

Preparing for the General Data Protection Regulation (GDPR)

**Beyond the
European Union**

**How to Prepare Your Organization for
Compliance with the New Regulation**



KANGURU™
Secure. Anytime. Anywhere.



Table of Contents

Overview	<i>Page 3</i>
What is the GDPR?	<i>Page 4</i>
• <i>Summary</i>	<i>Page 4</i>
• <i>Not Just For the European Union</i>	<i>Page 4</i>
• <i>Why Organizations Everywhere Should Be Aware and Prepared</i>	<i>Page 5</i>
Essence of GDPR: General Rules of the GDPR	<i>Page 6</i>
Specifics of the GDPR	<i>Page 9</i>
How Kanguru Can Help Organizations With Compliance	<i>Page 13</i>
• <i>Figure 1: How Specific Kanguru Products Can Assist With GDPR</i>	<i>Page 14</i>
• <i>Meeting the Mandatory Data Protection Officer Mandate</i>	<i>Page 16</i>
• <i>Meeting the Data Protection Mandate With Secure Storage Devices</i>	<i>Page 23</i>
• <i>Duplication, and Meeting the "Right to Be Forgotten" Clause</i>	<i>Page 27</i>
Conclusion	<i>Page 28</i>
Resources	<i>Page 28</i>



Preparing Your Organization for the General Data Protection Regulation (GDPR)

Overview

Perhaps you've just recently heard about GDPR, or you may have been aware of it for a while. The new law is putting European organizations and the whole world on notice with a strong message; if organizations do not secure the private and personal information of its European Union customers and clients, there will be serious consequences. It is also telling the rest of the world if you gather any personal information of EU citizens from an EU nation, regardless of your location, you are equally responsible for the safety and security of EU citizen's personal data.

Who is Affected?

If you offer goods or services to, or monitor / process personal data of EU citizens, you should pay close attention to this new regulation. Now is the best time to get ready for GDPR. Awareness is the first step, and Kanguru is here to help organizations be well prepared and in full compliance with this new regulation to better protect themselves and the data of their clients. Even organizations that are currently in compliance with other government regulations will find it sensible to review the GDPR to ensure they are in full compliance. Kanguru secure products and services can help organizations easily and quickly adopt good practices with GDPR, so they can be ready once it moves into full force.

Organizations in the United States are wise to prepare for this new regulation as well because of its far-reaching scope to anyone conducting business with any European nation. GDPR puts the law into the hands of its EU citizens to protect their private data, providing acute rights and privileges to seek damages which could cut deep into the pockets of organizations who are found to be non-compliant.⁽¹⁾

Whether your organization resides within the EU or not, preparing now will not only help you protect your client's information better in today's digital world and be compliant, but will help protect your organization from potential painful litigation that could result from a data breach. Kanguru is here to assist you in preparing, locking down, and securing information to be compliant with this new regulation.

What Is The GDPR?

Summary

GDPR is a new regulatory law, the acronym for *General Data Protection Regulation*, approved and adopted by the EU Parliament on April 14, 2016 and provides a higher standard of protection and privacy of personal data for citizens of the EU. The new regulation spells out a long list of security obligations and requirements that organizations must now follow in order to protect and secure private data. GDPR is a new regulation to reform and replace the existing **Data Protection Directive** which was the former standard since 1995. It has been in the works for more than 4 years by members of the European Union intending to give all EU citizens better control over their personal information in today's digital world. This new regulation goes into full effect after a 2-year grace period, and provides strong fundamental rights to citizens in order to protect their information. Any organization that is found in non-compliance after the enforcement date of May 25, 2018 could face massive fines, along with other serious and painful repercussions for organizations that mishandle information, or who are held responsible for a privacy data breach.^(1,2,3,4,5)



Not Just For The European Union

Although the main intent of the GDPR is to cover citizens of the European Union, the new regulation will have far-reaching consequences as business is conducted digitally with the EU from all points of the globe. As a result, it will not only affect European nations, but nations all around the world who conduct business with them, including the United States and the UK, regardless of whether the United Kingdom “Brexit” from the European Union or not.^(2,5)

Why Organizations Everywhere Should Be Aware and Prepared

Encrypting and securing information is extremely important to building good relationships and trust with clients, customers and partners. Organizations that carry out due diligence in preparing for the new GDPR will immediately realize the benefits of protecting their own organization from the dangers of a data breach and will build fundamental trust. They not only protect their clients and customers, but they protect themselves also, including employees, staff, trustees, management, and partners.

Organizations that do not adequately prepare are taking huge risks by leaving themselves open and vulnerable to potentially painful legal action against their organization, embarrassment, loss of business, loss of key partners and could even put themselves in danger of a shut down. The tremendous fines and litigation options alone could bankrupt an organization from this new governing law if they are found liable for non-compliance as a result of mishandling or causing a data breach from unsecured information.





Essence of GDPR

General Rules of the GDPR

In short, the best way to begin preparing your organization for the GDPR is to start with a good understanding of the general areas and scope that it covers. Unfortunately diving deep into the details of the highly-convoluted text can leave one's head spinning, so Kanguru has sifted through and pulled out key elements or rules that lay the groundwork for its larger principles. These principles are best practices that will put you on the right path toward preparing your organization for compliance with the new GDPR. ^(1,2,3,4,5)

Securely Store Sensitive Data Under Full Encryption Methods to Prevent Loss, Breach or Theft

Whether the method of data storage is on USB devices, within an online cloud structure, or an on-site / off-site server, personally identifiable data must be protected by full encryption methods with restricted access to qualitative users only under several layers of security. The secure environment should guard all sensitive data from the potential of tampering, loss, breach, theft or dissemination.

Secure All Methods of Transfer, Usage and Transmission of All Sensitive Data

In addition, any method of transfer, communication, transmission, and usage of personal data should be secured and protected from the threat of interception, loss, theft, dissemination or destruction. This includes countries outside of the European Union and abroad.

Monitor All Usage, Transfer, and Transmission of Sensitive Data

Procedures and measures must be in place to monitor sensitive data as it moves throughout the secure environment of an organization, to ensure its integrity, provide oversight of data transfers, and facilitate critical operations. Any issues that compromise the security of the data will need to be reported immediately.

Secure Data Automatically to Prevent Loss, Breach, and / or Unauthorized Access

All methods of technology should provide automatic security measures that encrypt and secure data by design and by default. Procedures alone are not enough to persuade individuals to follow best practices. The data must be automatically protected.

Sensitive Data Must Be Secured Across All Borders

If sensitive data passes over borders from the EU to other nations whether digitally or otherwise, the organization must be able to show that the data remains secure. The new GDPR provides for severe penalties and legal action for organizations within the EU, as well as organizations that do business with EU Nations, regardless of their location(s).



Provide Off-Site Data Backup and Network Protection Solutions

Safety measures and backups must be in place in order to secure information in the event of disaster so that data is not lost or destroyed. This includes protection from weather, fire, theft, malware attacks, viruses and hacking. Measures must be in place to protect sensitive data from tampering, destruction, dissemination, breach or unauthorized access.

Have Procedures / Audit Trails In Place to Demonstrate Compliance

Organizations should be able to show procedures and good practices for all sensitive data processing. EU Organizations with outsourced partners in other countries should require disclosure of strong procedures, policies, and good practices in handling sensitive information for EU Citizens.

Show Explicit Consent and Provide for the Rights of EU Citizens to Be Forgotten or Removed

EU Citizens who wish to be anonymous have the right to request to be forgotten, and their data erased. Organizations that work with sensitive data that identifies individuals or contains any information that specifically identifies a person in any way, must be able to show that the data was collected with the individual's explicit consent, not implied, and that the individual has a clear method to exercise their right to remove themselves from the database.

Transparency: Lawful and Fair Data Processing

The collection of personal data of EU Citizens must be transparent to the citizen(s) concerned, in a fair and lawful manner. They should be made aware of the risks, rules, safeguards and rights in relation to the processing of their personal data, and it should be time-limited as necessary for the purposes of which they are processed.

These general principles of the essence of GDPR can point your organization in the right direction for complying with the new regulation. However, the devil can be in the details, so it is necessary to dig deeper into the specifics of the regulatory language in order to achieve full compliance. Many of the principles are based upon meeting explicit criteria, so we go into more detail in the next section: Specifics of the GDPR.



Specifics of the GDPR

Building upon the previous foundational principles, the new GDPR contains some specific language that must be met. In order to comply with GDPR in particular, it's important to have a more granular understanding of the key specifics to line up with the new GDPR requirements:

A Mandatory Data Protection Officer ^(1,2,3,5)

The new law requires public EU organizations of 250 employees or more whose central business is processing or controlling personally identifiable data, to have a Data Protection Officer (DPO) in order to comply with GDPR. The DPO can be contracted out or hired internally, but this individual or team must be responsible for conducting oversight of all data processes. Chapter IV, Section 4 of the GDPR spells out some of the core duties that a Data Protection Officer should be responsible for. Some of these duties include monitoring, tracking, auditing, and ensuring the integrity of secured data.

Protection of Personal Information ^(1,2,3,5)

Organizations will be fully responsible for ensuring that the personal information they collect and the process for which it is collected and used is fully safeguarded and secure from breach or unauthorized access. The data should be secured from the time it is collected to the time it is deleted. This is especially important for any personally-identifiable information, including health and medical records, financial records, government records, etc. Organizations will need to show compliance with all methods of controlling and securing this data.

Secured Data Storage

In today's fast-paced digital world, data can be stored in several forms: local storage devices, computers, a remote online cloud service, or in the traditional manner of physically printed documents.

For local storage devices, sensitive data should be protected under good encryption with strong password protection. Every measure should be made to ensure that the data is protected regardless of whether the device itself is stolen, lost, or destroyed. To efficiently comply with GDPR, organizations should work with established security vendors rather than an unknown provider where the security implementation has not been independently validated. Devices that are FIPS 140-2 Certified and/or Common Criteria Certified demonstrate that they have been fully evaluated and approved by the highest standards, and will fulfill the GDPR regulation.

Computers that are connected to the internet should have strong measures in place that protect it from online intrusion such as password protection, firewalls and anti-virus software.

Cloud data storage providers should demonstrate that they acknowledge and conform to all GDPR standards regardless of their location, and be able to provide complete documentation that the data is stored under strong encryption methods.

Physical documents should be in locked storage with protections in place to prevent unauthorized access.

Secured Data Processes

Data can also be processed using a variety of methods: across the internet via E-mail and a variety of online services, mail carriers, wireless, phone, USB devices, local storage devices, network attached storage, physical transfers, and even by camera. All attempts must be made to secure the processing of personal data to cover each of these areas.

Integrated Data Protection by Design and Default ^(1,2,3,5)

Data protection must be an integral part of every new technology or means for which personally identifiable data is stored, and must show that it has adequate security measures in place. In other words, it should not be left up to an employee to secure and protect information. Relying on staff or employees to keep data safe leaves it open to vulnerability, laziness and user error. The protection needs to be automatic, by design and by default.

When woven into the fabric of the organization, security not only integrates good policy, but develops good habits as well.

Breach Notification Procedures ^(1,2,3,5)

Along with the requirements for protecting personally identifiable data, and a means of monitoring the data with a Data Protection Officer, a breach notification procedure must be made clear in the event a data breach or adverse event does occur. Organizations can no longer hide behind secrecy hoping an incident will go away. Authorities must be notified within 24 hours, and any delay must be justified. It is best for organizations to do everything within their power to first prevent an adverse incident, but it's also wise to already have a plan in place for disclosure regarding an incident to avoid further penalties or embarrassment.

Collecting Data ^(1,2,3,5)

Collection of personal data must be at the clear and explicit consent of the people involved, not implied, and all measures must be taken to ensure that it is kept within a secure environment designed to protect that data.

Circulation of Data and Third-Party Countries ^(1,2,3,5)

The new GDPR opens up free circulation of data throughout the EU for the benefit of commerce as a single regulation to cover all EU nations, but it must do so in a way that protects its security and integrity. For third party countries, the information will be heavily regulated and all third party countries must comply with this regulation.

This includes cloud storage services across the globe. If a cloud service cannot show adequate levels of protection to comply with the GDPR, you could be putting your organization at tremendous risk.

Global, Wide-Reaching Protection of Data Across Borders ^(1,2,3,5)

Outsourced organizations working with organizations of an EU nation must show guaranteed integrity and responsibility to ensure that all levels of identifiable data are protected. This also includes cloud computing storage and cloud service providers.

Clear and Precise Consent, Profiling and Right to Be Forgotten ^(1,2,3,5)

Collection of personal, identifiable data must show that it is clearly and explicitly done with the full consent of the EU Citizen, and must be made clear how that data will be processed. The organization must ensure that the data is collected within a secured environment that prevents any unauthorized access or breach.

Organizations must also provide means for EU Citizens to easily opt-out, be erased, or use their right to be forgotten as is the right of the citizen.

Pseudonymization - Incentive to make identification anonymous ^(1,2,3,5)

The new GDPR recommends organizations use Pseudonymization, a process that removes direct identifiers from the information, so that a connection to an identifiable person is not possible.

Codes of Conduct and Certifications Can Help Demonstrate Compliance ^(1,3,5)

Following certain Code of Conduct and certifications can provide guidance and demonstrate compliance of the GDPR.

Serious Consequences for Violating GDPR ^(1,2,3,5)

The new language of the GDPR authorizes opportunities for regulators to pursue complaints on behalf of EU Citizens, with far-reaching consequences. Tremendous penalties and fines can be assessed with a long list of violations to choose from.

GDPR provides EU citizens with rights and legal action to act upon organizations that cause, or are found responsible for a data breach of their information.



How Kanguru Can Help Your Organization with GDPR Compliance

The importance of complying with the GDPR cannot be overstated. Organizations across the EU as well as any nation that does business with EU nations will be wise to comply with this new regulation. With massive fines for organizations found in non-compliance, and the threat of lawsuits for violations, organizations can't afford NOT to comply with GDPR.

Kanguru's products and services deliver robust security and data storage protection to meet and even exceed the most stringent regulatory standards, along with strong certifications that back you up and demonstrate full compliance.

The key areas that Kanguru products can help:

- A Mandatory Data Protection Officer
- Monitoring Sensitive Data Activity
- Reporting on Violations
- Protecting Data
- Secure Data Storage
- Secure Data Processing and Transfer
- Protected Networks
- Integrated / Automatic Security by Design and Default
- Certified / Compliant Data Security Products
- Data Erasure and Creating Off-Site Backups

Figure 1 **How Specific Kanguru Products Can Assist With GDPR** provides a quick snapshot of how Kanguru products can help with the specific directives of GDPR.

Figure 1: How Specific Kanguru Products Can Assist With GDPR

KANGURU PRODUCT	Fundamentals	Assist with Compliance of GDPR
AES 256-BIT, HARDWARE ENCRYPTED DEFENDER® DRIVES Learn More	<ul style="list-style-type: none"> • 256-Bit hardware encryption (XTS Mode) • Password protection • FIPS 140-2 Certified (select drives) • Common Criteria Certified (select drives) • Optional virtual keyboard password entry • Brute-force protections (Defender 3000) • Waterproof (Defender 3000) • Tamper-proof • On-board Anti-Virus • Remote Management ready • Secure firmware • Physical write protect switch (select drives) 	<ul style="list-style-type: none"> • Protect sensitive data with full hardware encryption under strict password protection • Demonstrate compliance with FIPS 140-2 Certified, or Common Criteria Certified devices • Protect sensitive data from tampering with tamper-proof and brute-force housing • Protect sensitive data from viruses with on-board Anti-Virus scanning • Protect sensitive data from malware with RSA-2048 digitally-signed secure firmware • Protect the drive from computer viruses with a physical write protect switch • Protect sensitive data from walking away - with remote management of secure drives
SELF-SERVICE PASSWORD MANAGEMENT Learn More	A secure password recovery service for secure flash drives to protect against a forgotten password, which could lead to denied access to important files	Prevent denied access to sensitive and important data due to a forgotten password
REMOTE MANAGEMENT FOR SECURE DRIVES Learn More	Cloud-based remote management for an organization's secure data storage drives	Data Protection Officer can monitor locations of secure drives around the world, report, restrict permissions, notify users of policy updates, and schedule password changes

Continued ►

KANGURU ENDPOINT PROTECTOR Learn More	<p>Cloud-based control over what USB plug-in devices can and cannot be used on workstations, and monitor's social media, web content, communications and mobile devices for actions that may compromise sensitive content. 100% cloud-based without the need for centralized server install.</p>	<p>Data Protection Officer can create and enforce security policies, whitelist/blacklist devices, audit, report, and monitor violations</p>
DUPLICATORS Learn More	<p>Easily create multiple copies of hard drives, solid state drives, Blu-ray, DVD, CD, or USB for backup</p> <p>HDS-Pro and Mobile Clone Disk wipe feature complies with the NIST 800-88 guideline for clearing SATA Hard Drives</p> <p>The HDS-PRO Secure Erase feature complies with the NIST 800-88 guideline for purging data from SSDs that support the SATA Secure Erase command</p>	<ul style="list-style-type: none"> • Meet off-site backup requirements for backup and safe storage • Secure erase personal information from SSDs with NIST 800-88 compliance on select models • Erase all data from HD, SSD and USB drives
CUSTOMIZATION/ ENGRAVING Learn More	<p>Customize Kanguru Defender drives with identifiable engraving features for logos, serial numbers, contact information, etc.</p> <p>Unique electronic identifiers, read-only configuration and pre-loaded data features</p>	<p>Custom engraving helps increase the likelihood that someone will return a lost drive if found</p> <p>Unique Electronic Identifiers enable trusted devices to be recognized with Endpoint security. This means networks can whitelist them, and blacklist untrusted devices</p>

Kanguru secure products can assist your organization in multiple ways, overlapping many areas that ensure GDPR compliance on a variety of levels. We would be happy to personally discuss your specific requirements with you. Feel free to contact us directly during our regular business hours to ask questions, explore your requirements and needs, and find the best solutions for your organization.



Meeting the Mandatory Data Protection Officer Mandate

One of the clearest requirements of the new GDPR is that organizations must have a Data Protection Officer in place to oversee all aspects of secure data. Kanguru provides several robust tools for an administrator to monitor, customize, report and take action on a variety of security measures:

- **Kanguru Remote Management Console (KRMC)**
- **Kanguru Endpoint Protector**

Both of these options are 100% cloud-based and meet the highest standards for security, providing administrators with the ability to monitor sensitive data activities of an organization around the world from one convenient console. Since neither the KRMC console nor the Endpoint Protector console themselves actually store sensitive data, the administrative duties can be separate from the content, concentrating solely on its secure containment and monitoring its activities.

Kanguru Remote Management Console™ (KRMC™)

The Kanguru Remote Management Console is a robust tool for customizing and monitoring the location, activity and permissions of your organization's hardware encrypted flash drives, solid state drives, and hard drives anywhere in the world. By securing data in an environment of hardware encrypted drives, and then monitoring those drives from a secure administrator console, organizations fulfill a host of GDPR requirements:

Kanguru Defender® AES Secure Storage Drives
& Fully-Integrated Remote Management



- Locally-Stored and Offline is the Safest Place to Store and Secure Sensitive Data
- Full Administrative Oversight and Reporting
- Offers Multiple Layers of Security
- Administrates Activities Around the World
- Separates the Administrative Duties from the Sensitive Data
- Enables Multiple Tiers of Accountability

First, storing sensitive data on local, hardware encrypted drives automatically removes an element of compromise by online means, and has the added benefit of continued use during outages or shut downs. Where data stored in a cloud environment could be vulnerable on several key areas, locally-stored data is protected inherently by the physical aspect of the data being strictly and physically within the hands of the individual carrying the device. KRMC separates the data storage from the data management using the most convenient aspects of the cloud and local storage, placing the data in the physical confines of the user, and the administrative control in the hands of the administrator from a secure and convenient cloud interface.



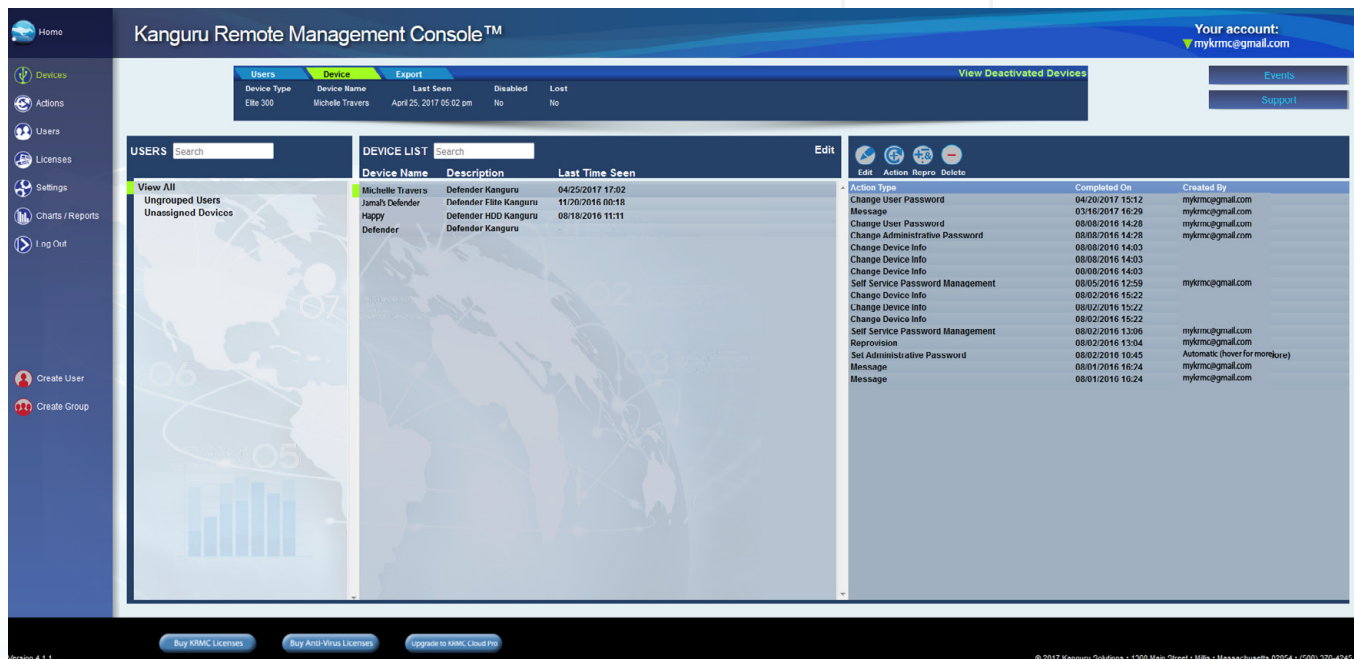
The Kanguru Remote Management Console (KRMC) provides granular details of last location, users, settings, and customization of secure Defender data storage drives. Administrators can control and monitor all of the privacy settings for an organization's devices containing sensitive data around the world.

With KRMC, administrators have full oversight, customization, and reporting capabilities for all activity involving secure drives containing sensitive data around the globe. The console can show the last location where a flash drive was plugged in, prevent a user from plugging into a certain location by domain, and can even allow the administrator to wipe or delete a flash drive if it is lost or stolen.

Multiple Layers of Security

KRMC offers multiple layers of security, from 2-Factor Authentication, to options for extra accountability. For example, KRMC-Cloud Pro offers multiple administrators under one super-administrator. If an organization had several silos of sensitive information that needed to be monitored by different administrators, certain encrypted drives could be assigned to certain administrators, with specific tasks and permissions delegated for that purpose, and each administrator would be under the watchful eye of the super-administrator. Since no data is seen within the administrator's console, there is no risk to sensitive data being compromised in this scenario, and each administrator simply monitors the activities of the drives within the organization's network. This creates a multi-level security environment of checks and balances which is perfect for demonstrating compliance with GDPR.

In addition, Kanguru offers Self-Service Password Management (SSPM) as a way to reset a user's password if the user forgets. This prevents forgetful users from being locked out of their important information. Data Protection Officers can use KRMC to manage who and who is not able to use this password recovery method.



Kanguru Remote Management Console™

Your account: mykrmc@gmail.com

Users	Device	Export	View Deactivated Devices	
Device Type	Device Name	Last Seen	Disabled	Lost
Elite 300	Michelle Travers	April 25, 2017 05:02 pm	No	No

Users	DEVICE LIST	Edit	
View All	Device Name	Description	Last Time Seen
Ungrouped Users	Michelle Travers	Defender Kanguru	04/25/2017 17:02
Unassigned Devices	Jamaal Defender	Defender Elite Kanguru	11/20/2016 00:18
	Happy	Defender HDD Kanguru	08/18/2016 11:11
	Defender	Defender Kanguru	

Action Type	Completed On	Created By
Change User Password	04/20/2017 15:12	mykrmc@gmail.com
Message	03/16/2017 16:29	mykrmc@gmail.com
Change User Password	08/08/2016 14:28	mykrmc@gmail.com
Change Administrative Password	08/08/2016 14:28	mykrmc@gmail.com
Change Device Info	08/08/2016 14:03	
Change Device Info	08/08/2016 14:03	
Change Device Info	08/08/2016 14:03	
Self Service Password Management	08/05/2016 12:59	mykrmc@gmail.com
Change Device Info	08/02/2016 15:22	
Change Device Info	08/02/2016 15:22	
Change Device Info	08/02/2016 15:22	
Self Service Password Management	08/02/2016 13:06	mykrmc@gmail.com
Reprovision	08/02/2016 13:04	mykrmc@gmail.com
Set Administrative Password	08/02/2016 10:45	Automatic (hover for more)
Message	08/01/2016 16:24	mykrmc@gmail.com
Message	08/01/2016 16:24	mykrmc@gmail.com

Version 4.1.1 | Buy KRMC Licenses | Buy Anti-Virus Licenses | Upgrade to KRMC Cloud Pro

© 2017 Kanguru Solutions • 1300 Main Street • Mills • Massachusetts 02054 • (508) 370-4245

KRMC enables administrators to customize the settings of an organization's encrypted drives, notify users of security policy updates, schedule password updates, and even report on the last location of a secure drive anywhere in the world.

Security Across Borders

Data officers can monitor activities of their physical drives anywhere in the world. If an organization has secure drives in EU nations, as well as a other countries, the advantages of the Kanguru Remote Management Console for GDPR compliance are abundantly clear. Administrators can monitor and report on activities and the locations of drives and where they've been plugged in, and even group

users by country if they wish to do so. Secure drives can be monitored by a single administrator in KRMC, or by multiple administrators monitoring activities by country or region based on the group segmentation of their choosing.

The separation of the administrative oversight responsibilities from the physical data makes for a much more enhanced security environment than cloud storage or server-based security setting. Authorized users are solely responsible for the sensitive data they carry in their hands and do not have to worry about the administrative duties or responsibilities of monitoring the data. They can conduct business as usual within a secure environment with all the conveniences of a flash drive. The administrators are simply responsible for the administrative actions of the storage drives, and have no hand in the data itself. This separation is a win/win for organizations looking to comply with GDPR.

With these multi-tiered levels of accountability, organizations maintain a variety of security aspects for sensitive data, and demonstrate clear compliance with GDPR.

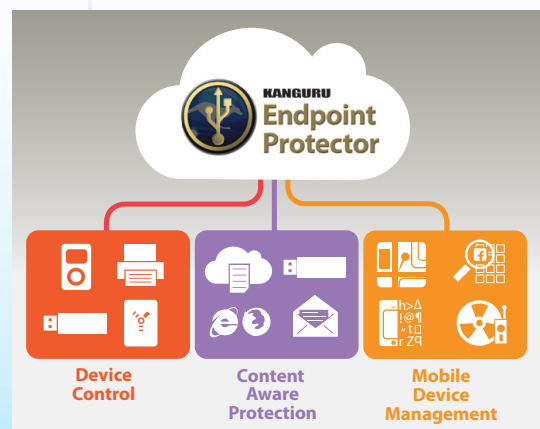
Learn more about Kanguru Remote Management Console (KRMC).

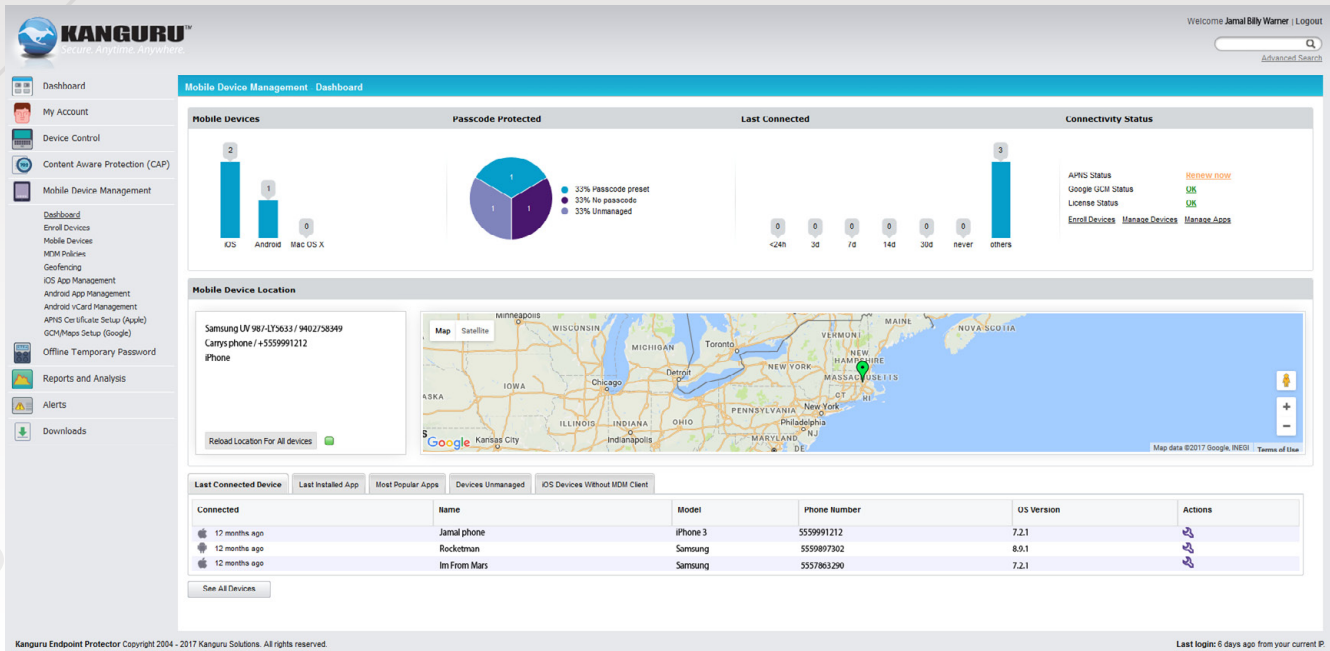
[Learn More](#)

Kanguru Endpoint Protector

Kanguru Endpoint Protector gives organizations the edge they need to manage today's BYOD (Bring Your Own Device) technology environments. With so many different methods and devices available to plug in and connect to an organization's infrastructure, organizations working with sensitive information need to be able to monitor incoming and outgoing activities, protect from malicious threats, and block unauthorized access. Kanguru Endpoint Protector provides the means for an administrator to monitor all activities from the convenience of one console:

- Device Control
- Content Aware Protection
- Mobile Device Management





Mobile Device Management Dashboard

Mobile Devices

OS	Count
iOS	2
Android	1
Mac OS X	0

Passcode Protected

Category	Percentage
33% Passcode present	33%
33% No passcode	33%
33% Unmanaged	33%

Last Connected

Time Range	Count
<24h	0
3d	0
7d	0
14d	0
30d	0
never	0
others	3

Connectivity Status

APRS Status: [Renew now](#)

Google UCH Status: [SOS](#)

License Status: [SOS](#)

Email Devices: [Manage Devices](#) [Manage Apps](#)

Mobile Device Location

Samsung I987-LY5633 / 9402758349
 Carysphone / +5559991212
 iPhone

Reload Location For All devices:

Last Connected Device

Connected	Name	Model	Phone Number	iOS Version	Actions
17 months ago	Jamal phone	iPhone 3	5559991212	7.2.1	🔗
12 months ago	Rocketman	Samsung	5559897302	8.0.1	🔗
12 months ago	Im From Mars	Samsung	5557863200	7.2.1	🔗

[See All Devices](#)

Kanguru Endpoint Protector Copyright 2004 - 2017 Kanguru Solutions. All rights reserved. Last login: 6 days ago from your current IP

Kanguru Endpoint Protector provides tremendous administrative control over an entire infrastructure, enabling administrators to whitelist/blacklist peripherals, monitor, control content, act and report on activities that violate security policies.

Each one of these segments control a variety of aspects within the infrastructure of an organization. They can be purchased individually or in bundles based upon the flexibility of their needs for a full-service Endpoint solution.

Device Control

With Device Control, organizations can manage the activity of USB and other portable storage devices and enforce strong security policies to protect vital data and the health of the network. An administrator can control what is allowed and disallowed on the system and enforce the use of trusted devices. Device Control provides several aspects of protection:

- Protect the organization from outside risks
- Prevent data theft
- Enforce encryption policies
- Stop the spread of device malware and viruses
- Whitelist / blacklist USB devices
- Block ports and devices
- Control device use

- Monitor data transfers
- Audit and Report on device and data transfers

Device Control (DC) is a great way for organizations to protect their network and data from potential risks. It greatly reduces the chances of a data breach by controlling avenues for theft, malicious behavior, and even human error. The easy-to-use, intuitive dashboard enables administrators to control what devices can and cannot be used on the network, and can whitelist/blacklist by company level, group level, user level or computer level. Device Control has a variety of reporting options which are also ideal for complying with GDPR.

Content Aware Protection

Monitoring and protecting sensitive content is the key aspect of GDPR, and Content Aware Protection provides the perfect means for protecting data from leaking outside of your establishment. CAP offers dynamic content filtering to ensure that sensitive data never leaves your network, whether copied onto devices, on an electronic clipboard, or through e-mail, instant messaging, applications, cloud or online services and even as screen captures.

CAP enables administrators to develop security policies regarding Cloud-based services, browsers, e-mail clients, media and other services to protect against careless employee behavior which can often contribute to data loss. Additionally, administrators can choose to silently or actively audit, and generate reports on any content that should not be leaving the organization. Administrators can create a dictionary of content by expressions, URL, or domain, and blacklist or whitelist that content, or prevent certain actions from taking place.

- Filter content across all platforms
- Specify policies and manage rules by extension levels
- Set passive or active reporting
- Create definitions to allow or deny content
- Generate CAP reports

Mobile Device Management

Mobile Device Management (MDM) enables administrators to maintain full control and detailed monitoring of mobile devices to make sure data is safe at any time and at any place it is carried,

while keeping pace with the BYOD trend. Instead of blocking devices altogether, organizations can manage devices, maintaining their convenience for authorized users, creating a stable, safe working environment.

The MDM dashboard enables administrators to define and enforce policies, silently monitor activity, take action, block devices and even log and report actions.

- Track and locate mobile devices
- Detect mobile device incidents and enforce remote data wipe or device locking in the event of device loss or theft
- Manage App use
- Manage passwords
- Enforce device encryption
- Log and report on device activity history
- Inspect data transfers
- Detect transactions (credit card, etc.)

Learn more about Kanguru Endpoint Protector.

[Learn More](#)



Meeting the Data Protection Mandate with Secure Storage Devices

Kanguru Defender Hardware Encrypted Drives

Physical Protection

There is no safer way to secure data than with locally-stored, hardware encrypted storage drives. When sensitive data is secured locally, the information is protected in multiple ways. First it is by default protected by the physical confines of the device itself, within the hands of the user, and away from risks that exist from online access. Data is within the device, and not in an unknown cloud service at an undisclosed location or an online connected computer.

There are also physical protections that prevent a third party from physically tampering with the drive. Brute-force protection and tamper-proof protections are built-in to several of the drives. Certain drives are protected with an epoxy compound that is water resistant, preventing physical access to the chip. Any subversive attempt to remove the epoxy compound destroys the flash chip, rendering it unusable and inaccessible.

Hardware Encryption (XTS Mode)

But physicality is not enough to secure sensitive data in order to comply with GDPR standards. Data storage must be protected under strict encryption methods. Kanguru Defender drives use the strongest cryptographic technology known as AES 256-Bit hardware encryption without the need for users to follow complex procedures. This has a strong advantage over software encryption, which

could often leave security procedures in the hands of a user who may not make security a top priority.

Kanguru Defender secure devices use FIPS validated AES 256-bit Hardware encryption (XTS-Mode) to secure data contents stored on the USB drive. Since the cryptographic processes are all done in hardware, there is virtually no performance impact when transferring data, unlike the severe performance impact when using software encryption programs. XTS-mode also provides enhanced security when used to encrypt large blocks of data (as in GB's) as it eliminates certain vulnerabilities and patterns which might be exploited in earlier symmetric key implementations. In addition, the password matching and other security operations are all done in the secure confines of the tamper-resistant, epoxy encapsulated cryptographic processor. In short, your data can not be compromised.

- 256-Bit Hardware Encryption (*XTS Mode*)
- Automatic Encryption
- FIPS 140-2 or Common Criteria Certifications (*select models*)
- Onboard Anti-Virus
- RSA-2048 Digitally-Signed, Secure Firmware
- Tamper-Proof Protection
- Brute Force Protection (*select models*)
- Waterproof (*Defender 3000*)
- Physical Write Protect Switch
- Customizable
- Self-Service Password Management

Automatic Hardware Encryption

Kanguru Defender secure drives encrypt data automatically. This takes the responsibility away from the user who is usually busy taking care of business and may not have security in mind. Once a drive is set up, all the user has to do is login, conduct their business, and logout. This helps develop good security habits throughout the organization.

Learn more about the benefits of hardware encryption.

[Learn More](#)

Demonstrate Compliance with FIPS Certified Devices

With FIPS 140-2 and Common Criteria Certifications, Kanguru products fully demonstrate that they have been thoroughly tested and manufactured to the highest standards. In addition, Kanguru can provide documentation for certified drives by special request to back it up with an extra measure of assurance.

Learn more about FIPS 140-2 and Common Criteria Certification.

[Learn More](#)

Onboard Anti-Virus

Every Kanguru Defender hardware encrypted flash drive comes with integrated onboard anti-virus (a 30-day FREE trial, users can choose to purchase an annual anti-virus subscription with real-time updating for a nominal fee). Built right into the flash drive, the anti-virus consistently scans the drive in the background, ensuring that all of your files will be safe and protected from viruses.

Learn more about onboard Anti-Virus on Defender drives.

[Learn More](#)

RSA-2048 Digitally-Signed, Secure Firmware

All Defender drives have on-board, RSA-2048 digitally-signed secure firmware to protect against the potential risk of the device being used as a vehicle to deliver third-party, malicious firmware-based attacks. Any attempt at changing the customized, onboard device firmware with an unauthorized, malicious version is impossible. Furthermore, there are self-tests run at startup of the cryptographic module which handles the firmware security within the USB drive itself that ensure the integrity of the original firmware. If the self-test fails, the device will not operate. This prevents what is called "badUSB" by security researchers in the Black Hat community.

Learn more about Digitally-Signed, Secure Firmware.

[Learn More](#)

Physical Write Protect Switch

Sometimes it is necessary to make a flash drive “read-only”, to prevent anything from writing to the drive. This is especially useful for running tests from a flash drive on a virus-infected computer. It is also a great feature for protecting data on the drive from being accidentally overwritten.

Most Kanguru drives have a physical write protect switch, making it very easy to toggle between write, and read-only modes. If a company computer knowingly contains a virus, a Defender flash drive with on-board anti-virus and physical write protect switch turned to read only mode can be an IT manager’s best friend in running tests and resetting files on the infected computer.

Custom Engraving

One valuable element of secure devices that is often overlooked is identifiers through customized engraving. Kanguru can customize your secure drives with logos, contact information, unique serial numbers, and more. This greatly increases the chances that someone who finds a lost drive will return it to its rightful owner. When a drive contains the word “CONFIDENTIAL” with a phone number to call if found, finders will be much more apt to return the drive than if it had no identification at all.

Learn more about Customization and custom engraving.

[Learn More](#)

Self Service Password Management

Sometimes people forget, but if a user forgets the password to their hardware encrypted drive, the results could be disastrous. The purpose of password protection is to keep authorized access solely within the hands of the user who knows the password. If the user forgets, they could be locked out from accessing important data. For this purpose, Kanguru provides a secure method of recovering access by resetting the password. This can also be controlled by the Data Protection Officer through the Kanguru Remote Management Console, allowing certain users to use the password recovery method as the Administrator sees fit.

Learn more about Self Service Password Management (SSPM).

[Learn More](#)



Duplication, and Meeting the “Right to Be Forgotten” Clause

Another requirement of GDPR refers to the rights of EU Citizens to request their data be removed. This new mandate is called the “Right to be Forgotten”, or “Right to Erasure”. Part of this mandate includes that if information is outdated or no longer necessary in relation to the purposes for which the data was collected or otherwise processed, the controller has an obligation to erase personal data without undue delay.

The Kanguru Pro Series of Duplicators has a variety of data erase features for HD, SSD and USB drives. For example, with the HDS-Pro series, there is a Secure Erase feature for SSDs with NIST 80-88 compliance for purging data from SSDs that support the SATA Secure Erase command. The HDS-Pro, and Mobile Clone Disk wipe feature also complies with NIST 800-88 guidelines for clearing SATA hard drives.

As an example, if an organization collects a wealth of personal data that is time-sensitive, with the understanding that the data will only be necessary to hold on to for a certain period of time, some initial foresight might call for the data to be kept on one or several particular hard drives that can be wiped once the data is no longer needed.

Meet Off-Site Backup Requirements

GDPR also states that organizations must make an effort to protect data from disaster or loss with off-site backups. The last thing you need is to lose sensitive and important data to a fire, flood, or otherwise. All Kanguru duplicators provide convenient backup features for duplication on Blu-ray, DVD and CD disks, Hard Drives, Solid State Drives and USB devices.

Kanguru duplicators offer an assortment of modes and features like Disk Mode, Brief Copy, Resize Copy, Smart copy, Synchronous and Asynchronous modes to make it easy and convenient to duplicate data in a variety of different environments.

Learn more about Kanguru Duplicators.

[Learn More](#)

Conclusion

Kanguru provides a great variety of products that are flexible, scalable, and affordable to meet your budget, and help you comply with GDPR. Data security does not have to be expensive. Kanguru can work with you and your budget to help you find the best solutions for your needs. It can also save tremendous headaches and expense when you consider the alternatives. The GDPR, as well as other regulations place very heavy fines, along with the potential for litigation procedures on organizations that are found to be non-compliant, so protecting your organization now is in your best interest. You will also reap the benefits of providing trust for your customers by demonstrating compliance. You protect yourself and your customers from the potential embarrassment of a painful data breach, possible litigation, massive fines, and customer recoil.

Feel free to contact us directly to ask questions, explore your requirements and needs, and find the best solutions for your organization.

sales@kanguru.com

(1) 508 376-4245

Business Hours: 9am - 5pm Monday - Friday (EST)

(convert your time zone using online [timeclock](#))

<https://www.timeanddate.com/worldclock/usa/boston>

Resources:

(1) **Official Journal of the European Union** - Regulation (EU) 2016/679 Of The European Parliament and of The Council - [<http://eur-lex.europa.eu/legal-content/EN/TXT/HTML/?uri=CELEX:32016R0679&from=EN>]

(2) **eugdpr.org** - [<http://www.eugdpr.org/the-regulation.html>]

(3) **International Association of Privacy Professionals** - iapp.org - [<https://iapp.org/resources/article/top-10-operational-impacts-of-the-gdpr/>]

(4) **Computer Weekly.com** - [<http://www.computerweekly.com/guides/Essential-guide-What-the-EU-Data-Protection-Regulation-changes-mean-to-you#guideCategory1>]

(5) **eudataprotectionregulation.com**; [<http://www.eudataprotectionregulation.com/what-you-should-know>]

This document is for guidance purposes only, and does not claim to offer legal advice or counsel, as it is not a complete or conclusive statement of the law. For full compliance of the GDPR specific to your organization, seek legal counsel with your security advisor or an authorized consultant in security and legal matters.



KANGURUTM
Secure. Anytime. Anywhere.

1360 Main Street

Millis Massachusetts 02054

Toll Free: 1-888-KANGURU

Main Office: 1-508-376-4245

sales@kanguru.com

www.kanguru.com