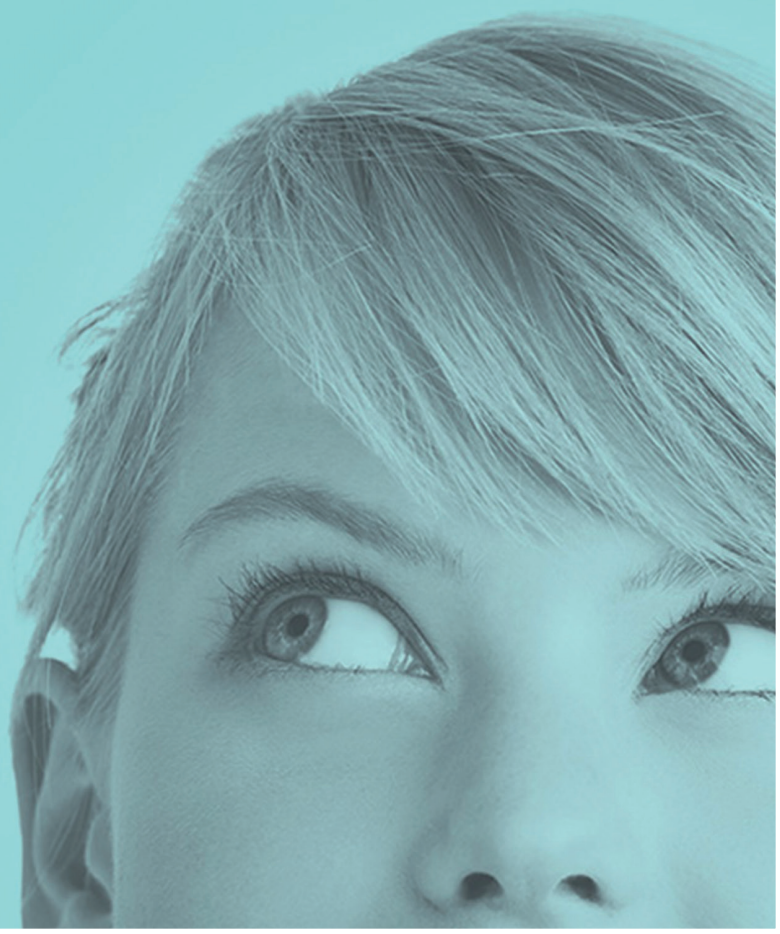
ASP Data, Security and GDPR Update

2018



CYBER ESSENTIALS

IASME Consortium®

ASP Data, Security and GDPR Update

GDPR is a regulation from the EU. It applies to the data collected and/or stored on all European Union citizens regardless of where the company collecting the data resides.

GDPR comes into effect on the 25th May 2018.

I'M IN USA/ME/AFRICA/REST OF THE WORLD SO THIS DOESN'T APPLY TO ME?

If you collect data on EU citizens or residents then it does apply to you. However, how the EU will enforce this remains to be seen.

WHO IS ASP?

ASP Solutions Ltd, a company registered in England : Company Number 03459973. Head office is at No1 Croydon, 12-16 Addiscombe Road, Croydon, CR0 0XT.

We've been are registered with the UK Information Commissioners Office (ICO) since 2002 : Z6573774.

We also have an office in the United States, ASP Inc at 2764 N. Green Valley Pkwy, #552, Henderson, NV, 89014-2120.

HOW DOES ASP ENSURE PERSONAL DATA IS DEALT WITH CORRECTLY?

ASP holds a Cyber Essentials and IASME GDPR Readiness certificate. Cyber Essentials is a UK Government backed scheme.

We operate our own data and security policies and processes.

We operate a multi-tier security approach to data security to protect against DDoS, hacking, theft/loss etc. Multiple off location back-ups are employed. ASP holds security policy reviews twice a year and report any issues to the management team on a weekly basis. We adhere to privacy and security by design best practices.

WHERE IS ASP'S CLIENT DATA HELD?

With various, security verified, ISPs – all data is stored in Ireland or the UK – within the EEA.

WHAT PERSONAL DATA DOES ASP HOLD?

We have assessed and rated the risk and sensitivity of data. We do not store children's data, nor data of a sensitive nature. There is a caveat to this though: Our CMS SHOWOFF, enables clients to create forms, so in theory they could collate such data. However, part of system training covers this, and we ask that clients inform us if this is required. Overall though the personal data we store tends to be: Name, address & email address. Although our systems can record IP addresses for security reasons (anonymised), for tracking purposes we do not track the IP address or associate to a person.

Clients can use third party marketing tags and web analytics – we do not have access to any personal data held in those.

We encourage our clients to record the minimum amount of personal data necessary.

DOES ASP HAVE A SECURITY RESPONSE PLAN POLICY?

Yes. A response team is established, the threat mitigated and affected parties informed ASAP. The ICO will be informed within 72 hours if required.

WHAT SECURITY AND DATA (GDPR) TRAINING DO YOUR STAFF RECEIVE?

All staff attend a workshop and are tested afterwards. Negligence is a potential disciplinary issue.

WHAT MAKES UP ASP'S SECURITY POLICY?

We have many policies including:

- Acceptable Use
- Clean Desk Policy
- Data Breach Response Policy
- Data Destruction Policy
- Data Protection Impact Assessments
- Email Policy
- Ethics Policy
- Firewall Policy & Log
- GDPR Policy
- IT Equipment Disposal Policy
- Password Policy
- Remote Access Policy
- Removable Media Policy
- Security Response Plan Policy
- Server Policy
- Software Installation Policy
- Strong Passwords Guidelines
- Vulnerability Scanning Policy
- WAF Policy
- Wi-Fi Policy
- Wi-Fi Standard
- Workstation & PC Security Policy.

All policies have been written by the CTO and approved by the CEO. As a rule, we do not share our security policies.

ASP IS A DATA PROCESSOR ON BEHALF OF CLIENTS.

Ultimately, we do not decide how the data is used. Our clients are the data controllers. Our CMS collates the data and the client uses it. We store data securely within the EEA and offer general GDPR advice to our clients regarding our SHOWOFF CMS. Our CMS promotes best practice.

WEBSITE VISITOR	WEBSITE CMS	CLIENT
Data Subject	Data Processor	Data Controller

The only outgoing emails from us will be transactional:

- Email 2 step verification
- Appointment confirmation
- Password change requests
- Requested 'plan your day' PDF's
- Etc.

HAS ASP APPOINTED A DATA PROTECTION OFFICER?

Yes, although technically we don't have to. It is our CEO, Arran Coole.

HOW DOES ASP ADHERE TO GDPR PRINCIPLES?

Article 5 of the GDPR requires that personal data shall be:

a) **Processed lawfully, fairly and in a transparent manner in relation to individuals.**
We adhere to this, we train clients on this too and our CMS encourages the correct process

b) **Collected for specified, explicit and legitimate purposes.**
We record the purpose for each form created by our clients, so there is a record for them. ASP does not use the data.

c) **Adequate, relevant and limited to what is necessary.**
ASP has always promoted minimal collection of data, why collect an address if you are not posting anything for example.

d) **Accurate and, where necessary, kept up to date.**
The data collected by ASP is generally securely exported via API into the clients CRM system, therefore we do not hold the up to date version.

e) **Kept in a form which … no longer than necessary.**
We hold the data as long as the Data Controller requires. Normally a show cycle.

f) **Processed securely.**
ASP adheres to high data security standards. We maintain a defence-in-depth approach to security – operating Web Application Firewalls on top of our up to date infrastructure firewalls. We test security assuming the WAF's have failed. In addition, we have a thorough security policy. Security issues are reported on a weekly basis as a standard agenda item. ASP's security budget is a six-figure amount. We have a Cyber Essentials Certificate.