FREQUENTLY ASKED QUESTIONS REGARDING GRYVES' CYBER OFFERING

Gryves as a company

Who is Gryves?

Gryves is an independent, management owned FinTech Company, providing a range of cyber security services and risk management operations. Besides its two assessment services for the SME market ('DOMAIN CYBER CHECK' and 'BUSINESS BASIC CYBER CHECK') Gryves also has specialised offerings for insurance companies and banks.

Gryves' assessment services for SMEs

What assessment services is Gryves offering to SMEs?

Gryves offers a two-stage, complementary assessment model to show companies quickly and easily how they present themselves in the digital environment on the one hand and how they are organizationally positioned against cyber risks within the company on the other.

'DOMAIN CYBER CHECK'

What is the DOMAIN CYBER CHECK?

The DOMAIN CYBER CHECK is a domain-based assessment that uses a few details about the company (domain, industry sector, country of domicile, size - sales and headcount) to provide a concrete overview of the company's digital footprint, the digital risk potential and possible cyber vulnerabilities.

What data is used by Gryves for their domain-based assessments and calculations?

Gryves collects the digital traces produced by the daily use of the Internet or e-mail and combines them with data from various publicly accessible databases and evaluates and processes all with the help of artificial intelligence.

What is the result of the DOMAIN CYBER CHECK?

The results of the DOMAIN CYBER CHECK are summarized in a report. This shows two KPIs and a list of identified 'findings' and possible vulnerabilities.

What do the two KPIs in the report stand for?

Cyber risk exposure: Probability that a company could be affected by a cyber event in the next 12 months.
Vulnerability that an expected cyber event could lead to a business interruption

What do the colours of the KPIs mean?

The KPIs are presented in a traffic light system, where yellow or red signal an increased risk.

What do the findings outline in the report?

The 'findings' in the report of the DOMAIN CYBER CHECK represent the discoveries made during the assessment. Findings, which consciously represent configured system settings at a company, are no problem. However, those that have not been deliberately configured or of which the company has no knowledge may represent a specific vulnerability and security risk.

How much time does it take to complete a DOMAIN CYBER CHECK?

It takes not more than five minutes.

Can a subscription be purchased for the DOMAIN CYBER CHECK?

Yes, the DOMAIN CYBER CHECK can be purchased as an instant assessment as well as in form of a subscription of three (one instant assessment and two within 12 months) or six assessments (one instant assessment and five within 24 months).

Data protection

Who has access to the reports and findings produced by Gryves?

Only the user that has ordered the report has access to it. A user must have a valid e-mail address that correlates to the domain for which an assessment gets ordered.

What measures are foreseen in the process to ensure that no unauthorised user has access to sensitive data?

A 2-factor authentication with a verification e-mail.

How does Gryves protect and use company data?

Gryves recognises that information security is an integral element of data privacy. While no data transmission (including over the internet or any website) can be guaranteed to be a 100% secure from intrusion, Gryves implemented a range of commercially reasonable physical, technical and procedural measures to help protect personal data from unauthorised access, use, disclosure, alteration or destruction in accordance with data protection law requirements.

Is Gryves fulfilling the EU GDPR requirements?

Yes, as far as GDPR is concerned regarding the data we leverages we follow the rules of GDPR.

General

What is the difference between outside and inside the firewall?

Gryves' DOMAIN CYBER CHECK assesses the company's digital footprint outside of its firewall by accessing solely publicly available data. Gryves penetrates at no time the systems of the assessed companies nor has it access to any of their data.

What is cyber risk?

Risks emerging from any form of digital attacks that every user of information and communication technology is exposed at, that compromises the confidentiality, availability or integrity of data or services, ransomware or even corporate espionage. The impairment of operational technology can eventually lead to business disruption, (critical) infrastructure breakdown or physical damage to

humans and property and can result in financial loss and disruption or damage to the company's reputation.

Cyber risk is not just a matter for the IT team, although they might be directly involved. Cyber risks might also get caused by the people working in and for a company, inadequate workflows and procedures and the technology that is underlaying as well as front facing.

Accordingly, also the company's (Risk) Management must regularly address this topic and requires an understanding of the constantly evolving risks.

Where to find independent information regarding cyber risk?

There are several websites where some current information about cyber risks can be found. In some countries regulators or organisations close to them maintain such websites, e.g. http://securityaffairs.co/wordpress/ or https://www.melani.admin.ch/melani/de/home/themen.html.

In addition, there are many different standards that can support the need for additional information, e. g. ISO 27000ff, NIST, NATO-Cyber standard.