**GDPR:**

The EU General Data Protection Regulation (GDPR) is a set of rules applicable to all individuals and companies which provide services to EU citizens (EUR-Lex, 2016).

Following a GDPR compliance test against the Group Four e-commerce website, critical compliance mistakes were discovered.

Every company and individual that provides products and services to EU citizens should have a privacy note (or notice), stating six important details (Biscoe, 2021):

* Contact Details. This includes the personal details of a person responsible for accessing and storing the data. These details include the name, address, and email address.
* The types of Personal Data stored. It is important to highlight all the data stored in detail without using generic terms.
* How the company processes the data. A company must disclose if it transfers the data to third-party companies.
* How long the data will be kept. According to the GDPR, the data should only be stored for as long as they are needed. Data can be stored for longer only if it is for the legitimate interests of the company.
* The basis of processing the personal data. The privacy notice should include a legitimate legal reason for storing all the data. Companies and individuals should only store data required for providing their services.
* Data subject rights. The privacy notice should include all the rights an individual has regarding his/her data. This should include the right of access, right to be forgotten, right to object, etc.

After our GDPR compliance test, we discovered that the website did not provide a GDPR privacy note.

Additionally, during our testing, we discovered that the website was operating using a vulnerable version of its Content management system (CMS) which includes publicly known security vulnerabilities. Furthermore, the website was not configured with HTTPS encryption. According to the GDPR, an entity storing personal data should ensure that maximum security and encryption systems are deployed (EUR-Lex, 2016).

**PCI DSS:**

The Payment Card Industry Data Security Standard (PCI DSS) is a set of rules aiming at creating a safe environment for online payment systems. As the website we performed the test on is an e-commerce site, we had to further test using the PCI rules.

Our testing showed that the website operates using a dated Content management system (CMS) which includes publicly known security vulnerabilities.

Furthermore, the website does not have a Web application firewall (WAF) deployed or HTTPS encryption, making the website vulnerable to common web attacks.

Recommendations:

* A GDPR privacy note should be drafted including all six important parts informing customers of the way their data are processed.
* The website’s Content management system should be kept updated to the latest version which fixes known vulnerabilities.
* HTTPS encryption should be used to encrypt the data transfers which include the payment details (e.g. Credit card number).
* A Web application firewall must be deployed to shield the website from external web attacks and data leaks.

References:

Biscoe, C. How to write a GDPR data privacy notice – template example [Available from: https://www.itgovernance.co.uk/blog/how-to-write-a-gdpr-privacy-notice-with-documentation-template-example](Available%20from:%20https://www.itgovernance.co.uk/blog/how-to-write-a-gdpr-privacy-notice-with-documentation-template-example) [Accessed 15 July 2021].

EUR-Lex (n.d.) Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC. Available from: <https://eur-lex.europa.eu/eli/reg/2016/679/oj> [Accessed 15 July 2021].

Security Standards Council (n.d.) PCI SECURITY Available from: <https://www.pcisecuritystandards.org/pci_security/> [Accessed 15 July 2021].