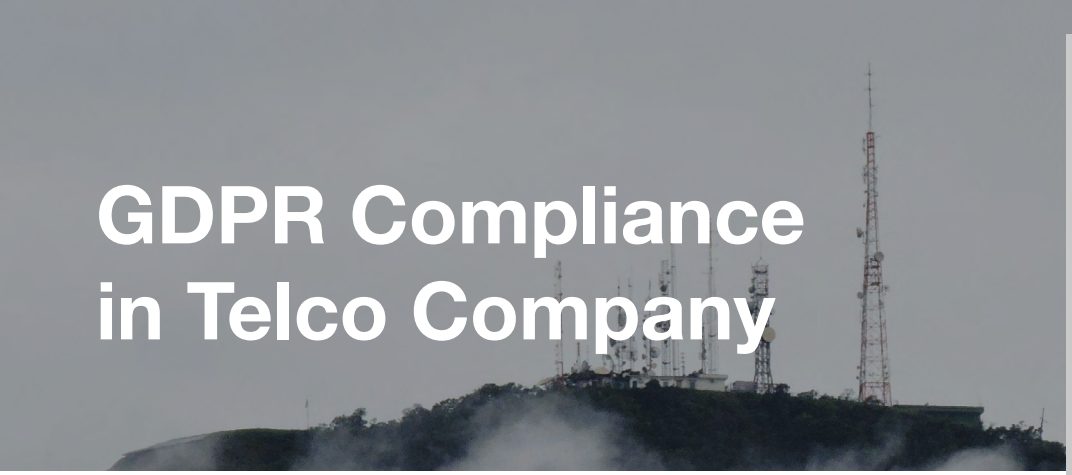
GDPR Compliance in Telco Company



A northern European telecommunications company deployed MENDEL, the network traffic analysis solution from GREYCORTEX as part of their efforts to comply with GDPR. MENDEL uses network traffic analysis to identify anomalous communications patterns between devices on the network. This data was analyzed according to several company-created limits regarding personal data.

MENDEL identified several different types of common attacks by malware, use of TOR services, bitcoin miners, etc. It also identified different types of policy violations which the telecommunications company had been previously unable to identify using their existing IT security and visibility infrastructure.

These included:

GDPR Article 33 Policy – Notice of Data Breach within 72 Hours

MENDEL identified two devices in the network (a workstation and a mobile device) which uploaded and downloaded data through sharing torrents and TOR sites, and sites which were also infected with malware. The mobile device specifically leaked sensitive data. MENDEL helped the telecommunications provider identify the breach quickly, and identify any effected parties within the relevant time period.

GDPR Article 32 – Secure Processing of Personal Data

MENDEL monitored the device communications on the network and identified several devices which were not configured properly, and which were sending personal identification numbers and passwords in plain text, including via forms available on the internet. Knowing this allowed the telecommunications company to secure the device's communications, and to continually identify possibly policy violations as to personal data.

GDPR Article 32 – Security Relevant to Risk

Because MENDEL identified multiple types of malware, as well as TOR communications, plain-text passwords, plain text personal identification number transmission, as well as outdated and insecure communications protocols, the telecommunications company was able to identify necessary upgrades to their security infrastructure (both from action and additional security tools) that were necessary to secure customer data in compliance with the law.

Industry:

Telecommunications Infrastructure Provider - Europe

Focus:

Compliance with privacy regulations, detection of unknown threats

Primary Detection:

Personally identifying information and passwords sent in plain text, outdated security tools

Secondary Detection:

Hidden malware, TOR, and torrent site use

Possible Damage to Company:

Risk of Data Breach, Strong Risk of GDPR violation, including significant fine