Overt Software Solutions Ltd

Client GDPR Data processor processing documentation

Version 1.0.12

Date: 03/05/22

Introduction

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

This document explains how we meet the requirements of UK and EU GDPR as a Data Processor for each of our services.

Note that this document does not constitute a contract. For further details please see our dedicated Security and Data Protection page at https://www.overtsoftware.com/security-and-data-protection/.

Data Protection Officer

You can contact our Data Protection Officer (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 955037
Email: dpo@overtsoftware.com

Data Processing Agreements with Data Controllers

Our Data Processing Agreements (DPA) contain our data protection commitments to you, the Data Controller, by us, the Data Processor. The following is a high level view of these commitments:

- 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 UK, EU or a member state.

Clients can view the DPA and see how to request a signed copy at https://www.overtsoftware.com/security-and-data-protection/.

For the avoidance of doubt, our DPA takes precedence over the information in this document.

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
    - Optional live support chat requesting name and email address (only if you request support via this feature)

Where is personal data located?

See the DPA.

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 periods can be changed on request by the Data Controller or by using the Overt IdP dashboard interface.

Sub-processors

See the DPA.

How we satisfy individual user rights

User right	Current 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 or you can change it through the Overt IdP dashboard interface. **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 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). Alternatively, you can query user data held in logs through the Overt IdP dashboard interface. If you are using our IdMTool (our optional user management service for clients without an existing onsite user store), then the designated administrators at the Data Controller organisation can extract user data through the IdMTool's 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 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
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. Alternatively, you can configure filtering rules yourself through the Overt IdP dashboard interface **Attribute Release Consent** The Attribute Release Consent feature explained above can be utilised to restrict processing

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). Alternatively, you can query user data held in logs through the Overt IdP dashboard interface. 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
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 through the IdMTool's user friendly interface **Filtering out users** We can configure different filtering rules to filter out specific users on request. Alternatively, you can configure filtering rules yourself through the Overt IdP dashboard interface **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

Technical and organisational security measures

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

- We are Cyber Essentials Plus 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
- All data is securely erased on termination of all services

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?

See the DPA.

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

See the DPA.

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 Plus 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
- All data is securely erased on termination of all services

Shibboleth ADFS/Azure AD Authentication Module

The Shibboleth ADFS/Azure AD Authentication Module (SAAM) utilises the Overt IdP service and optionally the Shibboleth SP service. 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?

See the DPA.

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

See the DPA.

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 the EZProxy 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 Plus 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
- All data is securely erased on termination of all services

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?

See the DPA.

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

See the DPA.

How we satisfy individual user rights

User right	Method
The right to be informed	Administrators can 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	Users can submit subject access requests and site administrators and privacy officers can process these requests
The right to rectification	Users can edit their data themselves when logged on. Users can also submit data modification requests and site administrators and privacy officers can process these requests
The right to erasure	Users can submit data erasure requests and site administrators and privacy officers can 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	Users can submit subject access requests and site administrators and privacy officers can 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 Plus 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
- All data is securely erased on termination of all services

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?

See the DPA.

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

See the DPA.

How we satisfy individual user rights

User right	Method
The right to be informed	Mahara 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 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 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 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 Plus 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
- All data is securely erased on termination of all services

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?

See the DPA.

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

See the DPA.

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. WordPress also has a feature assisting in privacy policy creation. The information provided in this document will help you create an applicable privacy notice for this service
The right of access	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to rectification	Users can edit their data themselves when logged on

The right to erasure	WordPress has features built-in to assist end users and Data Controllers 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	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to data portability	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to object	WordPress has features built-in to assist end users and Data Controllers 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 Plus 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)
∉ All WordPress instances use a reputable Web Application Firewall
∉ 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
- All data is securely erased on termination of all services

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?

See the DPA.

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

See the DPA.

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 Plus 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
- All data is securely erased on termination of all services

Overt MFA/SSPR (Cloud and appliance)

Purpose of processing data

- To provide multi-factor authentication solution for the Data Controller’s end users and service administrators
- To provide a self-service password reset solution for the Data Controller’s end users and service administrators
- 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, username, browser version and time of access for each service access request
- Data entered by the end user themselves may include:
    - Personal phone numbers for SMS one time passwords
    - Personal email address for email one time passwords
    - Answers to challenge questions for password resets
    - New passwords – these are not stored within the system itself
- Cookies to maintain session state and user preferences

Where is personal data located?

See the DPA.

Retention periods

Log files will be purged after 6 months by default. This period can be changed on request by the Data Controller.

Sub-processors

See the DPA.

How we satisfy individual user rights

User right	**ethod**

The right to be informed	There is a privacy policy link at the bottom of every page and directly placed on forms where personal data may be entered (e.g. phone number for an SMS token)
The right of access	We can extract any user data on request by the Data controller in a user friendly format (e.g. PDF)
The right to rectification	If the attribute source is maintained by the Data Controller (e.g. Active Directory or Azure) then some rectification processes will need to be performed by the Data Controller Other data within the portal can be rectified by the user themselves or by Overt Software on request by the Data controller
The right to erasure	We can erase any user data 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, albeit in an encrypted form, until the retention period has passed. This is typically 7 days
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 **Filtering out users** We can configure different filtering rules to filter out specific users from this service on request
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)
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 **Filtering out users** We can configure different filtering rules to filter out specific users from this service on request
The right not to be subject to automated decision making including profiling (automated processing of personal data to	No automated decision making takes place

evaluate certain things about an individual)	

Technical and organisational security measures

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

- We are Cyber Essentials Plus accredited, a UK Government backed security framework
- Where the Data Controller holds the authentication and attribute stores (e.g. Active Directory), most end user personal data is stored external to the Overt MFA/SSPR instance except for MFA token data, password challenge response answers and log entries
- Only the minimal set of attributes are retrieved from the Data controller’s attribute stores (e.g. 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 the Overt MFA/SSPR services are encrypted using TLS following industry best practices for cipher selection
- All communications between the Overt MFA/SSPR and the authentication and attribute stores (e.g. Active Directory) utilising our Overt-ADLink solution is encrypted using AES 128 or AES 256 in addition to the encryption provided by the LDAPS connection
- Optional MFA request lockouts/throttling 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 MFA/SSPR service utilise encrypted passwords following industry best practice
- Answers to challenge questions are encrypted using PBKDF2 and SHA512
- 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
- All data is securely erased on termination of all services
- The service is monitored 24/7. Alerts will be triggered to notify support engineers where appropriate

EZPZ SP

Purpose of processing data

∉ To provide a SAML Service provider service

∉ To provide technical support for this service

What data is processed?

∉ The value of attributes retrieved from the SAML IdP (e.g. username and email address) will be stored in the corresponding user account in the WordPress instance's database

Where is personal data located?

- Located on the Data Controller's premises or on a data centre of the Data Controller's choosing

Retention periods

The retention of data will be dependent on how the Data Controller manages their users in the WordPress database.

Sub-processors

There are no sub-processors.

How we satisfy individual user rights

User right	Methods
The right to be informed	Data Controllers can provide a privacy notice on their Wordpress site to include the use of username and email address to allow the site to function correctly. WordPress also has a feature assisting in privacy policy creation.
The right of access	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to rectification	Users can edit their data themselves when logged on, however if the username or email address is coming from an external Identity Provider, the data must be rectified by the owner of that service.
The right to erasure	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to restrict processing	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests

The right to data portability	WordPress has features built-in to assist end users and Data Controllers to fulfill these requests
The right to object	WordPress has features built-in to assist end users and Data Controllers 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 Plus accredited, a UK Government backed security framework
- Our staff only access personal data when requested by the Data Controller to resolve a support query
- Software security fixes are implemented promptly
- We have clear security and privacy policies and regularly perform security awareness and privacy training for all staff