smoothwall

The Web You Want

GDPR and Smoothwall's UTM/SWG

Introduction

This paper sets out how the UTM/SWG product range from Smoothwall and the features and services which are part of this product range (which we refer to as the UTM/SWG in this paper) meet the requirements of the General Data Protection Regulation (or GDPR).

This paper is intended to provide you, as a data controller, with the information you need to ensure that you comply with your obligations as a data controller under GDPR when using the UTM/SWG.

Smoothwall does not collect, store, use, process or handle in any way any of the personal data collected by the UTM/SWG, and it is therefore neither a data controller nor a data processor in respect of the UTM/SWG for the purposes of GDPR or the UK data protection regime.

This paper should be read as a guide only; it does not constitute legal advice and cannot be relied upon as such. We strongly recommend that you seek your own professional advice on ensuring that you are compliant with GDPR and UK data protection law.

Terms such as data controller and data processor are defined in the Glossary below.

The legal basis for the processing of personal data by the UTM/SWG under GDPR

The processing of personal data is only lawful under GDPR where one of the conditions in Article 6(1) applies. Where special categories of personal data (see Glossary below) are being processed, one of the conditions in Article 9(2) must also apply.

GDPR requires you, as a data controller, to decide which of the conditions is appropriate for the processing of personal data by the UTM/SWG.

The UTM/SWG collects the following information:

- the address or URL of any webpage which a user tries to access
- the words entered into a search engine and
- the fact that an attempt to access a restricted site has been made.

This information is logged against the username.

All information collected by the UTM/SWG is stored by you. You are therefore responsible for making sure that appropriate technical and organisational security measures are implemented to protect the personal data which is collected and stored by the UTM/SWG.

This means that depending on the words used in search terms and the websites which users visit or try to visit, some special categories of personal data may be collected. You will therefore need to determine, where appropriate, which conditions in Article 6(1) and Article 9(2) apply to the processing of personal data by the UTM/SWG.

You may decide that the appropriate conditions for your processing are one or more of:

- Article 6(1)(c) – compliance with a legal obligation which you are subject to
- Article 6(1)(e) – performance of a task in the public interest or
- Article 6(1)(f) – legitimate interests*.

*Public authorities (which are defined by the Data Protection Bill as authorities which are subject to the Freedom of Information Act 2000) are not able to rely on Article 6(1)(f) – legitimate interests for processing personal data.

You will need to make your own decision about which conditions are appropriate and you should consider whether you need professional advice to assist you with t his decision.

The full list of conditions in Article 6(1) and Article 9(2) are set out at the end of this paper.

How is consent managed?

If you have decided that one of the conditions in Article 6(1) or Article 9(2) other than consent apply to your processing of personal data by the UTM/SWG, then you will not need to obtain consent.

However, if you, as a data controller, determine that obtaining the data subject's consent is the appropriate legal basis for the processing of personal data by the UTM/SWG, you will be responsible for collecting a valid consent as defined by GDPR from each individual whose personal data is collected by the Smoothwall products that you use.

What does GDPR say about children?

Under GDPR and the UK's Data Protection Bill, children under 13 cannot give consent in relation to information society services (which does not apply to the UTM/SWG). Consent in this situation must be given by the person with parental responsibility for a child under 13.

However, as set out above, you may decide that consent is not the appropriate legal basis for processing personal data by the UTM/SWG.

Individual rights

GDPR gives data subjects the following rights:

1. The right to be informed
2. The right of access
3. The right to rectification
4. The right to erasure
5. The right to restrict processing
6. The right to data portability
7. The right to object
8. Rights in relation to automated decision making and profiling

The right to be informed
GDPR requires you as a data controller to provide data subjects with specific information such as who you are, what data you are collecting about them and how you use that data, including the purpose of the processing and the lawful basis for the processing. As an example, Smoothwall's privacy notice for

its Visigo products can be read here. We will provide you with any additional relevant information you need in relation to the processing of personal data by the UTM/SWG, to the extent that it is not already covered in this paper.

You must also include information on how long the personal data will be stored, or if this is not possible, the criteria that will be used to calculate the period for which the data will be stored, for example, one year after a data subject ceases to be a student or an employee as appropriate. You can configure the retention period within the UTM/SWG and you need to ensure that the settings you have configured are accurately reflected in your privacy statements that you provide to data subjects. Please note that it is your responsibility to set appropriate retention periods within the UTM/SWG that you use.

Some features of the UTM/SWG do involve the use of profiling, for example, you can configure the settings to send alerts to nominated individuals within your organisation when a user exceeds certain thresholds, such as trying to access pornographic sites more than 10 times. However, no automated decisions for the purposes of GDPR are made by the UTM/SWG.

The right of access

Individuals have the right to access the personal data which an organisation processes about them. Under GDPR, in most circumstances controllers will no longer be able to charge individuals a fee and will be required to respond to a request within one month.

The UTM/SWG can already provide individual user reports but this is currently summary data. We will be adding services in the Leeds release to extract all log information held within the UTM/SWG products that relate to individuals.

The right to rectification

As the UTM/SWG only collects data that reflects actual events, such as the words and phrases typed into a search engine, it is unlikely that the information we collect would be inaccurate and need to be rectified. The only time where we believe that rectification might be relevant is where someone has been using online services in another person's name - this is currently beyond the scope of anything the UTM/SWG is able to detect.

The right to erasure

The right to erasure or the right to be forgotten, as it is also known, is not an absolute right. As a data controller, you will need to consider each request on an individual basis to determine what, if any, personal data relating to the individual making the request, needs to be deleted. We will be adding services to the UTM/SWG in the Leeds release that will permit the deletion of individual user log information where you, as a data controller, decide that some or all of the information relating to a specific user which we process needs to be deleted.

The right to restrict processing

Data subjects have the right to restrict processing of their personal data where:

- the accuracy of the data is contested by the data subject
- the processing is unlawful and the data subject doesn't want the data to be deleted
- you no longer need the data for the purpose(s) for which it was collected, but the data subject requires the data in relation to a legal claim or
- you are processing the data on the basis of Article 6(1)(f) – legitimate interests and the data subject argues that their rights, interests and freedoms override your legitimate interests.

There is no ability in the UTM/SWG at the moment to restrict processing on a user-by-user basis. We are examining the feasibility of this as a solution, but in the meantime you will need to consider other ways of complying with a request of this nature for example, by providing anonymous (or shared) accounts to users who are entitled to restrict your processing of their data.

The right to data portability

The intention of this right is to allow a user to switch online service providers more easily. It only applies where the processing of personal data is:

- based on consent under Article 6(1)(a) or Article 9(2)(a) or on a contract under Article 6(1)(b) and
- the processing is carried out by automated means.

We anticipate that this will not apply to personal data collected by the UTM/SWG on the basis that our customers will rely on the other conditions for processing available under Article 6(1) and Article 9(2) rather than consent.

If you are relying on consent as the appropriate legal basis and you decide that you need to comply with a request to exercise the right to data portability, the UTM/SWG (in the Leeds release, February 2018) will allow you to extract the relevant information in respect of a specific user in a format which complies with the GDPR requirements.

The right to object

Where you rely on the conditions in Article 6(1)(e) – performance of a task carried out in the public interest or Article 6(1)(f) – legitimate interests, data subjects have the right to object at any time to the processing of their personal data. You will no longer be able to process the data subject's personal data unless you can demonstrate compelling legitimate grounds for the processing which override the rights, interests and freedoms of the individual.

There is no ability in the UTM/SWG at the moment to restrict processing on a user-by-user basis. We are examining the feasibility of this as a solution, but in the meantime you will need to consider other ways of complying with a request of this nature for example, by providing anonymous (or shared) accounts to users who are entitled to restrict your processing of their data.

Rights in relation to automated decision making and profiling
This provides safeguards for data subjects against the risk that a potentially damaging decision which produces legal effects concerning the data subject is taken without human intervention. While the UTM/SWG does provide automated decision making and profiling they result in reports that are designed to be used by humans for decision making. The UTM/SWG therefore does not make any decisions without human intervention. We therefore believe that this right will not apply to the processing of personal data by the UTM/SWG.

Some features of the UTM/SWG do involve the use of profiling, for example, you can configure the settings to send alerts to nominated individuals within your organisation when a user exceeds certain thresholds, such as trying to access pornographic sites more than 10 times. However, no automated decisions for the purposes of GDPR are made by the UTM/SWG.

Further points to consider

An important principle of GDPR is privacy by default or data minimisation which means ensuring that, by default, only personal data which is necessary for the purposes of the processing are processed.

The UTM/SWG only collects:
- the address or URL of any webpage which a user tries to access
- the words entered into a search engine and
- the fact that an attempt to access a restricted site has been made,

and logs this information against the username.

You, as a data controller, have the ability to configure the settings within the UTM/SWG to allocate users to specific user groups, such as a year group at a school. You will need to determine whether allocating users to groups in this way satisfies the requirement to only collect the data which is necessary for the purposes of the processing.

Access to user data must be controlled. Careful configuration of the UTM/SWG's user portal must be made to ensure that only those who should have access specific user data are permitted to do so.

Glossary

Data controller	the person (which may be an individual, a company, a public authority, agency or other body) who alone or jointly with others determines the purposes and means of the processing of personal data
Data processor	a person which may be an individual, a company, a public authority, agency or other body) who processes personal data on behalf of a controller
Data subject	an identified or identifiable living person
Special categories of personal data	• personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs or trade union membership • genetic data, • biometric data for the purpose of uniquely identifying a natural person • data concerning health • data concerning a natural person's sex life or sexual orientation

Conditions for processing under Article 6(1)

Article 6(1)(a)	the data subject has given consent to the processing of their data for one or more specific purposes
Article 6(1)(b)	processing is necessary for the performance of a contract to which the data subject is a party or in order to take steps at the request of the data subject to enter into a contract
Article 6(1)(c)	processing is necessary for compliance with a legal obligation which you, as a data controller, are subject
Article 6(1)(d)	processing is necessary in order to protect the vital interests of the data subject or another individual (i.e. it is a matter of life or death)
Article 6(1)(e)	processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in you as a data controller
Article 6(1)(f)	processing is necessary for the legitimate interests of you as a data controller or a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, particularly where the data subject is a child*

Conditions for processing under Article 9(2)

Article 9(2)(a)	the data subject has given explicit consent to the processing for one or more specified purposes
Article 9(2)(b)	processing is necessary for the purposes of carrying out the obligations and exercising specific rights of you as a data controller or of the data subject in the field of employment and social security and social protection law
Article 9(2)(c)	processing is necessary to protect the vital interests of the data subject or another individual where the data subject is physically or legally incapable of giving consent
Article 9(2)(d)	processing is carried out in the course of the legitimate activities with appropriate safeguards by a foundation, association or other not-for-profit body with a political, philosophical, religious or trade union aim, subject to specific conditions
Article 9(2)(e)	processing relates to personal data which are manifestly made public by the data subject
Article 9(2)(f)	processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity
Article 9(2)(g)	processing is necessary for reasons of substantial public interest, on the basis of EU or UK law
Article 9(2)(h)	processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care treatment or the management of health or social care systems or pursuant to a contract with a healthcare professional
Article 9(2)(i)	processing is necessary for reasons of public health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices
Article 9(2)(j)	processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes

smoothwall

The Web You Want

For further information on any of the items covered in this document, please contact your Smoothwall representative.

www.smoothwall.com
08701 999 500
enquiries@smoothwall.com