (Malaysia), Dr. Nik & Associates Sdn. Bhd.

Nouman Ahmed (Saudi Arabia), GeoSystems-Middle East

Dr. Victor Khoo (Singapore), Singapore Land Authority

Europe:

Ray Boguslawski (Italy), European Commission - Joint Research Centre

Dara Keogh (Italy), European Commission - Joint Research Centre

Francesco Pignatelli (Italy), European Commission - Joint Research Centre

Nane Engelhart (Netherlands), TomTom

Cassandra Moons (Netherlands), TomTom

North America:

Prashant Shukle (Canada), Canada Centre for Mapping & Earth Observation

Cristina Guirette Saldana (Mexico), INEGI

Scott Allbert (USA), M-Files

Ed Cox (USA), Prime Policy Group

Pat Cummens (USA), ESRI

South America:

Marcelo Fernandes (Brazil), TomTom

Zorka Marinovic (Chile), TomTom

Research, consolidation and editing:

Bart Schermer (Netherlands), Considerati

Jonathan Toornstra (Netherlands), Considerati

WGIC Steering Committee (Policy Committee Members WGIC):

Arnout Desmet (Belgium), Chair, TomTom

Dr. Zaffar Sadiq Mohamed Ghouse (Australia), Spatial Vision

James van Rens (USA), Riegl International

James Steiner (USA), Oracle

WGIC Support:

Barbara Ryan (USA), WGIC

Sharmishtha Seth (India), WGIC

Notes

Notes

World Geospatial Industry Council
Business Center, Unit 3
Barchman Wuytierslaan 10
3818 LH Amersfoort
The Netherlands
Email: info@wgicouncil.org
Website: www.wgicouncil.org