SOURCE DEFENSE

2018

WHAT YOU MUST KNOW ABOUT GDPR COMPLIANCE

A Universal Website Vulnerability Makes Compliance Impossible

Perspective for Risk & Compliance

Your Website Makes GDPR Compliance Impossible

Today, GDPR is impossible to comply with due to a universal, unaddressed vulnerability in website security that directly prevents your organization from ensuring customer data privacy. Your organization can only comply with GDPR and act as an adequate custodian of your customers' data if you can control which external entities have access to it. Corporate websites operating today contain a universal vulnerability that prevents the adequate control of customer data.

This unaddressed vector of data leakage and theft is introduced through the website technology supply chain. Website developers and marketing teams have integrated dozens of external 3rd party vendor tools into the average corporate website (for example: web analytics, social media, chat tools, etc.). This integration establishes unmanaged and unmonitored website connections with these multiple external 3rd parties. Further, it grants each of these external 3rd parties (and hackers that might exploit them) unlimited access to regulated customer data whether it is displayed to or entered by site visitors. Currently your organization has no way of controlling which vendors have access to what data and no way to prevent them from accessing all of it. Every corporate website is currently vulnerable to this exposure and remains in a non-compliant state. This includes yours.

There is a Lot at Stake

As is well understood, GDPR specifies a compliance framework upon which to build an infrastructure capable of maintaining responsible customer data privacy and control. Violation of GDPR provisions could result in fines of up to 4% of a company's global annual revenues for any organization handling the personal data of EU citizens. Although no single vendor is capable of delivering a completely holistic GDPR solution, this paper surfaces a critical website exposure that must be considered in **ALL** preparation associated with GDPR compliance.

GDPR Analysis – Problem Areas

Source Defense specifically addresses multiple articles defined in the GDPR framework that, without Source Defense's unique solution, your organization would remain in non-compliance. These are discussed below and offered for consideration as you evaluate, prioritize and endeavor to implement a data control infrastructure to ensure compliance with the GDPR.

Article 5 - Defines principles relating to the **processing** of personal data.

Your organization cannot control the processing of personal data without controlling the access and permissions of every 3rd party vendor integrated into your website. Today these multiple 3rd party vendors are not managed and have unlimited access to all areas of your website. They can read the customer data you display and capture the sensitive information your customers enter. More concerningly, hackers actively compromise these 3rd parties to exploit this level of access to steal this valuable customer data. Without total control over the access and permissions of every 3rd party vendor you cannot ensure compliant processing.

Specifically, the framework requires that private customer data:

- "Collected for specified, explicit and legitimate purposes and is **not further processed** in a manner that is incompatible with those purposes"
- "Processed in a manner that **ensures appropriate security** of the personal data, including **protection against unauthorised or unlawful processing** and against accidental loss, destruction or damage"

A recent study illustrates that the average website integrates 34 different 3rd party vendors. These unmanaged 3rd party tools have unlimited access to your website and customer data. Such access uncontrollably exposes your customer data to each of these external vendors as well as any hacker that might compromise them.

Articles 16, 17, & 18 – Defines a person's right to **rectify, erase, or restrict** personal data.

Correction, rectification, erasure, and restriction of personal data are not possible if this data is being captured or leaked by external 3rd parties integrated into your website or stolen by hackers that have compromised a 3rd party and exploited their unlimited access to your customers' data. As discussed above, without total control over the access and permissions of every 3rd party vendor you cannot ensure compliant data management.

- Article 16 specifies correction or rectification of personal data
- Article 17 defines the right to erasure ('right to be forgotten')
- Article 18 defines a person's right to restrict the processing of personal data

Article 32 – Requires and organization to ensure system **confidentiality**

Your website is an application, environment, and interface through which customer data is displayed, entered, and captured. Controlling and preventing external 3rd party vendors from accessing data beyond what is expressly permitted and necessary leads to non-compliance. Further, hackers that compromise these 3rd party vendors can leverage the unlimited website access to phish your customers and steal more information still. Through this vulnerability in your website hackers can deploy multiple techniques such as:

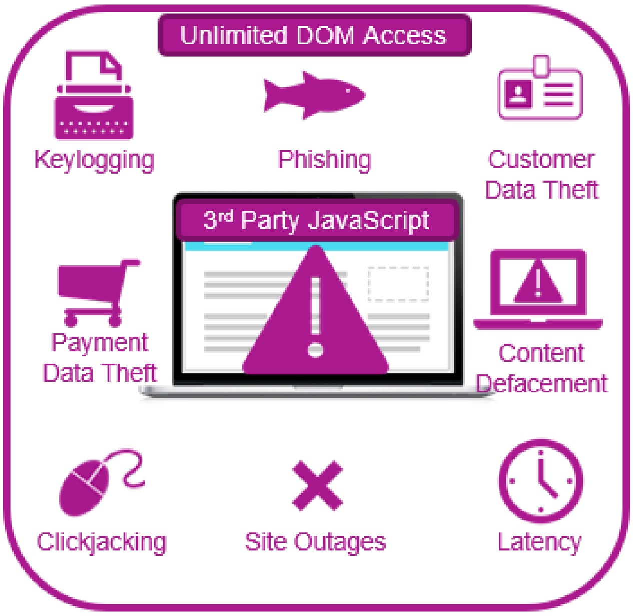
- capturing every keystroke
- manipulating your website forms
- injecting malicious pop up forms
- redirecting visitors to unauthorized external sites

Obviously, your system is not confidential unless these 3rd parties are adequately controlled and hackers are prevented from exploiting this condition.

Specifically, the framework requires to:

- "Ensure System **Confidentiality,** Integrity, Availability, & Resilience".

WHAT ARE THE POTENTIAL DAMAGES?



THE SOURCE DEFENSE SOLUTION

Supply chain attacks are on the rise as attackers seek to compromise your organization's sophisticated security controls via comparatively less sophisticated partners with intimate access to your business and data. Source Defense provides an entirely new and unique solution to prevent website supply chain attacks and prevent unauthorized access to customer data. Source Defense controls the access and permissions of all 3rd parties operating on a website. The Source Defense solution ensures 3rd parties may only deliver the intended user experience and that these tools may not be leveraged for malicious data extraction or website alteration. Further, it satisfies compliance requirements that under “normal” operation, these 3rd party tools themselves do not knowingly or unknowingly have unauthorized access to customer data.

Source Defense is a necessary solution for data privacy and GDPR compliance.

Find out more:

- What is My Risk?
  - Many Source Defense customers wish to understand their specific risk level. Contact us to receive a free assessment of current website exposure to 3rd parties.
  - Complimentary assessment (https://www.sourcedefense.com)
- Learn More?
  - Read the whitepapers (https://www.sourcedefense.com)
- How Does it Work?
  - Link to how it works (https://www.sourcedefense.com/technology)

Discover how many Unmanaged 3rd Party Vendors Operate on your Web Site Today

2018

SOURCE DEFENSE