Upholding information rights

Wycliffe House, Water Lane, Wilmslow, Cheshire SK9 5AF
Tel. 0303 123 1113 Fax. 01625 524 510 www.ico.org.uk

Direct Clothing Co. (UK) Limited
Office D160 First Floor
New Covent Garden
London, United Kingdom
SW8 5LL

[redacted]

18 July 2022

Dear [redacted]

Case Reference Number INV/0915/2021

I write to inform you that the Information Commissioner's Office ('ICO') has now completed its investigation into the personal data breach reported by Direct Clothing Co. (UK) Limited ('DCCUK') on 20 August 2021.

The case has been considered under the General Data Protection Regulation (the GDPR) due to the nature of the processing involved.

Case Summary

It is my understanding that on 19 August 2021, DCCUK were contacted by a customer who advised that their payment card had been defrauded after using DCCUK's website. An investigation by DCCUK found that a malicious code had been introduced to the website which allowed an unknown third party to obtain the payment card details of website customers.

The third party obtained access to DCCUK's environment via a WordPress vulnerability, although the specific vulnerability could not be determined due to the number of vulnerabilities present at the time of the incident. DCCUK believed that a third party IT provider was responsible for the security and maintenance of the affected website, however, this was not the case.

Our consideration of this case

I have investigated whether DCCUK has complied with the requirements of data protection legislation.

For more information about our powers under the data protection legislation please see the attached leaflet.

- ICO Enforcement Powers Leaflet – GDPR and DPA 2018

My investigation has found the following issues in relation to the security requirements of the GDPR:

- DCCUK had not applied any security patches or updates since at least February 2019. The NCSC guidance recommends organisations perform regular vulnerability scanning.[1]

- DCCUK were not conducting any vulnerability scanning or penetration tests. NCSC guidance recommends regular scanning.[2]

- DCCUK were not aware that a support and maintenance contract was not in place with their third party provider.

- DCCUK did not conduct adequate due diligence during the purchase of the company to ensure the technical security measures of their systems.

After careful consideration and based on the information provided we have decided to issue DCCUK with a reprimand in accordance with Article 58 (2) (b) of the GDPR.

Details of reprimand

The reprimand has been issued in respect of the following processing operations that have infringed the GDPR.

- Article 32 (1) which states taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk.

- Article 32 (1) (b) which states the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including the ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services.

[1] Vulnerability management - NCSC.GOV.UK
[2] Vulnerability Scanning Tools and Services - NCSC.GOV.UK

- Article 32 (1) (d) which states the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk including a process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.

Not only did DCCUK fail to implement appropriate technical security measures, it also demonstrated a lack of oversight and general awareness of the security measures in place to protect personal data for which it was responsible.

[redacted] DCCUK did not have a contractual agreement in place regarding the security of their systems with any third party provider at the time of the incident. As a result, regular patching, testing and monitoring was not being conducted.

[redacted]

Guidance was available which, had DCCUK consulted, would have highlighted the steps to take to ensure the security of its systems. This includes the ICO's security checklist. The NCSC also provides guidance and recommendations for small businesses to follow to secure their systems, had DCCUK consulted these guides, including following the Cyber Essentials, it is likely their systems would have been secured appropriately.

I would like to point out that if further information relating to this subject comes to light, or if any further incidents or complaints are reported to us, we will revisit this matter and further formal regulatory action may be considered as a result.

Further Action Recommended

The Commissioner recommends that Direct Clothing Co. (UK) Limited should take steps to ensure it is compliant with the GDPR. The information above details the compliance issues relevant to this investigation. The guidance provided in this reprimand should be considered by DCCUK

Further information about compliance with the data protection legislation which is relevant to this case can be found at the following link:

https://ico.org.uk/for-organisations/guide-to-data-protection/

We actively publicise our regulatory activity and outcomes, as this helps us to achieve our strategic aims in upholding information rights in the public interest. We may publish information about cases reported to us, for example where we think there is an opportunity for other organisations to learn or where the case highlights a risk or novel issue.

Therefore, we may publish the outcome of this investigation to publicise our regulatory authority and powers under the GDPR. We will publish information in accordance with our Communicating Regulatory and Enforcement Activity Policy, which is available online at the following link:

https://ico.org.uk/media/about-the-ico/policiesandprocedures/1890/ico_enforcement_communications_policy.pdf

Please let us know if you have any concerns about this.

Thank you for your co-operation and assistance during the course of our investigation.

We now consider the matter closed.

Yours sincerely

[redacted]

Lead Technical Investigations Officer
[redacted]

Please note that we are often asked for copies of the correspondence we exchange with third parties. We are subject to all of the laws we deal with, including the General Data Protection Regulation, the Data Protection Act 2018 and the Freedom of Information Act 2000. You can read about these on our website (www.ico.org.uk).

The ICO publishes the outcomes of its investigations. Examples of published data sets can be found at this link (https://ico.org.uk/about-the-ico/our-information/complaints-and-concerns-data-sets/).

Please say whether you consider any of the information you send us is confidential. You should also say why so that we can take that into consideration. However, please note that we will only withhold information where there is good reason to do so.

For information about what we do with personal data see our privacy notice at www.ico.org.uk/privacy-notice