Overt Software Solutions Ltd

Client GDPR Data processor processing documentation

Version 1.0.3

Date: 15/06/18

Introduction

The privacy and security of all personal data processed by Overt Software Solutions Ltd is paramount. We welcome the additional protection the General Data Protection Regulation (GDPR) will bring to all EU citizens.

This document explains how we meet the requirements of GDPR as a Data Processor for each of our services. For details on how we meet the requirements of GDPR as a Data Controller, please see the privacy notice at https://www.overtsoftware.com/privacy-policy/.

Data Protection Officer

We aren't required to appoint a Data Protection Officer (DPO) under the GDPR, but we have decided to do so voluntarily. You can contact our DPO with data protection related queries at any time using the following contact details:

Data Protection Officer
Overt Software Solutions Ltd
Unit 2 Hawford Business Centre
Hawford
Worcester
WR3 7SG

Telephone : 01905 886377
Email: dpo@overtsoftware.com

Service Level Agreements with Data Controllers

All of our Service Level Agreements (SLAs) contain our data protection commitments to you, the Data Controller, by us, the Data Processor. These are:

- only act on the written instructions of the controller;
- ensure that people processing the data are subject to a duty of confidence;
- take appropriate measures to ensure the security of processing;
- only engage sub-processors with the prior consent of the controller and under a written contract;
- assist the controller in providing subject access and allowing data subjects to exercise their rights under the GDPR;
- assist the controller in meeting its GDPR obligations in relation to the security of processing, the notification of personal data breaches and data protection impact assessments;
- delete or return all personal data to the controller as requested at the end of the contract; and

- submit to audits and inspections, provide the controller with whatever information it needs to ensure that they are both meeting their Article 28 obligations, and tell the controller immediately if it is asked to do something infringing the GDPR or other data protection law of the EU or a member state.

All SLAs also set out the duration of the processing, the purpose of the processing, the type of personal data and categories of data subject, and the obligations and rights of the Data Controller.

Services

This section shows details on the types of personal data, processing activities, retention periods, sub-processors, how we satisfy user rights and technical and organisational security measures for each of our services.

Overt IdP (Cloud and appliance)

Purpose of processing data

- To provide federated access and Single Sign On to service providers for the Data Controller's end users
- To provide technical support for this service
- If Cloud Overt IdP or encrypted offsite backups purchased
    - To provide backups for disaster recovery scenarios
- If the Overt IdP Dashboard is used
    - To provide a mechanism to allow the Data Controller's service administrators to manage the Overt IdP
    - To provide a mechanism to allow the Data Controller's service administrators to generate end user usage statistics of the Overt IdP

What data is processed?

- The IP address, username, browser version, service provider accessed and time of access for each end user access
- End user attributes required for operation such as username, password, pseudonymised user identifier
- Other end user attributes that may be required by third party service providers (e.g. eduPersonPrincipalName, eduPersonScopedAffiliation, email address, group membership)
- Cookies to maintain session state and user preferences
- If the Overt IdP Dashboard is used
    - Administrator accounts specifying a username, password and email address
    - Optional synchronisation of all users' group memberships

Where is personal data located?

- Cloud Overt IdP
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited
        - Non-EU hosting suppliers:
            - Dediserve Ltd
    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite Overt IdP
    - Located on the Data Controller’s premises or on a data centre of the Data Controller’s choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)
- Your Overt IdP will send personal data to Service Providers (SPs) as configured. The location of this data is dependent on the SPs your organisation subscribes to
    - Only anonymous or pseudonymous data is released by default to service providers
    - Other personal data must be configured to be released to a service provider

Retention periods

Personal data in log files are anonymised after 6 months by default. Log files will be purged after 3 years by default. Both of these periods can be changed on request by the Data Controller.

Our soon to be released Overt IdP Dashboard will allow the Data Controller to make these changes themselves at any time.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Current methods	Future methods
The right to be informed	**Privacy notice display** We can add a link to a privacy notice on every page on your Overt IdP (e.g. login, logoff, error pages) on the Data Controller's behalf The information provided in this document will help you create an applicable privacy notice for this service We can configure this feature for you on receipt of a privacy policy **Terms of Use feature** If you have determined consent is required on the IdP itself, you can address the issue of ensuring users are aware of your privacy policy and gaining opt-in consent by requiring the end user to agree to the privacy policy (or other terms of use) before they can login for the first time. This solution will also provide a consent audit trail as required by GDPR We can configure this feature for you on request **Attribute Release Consent feature** The attribute release consent feature of the Overt IdP provides a transparent mechanism for the user to control what attributes are being sent to a Service Provider (SP) when they login. This feature also allows users to refuse to send specific data to a service provider. Attribute release consent can be setup to apply to	Our soon to be released Overt IdP Dashboard will allow the Data Controller to make changes to their Overt IdP's privacy policy, Terms of Use and Attribute Release Consent features themselves through a user friendly interface

	all SPs or you may prefer to reduce the friction of the user login flow by only presenting the attribute release consent form where non-anonymous, non-pseudonymous attributes or specific SPs are used We can configure this feature for you on request	
The right of access	We can extract any user data on request by the Data controller in a user friendly format (e.g. PDF) If you are using our IdMTool, then the designated administrators at the Data Controller organisation can extract user data through the IdMTool's user friendly interface	Our soon to be released Overt IdP Dashboard will allow the Data Controller to resolve Subject Access Requests themselves through a user friendly interface
The right to rectification	If the attribute source is maintained by the Data Controller (e.g. Active Directory or Azure) then this must be performed by the Data Controller If you are using our IdMTool, then the designated administrators at the Data Controller organisation can make these changes through the IdMTool's user friendly interface	The IdMTool will optionally provide end users the ability to update some of the data held about them (e.g. first name, surname etc)
The right to erasure	We can erase any user data on request by the Data controller If you are using our IdMTool, then the designated administrators at the Data Controller organisation can delete user accounts through the IdMTool's user friendly interface Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days	Our soon to be released Overt IdP Dashboard will allow the Data Controller to erase personal data for a specific user held in log files on the Overt IdP themselves through a user friendly interface. Future logon events for the specified user will also be erased automatically

The right to restrict processing	**Disable account** If the attribute source is maintained by the Data Controller (e.g. Active Directory or Azure) then this can be performed by the Data Controller by disabling the user's account If you are using our IdMTool, then the designated administrators at the Data Controller organisation can disable user accounts through the IdMTool's user friendly interface **Filtering out users** We can configure different filtering rules to filter out specific users on request **Attribute Release Consent** The Attribute Release Consent feature explained above can be utilised to restrict processing	Our soon to be released Overt IdP Dashboard will allow the Data Controller to configure filter rules and Attribute Release Consent on their Overt IdP themselves through a user friendly interface
The right to data portability	We can extract any user data on request by the Data controller in a machine friendly format (e.g. CSV) If you are using our IdMTool, then the designated administrators at the Data Controller organisation can extract user data through the IdMTool's user friendly interface	Our soon to be released Overt IdP Dashboard will allow the Data Controller to resolve data portability requests themselves through a user friendly interface
The right to object	**Disable account** If the attribute source is maintained by the Data Controller (e.g. Active Directory or Azure) then this can be performed by the Data Controller by disabling the user's account If you are using our IdMTool, then the designated administrators at the Data Controller organisation can disable user accounts	See the "Future Methods" for "The right to erasure"

	through the IdMTool's user friendly interface **Filtering out users** We can configure different filtering rules to filter out specific users on request **Attribute Release Consent** The Attribute Release Consent feature explained above can be utilised to restrict processing	
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	No automated decision making takes place	No automated decision making will take place. However, our soon to be released Overt IdP Dashboard will allow the Data Controller to manually generate granular usage statistics via a user friendly interface. This solution allows administrators at the Data Controller organisation to filter on specific users (disabled by default) and other specific user attributes such as group membership. The administrator may manually derive decisions from this, such as cancelling a Service Provider subscription for a specific user group. We do not see this mechanism falling under the automated decision-making process. That said, if this profiling is challenged by a specific end user, their records can always be erased from all log files as explained in “The right to erasure” method. This results in their data not being available when generating statistics

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework

- Where the Data Controller holds the authentication and attribute stores (e.g. Active Directory, Microsoft Azure), all end user personal data is stored external to the Overt IdP instance except for log entries
- Only the minimal set of attributes are retrieved from the Data controller's authentication and attribute stores (e.g. Active Directory)
- Only anonymous or pseudonymised data is released to Service Providers by default
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and the Cloud Overt IdP and Overt IdP services are encrypted using TLS following industry best practices for cipher selection
- All communications between the Cloud Overt IdP and the authentication and attribute stores (e.g. Active Directory) utilising our Overt-ADLink solution is encrypted using AES 128 or AES 256
- Optional user lockout feature to mitigate common brute force login attacks
- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Administrator accounts of the Overt IdP Dashboard utilise encrypted passwords following industry best practice
- The IdMTool encrypts user passwords following industry best practice
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Shibboleth Service Provider

Purpose of processing data

- To provide a Shibboleth Service Provider (SP) service
- To provide technical support for this service
- If the service is hosted on our cloud or if encrypted offsite backups purchased
  - To provide backups for disaster recovery scenarios

What data is processed?

- The IP address, Identity Provider, Name Identifier, name of attributes retrieved and time of access for each user logon or logout event
- End user attributes sent by the end user's Identity Provider, such as a pseudonymised user identifier, eduPersonScopedAffiliation. Depending on the underlying web application utilising the Shibboleth SP, there may be more attributes processed
- Cookies to maintain session state

Where is personal data located?

- If the service is hosted on our cloud:
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited
        - Non-EU hosting suppliers:
            - Dediserve Ltd
            - ReliableSite.Net LLC
    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite
    - Located on the Data Controller's premises or on a data centre of the Data Controller's choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)

Retention periods

Log files will be purged after they become 20MB in total size by default (20 x 1MB files). This roughly equates to a total of 20,000 logon events being recorded on a typical setup. These limits can be changed on request by the Data Controller.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Methods
The right to be informed	You can add a link to a privacy notice on every page of your web site which utilises the Shibboleth SP software

	The information provided in this document will help you create an applicable privacy notice for this service
The right of access	We can extract any user data contained within the Shibboleth SP logs on request by the Data controller in a user friendly format (e.g. PDF)
The right to rectification	N/A - The SP does not provide the source for any data. Rectifications must be made at the IdP or web application
The right to erasure	We can erase any user data from the SP log files on request by the Data controller Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days
The right to restrict processing	The simplest way to restrict access for a specific user is for the IdP to prevent the user accessing the SP whilst the restriction is in place Web server or web application access rules may be used to limit who can access the web application. However, the Shibboleth SP will still process the required data sent to it by an IdP
The right to data portability	We can extract any user data contained within the Shibboleth SP logs on request by the Data controller in a machine friendly format (e.g. CSV)
The right to object	The simplest way to achieve this is for the respective IdP to prevent the user accessing the SP Web server or web application access rules may be used to limit who can access the web application. However, the Shibboleth SP will still process the required data sent to it by an IdP
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	No automated decision making takes place unless configured by the Data Controller

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Only the minimal set of attributes are accepted from IdPs, non standard attributes are added on request from the Data Controller
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and the Shibboleth SP service are encrypted using TLS following industry best practices for cipher selection
- All communications between the SP and IdPs are encrypted using TLS following industry best practices for cipher selection
- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Shibboleth ADFS/Azure AD Authentication Module

The Shibboleth ADFS/Azure AD Authentication Module (SAAM) utilises both the Overt IdP and Shibboleth SP components. All relevant information is therefore contained within those two sections of this document.

EZProxy

Purpose of processing data

- To provide an EZProxy service
- To provide technical support for this service
- If hosted on our Cloud or if encrypted offsite backups purchased
    - To provide backups for disaster recovery scenarios

What data is processed?

- The IP address, the resource accessed and time of access for each request
- End user attributes sent by the end user’s Identity Provider, such as a pseudonymised user identifier, eduPersonScopedAffiliation. Depending on the configuration of connecting IdPs and EZProxy, there may be additional attributes processed
- Cookies to maintain session state

Where is personal data located?

- If the service is hosted on our cloud:
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited
        - Non-EU hosting suppliers:
            - Dediserve Ltd
    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite
    - Located on the Data Controller’s premises or on a data centre of the Data Controller’s choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)

Retention periods

Log files will be purged after 1 year by default. These limits can be changed on request by the Data Controller.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Methods
The right to be informed	You can add a link to a privacy notice on EZProxy’s web pages The information provided in this document will help you create an applicable privacy notice for this service

The right of access	We can extract any user data contained within the Shibboleth SP logs on request by the Data controller in a user friendly format (e.g. PDF)
The right to rectification	N/A - EZProxy does not provide the source for any data. Rectifications must be made at the IdP or web application
The right to erasure	We can erase any user data from the EZProxy log files on request by the Data controller Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days
The right to restrict processing	The simplest way to restrict access for a specific user is for the IdP to prevent the user accessing EZProxy whilst the restriction is in place EZProxy access rules may be used to limit who can access resources. However, EZProxy will still process the required data sent to it by an IdP to authorisation decisions
The right to data portability	We can extract any user data contained within theEZProxy logs on request by the Data controller in a machine friendly format (e.g. CSV)
The right to object	The simplest way to achieve this is for the respective IdP to prevent the user accessing EZProxy
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	No automated decision making takes place

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Only the minimal set of attributes are accepted from IdPs, non standard attributes are added on request from the Data Controller
- Retention of log entries can be customised to ensure they are kept for only as long as required

- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and the EZProxy service are encrypted using TLS following industry best practices for cipher selection
- All communications between EZProxy and IdPs are encrypted using TLS following industry best practices for cipher selection
- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Moodle (Cloud and onsite)

Purpose of processing data

- To provide a Moodle platform for the Data Controller's end users
- To provide technical support for this service
- If hosted on our Cloud or if encrypted offsite backups purchased
    - To provide backups for disaster recovery scenarios

What data is processed?

- The IP address, browser version, page accessed and time of each access to the site
- End user attributes required for operation such as username and email address
- Other end user attributes configured or approved by the Data Controller such as firstname, surname, city
- History of individual's activity within Moodle, e.g. course and resource access stating times
- If Moodle enrolment data is sourced from an external Management Information System (MIS)
    - Unique student IDs and associated course codes
- Cookies to maintain session state and user preferences
- Personal data provided by the end users themselves
- Personal data provided by the Data Controller

Where is personal data located?

- If the service is hosted on our cloud:
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited

    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite
    - Located on the Data Controller’s premises or on a data centre of the Data Controller’s choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)

Retention periods

Personal data in web server log files will be purged after 4 weeks by default. This period can be changed on request by the Data Controller.

Retention periods of data within Moodle, such as Moodle’s own logs, backups, courses and resources are controlled by the Data Controller. We can assist with this configuration if required.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Method
The right to be informed	By May 25th 2018, Moodle 3.3.5+ will provide a new user sign on process, with ability to define multiple policies (site, privacy, third party), track user consents, and manage updates and versioning of the policies The information provided in this document will help you create an applicable privacy notice for this service
The right of access	By May 25th 2018, Moodle 3.3.5+ will implement the workflow for users to submit subject access requests and for site administrators and privacy officers to process these requests

The right to rectification	Users can edit their data themselves when logged on. By May 25th 2018, Moodle 3.3.5+ will implement the workflow for users to submit data modification requests and for site administrators and privacy officers to process these requests
The right to erasure	By May 25th 2018, Moodle 3.3.5+ will implement the workflow for users to submit data erasure requests and for site administrators and privacy officers to process these requests Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days
The right to restrict processing	Users can remove consent or request to have their personal data erased if they wish to restrict processing
The right to data portability	By May 25th 2018, Moodle 3.3.5+ will implement the workflow for users to submit subject access requests and for site administrators and privacy officers to process these requests
The right to object	Users can remove consent or request to have their personal data erased if they object
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	No automated decision making takes place

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Only the minimal set of attributes are retrieved from the Data controller's authentication and attribute stores (e.g. Shibboleth, Active Directory)
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and Moodle are encrypted using TLS following industry best practices for cipher selection

- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Mahara

Purpose of processing data

- To provide a Mahara platform for the Data Controller's end users
- To provide technical support for this service
- If hosted on our Cloud or if encrypted offsite backups purchased
    - To provide backups for disaster recovery scenarios

What data is processed?

- The IP address, browser version, page accessed and time of each access to the site
- End user attributes required for operation such as username, first name, lastname and email address
- Other end user attributes configured or approved by the Data Controller
- History of individual's activity within Mahara, e.g. artefact modifications stating times
- Cookies to maintain session state and user preferences
- Personal data provided by the end users themselves
- Personal data provided by the Data Controller

Where is personal data located?

- If the service is hosted on our cloud:
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited
    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite
    - Located on the Data Controller's premises or on a data centre of the Data Controller's choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)

Retention periods

Personal data in web server log files will be purged after 4 weeks by default. This period can be changed on request by the Data Controller.

Retention periods of data within Mahara, such as Maraha's own event logs are controlled by the Data Controller. We can assist with this configuration if required.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Method
The right to be informed	Mahara 18.04+ can be configured to display a privacy statement and obtain consent to the terms and conditions and the privacy statement of the site The information provided in this document will help you create an applicable privacy notice for this service
The right of access	Mahara allows users to export their data to HTML format
The right to rectification	Users can edit their data themselves when logged on
The right to erasure	Mahara 18.04+ allows users to delete their own account Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days
The right to restrict processing	Mahara 18.04+ allows users to remove consent or delete their own account

The right to data portability	Mahara allows users to export their data to Leap2A standard format
The right to object	Mahara 18.04+ allows users to remove consent or delete their own account
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	No automated decision making takes place

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Only the minimal set of attributes are retrieved from the Data controller's authentication and attribute stores (e.g. Shibboleth, Active Directory)
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and Mahara are encrypted using TLS following industry best practices for cipher selection
- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Wordpress

Purpose of processing data

- To provide a Wordpress platform for the Data Controller's end users
- To provide technical support for this service

- If hosted on our Cloud or if encrypted offsite backups purchased
    - To provide backups for disaster recovery scenarios

What data is processed?

- The IP address, browser version, page accessed and time of each access to the site
- End user attributes required for operation such as username, first name, lastname and email address
- Other end user attributes configured or approved by the Data Controller
- Cookies to maintain session state and user preferences
- Personal data provided by the end users themselves
- Personal data provided by the Data Controller

Where is personal data located?

- If the service is hosted on our cloud:
    - One of the following for hosting:
        - UK hosting suppliers:
            - RapidSwitch (iomart Hosting Ltd)
            - UK Dedicated Servers Limited
    - The following to store encrypted offsite backups
        - Hetzner Online GmbH (EU)
- Onsite
    - Located on the Data Controller’s premises or on a data centre of the Data Controller’s choosing
    - If encrypted offsite backups service purchased
        - Hetzner Online GmbH (EU)
- Some third party plugins may store data elsewhere (plugins are only installed if requested by the Data Controller)

Retention periods

Personal data in web server log files will be purged after 4 weeks by default. This period can be changed on request by the Data Controller.

Depending on the plugins installed, some retention periods of data within Wordpress may be controlled by the Data Controller. We can assist with this configuration if required.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Method
The right to be informed	Data Controllers can provide a privacy notice on their Wordpress site. By May 25th 2018, tools will be available to assist in privacy policy creation within Wordpress The information provided in this document will help you create an applicable privacy notice for this service
The right of access	By May 25th 2018, tools will be available to assist end users and Data Controllers within Wordpress to fulfill these requests
The right to rectification	Users can edit their data themselves when logged on
The right to erasure	By May 25th 2018, tools will be available to assist end users and Data Controllers within Wordpress to fulfill these requests Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days
The right to restrict processing	By May 25th 2018, tools will be available to assist end users and Data Controllers within Wordpress to fulfill these requests
The right to data portability	By May 25th 2018, tools will be available to assist end users and Data Controllers within Wordpress to fulfill these requests
The right to object	By May 25th 2018, tools will be available to assist end users and Data Controllers within Wordpress to fulfill these requests
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	The Data Controller will be responsible for these requests if this is applicable

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Only the minimal set of attributes are retrieved from the Data controller’s authentication and attribute stores (e.g. Shibboleth, Active Directory)
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- All communications between the end user and Wordpress are encrypted using TLS following industry best practices for cipher selection
- When hosted on our cloud or when backup services are purchased, backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff

Hosting (managed Infrastructure as a Service)

Purpose of processing data

- To provide a hosting platform for the Data Controller
- To provide support for the hosting platform and operating system
- To provide backups for disaster recovery scenarios

What data is processed?

- Personal data provided by the Data Controller
- Personal data provided by the end users themselves

Where is personal data located?

- UK hosting suppliers:
  - RapidSwitch (iomart Hosting Ltd)
  - UK Dedicated Servers Limited
- Non-EU hosting suppliers:
  - Dediserve Ltd
  - ReliableSite.Net LLC (US)

- The following to store encrypted offsite backups
    - Hetzner Online GmbH (EU)

Retention periods

The Data Controller has full control of the system so retention periods are configured by the Data Controller. We can assist with some retention configuration queries, but this is dependent on the services running on the system.

Sub-processors

The only sub-processors used are those which provide hosting hardware and infrastructure. They can only access our systems at our request to resolve underlying hardware issues.

- UK hosting supplier: RapidSwitch (iomart Hosting Ltd)
- UK hosting supplier: UK Dedicated Servers Limited
- EU hosting supplier: Hetzner Online GmbH

Our non-EU hosting suppliers are not classed as sub-processors as they have no access to our systems, they just supply the hardware and infrastructure.

How we satisfy individual user rights

User right	Method
The right to be informed	The Data Controller has full control of the system, so can add privacy statements where deemed necessary The information provided in this document will help you create an applicable privacy notice for this service
The right of access	The Data Controller has full control of the system so can fulfill these requests itself. We can assist with some subject access requests, but this is dependent on the services running on the system
The right to rectification	The Data Controller has full control of the system so can fulfill these requests itself
The right to erasure	The Data Controller has full control of the system so can fulfill these requests itself. We can assist with some erasure requests, but this is dependent on the services running on the system Note that we provide data recovery backups on our hosted solutions and when purchased separately. Personal data will still exist in these backups until the retention period has passed. This is typically 7 days

The right to restrict processing	The Data Controller has full control of the system so can fulfill these requests itself. We can assist with some processing restriction requests, but this is dependent on the services running on the system
The right to data portability	The Data Controller has full control of the system so can fulfill these requests itself. We can assist with some data portability requests, but this is dependent on the services running on the system
The right to object	The Data Controller has full control of the system so can fulfill these requests itself. We can assist with some processing objection requests, but this is dependent on the services running on the system
The right not to be subject to automated decision making including profiling (automated processing of personal data to evaluate certain things about an individual)	The Data Controller has full control of the system so can fulfill these requests itself if applicable

Technical and organisational security measures

Some of the measures we use to secure your personal data are:

- We are Cyber Essentials accredited, a UK Government backed security framework
- Retention of log entries can be customised to ensure they are kept for only as long as required
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- We can provide free SSL certificates to allow all communications between the end user and server applications capable of using TLS to encrypt data using TLS following industry best practices for cipher selection
- Backups are performed frequently to a different data centre, encrypted in transit and at rest (AES 256) and tested regularly
- Software security fixes are implemented promptly
- We configure our systems and applications following industry best practice to help mitigate intrusion
- All cloud hosted systems receive regular security scans
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff