Regulatory vs. Business Compliance

When working with the compliance monitor, you will likely very often see the term "regulatory" or "business" in combination with "compliance".

There is a simple reason for that: Compliance is more complicated than security monitoring.

> While security follows strict rules which count for any website on the internet, compliance is different.
>
> When a website distributes malware, or uses weak or no TLS encryption, it is clearly a security issue. But when a cookie is set without permission, things get a little blurry.

Analysis of compliance topics is a very individual part, where legislation is only a little of a help. We think that the law can be taken into account for any website (in a specific region at least).

TL;DR

Regulatory compliance focusses on checks, which can be performed on almost any websites, because they need to comply with the law. A well known regulation is the general data privacy regulation (GDPR).

Business compliance adds special checks for websites, which need to follow special/individual directives of the company. Therefore they are not required by law, but by internal policies.

Regulatory Compliance

Regulatory compliance describes rules and patterns, defined by law / legislation of a specific country. An example would be the GDPR for the EU. Per definition, a website accessible to european citizens needs to follow specific rules to protect the privacy of every single person.

One rule defines, that there must not be set any cookies before the visitor did not give consent. Technical speaking this is a difficult, as for a lot of web-applications, some cookies are needed to actually let them work. Those are called technical necessary. But this seems still to be a topic for the court.

Business Compliance

On the other hand we have the business compliance. This describes a set of rules, which can be freely defined by the companies themselves. Those are business decisions which need to be followed to e.g. secure the overall presence on the internet.

An example would be that the logo of the company should be placed always on the top left of a website.

Another rule might check if the link to the data privacy page is located on the top AND bottom of the website.

Also there might be the decision, that specific URLs need to be only accessible from the intranet of the company, and therefore send a statuscode 400 for external visitors.

Back to cookies: companies want to track their visitors to e.g. measure engagement, or optimize the overall experience for every visitor by studying their movements. Therefore a rule could also check if a specific cookie is set when the website is visited. (This needs of course some very good arguments in the cookie policy of the website, but especially the GDPR got you covered; Predominant legitimate interests (Art. 6 para. 1 lit f)).

Revision #1
Created 2021-06-15 11:55:28 UTC by Christian Baumgartner
Updated 2021-06-16 15:13:55 UTC by Christian Baumgartner