Logo, company name

Description automatically generated

**NOTICE OF DATA SECURITY INCIDENT**

**General Frequently Asked Questions (“FAQs”)**

1. Who is AKW?

Our full company name is AKW Medi-Care Limited (the “Company”). We are a business registered in England specialising in the sale of fixtures and fittings for kitchens, bathrooms and mobility support. We generally supply our products to dealers and trade suppliers that are engaged in supplying products to members of the public.

1. What happened?

Like many other businesses, we have recently experienced a phishing attack. The attacker sent an email to a member of our team with an attachment that looked genuine. They opened the attachment before our email protection system identified it as malicious. Unfortunately, the attachment contained a virus that enabled the attacker to access our employee’s inbox and find their credentials for our external email marketing platform, which is operated by DotDigital.

The attacker then gained access to DotDigital’s platform and downloaded AKW’s business contact email list.

As far as we are aware, the attacker has not sent any phishing emails to anyone on that list.

1. When did this happen?

The original email was received by our team member at approximately 3.30pm on 7 February 2023. The attacker downloaded a copy of our contact database from our DotDigital account the same day.

**We became aware of the incident within 48 hours of its occurrence.**

1. What personal data has been impacted?

The information stored in our contact database is comprised of basic identifiers (email addresses, individual names (first name and surname), company names and company postcodes).

**We found no evidence of any financial or other personal data having been compromised.**

Quickly after discovering the incident, we locked relevant user accounts and reset passwords to prevent unauthorised access from continuing. As far as we are aware, our communications platform has been secured and our contact database is no longer accessible, although that does not prevent the attacker from using information that they have already downloaded.

1. Why are you notifying me?

We are notifying you because your contact information was in the contact database that the attacker downloaded. While we have no evidence to suggest a high degree of risk, we wanted to advise you of what has happened, so that you are aware and can take appropriate action to protect your email account and other information, if necessary.

Our investigation remains ongoing and if any further information becomes available which we think materially alters the position, then we will provide further notifications along with a revised version of these FAQs as appropriate.

**We are unaware of any reason why you should be individually targeted.**

1. Who is responsible for this happening?

As with many phishing attacks, unfortunately it has not yet been possible to ascertain the attacker’s identity, location or exact motives. However, our investigations are continuing and we will let you know if any further material information comes to light.

1. Have you experienced anything like this before?

No. The Company takes its responsibilities under data protection laws very seriously and has implemented different technical and organisational security measures to prevent data security incidents (including phishing attacks) from happening. We continue to monitor and enhance the measures we take on an ongoing basis.

1. What is the risk?

The main risk is that the attacker may attempt to initiate contact with you with the aim of gaining access to your email account and other systems and/or information, or to use that information in the context of other unlawful activities.

There is also a risk that your contact data could be, either in the future or already, published on or acquired through the dark web. This could potentially then lead to other attackers attempting to contact you or use your information for unlawful purposes.

**We have no evidence suggesting that potential risks may have materialised.**

1. What can I do to protect myself?

Please be vigilant in relation to any emails you receive that originate from a suspicious external source, particularly if they contain suspicious content (such as links to file sharing sites) or attachments – in our case the attacker used an attachment that appeared to be a voicemail.

If you receive any suspicious emails then please do not open them or any attachments and immediately delete them, including from any back-up or deleted item folders.

1. I believe I have already been affected, what can I do?

If you have already received a suspicious email and opened an attachment, then you should urgently contact your organisation’s network administrator and your data protection manager so that appropriate action can be taken to protect relevant systems, accounts and information.

1. I want you to delete my information, what can I do?

You have the right under the UK GDPR to request that we delete the personal data that we hold about you, subject to certain exceptions.

If you would like to submit a request for us to delete your data, then please email us at [datasecurity@akw-ltd.co.uk](mailto:datasecurity@akw-ltd.co.uk)

1. What action are you taking?

As soon as we became aware of the incident, we immediately mobilised an internal team to conduct an investigation, including liaising with staff members and relevant service providers to understand the nature and cause of the breach, its likely effects and the risks involved to individuals. We were then able to contain the attack, including by promptly locking user accounts and resetting passwords. A communication was also issued to all our staff warning them about suspicious emails targeting the Company and of steps to take in the event that they received any such communications.

Having concluded our initial investigation, the following remedial actions are being pursued:

* Out of an abundance of caution, we are writing to all affected individuals to inform them of the incident and of protective action they can take.
* We have established a dedicated email account and telephone number for any individuals affected by this incident to contact us with any questions or concerns.

* We have reported this matter to the UK Information Commissioner’s Office (“ICO”) and will cooperate fully with any investigation launched by the ICO or the police in relation to this incident.
* We will be engaging an external IT partner, to help confirm that there are no unidentified risks emanating from this incident.
* Our existing policies, procedures and practices are being reviewed to identify any potential deficiencies with improvements to be implemented accordingly.
* While all our staff receive induction training including on the Company’s obligations under data protection laws, we will be launching refresher training to ensure that staff are appropriately educated and aware of prevailing threats.

1. My question hasn’t been answered by these FAQs, what can I do?

We hope these FAQs have been useful and have helped to address any concerns that you might have.

However, if you have any further questions please email us at [datasecurity@akw-ltd.co.uk](mailto:datasecurity@akw-ltd.co.uk) or call us on 01905 701310 (hours: 09:00-16:00) and we will respond as soon as possible.