GDPR

GENERAL DATA PROTECTION REGULATION

# THE LINK BETWEEN GDPR AND THE DARK WEB

## A GDPR CRASH COURSE

Designed to protect the data security and privacy of EU citizens, the GDPR was introduced as a replacement to the Data Protection Directive of 1995. As an overview, the regulations empower consumers with greater ownership over their personal information; highlights including the “right to be forgotten”, a fortified consent process, and more stringent breach notification protocol requirements. Aside from expanding the definition of “data processing” to include collection, retention, deletion, breaches, and disclosures of personal data, the penalties associated with infractions are no laughing matter. Since its implementation, multinational corporations have seen fines amounting to $23M. Or even worse, 4% of global revenue.

## DARK WEB + GDPR

So where does the Dark Web fit into this? Just recently, we covered a recent report by the Federation of Small Businesses (FSB) proclaiming that UK-based SMBs were suffering nearly 10,000 cyber attacks per day. Although the majority of these are serious security breaches, some are slipping through the cracks as “leaks” that go unnoticed. These manifest themselves as vulnerabilities caused by password recycling, lost devices, accidental website updates/ emails, and even rogue employee behavior.

Unlike more overt incidents, data compromises are much more difficult to detect, especially for small businesses with minimal security measures in place. Therefore, sensitive information collected from such leaks ultimately finds a home on the Dark Web, without anyone being the wiser. As we know, cybercriminals will exchange valuable credentials for cryptocurrency, and then leverage leaked information to orchestrate crippling fraud tactics.

UK SMBs were suffering

**10k**

cyber attacks per day

In the past, companies were able to sidestep any ties back to them due to loose privacy regulations and limited feedback loops. However, those days are soon coming to an end. The GDPR mandates that companies of all shapes and sizes must disclose consumer data breaches, and will also be held liable for such accidental leaks. For example, the Information Commissioner's Office (ICO) and National Cyber Security Centre (NCSC) of the UK has published specific guidance for risk management, data protection, detection, and minimization of impact.

## THE SOLUTION

The global standards for data protection may be rising, but so have the solution sets for SMBs. By partnering up with a trusted partner who has enlisted in proactive Dark Web monitoring solutions (like Dark Web ID™), you can future-proof your company from facing GDPR fines or dealing with business process interruptions. Case dismissed.

## NEED MORE PROOF?

See what Ryan Markel, President of Take Ctrl, LLC, has to say about working with our team:

> "My clients are so grateful that they are not aware when their passwords are compromised that they are telling their colleagues at other companies they have to work with us".

## ABOUT ID AGENT

ID Agent, a Kaseya company, provides the channel's leading Dark Web monitoring and security awareness training solutions, available exclusively through the reseller channel, to MSPs worldwide. Its flagship product, Dark Web ID, delivers validated intelligence to identify, analyze and monitor for compromised or stolen employee and customer data. This data helps protect businesses from risk of a breach, while its prospecting tool opens doors for MSPs to begin security conversations. The company's BullPhish ID™ provides cybersecurity awareness training and phishing simulation geared to the non-technical end user, to enhance a company's overall cybersecurity and further safeguard corporate systems. For more information, visit: www.idagent.com or go to LinkedIn, Twitter or Facebook.