How is SecuReporter in compliance with GDPR

GSBU NOV,2018

Table of Content

GDPR Overview

1

Why GDPR?

To ensure that adequate data protection is incorporated into the process of collecting personal data.

WHAT IS GDPR?

GDPR is a single regulation to strengthen, unify, and enforce personal data protection across the EU(28 countries, 1 law, 99 Articles)

PERSONAL DATA

Any information relating to **an individual, whether it relates to his or her private, professional or public life.** It can be anything from a name, a home address, a photo, an **email address**, bank details, posts on social networking websites, medical information, or a **computer's IP address**.

WHY IT'S IMPORTANT?

GDPR are legitimately enforced by EU laws. The maximum fines of **€20 million or 4%** of annual worldwide turnover are a significant increase on what could previously be enforced.

TAKE EFFECT

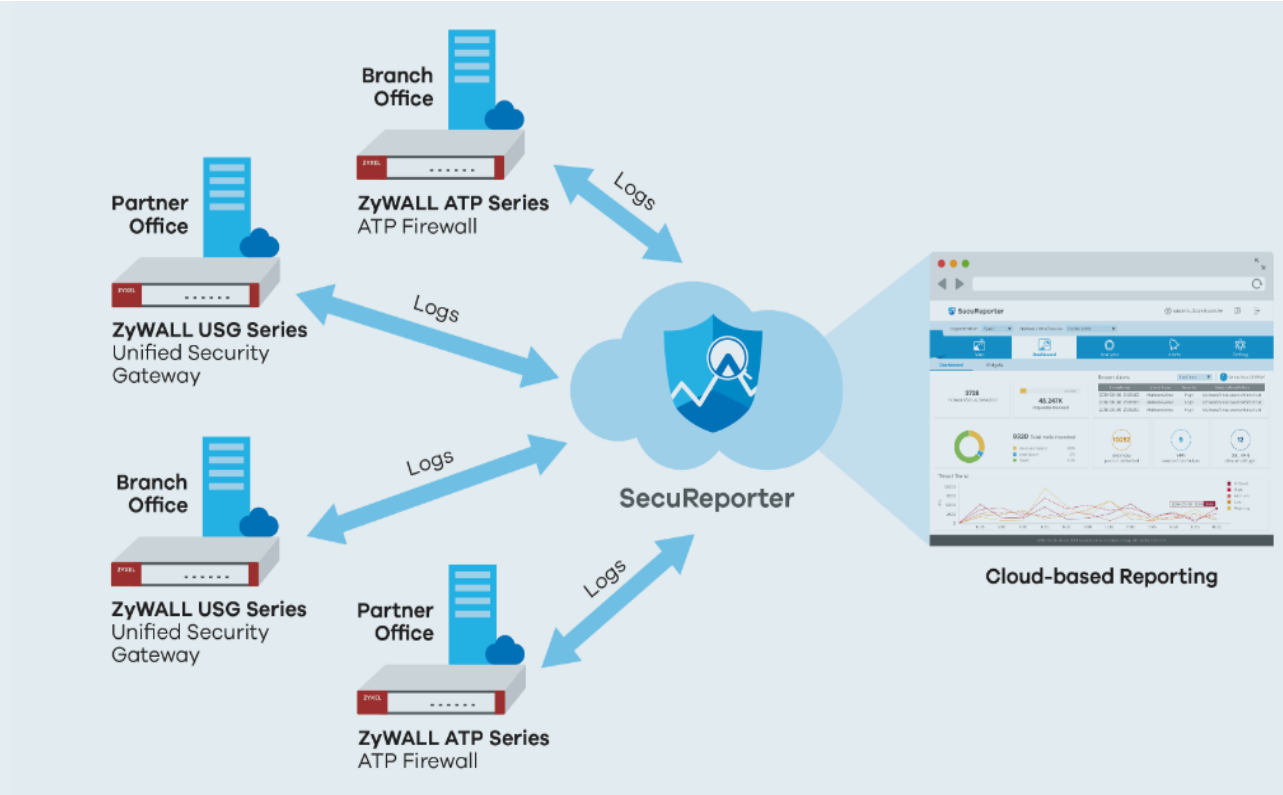
GDPR was ratified by member states in April, 2016 and will take effect on May 25, 2018.

GDPR home page: http://www.eugdpr.org/
GDPR reference: https://gdpr-info.eu/

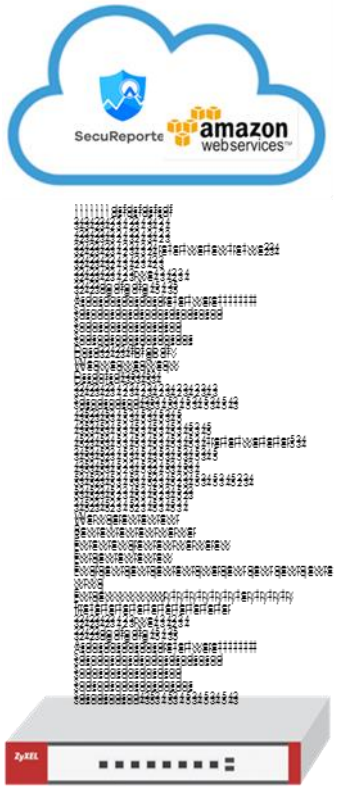
How is SecuReporter in Compliance with GDPR

2

SecuReporter Application Diagram



What Does SecuReporter Collect



Role	Definition	Detail
Agent	Owner of this Zyxel Device	Specified by his/her myZyxel.com email address
Individual	The User who uses the Zyxel Device to access the network	Individual's computer IP address, MAC, hostname of the Zyxel Device, and the account email address. For certain Zyxel Devices, the administrator can set up security policies that restrict access to both sensitive information and shared resources per user. This is done using a user-aware policy. With a user-aware policy, the individual's information is collected and logged in the Zyxel Device.

Art 12 - Informed Consent Criteria

The controller shall take appropriate measures to provide any information related to processing of the data subject in a concise, transparent, intelligible and easily accessible form, using clear and plain language.

Art 15 - Right of Access

The right to obtain from the controller confirmation including personal data and access to the personal data

Art 16 - Right to rectification

The right to obtain from the controller without undue delay the rectification of inaccurate personal data

Art.12 –
Informed Consent Criteria

Art.15 –
Right of Access

Art. 16 –
Right to rectification

- ✓ Declare personal data is collected by private policy and its purpose
- ✓ SecuReporter provides individuals with rectification of inaccurate personal data

Art. 45 - Transfers on the basis of an adequacy decision

A transfer of personal data to another country or an international organization may take place where the Commission has decided that the other country, territory or one or more specified sectors within that other country, or the international organization in question ensures an adequate level of protection.

Art. 45 –

Transfers on the basis of an adequacy decision

- ✓ SecuReporter stores all personal data at Amazon Web Services **Ireland si**te that complies with GDPR's principle.
- ✓ AWS is fully certified in compliance with GDPR

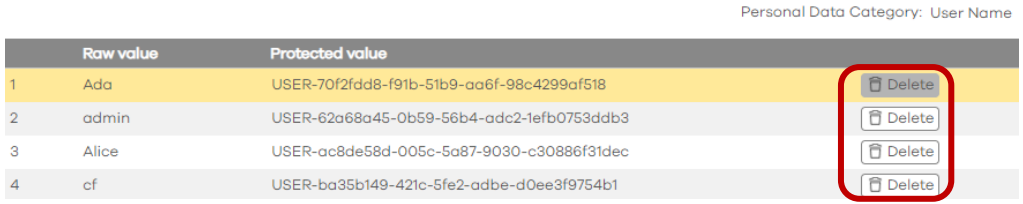
https://aws.amazon.com/compliance/eu-data-protection/?nc1=h_ls

Art 17 - Right to be Forgotten

Individuals have a right to obtain from the controller the erasure of personal data

Art. 17 –
Right to be Forgotten

- ✓ Offer tool that IT can erase specific user's personal data
- ✓ Provide personal data in a structured, commonly used and machine-readable format



Art 25 - Data Protection by Design and By Default

The controller shall implement appropriate technical and organizational measures for ensuring that, by default, **only personal data which are necessary for each specific purpose of the processing are processed.**

The controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, **implement appropriate technical and organizational measures, such as pseudonymization.**

Art. 25 –

Data Protection by Design and By Default

- ✓ SecuReporter only collects necessary personal data for analytic purposes
- ✓ Following **pseudonymization** design, users personal data and static are store in different table, personal data are replaced with artificial identification in analytics and download archive logs.

User	Artificial Identification
Yvonne	ID001
David	ID002
Amy	ID003

Artificial Identification	Time
ID001	2018-04-03
ID002	2018-04-02
ID003	2018-04-01

Art 30 - Records of processing activities

Each controller and, where applicable, the controller's representative, shall maintain a record of processing activities under its responsibility. That record shall contain all of the following information:

- the name and contact details of the controller and, where applicable, the joint controller, the controller's representative and the data protection officer
- the purposes of the processing

Art. 30 –
Records of processing activities

- ✓ SecuReporter keep records of its data processing with full details – the controller's name, the time and the purpose of the process.

Art 32 - Security of processing

the controller and the processor shall implement appropriate technical and organizational measure to ensure a level of security appropriate to the risk, including inter alia as appropriate:

- *the pseudonymization and encryption of personal data;*

Art. 32 –
Security of processing

✓ ATP/USG has **SSL** certificate signed by Zyxel to send logs to SecuReporter Communication are encrypted with TLS

Zyxel SSL

1111111dsfdsfdsfsdf
34342342342343424
42342343243243423
324234234234324retertwertewtretwe234
3242343243423423
32423423423rwe434234
32423dgdfgdfg45435
Asdasdasdasdasdretertweretttttttt
Sdsadasdasdsadasdsadsasad
Sadasdasdasdasdsad
Sadsadsadasdasdasdas
Dasd324234fbfgbdfv
534523452345345234523
34523452345234534534
Werwqerewrewrewr
Rewrewrewrewrwerwer
Ewrewrewqrewrewrwerwerew
Ewrqewrewrewrew
Ewqrqewrqewrqewrewrqwerqewrqewrqewrqewre
wrwq
Ewrqewwwwwwrytrytrytrytryterytrytrytry
Trreterterterterterterterterter
32423423423rwe434234
32423dgdfgdfg45435
Asdasdasdasdasdretertweretttttttt
Sdsadasdasdsadasdsadsasad
Sadasdasdasdasdsad
Sadsadsadasdasdasdas
Sdsadsadsad43534534534534543

Zyxel SSL

Art. 32 –
Security of processing

- ✓ Logs and databases are **encrypted** with encryption key
- ✓ The encryption key is stored on AWS KMS service, uses this algorithm with 256-bit secret keys.
- ✓ SecuReporter adopts AWS Snapshot to auto backup personal data at 8:00 am and 8:00 p.m. (UTC+8) every day.

Art 33 - Records of processing activities

In the case of a personal data breach, the controller shall without undue delay and, where feasible, no later than 72 hours after having become aware of it, notify the personal data breach to the supervisor with authority

Art 34- Communication of a personal data breach to the data subject

When the personal data breach is likely to result in a **high risk to the rights and freedoms of natural person**, the controller shall communicate the personal data breach to the data subject without undue delay.

Art. 33 –
Breach Notification

Art. 34 –
Communication of a personal data breach to the data subject

- ✓ SecuReporter proactively notifies the supervisor with authority no later than 72 hours wherever feasible after becoming aware of personal data breach.
- ✓ SecuReporter communicates any personal data breach to the data subject without any delay.

Data Processing Policy on SecuReporter

Non-Anonymous:

Personal data is clearly identifiable in Analyzer, Reports, and downloaded Archive Logs. Personal data cannot be removed from SecuReporter.

User	Time
Yvonne	2018-04-03
David	2018-04-02
Amy	2018-04-01

Data Processing Policy on SecuReporter

Partially Anonymous:

Personal data is replaced with **artificial identifiers** in downloaded Archive Logs.
IT can remove the ratification identification with real name, compliance with GDPR "Right to be forgotten".

User	Time
ID001	2018-04-03
ID002	2018-04-02
ID003	2018-04-01

Code	User
ID001	Yvonne
ID002	David
ID003	Amy

Data Processing Policy on SecuReporter

Fully Anonymous:

Personal data is **clearly** with anonymous information in Analyzer, Reports, and downloaded Archive Logs

User	Time
XX84234	2018-04-03
32423xd	2018-04-02
MEK#34	2018-04-01

SecuReporter with Amazon Web Site

SecuReporter offers service and store personal data based on AWS architecture.

AWS compliance with GDPR :
https://aws.amazon.com/compliance/eu-data-protection/?nc1=h_ls

SecuReporter adopts AWS service to comply with GDPR principles

SecuReporter with Amazon Web Site

	AWS's Commitment	SecuReporter adopts AWS Service
Access	AWS provide an advanced set of access, encryption, and logging features to help you do this effectively	AWS Security Group access control
Storage	AWS datacenters are built in clusters in various regions around the globe	Store personal data in AWS EU-Frankfurt , it follow GDPR's principle.
Security	AWS offer our customers strong encryption for customer content in transit or at rest	Pseudonymization for static and personal data. Personal data are encrypted
Security Assurance	AWS have developed a security assurance program using global privacy and data protection	AWS CloudWatch and Trusted Advisor for security protection


GDPR

GDPR Planning Checklist

1 Clarify and Identify what personal data fields you are collecting from EU citizens.

2 Describe the consent information and procedures that exist when collecting these data.

3 Describe the ability to communicate with data subjects.

4 Determine whether the current recordkeeping and data processing policies are adequate.

5 Check whether data security practices and technologies are in compliance with GDPR requirements

ZYXEL

Your Networking Ally