GDPR: Guidance on the ArcGIS Platform

Author: Esri UK and Esri Ireland

Date: 21st May 2018

Summary

The EU General Data Protection Regulation ("GDPR") places significant responsibilities on organisations that process personal data. We are committed to being compliant with GDPR, including helping our customers meet their GDPR obligations. Many of our customers make use of the ArcGIS platform to manage spatial data that may include personal data. The ArcGIS platform includes many tools and capabilities that can enable customers to address their GDPR obligations, and this document highlights those, as well as other aspects of how GDPR may influence the use of GIS, the deployment of the ArcGIS Platform and the interactions customers may have with us and/or Esri Inc.

Introduction

GDPR is effective from 25 May 2018. It sets out the rights of individual Data Subjects with respect to their personal data, and the responsibilities of those who process personal data as either a Data Controller or a Data Processor. All Data Controllers and Data Processors must be compliant with GDPR. ArcGIS is used by many of our customers to manage, process and analyse a wide range of data, which could include personal data. This raises questions as to how our customers can use ArcGIS to meet their responsibilities under GDPR, and how we are addressing such questions. This document answers the key questions that customers have raised with us to date about their use of ArcGIS and their interactions with us and Esri Inc.

GDPR

GDPR is complex and there is plenty of information available that discusses this in detail. In the UK, the Information Commissioners Office (ICO) is responsible for ensuring that organisations comply with GDPR and provide guidance to those organisations about their responsibilities. The ICO's guidance and information can be found via the ICO website: https://ico.org.uk. In Ireland the Data Protection Commissioner is responsible, and their guidance can be found at their website: https://www.dataprotection.ie/docs/Home/4.htm

GDPR Roles and Terminology

There are a number of terms or definitions that are used when discussing GDPR. The following list identifies the main ones that are relevant to this document. Further information can also be found via the Regulator websites referred to above.

"**Data Subject**" is an identified or identifiable living individual who can be identified, directly or indirectly, by reference to an identifier or information or other factors relating to the individual.

"**Personal Data**" means any information relating to a Data Subject, such as their name or address etc.

"**Data Controller**" is a natural or legal person (such as an organisation) which (either alone or with others) determines the purposes and means of the processing of the personal data.

Last Update: 21st May 2018

Updated by: John Clayson

"**Data Processor**" is a natural or legal person who processes personal data on behalf of a Data Controller.

Rights and Responsibilities

Under GDPR, Data Controllers and Data Processors have responsibilities and obligations; and Data Subjects have certain rights. The following list provides some key examples of such, but is not exhaustive.

Data Subjects have the right to:	Organisations will need to:
Access their personal data	Protect personal data using appropriate security
Correct errors in their personal data	Have notification processes for breaches
Erase their personal data	Ensure consents are valid (where required)
Object to processing of their personal data	Keep records detailing data processing
Export personal data	Provide clear information
	Detail the processing purpose(s)
	Abide to data retention / deletion requirements
	Train personnel
	Ensure appropriate contract terms are in place

The data protection 'principles' under GDPR requires organisations to ensure that personal data is:

- processed lawfully, fairly and transparently
- collected for specific, explicit and legitimate purposes
- adequate, relevant and limited to what is necessary for the purpose of the processing
- accurate and up to date
- only kept for so long as is necessary
- processed securely using appropriate technical and organisational measures to ensure integrity and confidentiality

In addition, where an organisation uses third party processors it must ensure that they will implement and maintain appropriate technical and organisational measures in order to meet the requirements of the GDPR and to ensure the rights of Data Subjects. There are further requirements where sub-processors are used by the Data Processor; and/or where personal data is transferred to a third country / international organisation.

GDPR - Our roles

Under GDPR organisations that process personal data using the ArcGIS platform may fall into different roles depending on the particular circumstances. For us, these can be categorised into the scenarios below:

#	Scenario	Organisation using ArcGIS	Individual to whom the personal data relates	Esri UK and Esri Ireland	Esri Inc
1	Organisation using ArcGIS Software 'on premise' to process personal data	Data Controller	Data Subject	N/A	N/A

Last Update: 21st May 2018
Updated by: John Clayson

#	Scenario	Organisation using ArcGIS	Individual to whom the personal data relates	Esri UK and Esri Ireland	Esri Inc
2	Organisation using Esri Inc hosted or managed software, or Esri Inc online services to process personal data. For example: ArcGIS Online	Data Controller	Data Subject	N/A	Data Processor
3	Organisation using Esri UK or Esri Ireland hosted or managed software, or Esri UK online services to process personal data	Data Controller	Data Subject	Data Processor*	Sub-Processor
4	As an individual you provide personal data so that we can grant you any necessary licences and/or provide you with the services	Data Subject		Data Controller	Data Processor**

This document focusses on the first 3 scenarios, however like any other organisation that acts as the Data Controller for personal data, we are also required to adhere to GDPR. You can find more details of our compliance at https://www.esriuk.com/en-gb/legal/gdpr/about.

* Esri UK or Esri Ireland engages a sub-processor to provide its hosted and managed infrastructure software and services.
** To the extent that licensing or product use and/or support requires Esri UK or Esri Ireland to process your personal data with Esri Inc.

Personal Data and GIS

Every organisation that manages data will need to undertake an assessment as to whether the information they manage falls into the category of personal data. GIS Systems and the technologies that underpin them are often used to manage data that could be classified as personal data. Examples of this include:

- Address information tied to individuals and stored in a spatially enabled CRM
- Information about the location of your workforce
- User profile information about users of your GIS system
- personal data that you collect in an online “report a fault” system

As a Data Controller you will need to use the tools provided by the system or third parties to carry out your GDPR obligations. The ArcGIS platform provides a number of capabilities to help you manage personal data within your GIS System

ArcGIS and GDPR

ArcGIS* is a platform for managing, analysing and visualising spatial data, and as such it contains many different components. The following sections outline how ArcGIS can help you in meeting the requirements of GDPR. If you are using ArcGIS to manage personal data, then the following questions are important.

- What technological security measures are available to ensure data security?
- What tools are available to identify what data is personal data?
- What tools are there to correct inaccurate or incomplete personal data?
- What tools are there to remove or delete personal data?
- What tools are there to restrict the processing of personal data?

Last Update: 21st May 2018
Updated by: John Clayson

- What tools are there to enable personal data to be extracted in a machine-readable, commonly used and structured form?
- How can I notify users of Apps I deploy about my privacy policy?

* The ArcGIS platform is proprietary to Environmental Systems Research Institute, Inc ("Esri Inc"), a corporation located in the United States of America. We are Esri Inc's authorised distributor of the ArcGIS platform to end users in Great Britain (Esri UK) and Ireland (Esri Ireland).

ArcGIS On Premises Deployment

Many organisations deploy and manage ArcGIS software on their own infrastructure, which may include infrastructure owned by a third party such as a cloud infrastructure provider. In this scenario you are responsible for meeting your GDPR obligations. You may also need to liaise with your infrastructure provider to understand their GDPR compliance as a Data Processor (or sub-processor, as applicable).

A typical deployment of ArcGIS on Premises would include ArcGIS Enterprise components and ArcGIS desktop tools such as ArcGIS Pro or ArcMap. If you are managing personal data it is likely that you are also making use of a relational database (RDBMS) such as Oracle, SQL server or Postgres to store and manage that data. You can decide if and how to store personal data within the system and it is your responsibility for ensuring that you meet any applicable requirements of GDPR.

System Design

Creating a robust system that can be used to manage personal data starts at the design stage. It is important to put in place a well understood data model with corporate standards for data and metadata. Key aspects to consider are:

- Have a well-designed data model
- Enforce metadata standards
- Have a data dictionary describing the types of data you manage
- Have a well-designed user access model
- Understand the key business processes supported by your GIS
- Have corporate guidelines for information standards

User Profile Management

As well as personal data that you choose to store and manage in the system, ArcGIS also requires basic information about the users of the system. This enables you to implement robust security and data sharing workflows within your organisation. ArcGIS enterprise is deployed with a named user model and every named user gets a profile in the system. The required components of a user profile are:

- First Name
- Last Name
- email
- Username
- ArcGIS License Level
- ArcGIS Role

Last Update: 21st May 2018
Updated by: John Clayson

This data is used by the system to enforce security, and also to allow user to share data and collaborate with each other. The system provides a number of tools to allow an Administrator to manage this information.

- Search Users – search for specific users
- Add User – you can invite new users to the system
- Update Profile – you can manage additional user profile information
- Delete user – Remove a user profile from the system

Data Security

ArcGIS includes a number of robust security mechanisms to enable you to protect access to personal data stored within the system, this will include functionality provided by the underlying RDBMS.

- RDBMS user security, allows you to limit who has access to specific tables within the database. This enables you to control who may have access to data of a personal nature
- You can use additional RDMBS security technology such as Data encryption with your ArcGIS deployment
- The ArcGIS named user model allows every user of the system to be uniquely identified and to enable access to data to be controlled at the individual level
- The ArcGIS named user model can be linked to your corporate Identity system such as Active directory or LDAP to allow you to manage your users securely across your organisation
- ArcGIS can also support additional security mechanisms such PKI authentication

Data Identification and Searching

While ArcGIS does not contain any tools designed specifically for identifying personal data, it does include a number of generic data search and analysis tools that can be used to search data and metadata for personal data. These can be combined with good data design and corporate standards around data dictionaries and metadata management.

- ArcGIS includes the ability to store metadata documents that live with your data and describe the contents and data types
- ArcGIS metadata documents are linked to the data and will move with the data as it is processed by ArcGIS
- ArcGIS metadata documents can be searched for keywords and content describing personal data
- ArcGIS includes database query tools that can be used to search within your GIS data for records that meet specific criteria
- In addition to formal metadata descriptions ArcGIS includes the ability to assign Tags to categorise data. These can be used to tag items and layers that contain personal data and then included in future searches

Data Correction and Editing

ArcGIS contains standard tools to allow users with the correct permissions to edit the content of data stored within the system. These tools can be used to correct or add to any personal data within ArcGIS.

- Data editing is controlled by user permissions and only available to authorised users
- ArcGIS Geometry editing tools can be used to edit location data
- ArcGIS Attribute Editing tools can be used to edit attribute data stored in the GIS

Last Update: 21st May 2018
Updated by: John Clayson

- Field Calculator tools can be used to make bulk changes to data

Data removal and Deletion

ArcGIS contains standard tools for deleting individual records and data tables within ArcGIS, combined with the search and identification tools these can be used to remove personal data from your system.

- The Delete features tools can be used to remove individual records from the ArcGIS system
- The delete table and delete feature class tools will enable you to remove datasets containing personal data

Data Processing Restrictions

A number of tools discussed in the previous section can be used to manage how personal data may be processed within the system.

- Metadata tools and tags can be used to identify personal data so that it is not processed inappropriately
- User access controls can limit access to personal data to specific users
- Additional metadata such as usage limits can be applied to datasets in ArcGIS

Data Extraction

ArcGIS contains a number of tools that will enable you to extract data in a structured form.

- Export data tools allow you to extract data in a variety of machine readable formats including
    - Json
    - CSV
    - Shp file
- Additional data extraction capability is provided by the data interoperability extensions for ArcGIS.

User Notification and Privacy statements

If ArcGIS is used to publish applications such as web apps that collect information from users, then it may be necessary to notify the users of an App that personal data is to be collected, and to link them to the relevant privacy policy. ArcGIS contains a range of mechanisms for notifying users of such policies.

- ArcGIS Portal allows you to customise the home page, as well as header and footer pages, enabling you to include privacy statements or links
- Many of the ArcGIS Application templates enable you to configure a splash page for users before they access the application
- Custom applications can include privacy notifications built using the ArcGIS SDKs
- Items stored in ArcGIS Enterprise can include descriptions and usage limit statements that could contain any privacy notices that are applicable.

Esri Managed Software: ArcGIS Online

ArcGIS is available as Software-as-a -Service (SaaS) in the form of ArcGIS Online, in this scenario you remain the Data Controller for any personal data that you choose to store in ArcGIS Online. However, Esri Inc is a Data Processor in this case, and there are additional sub-processors that are used in providing the ArcGIS Online service to you.

ArcGIS Online Infrastructure is hosted in data centres located in the United States of America, including those of Esri Inc, Microsoft Azure and Amazon Web services. Any personal data stored in ArcGIS Online may be transferred to those data centres.

All the tools previously discussed also apply to ArcGIS Online, allowing you as the Data Controller to manage what personal data you choose to store in ArcGIS Online. You can continue to manage this data in the same way that you would in an on-premises solution.

Any use of ArcGIS Online will require you to create user accounts, and the user profile data associated with these will be stored within ArcGIS Online. This data is used for the purposes of ensuring security and providing the service to you and is governed by the security and privacy controls discussed below. You can manage users by linking to an enterprise Identity management system such ADFS, or by using the user management tools discussed in the previous section.

Esri Inc has published several documents which relate to this, and which can be found via the following links:

- Document entitled: "ArcGIS Online: A Security, Privacy & Compliance Overview" http://downloads.esri.com/resources/enterprisegis/2017UC_ArcGIS_Online_Security.pdf
- The following link provides information relating to the security of the ArcGIS platform generally, and specific information relating to privacy and compliance information: https://doc.arcgis.com/en/trust/
- The following link contains Esri Inc's contractual provisions for where its Online Services or maintenance are provided, and where EU personal data is provided to Esri Inc. See document entitled "Data Processing Addendum". https://www.esri.com/en-us/privacy/privacy-gdpr

Architecture

Users of ArcGIS Online can choose not to process data containing personal data in ArcGIS Online, or to use ArcGIS Online in a hybrid cloud deployment. A hybrid deployment allows an organisation to host key databases and services within their own infrastructure, while making use of the capabilities and scalability of the cloud hosted ArcGIS Online. This enables an organisation to keep sensitive or personal data within its own infrastructure.

Security

One of the primary obligations of a Data Processor is to ensure the adequate security of any personal data that is processed. ArcGIS Online is a secure scalable system that is subject to a number of external security certifications. Full details can be found in the security and compliance pages of the ArcGIS trust site and details of the relevant security measures are documented in Esri Inc's Cloud Security Alliance Cloud control matrix: http://downloads.esri.com/RESOURCES/ENTERPRISEGIS/AGOL_CSA_CCM.PDF

Last Update: 21st May 2018
Updated by: John Clayson

Privacy

Esri Inc is certified under the EU-US Privacy Shield Framework governing data privacy, and you can find full details of Esri Inc's privacy assurance for ArcGIS Online as well as Esri Inc's general privacy statement and details of how Esri Inc use any personal data in the documents linked from Esri Inc's privacy pages.
https://doc.arcgis.com/en/trust/privacy/privacy-tab-intro.htm

Esri UK's Online Services: Software as a Service

Esri UK host a number of cloud based applications that build on top of ArcGIS Online including QuestionWhere, MyNearest and sweet. These applications are all designed to make use of ArcGIS Online, and so the privacy and security measures of ArcGIS Online are relevant in this case. Any data that you choose to collect through the use of these applications can be managed using the relevant tools discussed in the previous sections.
These applications are hosted on Esri UK's AppHub Hosting environment, which is running on the AWS cloud. Esri UK hosted applications do not collect or store any information provided by users of the applications, however Esri UK do log information generated during the operation of the service, such as web logs and IP addresses, we use this information for tracking errors and delivering a scalable, secure and reliable service.

Esri UK and Esri Ireland Managed Services

Esri UK and Esri Ireland's Managed Services Teams provide services to host and run an organisations ArcGIS Infrastructure in the cloud. This infrastructure will be operated in our cloud service providers' infrastructure. Each deployment will differ depending on an organisations requirements, but it provides the capability to deploy a managed ArcGIS system within EU data centres, helping an organisation tailor their GIS solution, for instance where the organisation prefers to keep personal data within the EU.

Conclusion

Each organisation that deals with personal data needs to ensure that they address any issues that GDPR raises. If you choose to store personal data in the ArcGIS platform then you remain responsible for that data and how it is managed and used within the system. ArcGIS is a powerful platform for helping with the task of managing personal data, and provides tools and capabilities that can address some of the specific requirements of GDPR.

If you utilise cloud services as part of your ArcGIS system, whether that is infrastructure provided by us, Esri Inc or another third party, or by utilising software as a service, then it is important that you understand how that impacts your responsibilities under GDPR. We, Esri Inc and our third-party Data Processors (or sub-processors) provide both technical and contractual measures to enable you to meet your GDPR requirements, as well as addressing those requirements for our own operations.

Last Update: 21st May 2018
Updated by: John Clayson