GDPR IT COMPLIANCE CHECKLIST

Produced for Colony Networking

19 April 2018

GDPR IT COMPLIANCE CHECKLIST

Produced for Colony Networking

INFORMATION REGARDING NEW GDPR LEGISLATION AFFECTING YOUR BUSINESS

The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) takes effect on 25 May 2018. It is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify existing data protection laws for all individuals within the European Union (EU).

The provisions of GDPR affect every Business and it is your responsibility to ensure compliance. Fines of up to 5% of your previous year's annual turnover can be incurred for failure to adhere to the provisions. Full details can be found at: https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

At Aspire we have researched the new requirements and are making the following recommendations to help ensure your personal data protection processes & policies systems are GDPR compliant:

Here are several ways businesses could do now to pave the way for a smoother transition:

1. Consider whether it is **even necessary to process personal data**. If so, it may be worth anonymising the data reducing the businesses exposure to the GDPR.

2. Audit and document all the personal data you hold, do you actually require it, making a note of where it came from, what it is for, and who has access to it both within the organisation, and externally, how long should you keep the data, this applies especially to emails. Do a mini risk analysis of all your data and be prepared to do a full DPIA (Data Privacy Impact Assessment) on any data deemed to be high risk or sensitive.

3. Review current privacy notices. The GDPR requires businesses to include certain additional information in their notices including, for example, the data subjects' right to complain to the Information Commissioners Office (ICO). The ICO has published a Code of Practice which sets out the new requirements.

4. If your business relies on consent, review how you obtain and record that consent. Under the new regime businesses will need to be able to demonstrate that consent has been freely given which will require them to produce clear records. Consent is just one of the 6 legitimate reasons for collecting, storing or using personal data though. The others are:
    1. Under legal obligation
    2. Under contract
    3. Client's best interest
    4. Public interest
    5. Corporate interest

5. If your business uses any third party, then provide a link to their policies as well as your own. e.g.

https://aspire-computers.com/wp-content/uploads/2017/08/Privacy-Policy.pdf
https://www.acronis.com/en-gb/company/privacy.html
https://www.datto.com/privacy-policy
https://cloudmarket.com/privacy-policy
https://www.mcafee.com/uk/about/legal/privacy.aspx
https://www.xero.com/uk/about/terms/privacy

6. In the event of a personal data breach, the Regulation will require your organisation to notify the authorities within 72 hours of becoming aware of the exposure so it's important your company has an effective cyber incident response management plan in place for how your company will respond to a data breach quickly and effectively.

7. Appoint a specialised Data Protection Officer to take responsibility for compliance and circulate the message with the rest of the business.

8. Ensure your paper-based documentation is handled and destroyed securely. Paper and physical data can be one of the biggest areas of loss and theft. Review your current cyber security, and ensure firewalls, encryption, and so on are robust.

IT Data Security Check

We recommend you identify all the devices on which your data is stored and consider how they are currently protected.

	Server	NAS	Local PC	Email System
Anti-Virus				
Back Up S/W				
Local Media				
Data Stored offsite				
Cloud				
Firewall				
Threat Detection monitoring				
VPN Encryption				
Hosted Mailbox				
Security Option				

GDPR IT COMPLIANCE CHECKLIST

Produced for Colony Networking

WEBSITE COMPLIANCE

We are making the following six recommendations to our customers to ensure their WordPress websites are fully GDPR compliant:

1. Add secure certification

   This means your site will appear with a 'HTTPS' prefix instead of 'HTTP' which is insecure. A green padlock in the browser address bar gives visitors the peace of mind that any personal data they share with your website will be handled securely. It has also recently been announced that as of July this year, the Google chrome browser will flag all non HTTPS sites as 'not-secure'.

2. Add Google reCAPTCHA to website forms

   reCAPTCHA is a free service that protects your site from spam; hacking and abuse. It uses advanced techniques to differentiate humans from robots, analysing the way visitors use a mouse to reduce your site's vulnerability to hacking.

3. Add cookie control

   Cookies are small files stored on a user's device. They hold a small amount of data specific to a particular client and website. Customers must provide explicit consent to the use of cookies on your website. As every website uses cookies of some description, every website needs to provide a way for visitors to provide consent.

4. Publish data usage policies

   GDPR requires website owners to publish information regarding their use of personal data. We recommend publishing a cookie policy, privacy policy and website terms and conditions as a minimum. E-commerce sites should also publish terms and conditions of sale. We advise all customers to seek legal advice over the contents of these documents but can provide customisable sample documents to get you started if required.

5. Add extra security

   As WordPress is such popular software, it is frequently targeted by hackers. Taking additional security measures makes your site far less vulnerable to hackers, and therefore keeps your customers' data safe.

6. Update software

Old, outdated software is much easier to hack, so we advise customers to regularly update core software, themes and plugins. An ongoing website support contract with Aspire means we will regularly update site software on your behalf to give you full peace of mind. Contact us for more information regarding support contracts.

Don't forget you are required by law to ensure GDPR compliance after May 25th. While it is unlikely that small businesses will be prosecuted straight away for non-compliance, we strongly recommend that you create a GDPR plan and implement it soon as possible.

Contact us on 01925 251143 or via web@aspire-computers.com if you have any further questions or require GDPR support.

Roz Healey, Web and Social Media Development Manager

Sophy Bostock, Web and Social Media Developer