WEBROOT
Smarter Cybersecurity™

# FAQ | Compliance

## Is Webroot GDPR compliant?

Yes, Webroot is GDPR compliant. As a security company, Webroot takes personal data protection seriously. As a data processor, we:

(i) Have implemented appropriate technical and organizational measures to ensure we keep data secure;

(ii) Keep detailed records of our processing;

(iii) Ensure that cross-border transfers adequately protect data subjects; and

(iv) Have procedures to notify data controllers of data breaches.

If you have any questions about our policies, please contact our Data Protection Officer at privacy@webroot.com.

## Is Webroot PCI compliant?

Yes. Webroot is committed to protecting consumer credit card data in compliance with the Payment Card Industry Data Security Standard (PCI DSS). Our alignment with this standard is reflected in the people, technologies, and processes we employ. Webroot conducts regular vulnerability scans and penetration tests in accordance with the PCI DSS requirements for our business model. In addition, our PCI compliance is attested to annually by Self-Assessment Questionnaires (SAQs).

## Is Webroot ISO 27001 compliant?

Yes, Webroot is certified as ISO 27001: 2013 compliant. We continue to invest in our information security programs, both in terms of people and technology. Additionally, much of our product infrastructure is hosted by Amazon Web Services (AWS), which is also ISO 27001 certified.

## What is Webroot's data security policy?

Webroot has comprehensive information security and data governance policies that govern how we protect information. Such policies include measures to address Access Control, Acceptable Use, Data Classification and Governance, Information Security, Data Protection, Data Retention, Vendor Requirements, Security Incidents, and more. To prevent vulnerabilities, Webroot cannot share these policies externally.

## What measures prevent unauthorized data access from external sources?

To prevent external access, either physically in our facilities or via the network, Webroot maintains a comprehensive Access Control Policy along with technical safeguards, including, but not limited to, network rules, firewalls, and VPN connections.

## What measures prevent unauthorized data access from internal sources?

Internally, Webroot maintains strict account Access Control lists as part of its Access Control Policy and requires authorized employees to maintain private credentials for access. Only authorized employees with specific permissions in Webroot systems have access to applicable systems. To have such permissions, an internal individual must require access to perform the duties of their job.

## What are Webroot's business continuity plans?

Because of the specific and sensitive nature of business continuity plans, Webroot does not share them externally. We understand the importance of maintaining a strong BCP program, and have implemented measures to ensure we can continue our operations in the event of a business disruption.

## What personal data does Webroot collect?

Privacy is very important to Webroot, and we want our users to understand how we collect, process, use, and disclose their personal information when they use our website, online services, or products. Read our applicable privacy statements at www.webroot.com/privacy. If you have questions about Webroot's handling of personal data, please email privacy@webroot.com.

## How can customer data be updated in our systems?

Data maintenance varies depending on the applicable Webroot product, but, generally, customers can update their own data by contacting the Webroot support team or updating their account information in their Webroot management console (as applicable).

continued »

## How can I opt out of Webroot marketing messages?

Email unsubscribe@webroot.com and your email address will be added to a suppression list. After that, you will only be contacted with transactional messages, if applicable.

## More Compliance Questions?

If you have additional questions about Webroot and data privacy compliance that were not addressed elsewhere, please click here to get in touch with us.

**About Webroot**

Webroot was the first to harness the cloud and artificial intelligence to protect businesses and individuals against cyber threats. We provide the number one security solution for managed service providers and small businesses, who rely on Webroot for endpoint protection, network protection, and security awareness training. Webroot BrightCloud® Threat Intelligence Services are used by market leading companies like Cisco, F5 Networks, Citrix, Aruba, Palo Alto Networks, A10 Networks, and more. Leveraging the power of machine learning to protect millions of businesses and individuals, Webroot secures the connected world. Headquartered in Colorado, Webroot operates globally across North America, Europe, and Asia. Discover Smarter Cybersecurity® solutions at webroot.com.

**World Headquarters**
385 Interlocken Crescent
Suite 800
Broomfield, Colorado 80021 USA
+1 800 772 9383

**Webroot EMEA**
6th floor, Block A
1 George's Quay Plaza
George's Quay, Dublin 2, Ireland
+44 (0) 870 1417 070

**Webroot APAC**
Suite 1402, Level 14, Tower A
821 Pacific Highway
Chatswood, NSW 2067, Australia
+61 (0) 2 8071 1900