



Think Outside
the Firewall™

RiskIQ Digital Footprint™: GDPR Compliance

Do You Know Where You're Collecting Personally Identifiable Information (PII)?

Business Benefits

- Quickly pinpoint internet-exposed assets that collect PII or which deploy cookies
- Verify security of the PII-collecting websites with SSL certificates and encryption
- Understand potential vulnerabilities in your attack surface that leave you exposed
- Easily report on compliance with GDPR PII and Cookie requirements

“Before an organization can address GDPR, it needs to fully understand the extent of its online data gathering activities. With enforcement of GDPR less than a year away, the time to act is now.”

– Bob Tarzey
Analyst and Director, Quocirca Ltd

The EU General Data Protection Regulation (GDPR) takes effect on May 25, 2018, and introduces more stringent requirements for how businesses handle and secure personal data. In the area of data collection, the regulation requires that personally identifiable information (PII) is securely captured and processed. Many data capture forms found on websites fall within the scope of GDPR as they collect PII, such as name, username, email address, phone number, birthdate, or any other form of identification.

As part of the regulation's fairness and transparency guidelines, organizations must clearly state at the point of capture how they'll be using an individual's data. “Opt-out” language and prefilled consent tick boxes are no longer allowed, and organizations must be able to prove that a person gave his or her consent. Therefore, permission to use data must be explicit and demonstrated through an action, such as manually ticking a box. Online identifiers such as cookies also fall within the scope of GDPR, and their use, therefore, needs to be accompanied by appropriate notices.

Understanding What You Have

The challenge for larger organizations is the sheer volume and complexity of websites and web applications that need to be identified and inspected for GDPR compliance.

RiskIQ Digital Footprint™ helps organizations address this challenge by

- Discovering and inspecting their public-facing web assets, including websites and associated pages and forms where PII is collected or cookies used
- Highlighting both security and GDPR violation exposures enabling security and governance and risk and compliance (GRC) teams to better understand, and in some cases reduce, their attack surface and achieve compliance

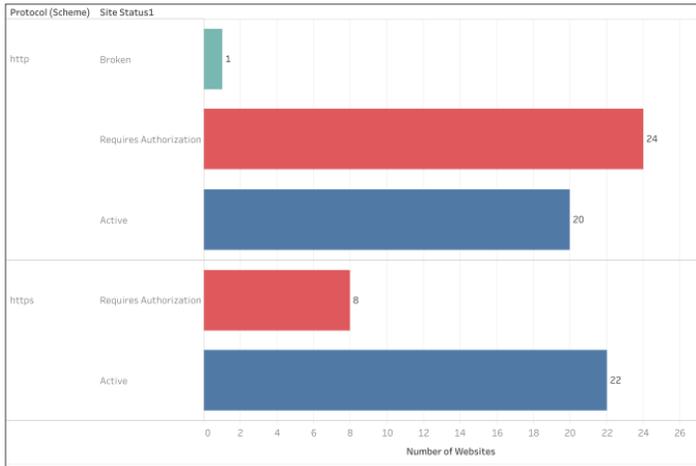
Supporting your Compliance and GDPR Programs

Digital Footprint provides an inventory of internet-facing assets as well as details about those assets, such as forms, cookies, software, applications, and frameworks running. This allows for RiskIQ to correlate CVEs to internet-exposed assets to help vulnerability management teams prioritize patching of software and devices outside the safety of the firewall.

To assist with GDPR compliance, Digital Footprint supports the initial assessment and on-going audit processes by helping organizations identify websites belonging to them, as well as the pages on those websites that collect PII. The PII/GDPR analytics feature flags pages where data collection is not encrypted, where outdated, untrusted encryption mechanisms are being used, or where certificates have expired. As an active compliance tool, the solution can identify the appearance of new sites and collection forms and ensure the presence of approved data usage notices.

Available to U.S. organizations who subscribe to Digital Footprint Enterprise, users will see PII assets highlighted in their inventory and be able to filter based on compliance violation types. Information such as affected webpages and host, domain, and ASN details are available via a central web portal. Users will also be able to configure compliance events to automatically trigger workflows to mitigate the GDPR risk associated with assets. The remediation process can either be audited in Digital Footprint or through integration with existing workflows in other security products, such as SIEMs (security information and event management).

Logon Page Posture



Make accurate and strategic compliance decisions

Be prepared for the GDPR with a full understanding of the scale of your digital presence and active visibility into your assets collecting PII

With RiskIQ Digital Footprint, find internet-facing assets that may be collecting PII such as:

- Corporate website
- Known microsites managed by marketing
- Marketing landing pages
- Microsites created by vendors or as one-off pages
- Servers and web pages that were part of a merger or acquisition but not inventoried
- Abandoned servers or domain names
- Pages created outside of standard procedures



RiskIQ provides comprehensive discovery, intelligence, and mitigation of threats associated with an organization’s digital presence. RiskIQ’s platform delivers unified insight and control over external web, social, and mobile exposures. Thousands of security analysts use RiskIQ to expedite investigations, monitor their attack surface, assess risk, and remediate threats.

Learn how RiskIQ Digital Footprint could help protect your digital presence by scheduling a demo today.

22 Battery Street, 10th Floor
 San Francisco, CA. 94011

✉ sales@riskiq.net 🌐 RiskIQ.com

☎ 1 888.415.4447 🐦 @RiskIQ

Copyright © 2018 RiskIQ, Inc. RiskIQ, the RiskIQ logo and RiskIQ family of marks are registered trademarks or trademarks of RiskIQ, Inc. in the United States and other countries. Other trademarks mentioned herein may be trademarks of RiskIQ or other companies. 03_18

The only warranties for RiskIQ products and services are set forth in the express warranty statements accompanying such products and services. Nothing herein should be construed as constituting an additional warranty. RiskIQ shall not be liable for technical or editorial errors or omissions contained herein.