



# IT Guide to **GDPR** Compliance & Security

## General Data Protection Regulation

---

Coming: May 25, 2018

GDPR is a European Union-driven **regulation** (specifically the European Parliament, the Council of the European Union and the European Commission) that will **strengthen data protection laws** throughout the EU.



- GDPR brings a new set of "digital rights" and aims primarily to give control back to **EU citizens and residents** over their personal data
- Regardless where your business is located, if you process, store or manage **personal data of any EU resident** – you must be GDPR compliant

# Key Definitions

---

## Data Subject

➤ An **identified or identifiable natural person** who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier

## Personal Data

➤ Any information **relating to a Data Subject**, racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership

## Processor

➤ A natural or legal person, public authority, agency or any other body which **processes Personal Data** on behalf of the controller

## Processing

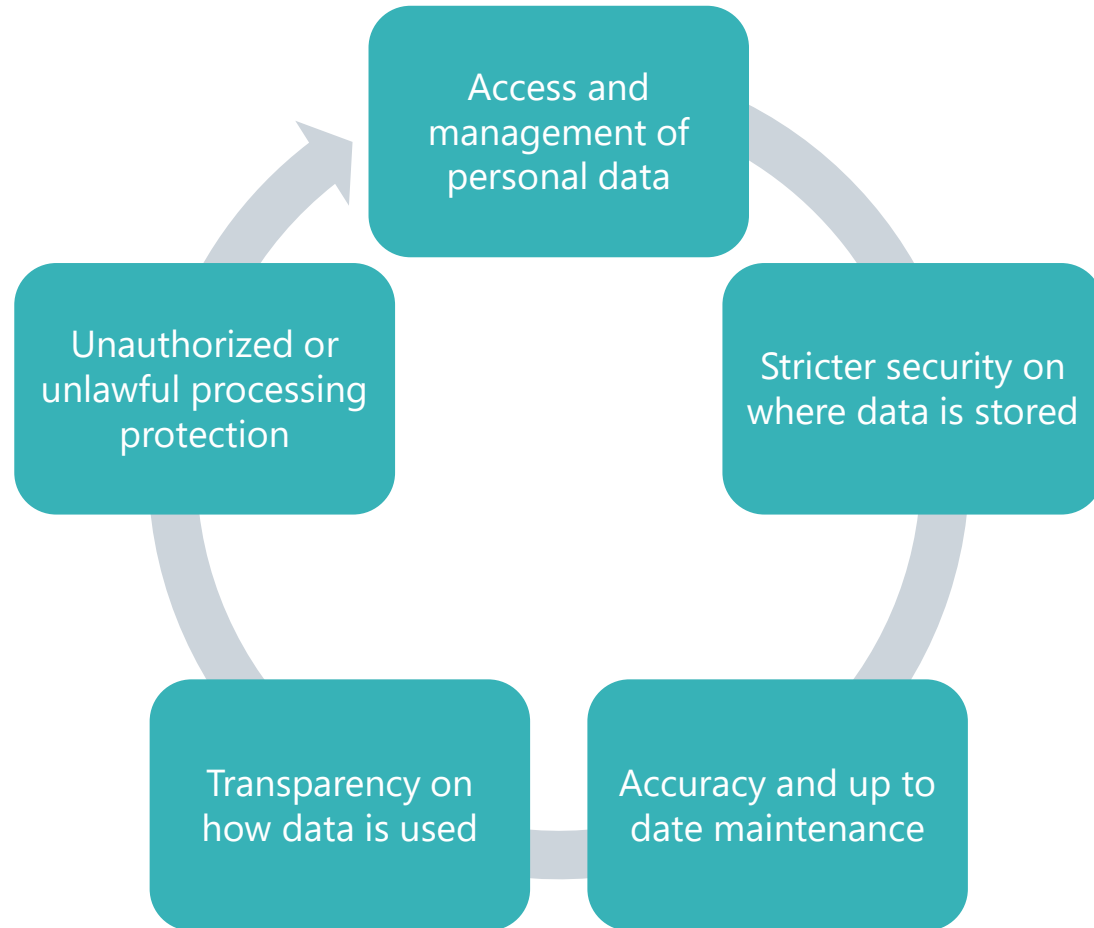
➤ Any operation or set of operation which is **performed on Personal Data** or on sets of Personal Data

## Controller

➤ The natural or legal person, public authority, agency or any other body which alone or jointly with others determines the **purposes and means of the processing of Personal Data**

# Benefits for my Business

---



## Did you now?

Security is the core of GDPR's data protection requirements!



Meet security requirements with an intelligent solution!

*Key changes to address GDPR bring many advantages for business*





Under GDPR organizations in breach of GDPR can be fined up to **4% of annual global** turnover or €20 Million (whichever is greater)!

---

# Data Breach

A breach of security leading to the **accidental or unlawful destruction**, loss, alteration, unauthorized disclosure of, or access to, personal data transmitted, stored or otherwise processed.



In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, **notify the personal data breach** to the supervisory authority!

Personal Data includes:

- › Name
- › Bank details
- › Location
- › IP address
- › Email content
- › Pictures
- › Recordings of security cameras
- › HR or CV databases
- › Cookies
- › Social Media Posts
- › Medical information

# How do I get started?

---

Detect all the **personal data you possess** and discover where it resides

Discover



Govern the **use and access** of personal data, restrict certain data from further processing

Manage



Establish security controls, **detect, prevent, respond** to vulnerabilities and data breaches

Protect



Manage data requests, **report data breaches**, and keep required documentation

Report



# What solution should I use?

---



Enterprise Server Monitoring &  
Administration Tool



Smart. All-Powerful. Robust.



DOCUMENTATION



MONITORING



REPORTING



MANAGEMENT



# How can SysKit Monitor help me?

## Monitor User Activity

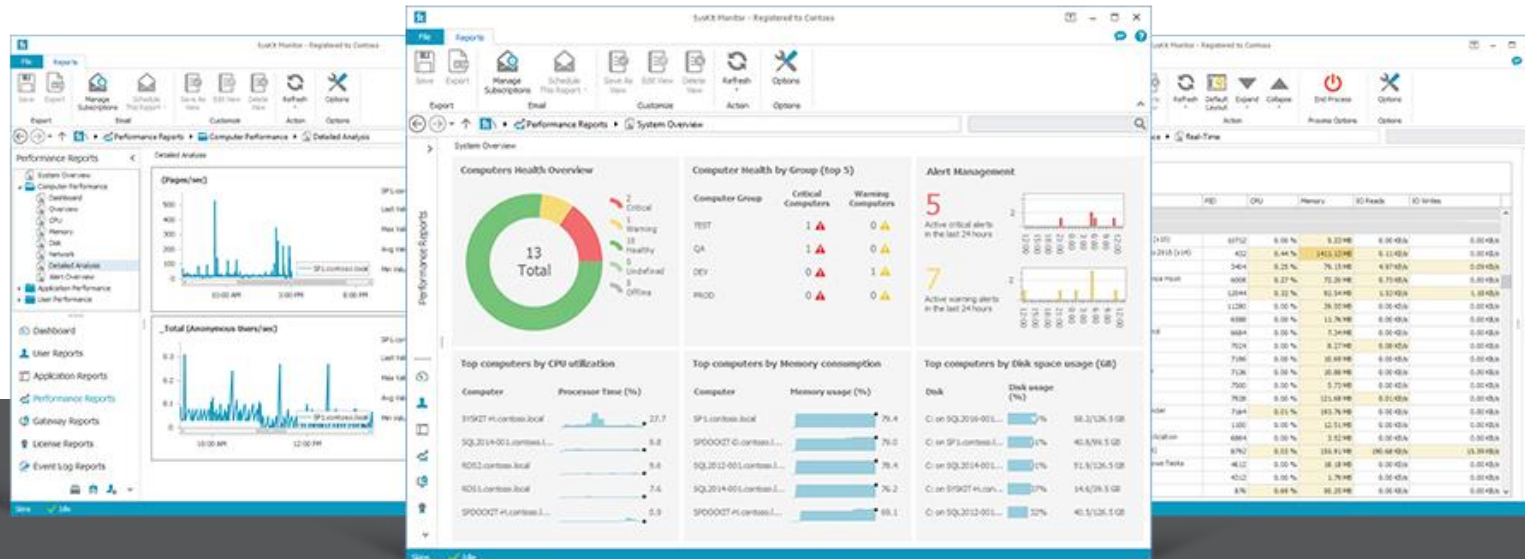
Monitor who has accessed to your system where personal data resides.

## Audit Logon & File Access

Audit failed logon attempts on your Windows or Citrix servers and avoid possible intruders from entering your company domain.

## Track RD Gateway Connections

Check who uses your RD Gateway to access your corporate network from the outside.





# Monitor User Activity

- Have an overview of all the users who have accessed the **business critical system to avoid personal data breaching** outside company
- Visualize users' access over the course of one day to sensitive data or **monitor users' live** (first log-on, log-off time, total time connected etc.)
- Schedule **daily or weekly email reports** on who exactly has accessed to the environment and how long he was active on any servers within the environment.

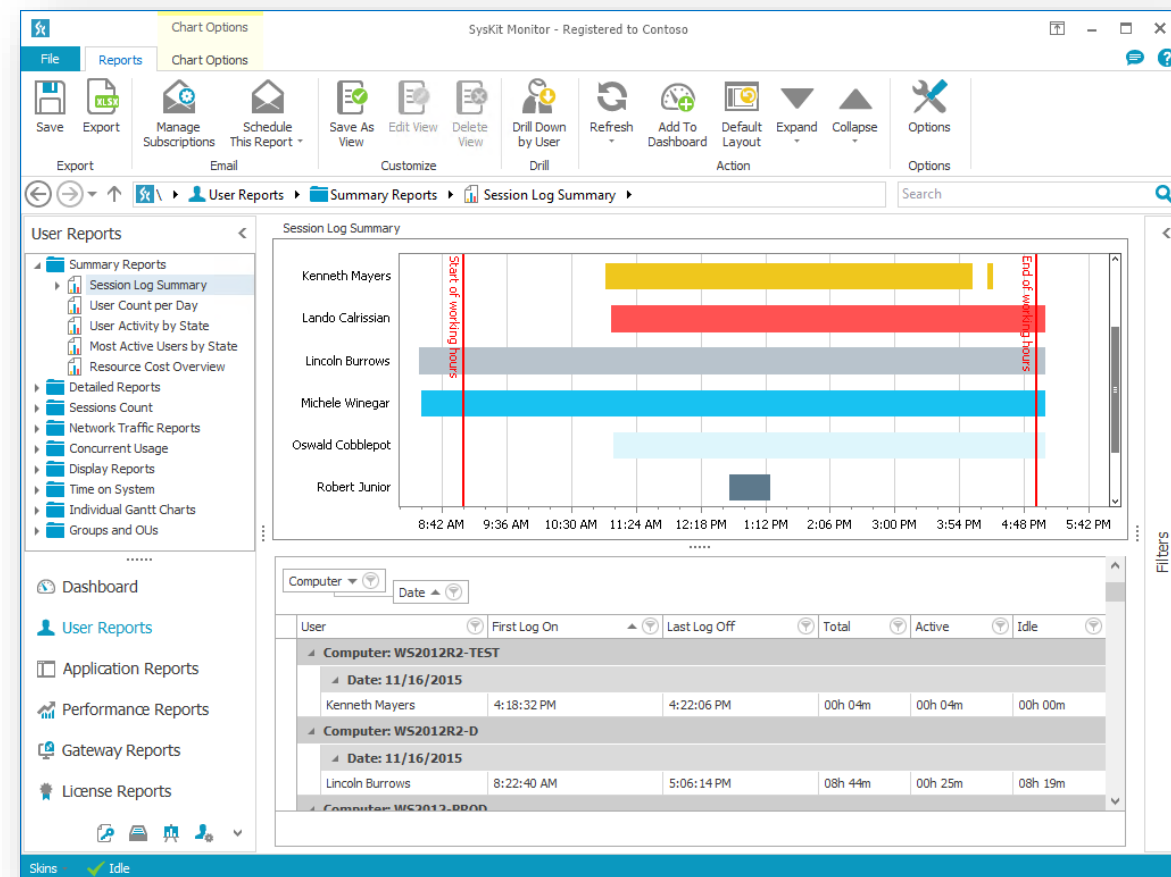
In case of a **personal data breach**, with SysKit Monitor you can track **who and when accessed different files** – once you become aware of a breach there is 72-hour limit to prepare the report.

Using SysKit Monitor, quickly and easily generate a **report for the controller or supervisory authority** and avoid high penalties.



Meet GDPR compliance requirement

Data controllers must now constantly monitor user activity and detect risky behavior.





# Audit Logon & File Access



Meet GDPR compliance requirement

Audit data access and flow across their entire network, detect data breaches.

- › Detect failed logon attempts if somebody tries to access your systems with personal data – detect treats on time
- › Get a warning if there are multiple logon attempts to the servers or suspicious behavior

Auditing data breaches is the most important thing you need to do for the GDPR compliance - if there is a security breach by malicious attacker this should be reported immediately to the supervisory authority within 72 hours.

With SysKit Monitor you can provide Logon Audit report that shows a complete logon history on who and when has accessed your environment, how long he was trying that and if on end someone managed to log on your servers. Using this type of the report you can even get the IP address of the remote attacker and geolocate the country or even city where the attacker is, and if you get asked by supervisory authority this details you will have those in your hand.

In SysKit Monitor, File Access Auditing allows you to see who accessed, modified, or deleted files - if any unauthorized user tried to open, modify, or delete any files, you will know. If you have configured file system auditing, SysKit Monitor provides you with a clear view of file access history.

Success	Account Name	Account Domain	Failure Reason	Source Workstation N...	Recorded On
<b>Computer: A_WS2008R1X64</b>					
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 6:53:34 PM
✗ Failure	Phill Keneey	DOMAIN	Correct username but wrong p...	CLIENT 1	10/29/2015 6:48:34 PM
✓ Success	Wendy Torres	DOMAIN	-	CLIENT 3	10/29/2015 6:44:01 PM
✓ Success	Phill Keneey	DOMAIN	-	CLIENT 1	10/29/2015 6:38:56 PM
✓ Success	Phill Keneey	DOMAIN	-	CLIENT 1	10/29/2015 6:33:29 PM
✓ Success	Lynn Mendez	DOMAIN	-	CLIENT 5	10/29/2015 6:28:25 PM
✓ Success	Phill Keneey	DOMAIN	-	CLIENT 1	10/29/2015 6:23:25 PM
✓ Success	Phill Keneey	DOMAIN	-	CLIENT 1	10/29/2015 6:18:26 PM
<b>Computer: EXCHANGE1</b>					
✓ Success	Wendy Torres	DOMAIN	-	CLIENT 3	10/29/2015 6:08:23 PM
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 6:03:23 PM
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 5:58:23 PM
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 5:53:22 PM
<b>Computer: SQL2014</b>					
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 5:43:18 PM
✓ Success	Allan Barnett	DOMAIN	-	CLIENT 4	10/29/2015 5:38:18 PM
✓ Success	Allan Barnett	DOMAIN	-	CLIENT 4	10/29/2015 5:33:21 PM
✓ Success	Kate Terry	DOMAIN	-	CLIENT 2	10/29/2015 5:28:16 PM
✓ Success	Allan Barnett	DOMAIN	-	CLIENT 4	10/29/2015 5:58:23 PM
✓ Success	Allan Barnett	DOMAIN	-	CLIENT 4	10/29/2015 5:53:22 PM

# Track RD Gateway Connections

- Measure and monitor connections to your servers or workstation made via RD Gateway and track their external IP address
- Add multiple RD Gateways and track user activity
- Analyze both real-time and historical data about users and activities

RD Gateway Connection Monitoring is crucial for the GDPR security since outside user connections to your environment are extremely critical and risky. RD Gateway secures the servers behind the firewall – you will be aware if somebody is attacking your RD Gateway as well as if a malicious user manages to gain access to the internal resources.

RD Gateway is the single server (or in load-balanced scenarios more servers) that are exposed on the Internet and therefore a single point of the security breach.

To get access to the internal resources malicious attacker needs first to break the RD Gateway which needs to be monitored with high priority and all the users that are connecting through the RD Gateway. SysKit Monitor allows you to monitor RD Gateway connections on top of the RD Session host monitoring.



Meet GDPR compliance requirement

Identify and prioritize gaps in security and monitor risky connections to your network from the outside.

The screenshot displays the SysKit Monitor interface for a computer named 'SP2010-WFE'. The main window shows a 'Connection Log Summary' table with the following data:

User	First Log On	Last Log Off	Total	Active	Idle
<b>Computer: SP2010-WFE</b>					
<b>Date: 10/28/2015</b>					
Lincoln Burrows	12:12:44 PM	11:59:59 PM	11h 47m	10h 56m	00h 51m
<b>Date: 10/29/2015</b>					
Lincoln Burrows	12:00:00 AM	11:59:59 PM	28h 21m	16h 54m	11h 27m
Kenneth Mayers	11:56:49 AM	11:59:59 PM	216h 52m	107h 26m	109h 26m
Roger Lay	12:03:15 PM	11:59:59 PM	11h 57m	11h 57m	00h 00m
Oswald Cobblepot	12:06:57 PM	11:59:59 PM	23h 44m	11h 53m	11h 51m
Robert Junior	12:06:57 PM	11:59:59 PM	23h 34m	21h 59m	01h 35m
<b>Date: 10/30/2015</b>					
Kenneth Mayers	12:00:00 AM	4:31:36 AM	90h 32m	45h 16m	45h 16m
Lincoln Burrows	12:00:00 AM	11:59:59 PM	16h 52m	12h 20m	04h 32m
Oswald Cobblepot	12:00:00 AM	4:31:36 AM	09h 03m	04h 32m	04h 32m
Roger Lay	12:00:00 AM	10:28:26 AM	05h 47m	05h 05m	00h 42m
Robert Junior	12:00:00 AM	11:59:59 PM	44h 22m	27h 48m	16h 34m
<b>Date: 10/31/2015</b>					
Lincoln Burrows	12:00:00 AM	4:31:34 AM	04h 32m	04h 32m	00h 00m
Robert Junior	12:00:00 AM	4:31:34 AM	13h 35m	09h 03m	04h 32m

# One tool to monitor them all!



Citrix XenDesktop  
and XenApp  
monitoring



SharePoint, SQL  
Server, and Windows  
Server monitoring



Remote Desktop  
Services and  
Gateway monitoring

# The clock is ticking...

Start your GDPR journey today & prepare for May!



Download Free Trial

Relevant GDPR Articles:

- [Article 28](#)
- [Article 32](#)
- [Article 33](#)
- [Article 34](#)

Sources:

- [Key Changes](#)
- [GDPR Terms](#)
- [General Info](#)
- [Principles](#)

This guide was created as commentary on the GDPR according to careful research for informational purposes. However it cannot and does not intend to replace an in-depth legal, process, and technical assessment.