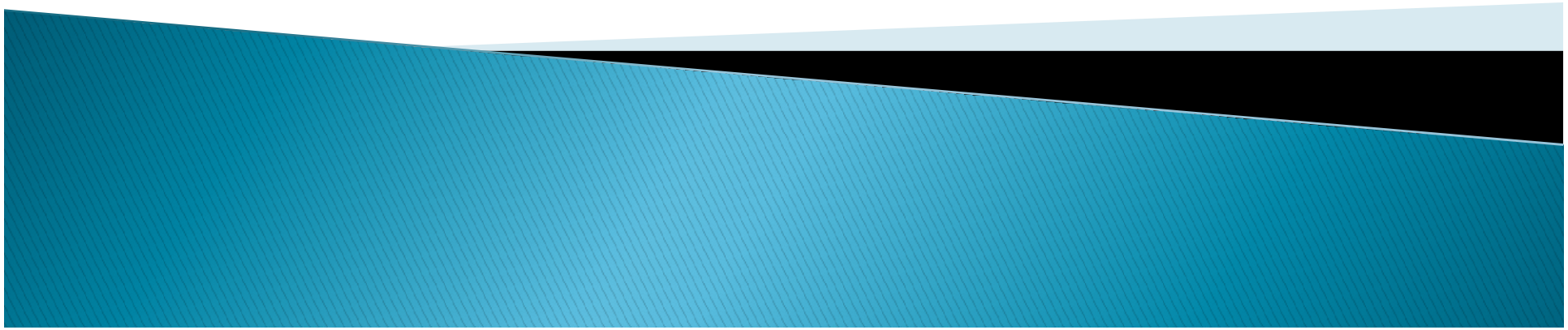
Security Standards

Group 1- loadedwithstuff.co.uk



Assumptions made

loadedwithstuff.co.uk

- Payments can be made directly on the website and does not integrate with a third-party company for payment processing.
- The e-commerce website provider stores and manages the user data.
- The Company operates and delivers products worldwide.

Applied standards to the website

loadedwithstuff.co.uk

GDPR

- Website allows account creation for users
- Delivery information such as names and addresses are required.

PCI Security Standards

- Payments are processed through the website.

ICO

- Company is based and operates in the UK.

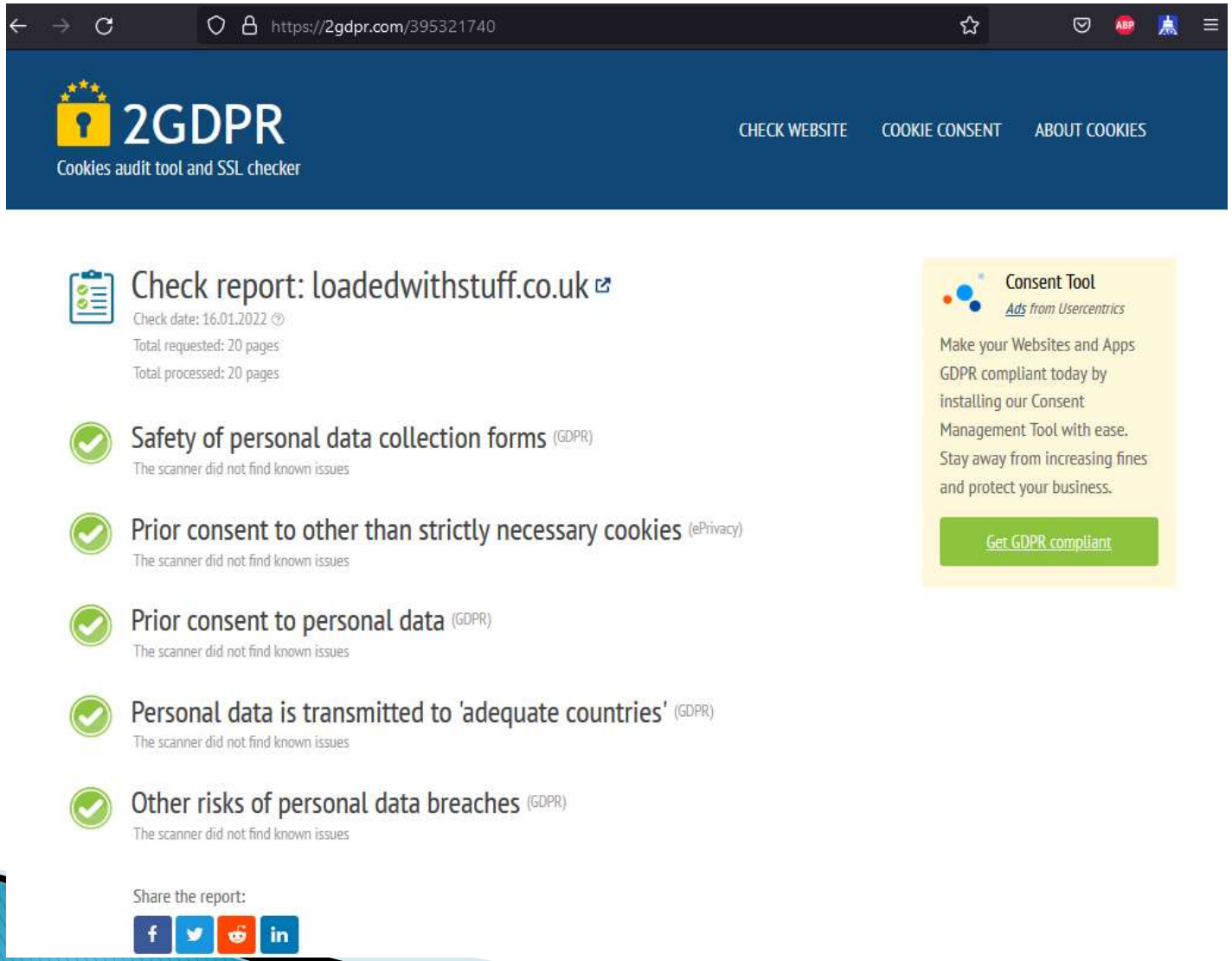
GDPR standards

loadedwithstuff.co.uk

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
  - Does the website only ask for relevant information?
- Accuracy
- Storage limitation
- Integrity and confidentiality (security)
  - Is the data encrypted?
  - Is there a password policy?
  - Accountability

GDPR Standards Check

loadedwithstuff.co.uk



2gdpr.com (2022)

PCI-SSC standards

loadedwithstuff.co.uk

How to determine website compliancy:

"There is only one way for a consumer to tell if a website is PCI compliant. If the website accepts credit card payments, it is compliant. If the site sells merchandise and does not accept payment, it is not compliant."(Torpey, n.d.)

Compliant:

- American Express
- MasterCard
- Visa

Non-Compliant:

- PayPal

PCI-SSC Standards

loadedwithstuff.co.uk

- PIN Transcation Security Point of Interaction (PTS POI)
  - Is the payment website protected against espionage?
- Payment Application Data Security Standard (PA-DSS)
  - Which payment methods are used?
- PTS Hardware Security Module (HSM)
- Point-to-Point Encryption (P2PE)
  - Is encryption in use? Does the encryption offer sufficient protection?
- PCI 3.D Secure Software Development Kit (3DS SDK)
  - Is a current Secure Software Development Kit being used?
- Software-based PIN Entry on COTS (SPoC)
- Secure Software
  - What software is in use? Is the software up to date?
- Secure Software LifeCycle (Secure SLC)
- Contactless Payments on COTS (CPoC)

Recommendations

loadedwithstuff.co.uk

- Use of up-to-date firewall configuration
- Strong password policy
- Protected storage of user information
- Encrypted transmission across open networks
- Restrict physical access to database
- Monitoring of all access to network resources
- Regular penetration testing of security systems
- Implement a least privilege policy
- Implementation of Multi-Factor Authentication (MFA)

Recommendations

loadedwithstuff.co.uk

According to PCI (2022):

GOALS	PCI DSS REQUIREMENTS
Build and Maintain a Secure Network	1. Install and maintain a firewall configuration to protect cardholder data 2. Do not use vendor-supplied defaults for system passwords and other security parameters
Protect Cardholder Data	3. Protect stored cardholder data 4. Encrypt transmission of cardholder data across open, public networks
Maintain a Vulnerability Management Program	5. Use and regularly update anti-virus software or programs 6. Develop and maintain secure systems and applications
Implement Strong Access Control Measures	7. Restrict access to cardholder data by business need-to-know 8. Assign a unique ID to each person with computer access 9. Restrict physical access to cardholder data
Regularly Monitor and Test Networks	10. Track and monitor all access to network resources and cardholder data 11. Regularly test security systems and processes
Maintain an Information Security Policy	12. Maintain a policy that addresses information security for employees and contractors

References:

loadedwithstuff.co.uk

ICO (2021). Information Commissioners Office – Guide to the General Data Protection Regulation – Security. Available from: https://ico.org.uk/for-organisations/guide-to-data-protection/guide-to-the-general-data-protection-regulation-gdpr/security [Accessed 09 December 2021]

Torpey, J. (n.d) How Do I Tell If a Website Is PCI Compliant. It Still Works. Available from: https://itstillworks.com/do-tell-website-pci-compliant-5968912.html [Accessed: 17.01.2022]

2GDPR (2022) Cookies audit tool and SSL checker. Available from: https://2gdpr.com/ [Accessed:16.01.2022]

PCI (2022) PCI Security Standards Overview. Security Standards Council. Available from: https://www.pcisecuritystandards.org/pci_security/standards_overview [Accessed: 16.01.2022]

PCI (2022) Maintaining Payment Security. Security Standards Council. Available from: https://www.pcisecuritystandards.org/pci_security/maintaining_payment_security [Accessed: 17.01.2022]