Data Security Policy

November 2022

Version v171122

www.adaptive.co.uk

dataprotection@adaptive.co.uk

Tel: 0800 321 3187

This document is subject to change without notice. The latest version of this policy can be found at www.adaptive.co.uk/policies

Contents

Scope of this document

This document discussed data security in two distinct areas:

1. Overview of GDPR
2. Security of data between the user's browser and the web server; this is covered in the section on SSL certificates
3. Security of the data on the web server and who has access to it.
4. Cookies

GDPR Overview

The General Data Protection Regulation (GDPR) came into effect on 25 May 2018. Among its many provisions it requires that Data Controllers and Data Processors make all reasonable efforts to keep personally identifiable data secure and only available to those with a legitimate reason for access. Additionally, certain types of data are deemed 'sensitive' and require extra levels of protection; these data types include:

- race;
- ethnic origin;
- politics;
- religion;
- trade union membership;
- genetics;
- biometrics (where used for ID purposes);
- health;
- sex life; or
- sexual orientation.

If your site records this sort of personally identifiable user data get in touch to see what solutions are available to ensure you remain GDPR compliant.

SSL certificates

What is SSL?

SSL is the standard security technology for establishing an encrypted link between a web server and a browser. This link ensures that all data passed between the web server and browser remain private. When active, this shows in your browser it two ways:

The URL of your website will begin with https:// rather than the non-encrypted http://

There will be a closed padlock icon next to the address to show the connection is secure

Having an SSL certificate for your site is desirable for several reasons:

- A certificate can help verify ownership of the domain
- Google will rank your site higher in search results if it is using SSL
- Chrome and other browsers now flag websites as insecure if they do not use SSL.
- Data transmitted between the browser and server will be encrypted. Anyone intercepting this data will be unable to determine its contents or the URLs of pages being requested

Please get in touch to discuss adding an SSL certificate to your site.

Sites hosted in Pantheon come with SSL for all environments as standard.

Drupal data security

Database security

Data for Drupal websites is held in a database using MySQL database server software. This server may be running on the same physical computer as the rest of the website, or it may be on a separate machine, but on the same network. In both cases, firewall rules prevent any direct connection from the outside world; the only connections permitted are to the web server running your site and the database administration tools on Adaptive's internal network.

In addition to these measures, good practice dictates that unique usernames and complex passwords are used per site, which give access only single databases on the main database server.

Access to your website's database is limited to the developers working on your site. If required, for example where you are storing sensitive personally identifiable data, we can arrange for developers to work with anonymised versions of your database. Please let us know if you think this is necessary.

Password security

Drupal does not store users' passwords in its database. Instead, the password is combined with a random text string (called a 'salt') that is unique to the given installation of Drupal. This value is then run through a one-way encryption function (called 'hashing') over sixteen thousand times to generate a final random text string (called a 'hash value'). When you attempt to log in again, the password you supply is run through the same function to see if it matches the stored value - if it does, your login will be successful.

It is infeasible to reverse this process to determine the original password from the stored hash value. Also, due to each installation of Drupal having its own unique salt value, the same password on two different sites will result in very different hash values.

This also explains why there is no password recovery option in Drupal, only a password reset function, as it is impossible to reverse the process to recover the password from the hashed value stored in the database.

It should be noted that the above is only effective when complex, hard-to-guess passwords are used and you don't use the same password on other sites where password security may not be as stringent! You can check whether any accounts associated with your email address have been compromised by doing a lookup at this site: https://haveibeenpwned.com/

General data security

When accessing data through the site administration system, Drupal's role and permission system comes into play. Each user is assigned one or more roles; each role has a set of attached permissions that determine which types of data a user is able to read, edit or delete. Additionally, there may be workflows in place that allow certain user roles to create or edit content, but not publish it - this requires the permission of a higher user role.

Cookies

Under the GDPR cookie requirements have changed since the the EU Cookie Directive came into play. Previously it was enough to inform users that cookies were being placed and by continuing to use the site this implied consent. Some cookies are now considered personally identifiable information and are subject to the same explicit, informed consent requirements data captured through other means, such as forms. There are some exemptions to these rules: functional cookies required for the technical operation of a site do not require a user's consent. For example, cookies that store the login state for a user's account.

For cookies containing personally identifiable information, for example Google Analytics tracking cookies, you are now required to inform users that these are being placed and both allow them to decline consent and withdraw this consent at any point as easily it was given.

The preferred solutions for managing cookie consent on websites are Cookiebot or CivicUK.

References:

- https://www.itgovernance.eu/blog/en/how-the-gdpr-affects-cookie-policies
- https://eugdprcompliant.com/cookies-consent-gdpr/
- http://www.dmnews.com/retail-week/gdpr-cookies-personal-data/article/738977/

Data Protection Representative

Adaptive's data protection officer is Dan Frost, dataprotection@adaptive.co.uk

Our ICO registration number is ZA371181.

Risk assessments

You should undertake a risk assessment for any personally identifiable data you gather, whether through your website or by other means.

For more information of data risk assessments see https://ico.org.uk/for-organisations/resources-and-support/data-protection-self-assessment/

Data breach process

Our clients, as data controllers, must have their own data breach policy and processes to be GDPR compliant. Adaptive's own data breach is available at www.adaptive.co.uk/policies

For more information on reporting data breaches see https://ico.org.uk/for-organisations/report-a-breach/

Data transfers

For transferring personal data to our clients or third parties we use WeTransfer, an EU based secure file transfer service. All files are secured by a password when the download link is sent. We strongly encourage all clients to use this, or a similar EU-based service, for sending any personal data to us.

For more information on WeTransfer's privacy policy see https://wetransfer.com/legal/privacy

Data retention policies and timescales

You must advise us how long you wish to retain data and of any criteria used to remove data. By default, we have a rolling 7 day backup policy of data and code.

Website hosting

All our websites are hosted either with Amazon Web Services in their Dublin data Centre, Pantheon in their Netherlands data centre, or with Platform.sh in their UK data centre.

For more information about their respective data security and GDPR compliance see:

- AWS: https://aws.amazon.com/compliance/gdpr-center/
- Pantheon: https://pantheon.io/security
- AWS: https://d1.awsstatic.com/whitepapers/Security/AWS_Security_Whitepaper.pdf
- Platform.sh security and compliance: https://docs.platform.sh/security.html