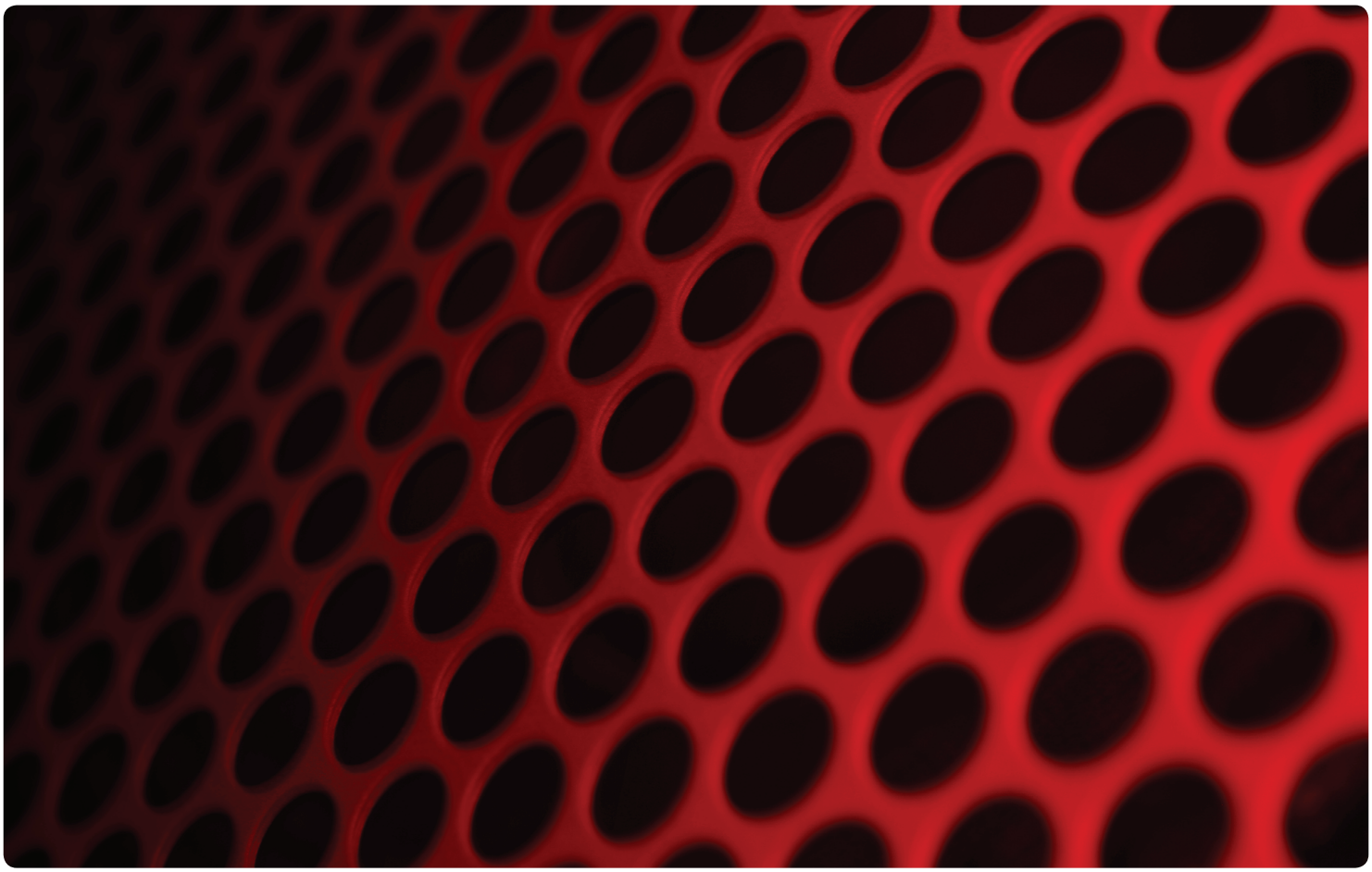
Risk of Data Breaches

How To Prevent Them in Compliance with EU GDPR



Kingston TECHNOLOGY

Introduction

Everyday working life has changed radically and so have traditional ways of working: thanks to mobile storage media, we can access our data practically at any time from any location, and can work on our data wherever we are. We benefit from this **permanent availability** of business information and can create **mobile working versions** or backup copies, thereby optimising our own working hours and, ultimately, effectively shortening operations.

There is a downside to data mobility, however. Lost or stolen USB drives pose a serious risk. **72%** of all companies asked in a survey* reported that they could no longer find individual USB drives. This is especially dramatic because 25% of the companies surveyed had stored **sensitive data** on them. Such data breaches undermine **customer confidence** in the relevant company and are therefore accompanied by a loss of image as well as costs. These figures do not include the risks arising from the publication or criminal use of data.

The legislator has reacted to the increasing risk of data breaches. The **EU General Data Protection Regulation** (EU GDPR) causes companies to assume their responsibilities to an even greater extent as of May 2018. Among other things, severe penalties can be imposed if mandatory provisions are not complied with.

In this white paper you will find out:

- What you need to know about data mobility and data breaches
- What the EU GDPR requires and how companies have to react to the new regulations
- What you can do specifically to avoid data breaches

CONTENTS

* Survey by Kingston Technology in Germany 2016 (number of replies: 200)

The EU GDPR Is Based On Prevention

The European General Data Protection Regulation (EU GDPR) replaces the previous national regulations on data protection and becomes enforceable from 25th May 2018 after a two-year transition period. The primary goal of the EU GDPR is to improve **the protection of data and the fundamental rights of EU citizens**.

The EU GDPR applies not only to European companies, but also to all organisations that offer goods and services (including those that are free of charge) to EU citizens and record their personal data in doing so. The EU GDPR does not differentiate between large corporations, SMEs or small start-up companies. This is why data protection should be examined in all companies that collect, process and store personal data.

The objective of protecting personal data is upheld by significant penalties: breaches of data protection, against which no appropriate measures were taken, can be prosecuted with up to **4% of a company's consolidated annual sales or up to 20 million Euros.**

Furthermore, all data protection breaches must be disclosed to the responsible supervisory authority and those persons affected by it. Apart from financial penalties, the consequences can be extremely far-reaching for a company in terms of their reputation, customer confidence and sales.

These measures are intended to ensure that data breaches are avoided as much as possible. They intend to minimise the disclosure of personal data and encourage companies to take preventative measures. However, the EU is aware that absolute data protection is not viable. Nevertheless, the new directive should achieve the **best-possible prevention**.

Predictive Risk Analysis Helps

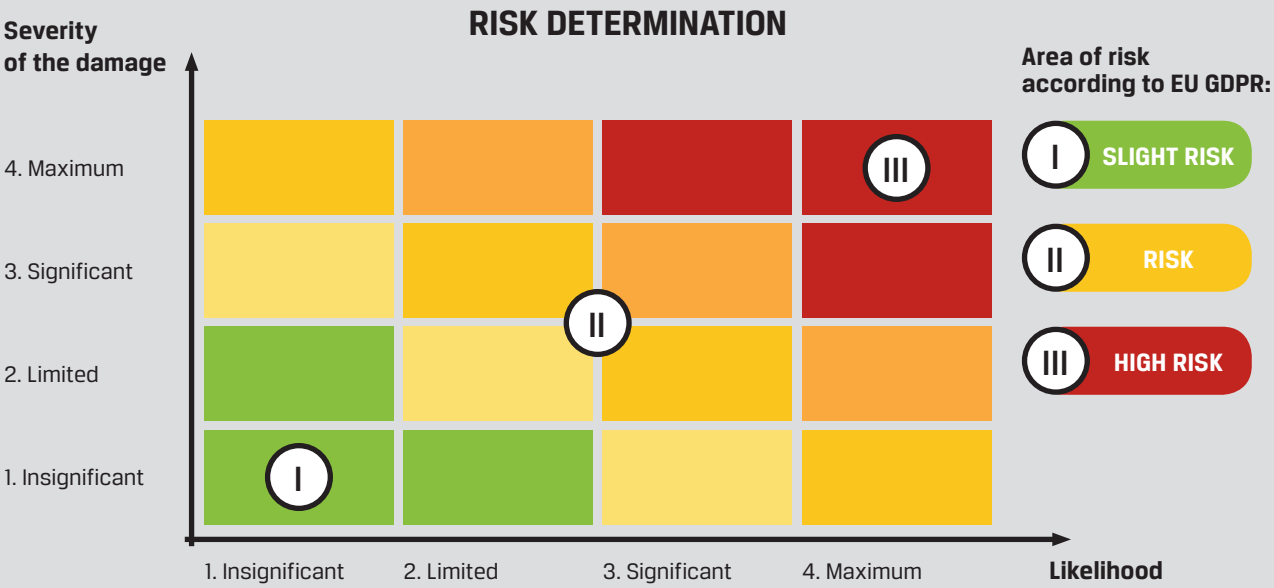
To prevent data protection breaches, you need to know where they can occur. Potential risks therefore have to be identified and analysed. All areas of a company in which data is handled should be examined thoroughly. Where is personal data collected? How is it processed and stored?

This risk analysis is required by the EU GDPR. The likelihood and the severity of possible damage should be considered. The Data **Protection Officer** can use this information to take specific appropriate measures.

A **risk matrix** can help to identify the potential risks of data storage. This highlights where there is a need for action. Each potential risk can be located precisely by its likelihood and by using the severity of the damage. The three risk groups Low – Medium – High then indicate the need for action and the necessary use of security.

Article 32 Paragraph 1 of the EU GDPR states:

"Taking into account the **state of the art**, the **costs of implementation** and the **nature, scope, context** and **purposes of processing** as well as the risk of **varying likelihood** and **severity for the rights and freedoms of natural persons**,the controller and processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk[.]"



A **comprehensive overview** of all locations where personal data is stored facilitates the analysis, showing precisely where action is most urgently required. The **reasons** for the risk assessment can be taken directly from the columns for sources of risk, likelihood and the extent of the damage. In this way, risks can be effectively eliminated as optimal preparation for the key date of 24th May 2018.

The EU GDPR Proposes These Security Measures

The core objective of the EU GDPR for processing personal data is to "ensure a level of security appropriate to the risk" (Article 32 Paragraph 1). Following on from the risk analysis, protective measures must be taken accordingly that are appropriate on the one hand, and can guarantee security on the other.

Fortunately, the EU GDPR also provides specific information regarding how extensive security precautions for sensitive data should be. Article 32 Paragraph 1 also states: "[T]hese measures include [...]: [...] the **pseudonymisation** and **encryption** of personal data." Both procedures can therefore be applied to EU GDPR-compliant security.

To pseudonymise personal data records, names are replaced **by random numerical codes** and the key is stored in a **master table**. This process has the major advantage that it can be fully automated. However, the master table has to be available at all times, and must not be lost or overwritten. It is also critical that a name is not always necessary to identify the underlying person. For example, their identity can also be determined by their gender, date of birth and place of residence. A **residual risk** therefore remains.

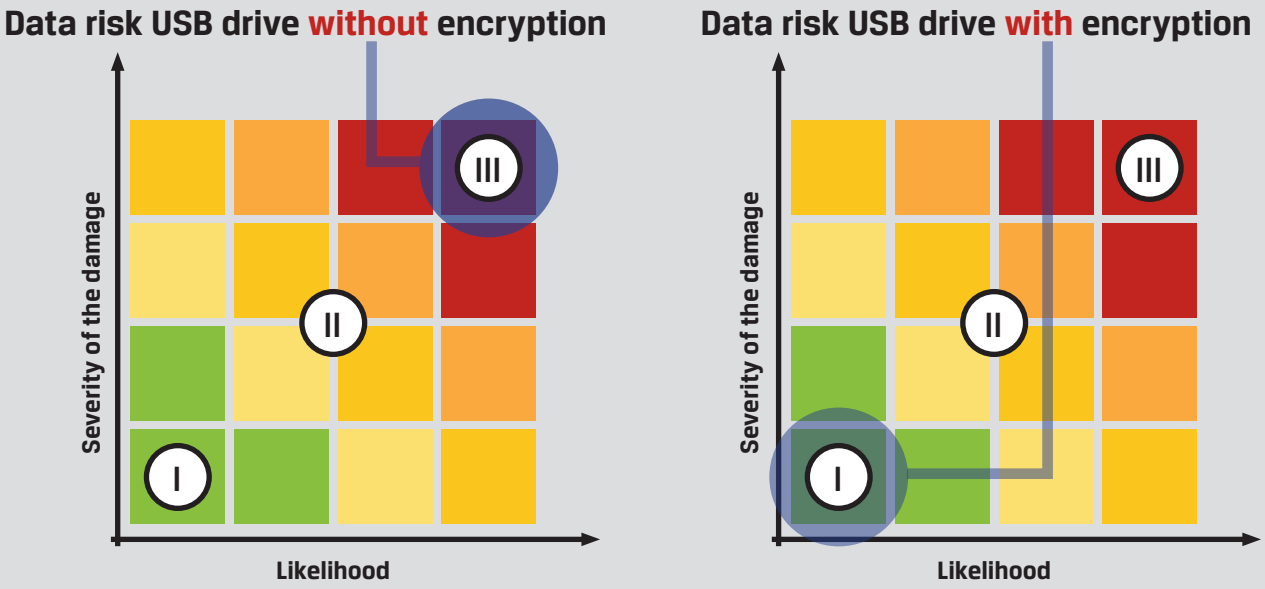
Encryption is another security measure that is recommended in the EU GDPR. Data in any condition and at any point in time of the transmission must be encrypted.

Voluntary **manufacturer certifications such as FIPS 197 or 140 – Level3** are the mark of high-quality encryptions. These guarantee a certain security standard and in future will have an even more important role as evidence in the context of EU GDPR.

If personal data is encrypted securely – 256-Bit AES encryption is state of the art – it cannot be used even in the event of data theft or a data breach. The obligation to inform the person(s) affected or a public announcement no longer applies because no risk exists. The responsible supervisory authority has to be notified nevertheless.

Encrypted USB Drives Any Place, Any Time: Kingston Technology

According to the survey mentioned above, companies who save personal data on unencrypted USB drives are placing themselves at high risk, because these are often lost, stolen or else they cannot be located. Risks here should be assessed as high overall, because both the likelihood and the potential severity of the damage can be regarded as high. Both of these can be significantly reduced by using encrypted USB drives, meaning that the overall risk can be classified as "insignificant".



With its DataTraveler DTVP3.0 and DT4000G2 product lines and the IronKey D300 and S1000, Kingston Technology offers a variety of USB drives that meet the highest security standards mentioned above. The data stored is 100% encrypted and complex password protection with minimum requirements protects against unauthorised access. For example, after 10 unsuccessful logon attempts, the data can no longer be accessed.

The USB drives from Kingston are encrypted according to the security standard **AES-256** in XTS mode. This algorithm corresponds to current security standards. Certifications in accordance with **FIPS 197** and **FIPS 140-2** ensure that your data is absolutely secure even if it is stolen or lost. The DataTraveler 4000G2, IronKey D300 and IronKey S1000 versions also offer

physical protection from manipulation in accordance with FIPS 140-2. For some of its USB drives (DTVP3.0, DTVP3.0AV, DT4000G2 with Management and D300), Kingston also offers a **personalisation program** with which they can be integrated in an endpoint management solution by using serial numbers and product IDs for example, or the number of permitted password entry attempts can be defined.

Kingston Technology has joined forces with **DataLocker** so that it can offer management solutions as well for its encrypted USB drives. DataLocker provides the SafeConsole software program and Enterprise Management System (EMS) for Kingston's encrypted DataTraveler and IronKey USB drives, allowing you to centrally manage the USB drives in your company.

Kingston's DataTraveler Vault Privacy 3.0 and DataTraveler 4000 G2 are available as Managed versions (Management optional) and both support central management by using SafeConsole from DataLocker. IronKeys D300 and S1000 are also available as Managed models and both support the IronKey EMS from DataLocker.

These solutions enable **compliance requirements** to be met more easily and employees can be provided with **additional support**, for example with remote password reset or automated anti-malware scanner functions. They also simplify compliance with comprehensive security guidelines because they enable system administrators to control all of a company's drives easily.

Should an encrypted USB drive from Kingston get lost, this does not automatically mean a data incident. Encrypted mobile storage media thus eliminate a well-known, often underestimated and neglected security risk in companies. Close up small but dangerous security gaps by using encrypted USB drives, thereby **avoiding data protection breaches in accordance with EU GDPR.**

DO YOU HAVE ANY FURTHER QUESTIONS?

Don't hesitate to contact us:

+44 (0) 1932 738888

EncryptedUSB@kingston.eu

www.kingston.com

This white paper was created by the B2B Media Group GmbH on behalf of Kingston Technology Europe Co LLP and Kingston Digital Europe Co LLP.
http://www.b2bmg.de / kontakt@b2bmg.de