

GETTING TO THE GDPR FINISH LINE

WatchGuard®

Table of Contents

Racing the clock! 3

Who's in the race? 4

What's considered personal data? 5

Watch out for course hazards. 6

- Data breach notifications 6
- Explicit consent 6
- Data transfer out of the EU 6
- Data Protection Officer (DPO) appointment 7
- Penalties/costs of non-compliance 7

The winning strategy. 8

Crossing the finish line 9

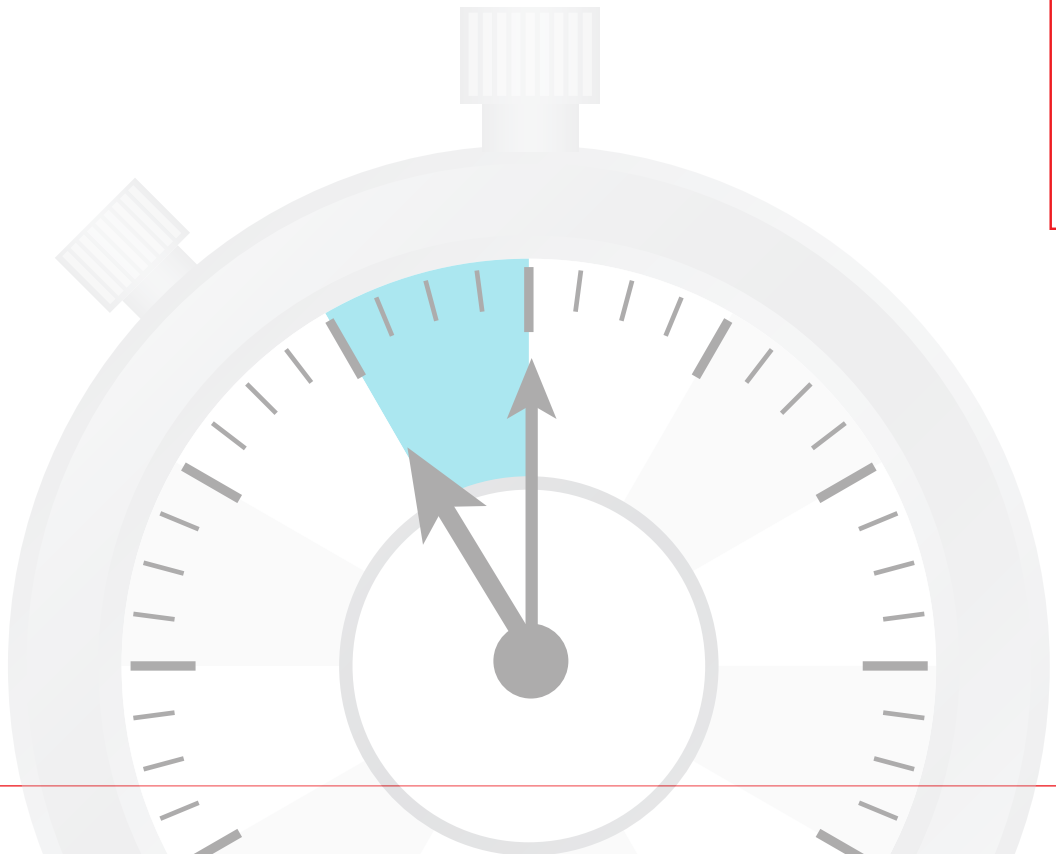
GDPR planning checklist 14

Racing the clock!

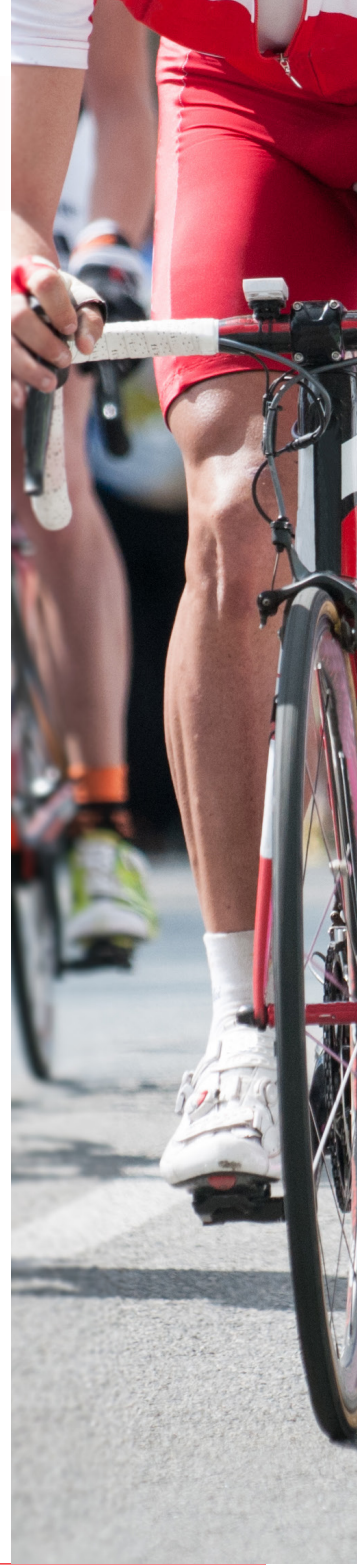
With the April, 2016 adoption of (EU) 2016/679, commonly known as the General Data Protection Regulation (GDPR), companies just like yours are now racing to achieve compliance before it becomes effective on **May 25, 2018**, or possibly face huge fines and potential lawsuits. This effort is larger and more difficult because this Regulation significantly expands the scope of responsibility from the 1995 Data Protection Directive (Directive 95/46/EC) that was previously in effect.

The good news – **you are not alone!** Just like the peloton in a bicycle race, most companies are about in the same spot in the compliance process, and we will reach the finish faster and easier with cooperation.

Therefore, this eBook shares key information on GDPR and offers solutions to guide your compliance initiative and improve your data security.



The General Data Protection Regulation takes effect **May 25, 2018**



Who's in the race?

Organizations that collect, store, and/or process personal information need to comply with the GDPR if they:

- offer goods or services to EU citizens residing in the EU

  OR

- monitor the behavior of EU citizens residing in the EU

This includes organizations not based in nor with any presence in the EU, and also includes those with EU employees but without EU customers. So long as you are handling some form of personal information regarding EU natural citizens…you're in!

All organizations that meet these criteria must comply. However, businesses and organizations that process more than 5,000 individuals in any 12-month period have an expanded set of requirements.

The Regulation refers to organizations required to comply with the GDPR as either "controllers" or "processors." Controllers are the entities that determine the purposes, conditions and means of the processing of personal data, while the processors are the entities that process the personal data on behalf of the controller.

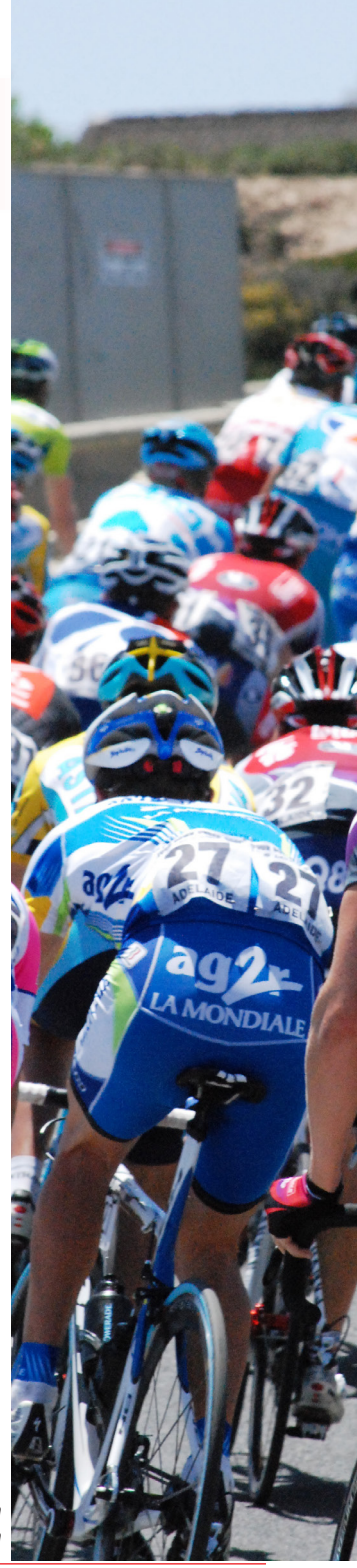
> For instance, a healthcare clinic may outsource their lab work to another facility. The clinic would need to share a certain amount of personal information they have collected with the lab service in order to return results to the correct patient. In this scenario, the healthcare provider is the controller, and the lab vendor is the processor for GDPR consideration. There are some differences in Regulation requirements for each role, and so you'll want to determine whether one or both apply to your organization.

What's considered personal data?

The GDPR interprets the definition of personal data broadly. Any piece of information that can be used to directly or indirectly identify a person is considered personal data. It can be anything from a name, photo, email address, bank details, national ID number, posts on social networking websites, medical information, and even a computer IP address that relates to a specific user's account or device.

> As an example, if you were operating a race and capturing or assigning race bib numbers in a computer system – where the bib numbers are associated with a specific individual - then it would be considered personal data. Moreover, those numbers are often easily cross-referenced with personal data such as registrant name, address, photo, pre-race medical screening and other information.





The peloton
Photo: Sue Hixson

Watch out for course hazards.

The GDPR includes a number of items that were not a part of the older Data Protection Directive, and may trip you up if you are not looking for them. Here's a description of some of the more significant new requirements, but consult the Regulation for complete details and a full list.

- **DATA BREACH NOTIFICATIONS:** Controllers and processors are now required to notify supervisory authorities within 72 hours of learning of a breach, and to notify the people to whom the data applies (data subjects) "without undue delay."

> It should be noted that a breach of **encrypted data** is **specifically excluded** from notification requirements and so may factor in to your compliance strategy.

- **EXPLICIT CONSENT:** The GDPR requires that at the time you collect personal data, explicit consent must be given by the data subject. This means that organizations can no longer bury generic consent in a long form full of legalese. Instead, organizations must offer specific information on what data is collected, how the data will be stored and processed, and must use clear and plain language. In this context, nothing short of "opt-in" will satisfactorily address the regulation. Furthermore, it must be as easy to withdraw consent as to give it.
- **DATA TRANSFER OUT OF THE EU:** Personal data may not leave the EU unless you have approval from the Supervisory Authority, or where the data subject is informed of the data transfer and associated risks, and authorizes the transfer.

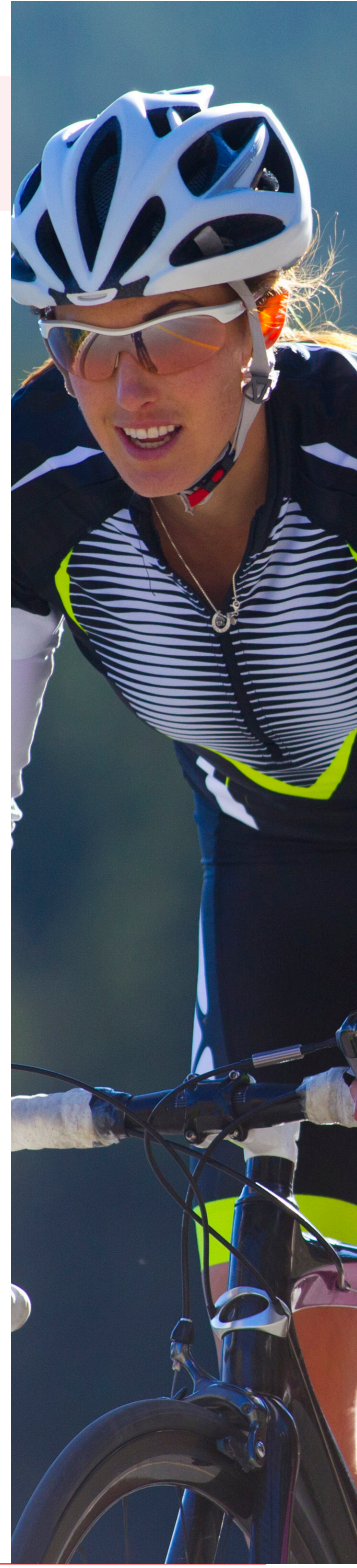


- **DATA PROTECTION OFFICER (DPO) APPOINTMENT:** If you process the data from more than 5,000 individuals in any 12-month period then you must appoint (hire, assign, or contract with) a DPO for your organization. The DPO is your representative to the Supervisory Authorities who monitor and ensure compliance with the Regulation. He or she is also the contact for any requests or complaints from data subjects. In addition, they lead your compliance activities, such as required by the Data Protection Impact Assessment (DPIO), and handle communication on security policies, assessments, compliance, requests from data subjects and breach notifications among others. Per the regulation, the DPO reports to the executive level manager, and is a two-year appointment that may be extended.

Organizations can be assessed a fine up to **€20 million** or **4%** worldwide revenue

- **PENALTIES/COSTS OF NON-COMPLIANCE:** Businesses and organizations that do not comply with the GDPR can be assessed a fine up to €20 million or 4% worldwide revenue. The fines are tiered and are assessed even for first-time offenses, and can include a fine of 2% worldwide revenues for not having records in order (Article 28), for example. What's more, organizations may incur additional expenses including legal fees and court-ordered remedies if EU citizens feel their rights have been infringed, sue for damages, and win their case.





The winning strategy.

Becoming compliant with the GDPR requires a significant effort for nearly all businesses, and will most certainly include adding:

- Data protection measures **using the latest, most effective network security technology** that:
  - **protects data** during storage and transmission
  - ensures **situational awareness** of risks
  - enables **preventative, corrective and mitigating action in near real time** against vulnerabilities or incidents detected that could pose a risk to data
  - provides **tools for assessing** the effectiveness of security policies
- Data recovery mechanism that restores access to data when an incident disrupts availability
- New or improved processes and reporting structures for tracking consent, notification of breaches and compliance

You should also consider where you have the opportunity to reduce the scope/risk of GDPR impact, so that the burden associated with monitoring, record-keeping, and compliance activities associated with the GDPR are reduced.
For example:

- **Reduce** the number of personal data fields collected/processed
- **Reduce** the amount of time that personal data is held/processed
- **Encrypt data** in storage and during transmission
- **Mask IP addresses** and anonymize other types of user information
- **Reduce** the number of authorized staff who can access personal data
- **Increase** your ability to prevent and remediate threats to personal data

We've included a GDPR Planning Checklist at the end of this eBook that helps to get you started with GDPR compliance planning.

The checklist and supporting questions take you through an evaluation of current policies and security practices so that you can see alignment and gaps with the Regulation.

Crossing the finish line!

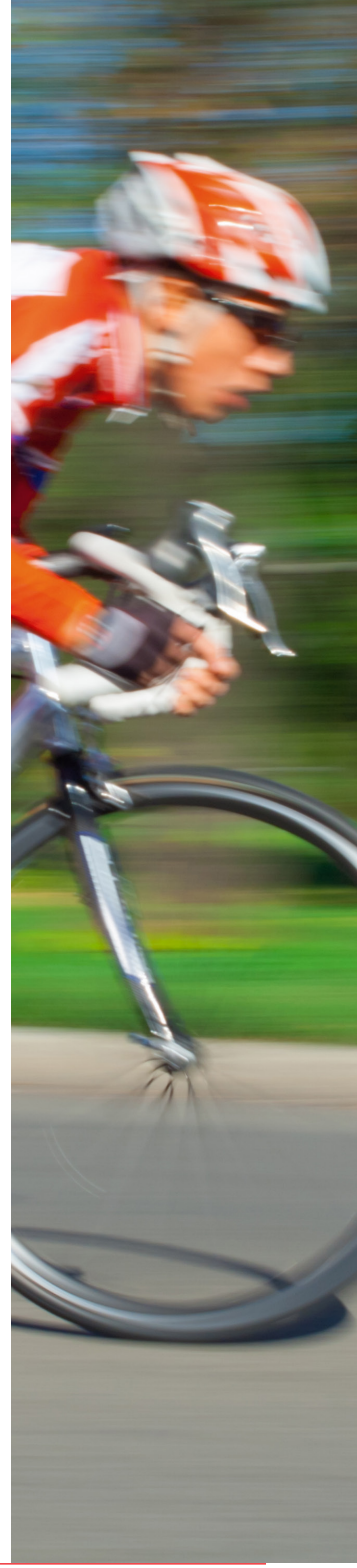
Now that you have some good ideas about how to start to build a GDPR-compliant organization, you are undoubtedly looking to fill gaps and deficiencies with the fast, easy answers that satisfy the Regulation and complete this monumental task in time. WatchGuard can help to achieve compliance with highly effective data security technology and practices.

Moreover, we made it easy. WatchGuard has the data security upgrade needed to comply with GDPR data security measures, all in one easy-to-use package with our Total Security Suite. Delivering strong, enterprise-grade security, a WatchGuard Firebox® security appliance with Total Security Suite addresses 16 of SANS Top 20 Critical Security Controls (v6) and so provides the comprehensive product needed for GDPR compliance.

A WatchGuard Firebox security appliance with Total Security Suite addresses
16 of SANS **Top 20** Critical Controls

SANS Top 20 Critical Security Controls V6

CS1	Inventory of Authorized and Unauthorized Devices	*Yes*	CS11	Secure Configurations for Network Devices such as Firewalls, Routers, and Switches	*Yes*
CS2	Inventory of Authorized and Unauthorized Software	*Yes*	CS12	Boundary Defense	*Yes*
CS3	Secure Configuration for Hardware and Software on Mobile Devices, Laptops, Workstations, and Servers	*Yes*	CS13	Data Protection	*Yes*
CS4	Continuous Vulnerability Assessment and Remediation	*Yes*	CS14	Controlled Access Based on the Need to Know	*Yes*
CS5	Controlled Use of Administrative Privileges	*Yes*	CS15	Wireless Access Control	*Yes*
CS6	Maintenance, Monitoring, and Analysis of Audit Logs	*Yes*	CS16	Account Monitoring and Control	*Yes*
CS7	Email and Web Browser Protections	*Yes*	CS17	Security Skills Assessment and Appropriate Training to Fill Gaps	*N/A*
CS8	Malware Defenses	*Yes*	CS18	Application Software Security	*Yes*
CS9	Limitation and Control of Network Ports, Protocols, and Services	*Yes*	CS19	Incident Response and Management	*N/A*
CS10	Data Recovery Capability	*No*	CS20	Penetration Tests and Red Team Exercises	*N/A*

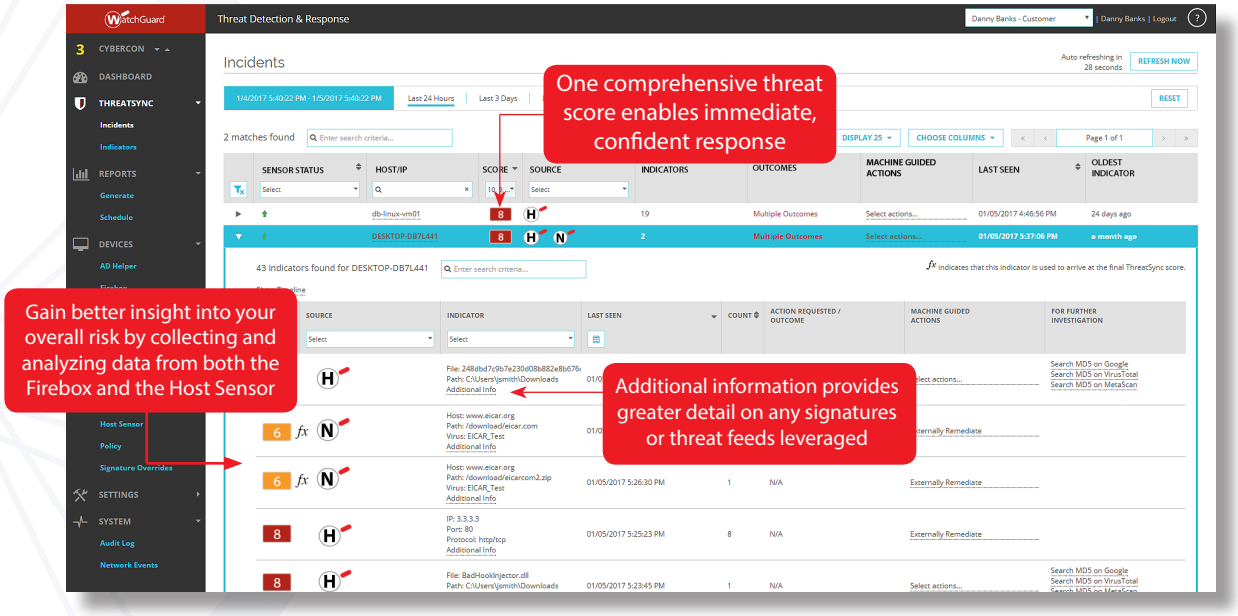


Crossing the finish line!

Our Total Security Suite offers unique solutions to specifically address GDPR requirements including:

Threat Detection and Response (TDR) – The GDPR requires "situational awareness," which WatchGuard provides with our distinctive ThreatSync feature. ThreatSync correlates security information from network and endpoint devices to make you aware of escalating security incidents in an easy-to-decipher dashboard.

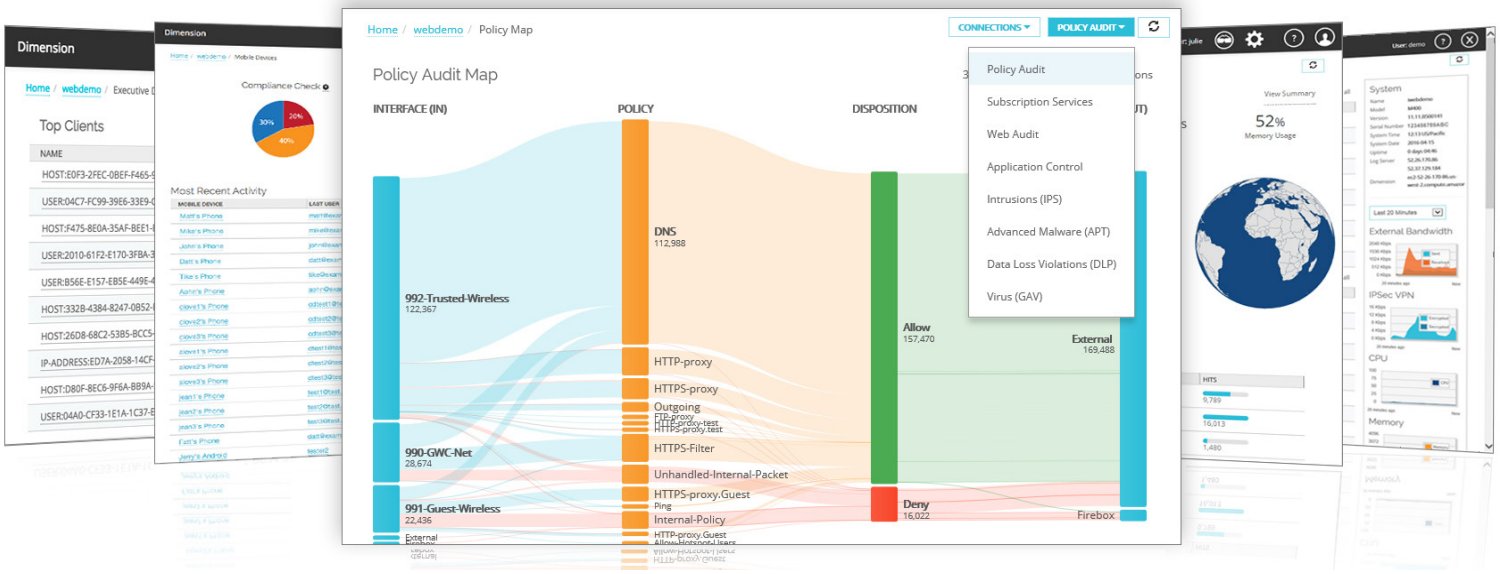
Furthermore, you can create policies to remediate "high-scoring" incidents automatically, more than meeting the requirement for "preventative, corrective and mitigating action in near real time." Even better, once a threat is remediated, the information is shared with our threat intelligence feed so that it identifies and prevents it from re-entering your network! And since TDR is a cloud-based service, you can choose to have your data stored in the EU to comply with the data transfer article in the Regulation.



Threat Detection & Response

WatchGuard Dimension™ – For GDPR requirements that focus on ready access to meaningful log data and reports that demonstrate compliance, Dimension delivers a swift and effective solution. It provides big-data style visibility and reporting tools that uniquely identify and distill key network security issues and trends, accelerating the ability to combat threats, report on all network security activity, and set meaningful security policies across the network.

What's more, Dimension includes a powerful User Anonymization feature that can replace all personally identifiable information (PII) in Dimension's reports, dashboards, and summary pages with hashed placeholder text. It hashes user names, IP addresses, host names, and mobile device names with never-repeated, randomly generated alphanumeric sequences to ensure data in transit is masked.



WatchGuard Dimension



Crossing the finish line!

Encryption & VPN – Keeping personal data encrypted in storage and during transit is a key strategy for success for compliance success, as it significantly reduces the notification requirements after a data breach. WatchGuard's Firebox UTM solutions feature drag-and-drop VPN creation between branch offices and HQ. In addition to fast and easy set-up, our VPNs are built to last, and known for their stability – which is critically important when your business relies on consistent data availability.

When considering all the strong security and VPN features, visibility and user anonymization with Dimension, and situational awareness and automated remediation with Threat Detection and Response, WatchGuard's Firebox with Total Security Suite is the clear winner to help you reach the finish in time for GDPR compliance!



The First Man to Cycle through the Eurotunnel
Photo by: Chris Froome

WatchGuard's Total Security Suite

FUNDAMENTAL SECURITY SERVICES

- INTRUSION PREVENTION SERVICE (IPS)
- REPUTATION ENABLED DEFENSE SERVICE (RED)
- SPAMBLOCKER
- GATEWAY ANTIVIRUS (GAV)
- WEBBLOCKER URL FILTERING
- NETWORK DISCOVERY
- APPLICATION CONTROL

ADVANCED SECURITY SERVICES

- APT BLOCKER – ADVANCED MALWARE PROTECTION
- DATA LOSS PREVENTION (DLP)
- THREAT DETECTION AND RESPONSE
- DIMENSION COMMAND



GDPR Planning Checklist

Our GDPR Planning Checklist helps you get started in evaluating and implementing GDPR compliance measures. This resource is not an exhaustive list of requirements and should be used in conjunction with other resources to build a comprehensive compliance plan.

☑ Identify the personal data fields that you are collecting from natural EU citizens.

- What personal data is collected and/or processed?
- Where is it stored or transmitted? For how long?
- What retention policies or processes apply to this data? Can this be reduced?
- Is it under your control or that of a contractor?
- Does this data remain in the EU at all times?

☑ Characterize the consent information and processes that exist when collecting this data.

- Are data subjects asked in clear language for explicit consent to collect and process their data?
- Is consent granted at the time of collection?
- Does the consent communication identify and provide contact information for the controller, processor and DPO (where appropriate)?
- Does it describe the purpose of processing, security of processing, and legal basis?
- Does it provide the period for which the data will be stored?
- Does it name the recipients or category of recipients of the data?
- Does it explain the data subjects' right to access, rectify, request erasure or make portable their data, as well as their right to complain to a supervisory authority?
- Does it state the intent to transfer the data outside of the EU?
- Does it stipulate whether data collection is mandatory or optional, as well as the consequences of not providing said data?
- Is it just as easy to withdraw consent as provide consent?

☑ Characterize the ability to communicate with data subjects

- How do data subjects access, rectify, have erased, and extract their data for transfer?
- How do data subjects withdraw consent?
- How does the organization contact data subjects to report a breach?

Determine if current record-keeping measures and data processing policies are adequate.

- Is there a record of data subject response to consent?
- Is there a record or log of data processing events involving personal data?
- Are these records secure and allow for queries, searches or reports by authorized personnel?
- Are policies kept current that describe how data processing is performed in compliance with the Regulation?
- If a controller is outside the EU, is there a designated representative within the EU, and is this documented?
- If data processing services are contracted, does the legal agreement include the necessary clauses to ensure proper security and handling of personal data so as to be in compliance with GDPR?
- Is there sufficient access control to servers and buildings to prevent unauthorized individuals from accessing personal data?

Determine if data security practices and technology are adequate to meet GDPR requirements.

- Are appropriate technical and organizational measures taken to ensure that data is protected from accidental or unlawful destruction, loss, or alteration and unauthorized or unlawful storage, processing, access or disclosure?
- Does the security policy address the following:
  - how to protect data during storage and transmission
  - how to restore access to data when an incident disrupts availability
  - how to ensure situational awareness of risks and enable preventative, corrective and mitigating action in near real time against vulnerabilities or incidents detected that could pose a risk to data
  - describe the process for regularly assessing the effectiveness of security policies
- Is there a process for providing breach notifications within 72 hours?
- Is there a record of a Data Protection Impact Assessment (DPIA) assessing whether processing operations are likely to present specific risks? Was it completed within the last two years, or immediately when there was a change to specific risks in processing operations?
- Is there a designated Data Protection Officer (DPO)?

The answers to these checklist questions should help to identify where you may have deficiencies so that they can be addressed before running out of time.





Visit **www.watchguard.com** to learn more

Global Headquarters
United States
Tel: +1.206.613.6600
Email: sales@watchguard.com

European Headquarters
The Netherlands
Tel: +31(0)70.711.20.85
Email: sales-benelux@watchguard.com

APAC & SEA Headquarters
Singapore
Tel: +65.6536.7717
Email: inquiry.sea@watchguard.com

WatchGuard®

1. http://www.eugdpr.org/
2. https://en.wikipedia.org/wiki/General_Data_Protection_Regulation
3. https://www.sans.org/media/critical-security-controls/critical-controls-poster-2016.pdf

Limitation of warranties: The information in this document is provided "as is" without any representations or warranties, express or implied. Professional assistance: You must not rely on the information in this document as an alternative to legal advice. If you have any specific questions about any legal matter you should consult your attorney or other professional legal services provider.

©2017 WatchGuard Technologies, Inc. All rights reserved. WatchGuard, the WatchGuard logo, and Firebox are registered trademarks of WatchGuard Technologies, Inc. in the United States and/or other countries. All other tradenames are the property of their respective owners. Part No. WGCE66998_031017