Kingston Technology

Kingston approach on GDPR Regulations
Encrypted USB Solutions

Gabriel Gidea
Business Development Manager Romania
& Bulgaria

September 25, 2017

Ce este Regulamentul General privind Protecţia Datelor (EU GDPR)

Ce înseamnă EU GDPR?

Cum asigurăm conformitatea cu EU GDPR?

Cum vă poate ajuta Kingston

Cum prevenim breşele de securitate şi devenim conformi cu GDPR

- Nu există certificare “Conform cu GDPR”, însă organizaţiile pot deveni conforme cu GDPR

- Recomandările Kingston de conformitate cu GDPR pentru circulaţia datelor:
  - Înţelegerea noilor reglementări şi a impactului pe care acestea îl au asupra afacerii şi datelor mobile
  - Evaluaţi ce date (cu caracter personal) procesează organizaţia dumneavoastră, cine are acces la ele şi ce date “părăsesc” compania
  - Stabiliţi o strategie pentru date, cine are acces la date, la ce tip de date şi pe ce cale
  - Luaţi în calcul tehnologia – managementul dispozitivelor şi/sau criptarea
  - Asiguraţi-vă că angajaţii cunosc GDPR şi sunt instruiţi conform celor mai bune politici de protecţie a datelor

- **Dacă datele pierdute sunt criptate, vorbim despre o breşă de securitate, nu şi de o încălcare a securităţii datelor (raportarea nu e necesară)**

Politici pentru circulaţia datelor – Care sunt avantajele criptării?

Porturi USB blocate

+ securitate maximă

- Limitează flexibilitatea angajaţilor

- Costuri/training cu o altă soluţie de transfer de date

Politică de criptare USB

+ flexilitate a angajaţilor

+ Securitatea datelor

+ Gestiunea dispozitivelor

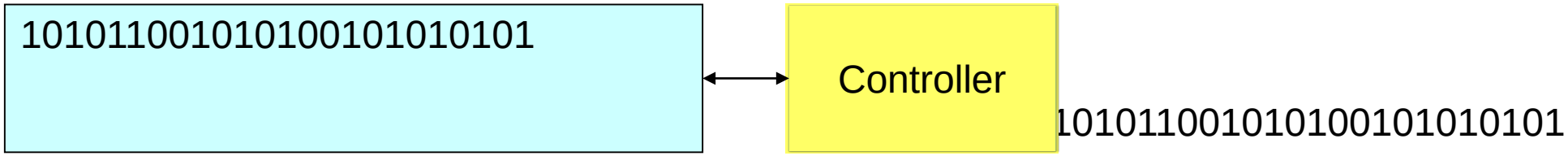
- Investiţie hardware

Kingston Technology

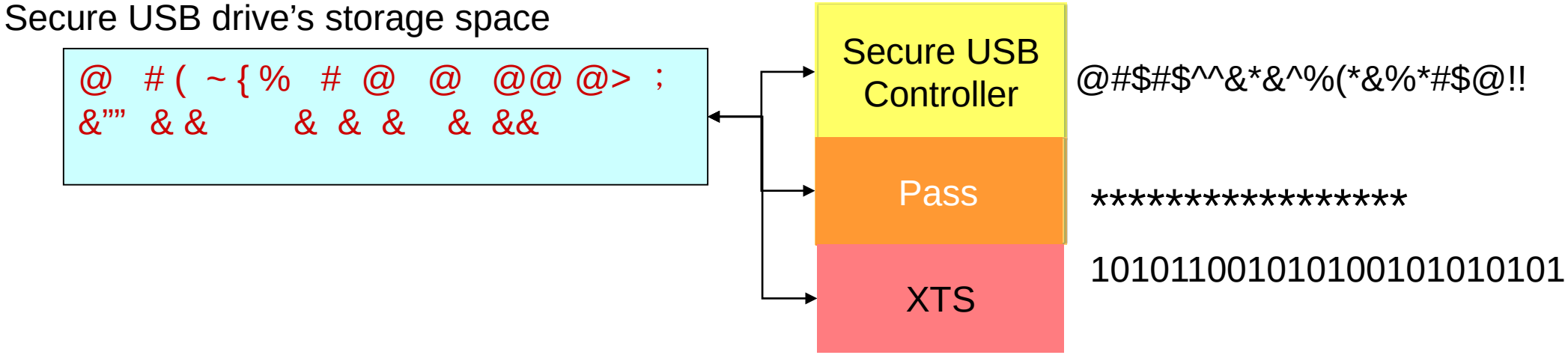
Encrypted USB’

How does a Secure USB work?

Standard USB drive's storage space



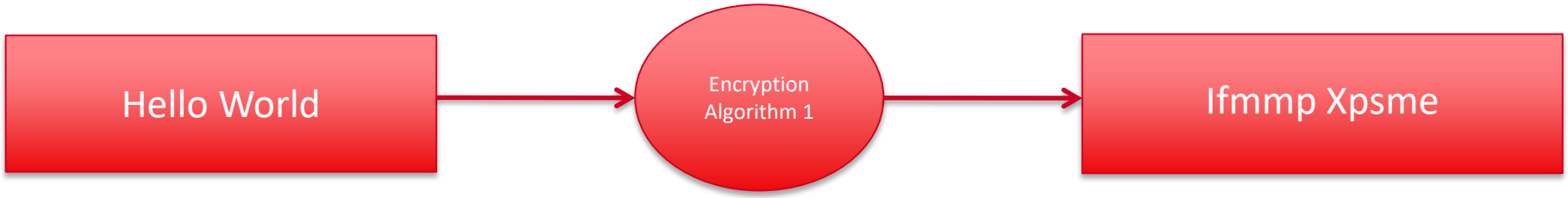
Secure USB drive's storage space



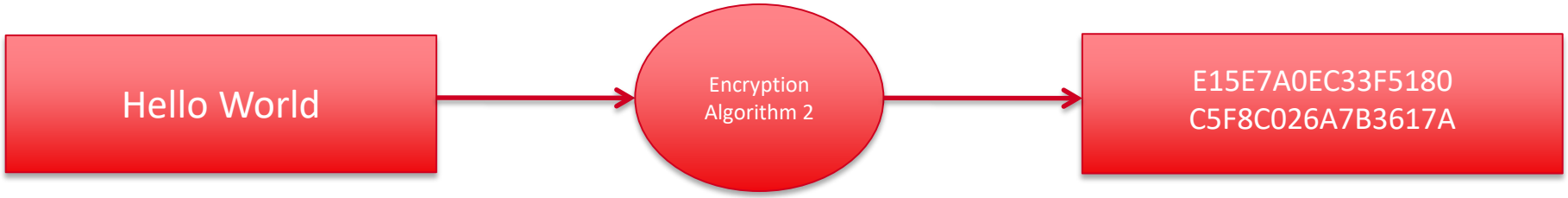
Only you are responsible for the information stored on the USB drive.
Only you know how important the information stored is.
Only you have the right to decide whether to use this information.
You never know who could try to access your USB drive when you lost it.

How does encryption work?

- Turns standard files into non-readable strings of ASCII characters
  - Encrypted files can be read, but not understood by humans



  - Encryption Algorithm 1 uses key = 1, and algorithm rule “shift character to right by key”. This is known as Caesar Cipher. Very simple and very easy to break!



  - Encryption Algorithm 2 uses key length 192, and algorithm rule Triple DES. The password is “K1ngston”. Without password this cannot be decrypted!

How does encryption work?

- Encryption algorithms are improving and currently AES 256-bit encryption is the de facto on Secure USB drives. But not all AES 256-bit products are created equal!
  - Three popular block cipher modes exist: ECB, CBC and XTS. Kingston uses XTS on most advanced Secure USB drives.
- What does 256-bit mean? It's the length of the key:

10101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101
01010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010101010
101010101010101010 (one 256-bit key)

- That's a lot of combinations. Paired with brute-force/dictionary attack prevention mechanism, our Secure USB drives are very well secured for password attacks.
- Without a password, you can only guess the key. For AES 256-bit keys, that's 2^{256} or… $1.15792089 \times 10^{77}$ possible keys! The age of the universe is roughly 1.4×10^{10} years old.

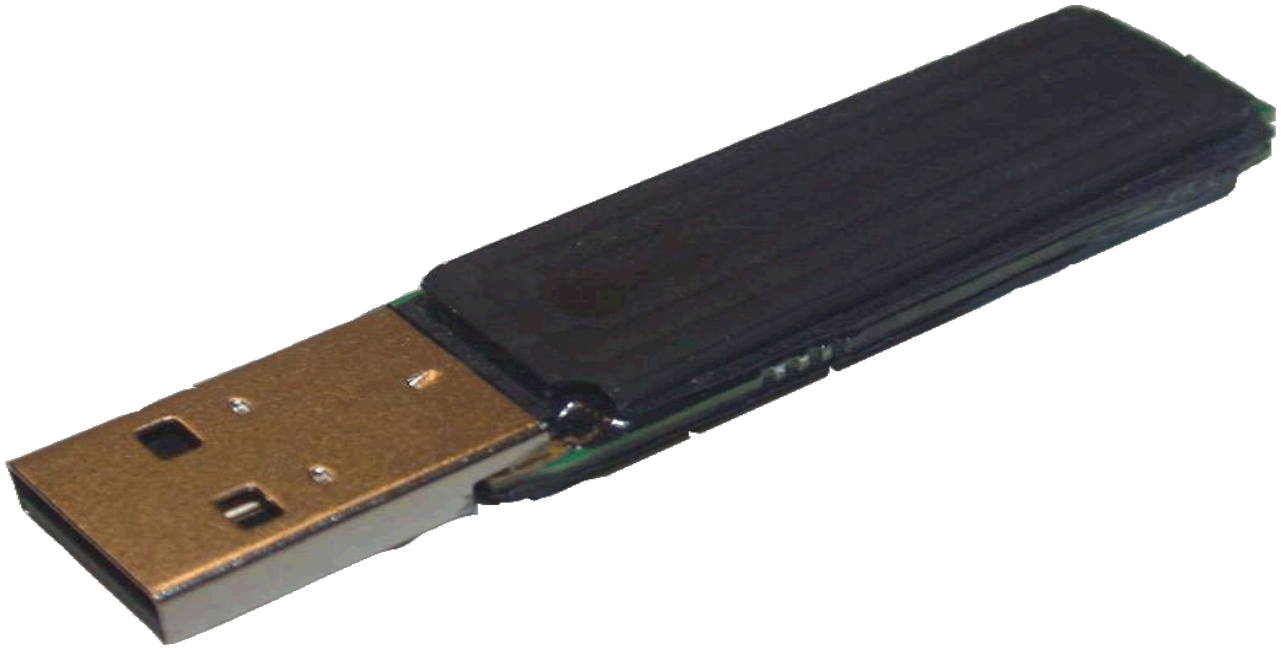
Encrypted DataTraveler Line-Up

Lower Cost → Most Secure

USB 3.0	Locker+ G3	Vault Privacy 3.0	2000	4000G2
Encryption	Hardware Encryption	AES 256-Bit Hardware Encryption	AES 256-Bit Hardware Encryption	AES 256-Bit Hardware Encryption
Feature	USBtoCloud™ Software	XTS Block Cipher Mode	OS independent	XTS Block Cipher Mode
FIPS	n/a	FIPS 197	FIPS 197	FIPS 140-2 Level 3
Capacities	8GB-64GB	4GB-64GB	4GB-64GB	4GB-64GB
Anti-Virus	Available through USBtoCloud™	Anti-Virus SKUs Available	n/a	n/a

FIPS140-2 Module Validation

- Module validated to FIPS 140-2, not just the cryptographic processor



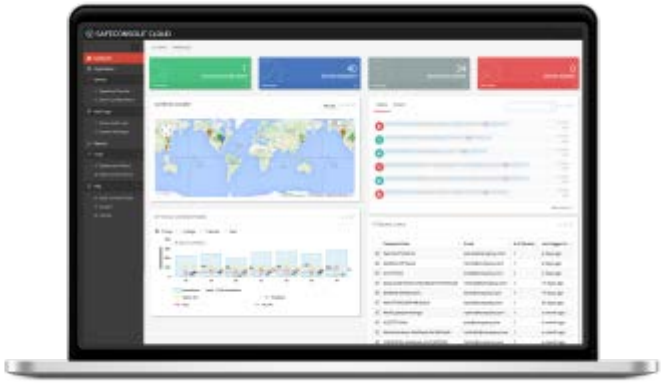
FIPS 140-2 Epoxy physical security barrier

Kingston Encrypted USB Common Features

- All Kingston enterprise security products provide **hardware based authentication**
- 100% AES-256 hardware based encryption – no public storage area for maximum protection
  - Lockout after 10 incorrect password entries wiping keys and formatting the drive
    - Device can be reset for reuse, but data will be lost
  - Enforced complex password with minimum password length

- Rugged, waterproof metal casing
- **Wear-leveling**: Both static and dynamic wear-leveling is used. Under extreme drive usage (writing 80% drive capacity each and every day) drive endurance would exceed 10 years of use!
- **Security Assurance** - Third party security penetration test program providing independent security verification. (Results available under NDA)
- **5 Year warranty** with free global technical support
- Customisable drives and features available including serialization, co-logo, custom profiles, custom password requirements, and more.

SAFECONSOLE®



Secure USB Management allows an organization to quickly and easily establish a command center to inventory, audit and control their secure USB storage devices.

- Remote Password Reset
- Password Policy
- Device Audit
- Device State Management
- Geolocation and Geofencing

- Kingston management ready SKUs (DT4000G2DM & DTVP30DM) support the latest SafeConsole Management software from DataLocker.
- The drives can function without the use of SafeConsole helping purchasing decisions.

Kingston/DataLocker each focus on their strengths

IRONKEY™

Kingston TECHNOLOGY

Kingston acquired the Ironkey encrypted USB product line and Windows To Go.

DATALOCKER®
SIMPLY SECURE

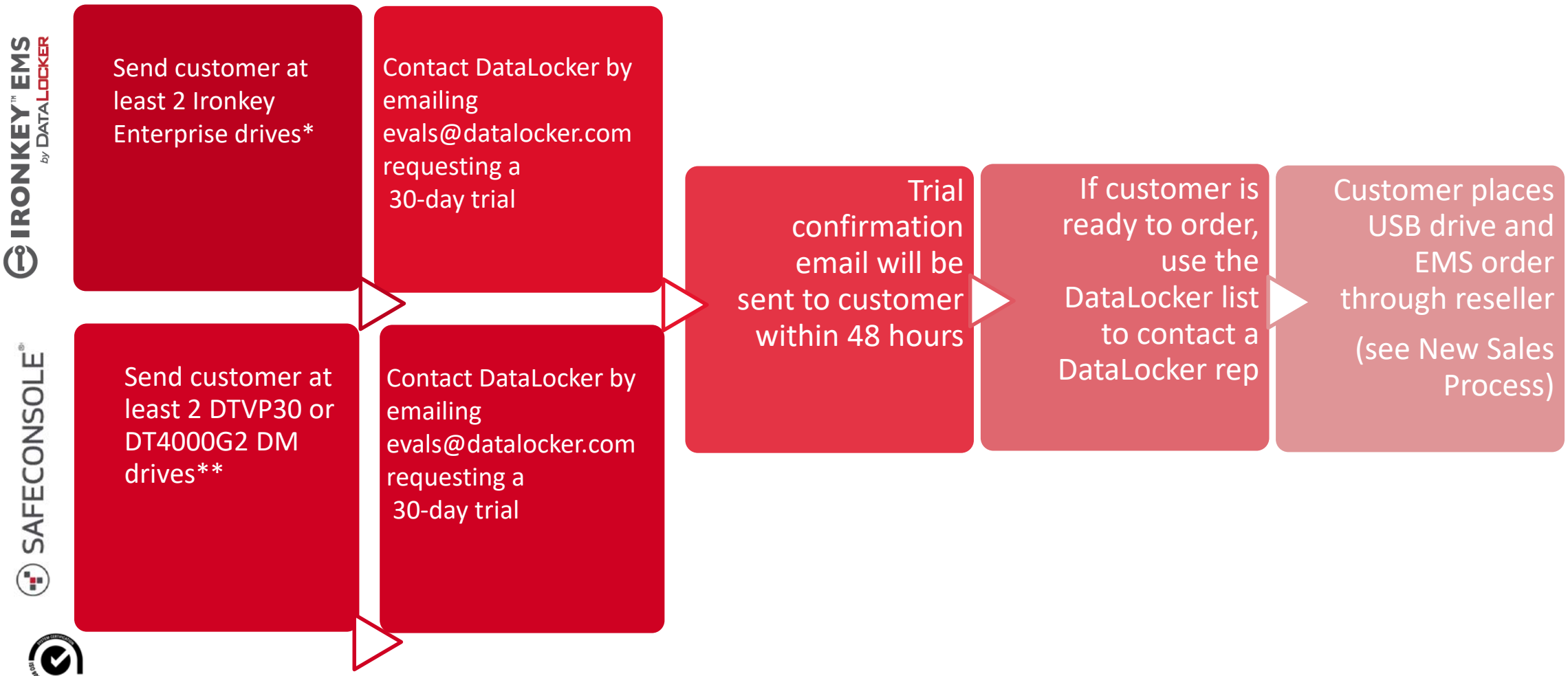
DataLocker acquired the management service, EMS, and Ironkey hard drives.

DataLocker® Inc. is our software partner, they manage the SafeConsole® and Enterprise Management Services (EMS) platforms that both Kingston and IronKey managed encrypted drives utilize.
Kingston is specialised in hardware while DataLocker is focused more on software. By combining our expertise together we offer a truly complete service to our customers.

IronKey FIPS 140-2 Level 3Line-Up

USB 3.0	D300	S1000
Encryption	AES 256-Bit Hardware Encryption	AES 256-Bit Hardware Encryption
Feature	XTS Block Cipher Mode	XTS Block Cipher Mode
FIPS	FIPS 140-2 Level 3	FIPS **140-2 Level 3**
Capacities	4GB-128GB	4GB-128GB
USB 3.0 / 2.0	USB 3.0	USB 3.0

EMS/SafeConsole Evaluation Process



Kingston Technology

Studiu de caz – Securitatea Digitala

SECURITATEA DIGITALĂ ȘI PROTECȚIA DATELOR

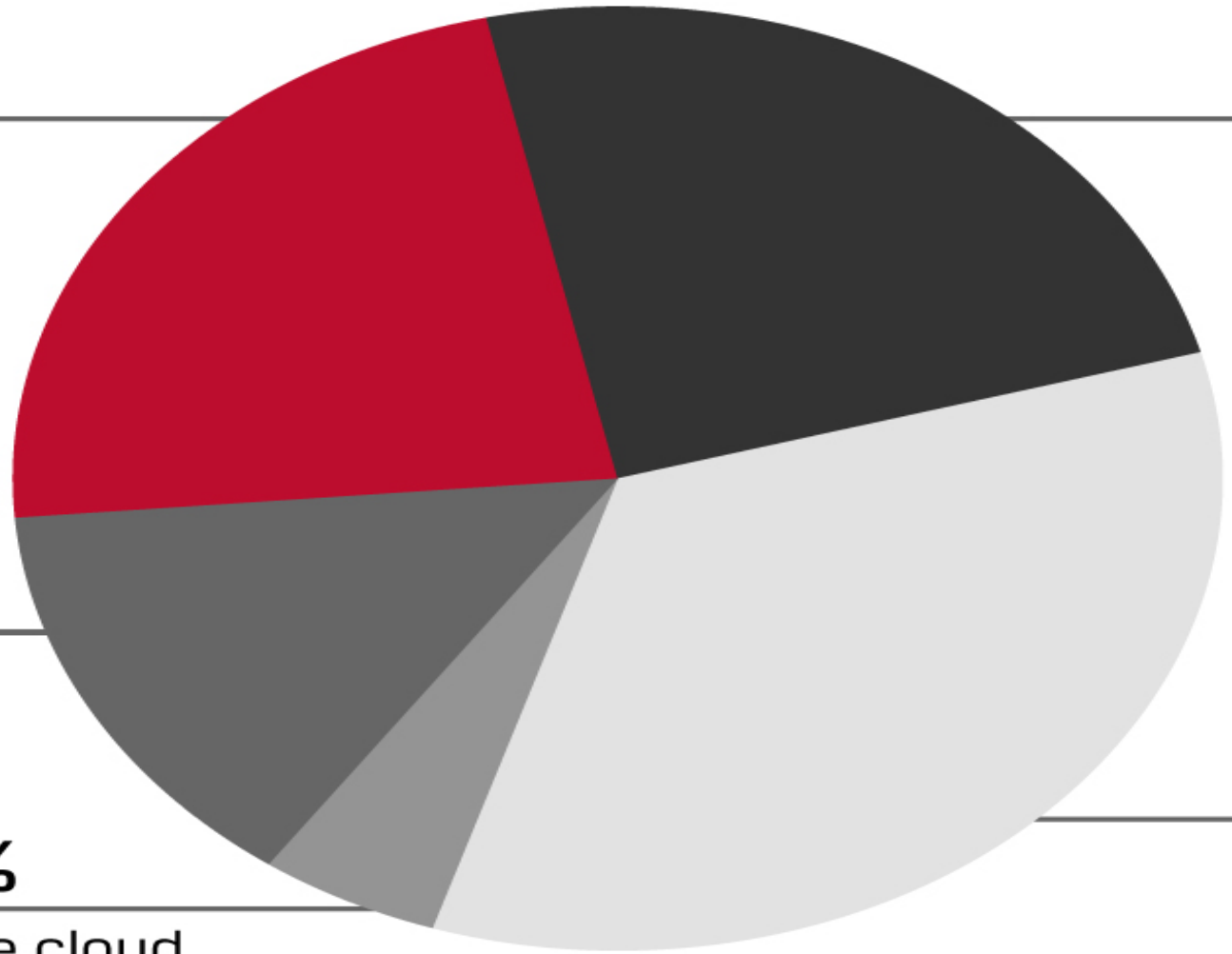
58,93% din angajați lucrează cu informații sensibile

Compania dumneavoastră recurge la protejarea datelor transferate prin soluții cu criptare?

Da - 57,81%	Nu - 42,19%

2 din 3 angajați nu cunosc principalele prevederi ale directivei europene cu privire la protecția datelor

Principala metodă de transfer al datelor sensibile în cadrul companiei:



22,85%
Stick USB
cu criptare

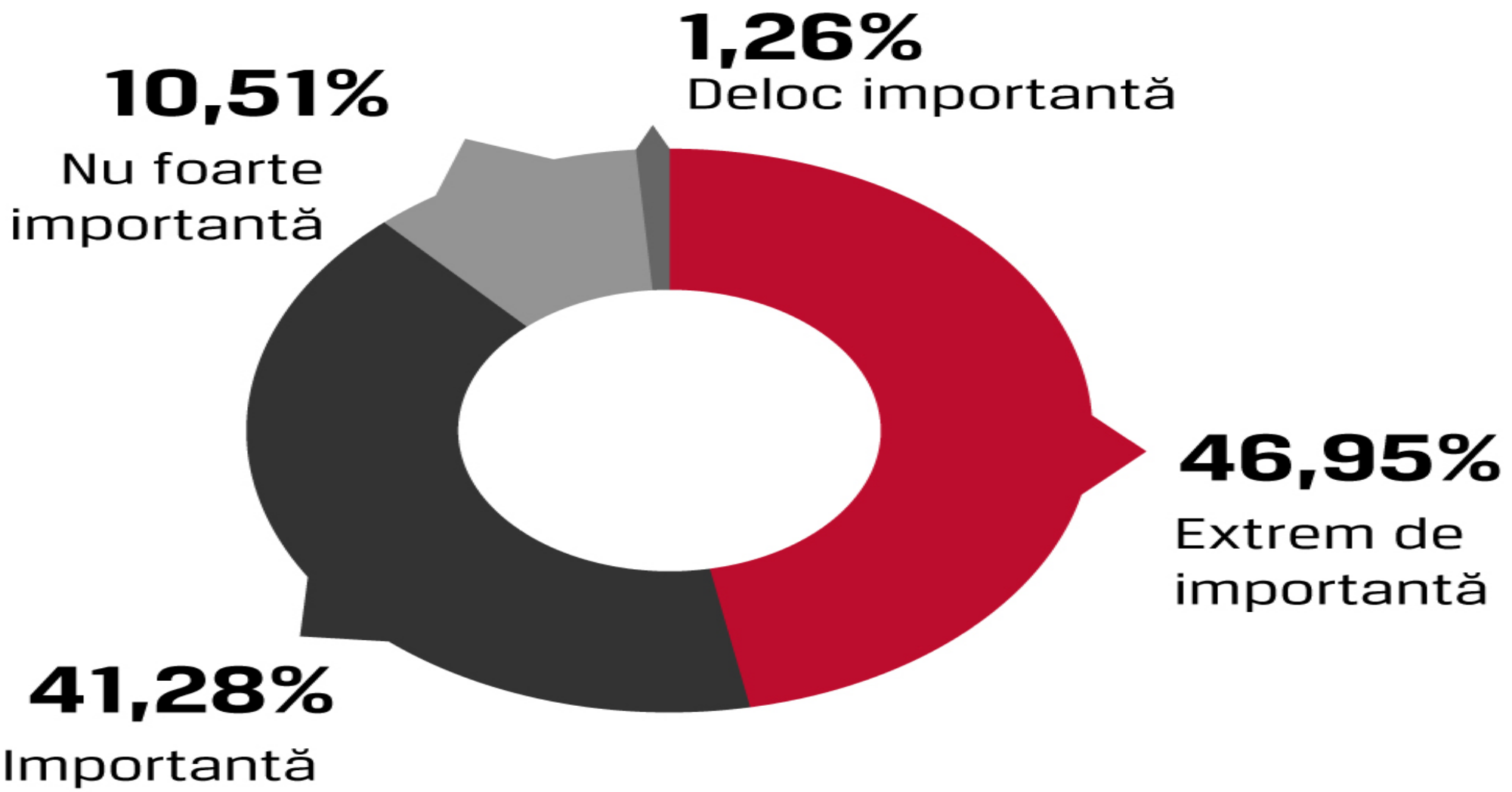
24,18%
Stick USB
fără criptare

13,88%
Altă metodă
de transfer

4,84%
Serviciu de cloud

34,27%
Cloud cu
securizare

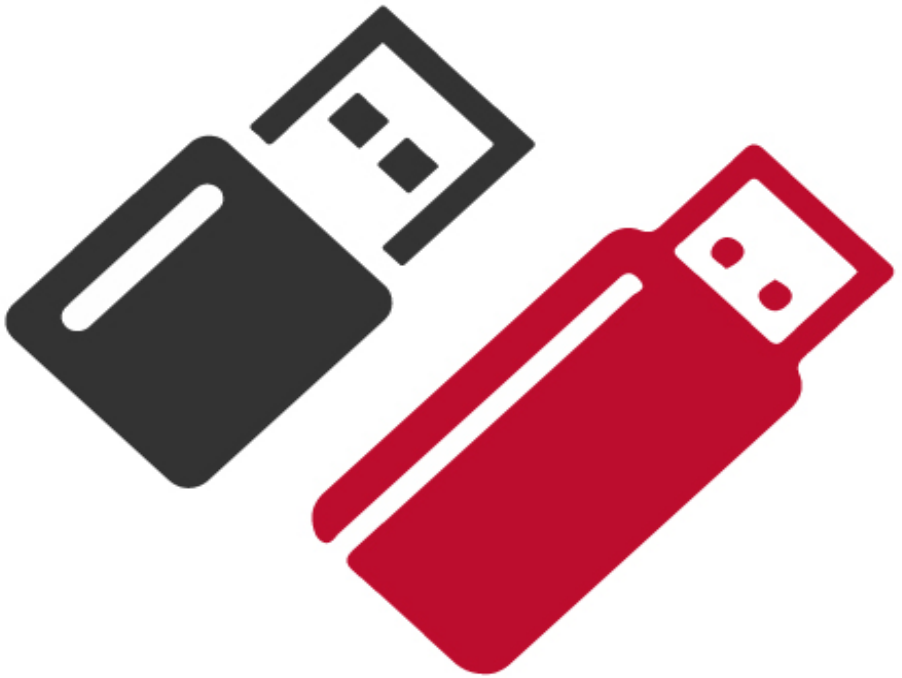
Importanța securizării transferului de date în cadrul companiei, conform angajaților:



80%

din angajați se așteaptă ca bugetul companiilor dedicat securității digitale să crească

Care e primul brand la care vă gândiți când vine vorba de stick-uri cu criptare?



Kingston	57,60%
SanDisk	12,75%
ADATA	7,85%
Verbatim	6,45%
IronKey	5,05%
Transcend	2,59%
Kanguru Solutions	1,26%
LaCie	1,05%
Apricorn	0,35%
Imation	0,35%
Altul	4,70%

Thank you and don’t forget and stay safe and secure!

ggidea@kingston.eu