

Subject: Notice of Unauthorised Access to Glofox Data

Dear Glofox Admin,

We have been notified of a security incident during which an unknown third party accessed certain data related to Glofox users. We are currently undertaking a full investigation, but we want to let you know as early as possible.

What Happened?

On Saturday 14th November, we became aware that an unknown third party had gained unauthorised access to some user data, including names, email addresses, phone numbers, hashed/scrambled passwords, and other optional information like date of birth. No plain text passwords have been exposed.

The user data related to an archive of information from the 27th of March 2020. No data collected after that date was accessed.

We can confirm that **no credit card or payment method data was accessed**. As part of our normal security measures, we do not store any of this information in our systems.

We can confirm that x of your clients were impacted. y% of these had a password in Glofox. z% of these had a date of birth in Glofox.

We are now completely confident that we have identified and closed the path that led to the unauthorised access.

What Should Glofox Administrators Do Now?

- We have reset your Glofox account password and the passwords related to your staff to prevent unauthorised access to your account. You and your staff will need to follow the Glofox forgot password flow the next time you log in.
- Even though no plain text passwords have been exposed, as a precaution, if you or your staff use your Glofox password on other websites, we recommend that you change these passwords. We ask that you pass this recommendation onto your staff.

Do You Need to Inform Your Members?

We do not believe that the overall risk associated with your members' data is high. However, you may decide to notify your members. If you decide to do so, here is a suggested message you can send them.

Hi <first name>,

We have been informed of a security incident on the Glofox platform that may impact some of your personal details.

The personal details may include your name, email address, phone number, hashed/scrambled (i.e. not plain text) password, and other optional information like date of birth.

No financial information or credit card details have been exposed.

While no plain text passwords have been exposed, as an abundance of caution we recommend that you reset your password for Glofox and, if you have been using your old password across multiple websites, we recommend to change those passwords also.

Glofox has informed us that this is an isolated incident and they have identified and closed the path that led to the breach.

What We Are Doing?

Data security is a top priority for us here at Glofox. We have significantly invested in our security infrastructure over the past 12 months. While we are deeply disappointed that this incident has occurred, we will continue to invest in our infrastructure to prevent incidents like this in the future.

As we are the controllers in respect of the personal data of your account administrators, and although we do not believe that the overall risk associated with this data is high, we have taken the decision that we will notify our relevant data protection supervisory authorities.

In respect of the personal data of your members, you will separately need to assess whether you have any obligation to notify your local data protection supervisory authority of this incident.

We have initiated communications to all of our impacted customers and will be in touch if we have any more information or actions.

If you have any questions, please contact our team at dataprivacy@glofox.com.

Kind Regards,

Conor O'Loughlin

CEO