Preparing for GDPR–Barracuda can help

The General Data Protection Regulation (GDPR) is scheduled to go into effect on May 25, 2018. The GDPR replaces the Data Protection Directive that has been in place since 1995. It applies to all organisations that process personal data of an EU citizen in connection with the offering of goods or services, or that monitor individuals in the EU. While the broad guidelines are similar to the Data Protection Directive, GDPR adds new requirements and additional protections for the personal data of EU residents. Penalties for non-compliance may be harsh, up to €20,000,000 or four percent of an organisation's total global revenue.

How Barracuda Helps You Comply with GDPR

GDPR does not prescribe a specific set of technologies or processes. Rather, it lays out guidelines and requirements for data protection including storing, processing, sharing, retention, recovery, transfer, and more. GDPR requirements impact both data security and data management.

Complying with GDPR is not simply an IT challenge. It requires a combination of technology, processes, and education, along with an expanded scope of diligence, focus, and effort. While no one product can make you GDPR compliant, the right security technologies can be a critical part of a comprehensive strategy to achieve, maintain, and document compliance.

Data Protection and Security of Processing

The GDPR makes controllers responsible for ensuring that processing activities are performed in compliance with the Regulation. Controllers must implement appropriate technical and organisational measures to ensure they will be able to demonstrate that processing is performed in accordance with the Regulation.

Barracuda Support for Data Protection and Security of Processing

Barracuda security and data protection solutions deliver a broad range of state-of-the-art security and data protection technologies to extend advanced protection across key threat vectors.

They offer multiple deployment options, including hardware and virtual appliances, and public cloud deployments. They dramatically reduce the attack surface and enforce a consistent security policy across all data sources and traffic, and across all locations and users.

They are designed for highly distributed, cloud-connected networks, and optimised for centralised, single-pane-of-glass management and visibility.

Combat Network Breaches with Barracuda CloudGen Firewall

Barracuda CloudGen Firewalls provide advanced security at all network and data-transfer boundaries. Their comprehensive firewall technologies include Layer 7 application profiling, intrusion prevention, web filtering, protection against malware and advanced threats, antispam protection, and network access control. Advanced Threat Protection efficiently blocks unknown, zero-day threats, and intelligent traffic management optimises performance.

Combat Hacking with Barracuda Application Security Solutions

Barracuda web application firewall solutions scan and secure your online applications, eliminating both known and zero-day vulnerabilities. They defeat today's most sophisticated, complex threats, including DDoS attacks, with advanced inspection capabilities that do not impact throughput. They inspect inbound traffic to combat web-based attacks including the OWASP Top 10, and outbound traffic to prevent data loss and leakage. And they improve overall app performance with built-in application delivery features including SSL offloading, load balancing, and content caching.

Combat Email-Borne Threats with Barracuda Essentials

Barracuda Essentials provides the most complete, simple, and affordable solution for protecting business emails and data in Office 365, Microsoft Exchange, and G Suite. It combines our award-winning email security and our advanced archiving technology to ensure and document regulatory compliance while simplifying e-discovery searches. Includes Advanced Threat Protection, and is compatible with both on-premises and hybrid deployments. For Office 365, Barracuda also offers full cloud-to-cloud backup and recovery of all your emails and files.

Preventing Data Breaches, Leakage, and Loss

Barracuda security and data protection solutions include powerful capabilities that prevent data exfiltration and prevent hacks, data theft, and other breaches. They make it easy to regulate data access at a granular level. They allow you to prevent data leakage, and make it fast and easy to recover from data loss when it does happen.

Combat Breaches and Unauthorised Access with Barracuda CloudGen Firewall

Barracuda CloudGen Firewall includes advanced features to combat data breaches:
- Complete visibility and control of all network traffic
- Regulation of application, user, and content policies
- Dynamic traffic analysis for real-time protection
- URL filtering, IDS, and IPS to prevent unauthorised access to confidential data
- Detects and blocks outbound phone-home activity
- Secure VPN access for remote locations and users

Combat Hacks and Data Theft with Barracuda Application Security Solutions

Barracuda web application firewall solutions are designed to extend protection against hacks and data theft across your hybrid, distributed, cloud-connected network. They secure both on-premises and cloud-hosted applications and websites, and help you enforce strict control over access to resources:

- Integrate AD, RADIUS, or LDAP-compatible authentication services
- Enable multi-factor authentication
- Control access based on geolocation

They also secure your web applications against botnets, and inspect all outbound traffic to block sensitive data and enforce DLP policies.

Combat Email-Borne Exfiltration with Barracuda Essentials and Sentinel

Barracuda Essentials and Barracuda Sentinel work together to deliver the most complete, advanced protection available to prevent data exfiltration and theft via email.

- Blocks ransomware and other advanced threats
- Prevents targeted threats like phishing, spear phishing, domain spoofing, and CEO fraud
- Inspects outbound email for leakage of sensitive data
- Encrypts, quarantines, or blocks outbound emails based on content, sender, or recipient
- Includes cloud-based archiving and backup to recover from malicious or accidental data loss

Combat Data Loss with Barracuda Backup and Archiving

Barracuda Backup creates secure, redundant, real-time backups of your data that are replicated offsite with AES 256-bit encryption to protect against ransomware and other malicious attacks, along with natural disasters, hardware failures, and human error. Multiple restore options include bare-metal restores for physical servers and fast, image-based restores for virtual environments to minimise downtime, lost productivity, and legal exposure resulting from data loss.

Barracuda archiving solutions securely index and preserve unmodified copies of every email message and attachment at the time it is sent or received. In some products, historical email data can also be imported to provide a complete archive. Advanced search and audit trails help you demonstrate regulatory compliance.

Breach Notification

GDPR requires that Controllers notify supervisory authorities within 72 hours of becoming aware of a personal data breach. When the breach is likely to result in a high risk to the rights and freedoms of natural persons, a Controller much also notify the data subject without undue delay.

Barracuda Support for Breach Notification

Barracuda security and data protection solutions include robust, detailed, and easy-to-customise logs, reports, and dashboards, making it easy for you to analyse, remediate, and notify quickly, accurately, and completely in the event of a data breach or other security incident.

Right to Erasure ("Right to Be Forgotten")

In certain instances, the data subject may require the controller to erase any personal data concerning him or her.

Barracuda Support for Right to Erasure

Many Barracuda products allow customers to define data retention periods through configuration, and to manually delete data records upon request of the data subject.

Records of Processing Activities

Controllers must maintain records of processing activities, including name and contact details of the Controller, purpose of the processing, description of categories of data being processed, transfer to a third country, time limits for erasure, and a general description of technical and organisational measures.

Barracuda Support for Recording Processing Activities

- Barracuda CloudGen Firewalls provide both real-time and historical application visibility that records application traffic on the corporate network. Intended to enable QoS optimisation for critical applications, this capability also records relevant processing activities.

- Barracuda web application firewall solutions enable powerful, graphical reporting on compliance, threat activity, web traffic, and much more. More than 50 pre-defined report templates are included, and you can customise broadly using multiple filters. Reports are interactive, allowing you to drill down to highly granular info. Reports are based on comprehensive logging of all client requests, administrator modifications, and firewall actions.

- Barracuda archiving solutions preserve an accurate record of all system activities, helping you maintain and demonstrate regulatory compliance. Powerful search capabilities let you easily find and export data related to specific activities if needed for reporting or analysis.

Please visit www.barracuda.com/solutions/gdpr or contact your Barracuda representative
to learn more about how we can help support your GDPR compliance plan.

How Barracuda Complies with GDPR

Barracuda Support for Compliant Data Transfers

Barracuda has certified that it complies with the EU – US Privacy Shield Framework and the Swiss – US Privacy
Shield Framework as set forth by the US Department of Commerce and approved by the European Commission
regarding the collection, use, and retention of Personal Information transferred from the European Union
and Switzerland to the United States, respectively. Use this link to obtain details on Barracuda's Privacy Shield
Certifications: https://www.privacyshield.gov/participant?id=a2zt0000000TQk6AAG&status=Active
Please see our privacy statement and security documentation at:
https://www.barracuda.com/legal/privacy
https://www.barracuda.com/support/security

Disclaimer

The intention of this paper is to provide a high-level overview of how Barracuda products may help you comply
with GDPR's technical requirements. Essential details relevant to your organisation may be missing. To ensure
compliance, please consult your lawyer, legal department, or data protection officer. GDPR requires a set of
technical and organisational measures as well as documentation, defined processes, and training. Barracuda
Networks and its comprehensive security and data protection solutions can contribute to meeting
those requirements, but cannot, and do not, guarantee full compliance.