Malwarebytes

GETTING READY FOR GDPR COMPLIANCE

Corporate readiness for the most important change in data privacy regulation in 20 years.

This guide explains basic provisions of the new General Data Protection Regulation (GDPR), the most important change in data privacy regulation in 20 years. This Getting Ready guide explains what GDPR is, how it affects data privacy and security, and how your business can identify and implement changes required to be in compliance with GDPR.

> IN OUR DATA-DRIVEN ECONOMY, DATA PROTECTION IS CENTRAL TO CUSTOMER TRUST. IT GIVES A COMPETITIVE ADVANTAGE TO BUSINESS, WHICH CAN USE THEIR HIGH PRIVACY STANDARDS TO ATTRACT AND RETAIN CUSTOMERS.
>
> *Věra Jourová,*
> *EUROPEAN COMMISSIONER FOR JUSTICE, CONSUMERS, AND GENDER EQUALITY*

THE ESSENTIAL GDPR FACTS

WHO

If your business handles the personal data of European Union (EU) residents, you are subject to GDPR, even if your business is located outside the EU. It's never been more important to ensure that your data protection policies and security technologies are effective, as well as in compliance with GDPR.

WHY

Currently, each country in the EU has its own data protection laws, so doing business in the EU meant companies had to deal with different laws for each country. GDPR means one consistent regulation for data privacy.

WHAT

The goal of the GDPR is to protect all EU citizens from data and privacy breaches by harmonizing data privacy laws across all European Union member states.

WHEN

GDPR goes into effect on May 25, 2018. Organizations must be ready to demonstrate compliance by that date.

> THE GDPR WILL AFFECT NOT ONLY EU-BASED ORGANIZATIONS, BUT MANY DATA CONTROLLERS AND PROCESSORS AROUND THE GLOBE. WITH RENEWED FOCUS ON INDIVIDUAL DATA SUBJECTS AND THE THREAT OF FINES OF UP TO €20 MILLION OR 4% OF ANNUAL GLOBAL TURNOVER FOR BREACHING GDPR, ORGANIZATIONS HAVE LITTLE CHOICE BUT TO RE-EVALUATE MEASURES TO SAFELY PROCESS PERSONAL DATA.
>
> *Bart Willemsen*
> *Research Director*
> *Gartner*

GLOBAL IMPACT

Key Terms

DATA CONTROLLER

Any business or organization that collects and handles the personal data of EU residents.

DATA PROCESSOR

A business that processes personal data on behalf of a Data Controller. For example, if your business uses a third-party cloud processing service, that service is considered a Data Processor for purposes of GDPR compliance.

DATA SUBJECT

An EU resident whose personal data is handled by your business.

PERSONAL DATA

The new regulation covers a wide range of personal data, including:

- Name, address, phone numbers, ID numbers, email addresses, and banking details
- Web data, including location, IP address, cookie data, and RFID tags
- Health, genetic, and biometric data
- Racial or ethnic data, sexual orientation, religious and political opinions

KEY GDPR COMPONENTS

The GDPR updates and expands data privacy and protection in several ways.

SCOPE

Any business that processes personal data of EU residents is now covered by the GDPR. Previously, if your business was not located in the EU, data privacy and protection regulations were ambiguous. Now, if you handle personal data of EU residents, the regulation applies to your business no matter where it is located. If your business requires that you perform regular and systematic monitoring of data subjects on a large scale, or you work with special categories of data, you will also need to appoint a Data Protection Officer responsible for GDPR compliance.

CONSENT

The conditions for consent require companies to use intelligible and easily accessible forms that clearly state the purpose of the data processing. The ability to withdraw consent must be as easy and simple as the ability to give consent.

PENALTIES

If you are in breach of GDPR, your business can be severely fined, up to 4% of your annual global revenue or 20 million Euros (whichever is greater). These penalties apply to both controllers and processors, so cloud processing is not exempt from GDPR.

DATA SUBJECT RIGHTS

GDPR provides more rights to EU residents in how their personal data is collected and handled. In many cases, this will affect how your company does business with your customers.

BREACH NOTIFICATION

When there is a data breach that may affect the "rights and freedoms of individuals," notification must be done within 72 hours of the breach. Data processors must notify data controllers without undue delay when they discover a data breach. These elements should be included in your disaster recovery program.

RIGHT TO ACCESS

Data controllers must provide a copy of personal data when the data subject requests it. The information must be free of charge and in an electronic format.

RIGHT TO BE FORGOTTEN

When data is no longer relevant to the original purpose or the data subject has withdrawn consent, the person can request erasure of that personal data.

DATA PORTABILITY

The data subject has the right to receive personal data concerning them and transmit that data to another controller.

PRIVACY BY DESIGN

Data Controllers may hold and process only the data necessary for work (data minimization) and limit access to that personal data to those needing it for the processing.

3 STEPS TO BECOMING GDPR COMPLIANT

Implementing GDPR will require changes to how your business collects, uses, and stores customer data. In addition, when customers exercise their data rights, you will need a response plan and process in place to release that data or remove it entirely. Your security and IT teams can take the lead in securing data and updating related processes. From Marketing and HR to Finance, every department must be involved preparing for GDPR.

1

IDENTIFY CURRENT PRACTICES

- Audit the data and data flows used by your business, including sources, how data is used, how long it is retained, and if any of it is handled by third-party data processors.
- Look at the hardware infrastructure, disaster recovery, and other elements of data security within your business and with any third-party data processors.

2

PERFORM A GAP ANALYSIS

- Determine what data is required going forward and what data can be removed. The less data you need to secure, the easier it will be to comply with GDPR, and this also reduces your data exposure in the event of a data breach.
- Understand where the data is stored and how accessible it is to meet requests from data subjects.
- Work with every department to identify the required software and systems changes to comply with GDPR and how your team can support these efforts.

3

BUILD YOUR ROADMAP

Your specific steps to GDPR compliance depend on the type of business you're in and what personal data you have or need to operate. Place data protection at the core of every decision you make, so your efforts form a long-term commitment to user privacy and data security.

- Update data management and security processes involving personal data, including storage and long-term retention.
- Create audit trails for data collection and processing, especially hand-offs to third-party data processors.
- Be transparent about what data you collect and why, so that everyone in the organization and your customers understand that data protection and privacy is a key priority for your business.
- Contact EU residents asking them to opt-in or give explicit consent when needed to be on your existing marketing lists of customers or prospects. Consent text must be clear and informative, explaining how and when their data will be used.
- Identify which department will work with requests from EU residents, and then develop the processes to meet the new GDPR rights for data subjects. In addition, you will need to determine which EU member state is your supervisory authority.
- As part of your business continuity plan, build a clear process for responding to data breaches quickly and efficiently.

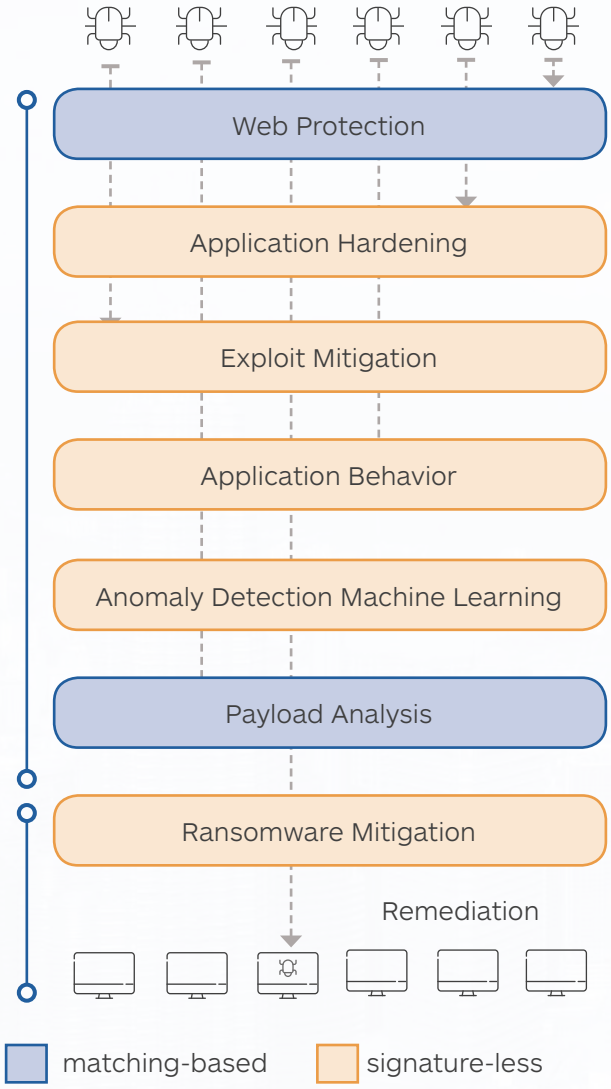
> KEEPING PERSONAL DATA SECURE AND PREVENTING DATA BREACHES IS A FUNDAMENTAL TENANT OF GDPR. MALWAREBYTES SOLUTIONS HELP COMPANIES ATTAIN THIS PRINCIPLE WITH BEST-IN-CLASS SECURITY AND REMEDIATION SOLUTIONS.
>
> *Ed Brown*
> *Vice President & General Counsel*
> *Malwarebytes*

HOW MALWAREBYTES CAN HELP

Malwarebytes helps address the problem GDPR is designed to eliminate—the breach itself. With Malwarebytes, organizations can take proactive steps to protect their data and maximize the value of their compliance investments.

Malwarebytes makes it easy to achieve effective endpoint protection that optimizes your IT resources and cost efficiency.

Our solution combines best practice detection layers to deliver leading endpoint security with simplified management and minimal end-user impact. This creates an interlocking web of techniques that work together to not only block malware but also its deployment and execution on the endpoint.



PROTECTION LAYERS

Our platform delivers the following real-time protection layers:

Web Protection

Web protection protects users by preventing access to malicious websites, ad networks, scammer networks, and "bad neighborhoods."

Application Hardening

Application hardening reduces the vulnerability surface, making the computer more resilient, and proactively detects fingerprinting attempts by advanced attacks.

Exploit Mitigation

Exploit mitigations proactively detect and block attempts to abuse vulnerabilities and remotely execute code on the machine, which is one of the main infection vectors nowadays.

Application Behavior

Application behavior ensures that installed applications behave correctly and prevents them from being abused to infect the machine.

Anomaly Detection Machine Learning

Anomaly detection machine learning proactively identifies viruses and malware based on anomalies from known and good files.

Payload Analysis

Payload analysis is composed of heuristic and behavioral rules to identify entire families of known and relevant malware.

Ransomware Mitigation

Ransomware mitigation is a behavior monitoring technology that detects and blocks ransomware from encrypting users' files.

INCIDENT RESPONSE LAYER

Thorough Remediation

In addition to real-time protection layers, our solution delivers automated, accurate, and thorough remediation. This provides your organization with critical coverage for the entire attack lifecycle – from initial infection attempts through an actual infection.

GDPR-Ready Security Capabilities

The table below provides an overview of Malwarebytes' key capabilities that help you meet the security outcomes of a GDPR-ready organization:

PERSONAL DATA PROTECTION

- Rules- and AI-based protection layers work together to form an interlocking web of endpoint protection that safeguards your customer data
- Provides most comprehensive real-time detection with seven protection layers
- Provides critical coverage for the entire attack lifecycle–from initial infection attempts through an actual infection

EMPLOYEE PROTECTION

- Protects your data by preventing malware from gaining a foothold on your endpoints
- Delivers effective offline protection with our signatureless layers when your employees are not at the office
- Web Protection layer protects your employees from connecting to malicious websites
- Ransomware Protection prevents your data files from becoming encrypted and held for ransom
- Restores user devices after a malware infection
- Supports multiple platforms, including Mac, Windows, and Android

DATA CENTER PROTECTION

- Delivers protection against malware and unknown threats for the servers across your environment

INCIDENT RESPONSE

- Incident response layer delivers automated, accurate, and thorough remediation to eliminate manual, ad hoc efforts
- Shortens attack dwell time
- Improves speed of detection and response with integrations to your existing security orchestration tools

SUMMARY

For most organizations, GDPR is a game-changer, and getting compliance-ready should be top of mind for your organization's business and security leaders. It's important to prioritize new programs and solutions that ensure your organization is ready for the enhanced regulatory environment.

Malwarebytes helps organizations focus on the security essentials of protecting personal data by using multiple layers of pre- and post-execution engines to stop malware and other threats before and after they execute.

LEARN MORE:
MALWAREBYTES.COM/GDPR

Malwarebytes