OS Web Service / API Guidance

Use of OS data on your website – via OS APIs or your own services

Your member licence allows you use OS data on your website in support of your core business.

As you are likely to be publishing more of your information on the internet, and with the introduction of the Government's Digital Service Standards (see below), we have updated our guidance and are reminding you of your obligations to protect not only our premium data but, perhaps more importantly, your own core data from unauthorised access and subsequent use.

If you are using any of our premium (Licensed) data, you have a responsibility to use your *"best endeavours to use adequate technological and security measures, including but not limited to measures we may reasonably recommend from time to time, to ensure all OS Licensed Data and login details which we provide to the Licensee and/or which the Licensee holds or is responsible for are secure from unauthorised use or access"*.

Unauthorised use can, for example, be simply 'web scraping'. This is a form of copying, in which specific data is gathered and copied and likely put into another local database, for later retrieval or analysis. Typically, this refers to automated processes implemented using a 'bot' or 'web crawler'; although it can be done manually by a software user.

Unauthorised access could take the form of someone using their technical knowledge to bypass identity controls (i.e. a log in) you have put in place before a user is able to access and use your service. They could then access your systems and data (i.e. hacking), putting your organisation at risk (see below for further guidance on hosting your own services)

Unauthorised access could also take the form of unauthorised usage of 3rd party web services, such as those from OS. Such unauthorised access is likely to be a result of having limited or no protection of the web service credentials (such as an API key)

It is appreciated that 'web scraping' is a lot harder to for you to protect against than unauthorised access or hacking – especially without negatively impacting your end users. Most methods to deter data scraping (see this GitHub article for a useful overview) need to be implemented on the client-side (i.e. commonly a public-facing website).

Best practice in this area involves monitoring activity (part of the Digital Service Standards) and then taking actions such as rate limiting access to the site itself by IP or blocking access, changing website HTML to break the automation of the data scraping or creating fake honeypots of data. Captcha's are also often used; it is acknowledged that they do introduce accessibility problems, however they may prove useful in cases where you detect suspicious activity (for example, you detect bot-like behaviour and need to test whether the user is human).

Are you meeting the Government's Digital Service Standards?

The Digital Service Standard is a set of 18 criteria to help government create and run good digital services. All public facing transactional services must meet the standard. It's used by departments and the Government Digital Service to check whether a service is good enough for public use.

Part of the Digital Service Standard that central government services must meet includes showing that they understand the legal concerns including data protection - as well as monitoring their service to identify any problems that might affect it including attacks on the service.

Definitions

API means an Application Programming Interface allowing the creation of application for access to OS Data

Map API means any API that primarily or wholly provides a visual map, usually in a particular style. This includes APIs compliant with the OGC WMS or WMTS standards.

Feature API means any API that primarily or wholly provides geospatial feature data. This includes APIs compliant with the OGC WFS standards.

WFS means a service provided by the Licensee in accordance with the OGC Web Feature Service standard protocol for serving georeferenced data over the internet

WMS or WMTS means a service provided by the Licensee in accordance with the OGC Web Map Service or OGC Web Map Tile Service standard protocol for serving georeferenced map images over the internet.

Proxy server/script is a computer/script that functions as an intermediary between a web browser and the internet.

Guidance for hosting your own APIs using OS Data

Background

This guidance applies where a party to the PSGA Member Licence makes Licensed Data (as defined in those Licences) available using a Web Map Service (WMS), Web Map Tile Service (WMTS) or Web Feature Service (WFS) or other equivalent mapping or Feature APIs. It seeks to reduce the risk of unlicensed use of that data without adversely impacting on the services offered by Members.

Clause 4.1.2 of the Member Licence requires you to:

"Use your best endeavours to use adequate technological and security measures, including but not limited to, measures we may reasonably recommend from time to time, to ensure that all Licensed Data and Login Details which we provide to you and/or which you hold or are responsible for are secure from unauthorised use or access"

Our recommendations for appropriate technological and security measures in this context are detailed below. Adherence to these recommendations will ensure compliance with clause 4.1.2.

Note that this Guidance does not apply to use of WMS, WMTS or WFS in the context of INSPIRE End User Licensing; PSGA members should instead refer to paragraph 7 of Appendix 1 to the PSGA Member Licence

Making Licensed Data available via API

Where Licensed Data is made available via API, this will need to be for your Core Business, and in accordance with the provisions of clause 2.6 or Appendix 1 to the Member Licence. Subject to such provisions, and assuming that you are entitled to publish the data via API, the provisions of the paragraphs below must be employed.

1. Licensed data made available via WMS or WMTS or other Map API

(i) Data with a background watermark

If you choose to include a background watermark to identify the source of the Licensed Data you make available via WMS or WMTS or other Map API then it must appear at least once and cover at least 10% of the map image reproduced and any one or a combination of the security measures (a) to (d) (see below) must be employed. The same applies where you have a statutory obligation to publish planning applications on the internet and elect not to include a background watermark on mapping extracts that form part of a planning application.

(ii) Data without a background watermark

If you choose not to include a watermark when you make Licensed Data available via WMS or WMTS or other Map API, you must include security measure (a) "Server-side proxy" plus other measures (for example b) to d) you employ to protect the Licensed Data

Security Measures

a) **Server-side proxy** - Licensed Data is made available on an internet webpage administered by you and hosted on your own network or made available on an internet webpage administered by a third-party Contractor on your behalf and hosted on their network. All end points (i.e. URLs to which the request for the WMS/WMTS/Map API is being made) which could otherwise be used to access the API, must be server side or remain hidden from the client view, in each case so as not to allow alternative direct access by unlicensed individuals – see our advice above.

   This option would be most suitable for use of a WMS/WMTS/Map API with your public facing websites and services; for example, showing a service provision, such as the location of public buildings or Authority run leisure facilities. This option would also be suitable where you are making Licensed Data available for viewing via a mobile app.

b) **Username and password** - Licensed Data is only made available to users who have been provided with a unique username and password for the WMS/WMTS/Map API (to be clear, this is not intended to cover the situation where members of the public at large are eligible to create/be assigned an automatically generated usernames and passwords). This must be entered by the relevant user each time he/she accesses the WMS/WMTS/Map API

   This option may suit a service that is accessed by contractors who are carrying out works on your behalf or even other PSMA Members who may be engaged in a joint project or service delivery. For example, a username and password can be issued by you to each individual or organisation to whom you wish to grant access to your WMS/WMTS/Map API.

c) **Predefined IP range** - Licensed Data can only be accessed from a predefined IP address, or from a range of predefined IP addresses.

This option may be suitable if you wish to grant regular access to a contractor working for you on the delivery of a service to the public. They would be able to access the service whenever necessary from more than one terminal or even location after supplying you with a single or number of IP addresses that can be granted permission to access the WMS.

d) Implement appropriate **access control (for example API keys / tokens with URL referrer checks, OAuth etc)** using existing software solutions and/or a federated solution such as the UK Access Federation (http://www.ukfederation.org.uk/). Solutions are available as open source e.g., Shibboleth, and also proprietary software. If this option is adopted it is recommended to use one based on accepted standards so that it can be made interoperable with others later on.

2 Licensed data made available via WFS or other Feature API

(i) Data with a background watermark

If you are using the WFS or other Feature API as a map then you can choose to include a background watermark to identify the source of the Licensed Data you make available via WFS or other Feature API. It must appear at least once and cover at least 10% of the map image reproduced and the provisions relating to a WMS (see above) shall apply. The same is true where you have a statutory obligation to publish planning applications on the internet and elect not to include a background watermark on mapping extracts that form part of a planning application.

(ii) Data without a background watermark

Where Licensed Data that does not or cannot carry a watermark is made available via WFS or other Feature API, Ordnance Survey recommends that you use the following methods to protect it:

a) **Server-side proxy** - Licensed Data is made available on an internet webpage administered by you and hosted on your own network or made available on an internet webpage administered by a third-party Contractor on your behalf and hosted on their network. All end-points, (i.e., URLs to which the request for the WFS or Feature API is being made) which could otherwise be used to access the API, must be server side or remain hidden from the client view, in each case so as not to allow alternative direct access by unlicensed individuals - see our advice above.

and one or both of the following safeguards:

b) **Username and password** - Licensed Data is only made available to users who have been provided with a unique username and password for the WFS or Feature API (to be clear, this is not intended to cover the situation where members of the public at large are eligible to create/be assigned an automatically generated usernames and passwords). This must be entered by the relevant user each time he/she accesses the WFS or Feature API.

c) **Predefined IP range** - Licensed Data can only be accessed from predefined IP addresses, or from a range of predefined IP addresses.

d) Implement appropriate **access control (for example API keys / tokens with URL referrer checks, OAuth etc)** using existing software solutions and/or a federated solution such as the UK Access Federation (http://www.ukfederation.org.uk/). Solutions are available as open source e.g., Shibboleth, and also proprietary software. If this option is adopted it is recommended to use one based on accepted standards so that it can be made interoperable with others later on.