

Report on Supply Chain Compliance Volume 3, Number 15. August 06, 2020

WhatsApp vulnerabilities present significant data breach risk

By Sascha Matuszak

A series of security vulnerabilities^[1] found in the messaging service WhatsApp presents significant risks of malware being inserted via the app, which can result in data breaches and other adverse events. WhatsApp is used by more than one billion people worldwide and is touted as a secure system due to end-to-end encryption. The app's code can be manipulated, however, and used to insert malware.

For companies whose employees use WhatsApp to communicate, the risk of experiencing a data breach is serious and needs to be addressed. Data breaches must be reported to authorities under several data protection regulation frameworks, including GDPR. Inadequately protecting sensitive data can result in fines, theft of proprietary intellectual property and loss of control of critical networks to hackers.

Two enforcement actions in January^[2] — taken by the United Kingdom's Information Commissioner's Office and the German Federal Commissioner for Data Protection and Freedom of Information — highlight the regulatory risk of not protecting sensitive data adequately.

This document is only available to subscribers. Please [log in](#) or [purchase access](#).

[Purchase Login](#)