DATALOCKER®
SIMPLY SECURE

WHITE PAPER

GDPR is coming - prevent lost portable data and avoid €20 million or more in fines

On 25 May 2018 the European Union's General Data Protection Regulation (GDPR) come into force. It is therefore high time to get ready as the changes that may be required can be significant. The EU law also has a extraterritorial clause meaning that it applies to any organization that in some way handle data originating from EU citizens. The ICO in the UK have been outspoken that UK business need to get in line and will not receive a free pass on compliance due to Brexit.[1]

CONCERNS FOR ANY EU, UK OR GLOBALLY ACTIVE ENTITY

Every company doing business in the European Union has some challenges ahead.[2] *-IAPP President and CEO J. Trevor Hughes*

The European Union's General Data Protection Regulation (GDPR) law means that organizations, that handle EU citizens data will face fines if they are found to be non-compliant as per **Article 83 section 5.**[3]

...be subject to administrative fines up to 20,000,000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher...

It should be noted that these fines are not meant solely to be issued due to data breaches but are intended to also be issued if an organization is found to be non-compliant to the law, without a breach having occurred.

"Thanks to an extraterritoriality clause, even a company or service provider with no physical EU footprint still has to comply with the EU data protection legislation if it processes EU citizens' data making it of global concern." stated Duncan Brown, research director at IDC to SearchCIO.[4]

THE GDPR AND PORTABLE DATA STORAGE

This paper focuses on the implications of the GDPR on portable data storage. The GDPR spans all data aspects of business and will in general mean that companies will need a broad approach to ensure compliance.[5] The ICO has put together some of the most relevant resource of any of the EU country authorities at http://dpreform.org.uk/. On the ICO website you can find a 12 step guide that provides a very good overview of the work ahead. IAPP has also produced guidelines and will be hosting conferences dedicated to GDPR work.[6]

However, the risks associated with portable storage means that it is vital to consider the practical implementation aspects of this area from the onset.

[1]https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2017/05/businesses-warned-to-prepare-with-one-year-until-data-protection-law-change/
[2]http://www.prnewswire.com/news-releases/iapp--truste-launch-gdpr-assessment-solution-to-help-companies-prepare-for-strict-new-eu-privacy requirements-300245065.html
[3]http://www.privacy-regulation.eu/en/83.htm, http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[4]http://searchcio.techtarget.com/news/4500267769/New-EU-data-protection-legislation-will-challenge-US-IT-execs
[5]https://ico.org.uk/media/1624219/preparing-for-the-gdpr-12-steps.pdf
[6]https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/

AVOID FINES AND THE NEED TO REPORT DATA BREACHES TO AUTHORITIES WITHIN 72 HOURS

With the right tools it is possible achieve a easier and more cost efficient portable storage policy.

A hardware encrypted and managed storage device **cannot expose any data if lost, therefore the loss does not need to be reported to authorities as per Article 34 section 3a**:

The communication to the data subject referred to in paragraph 1 shall not be required if any of the following conditions are met:

(a) the controller has **implemented appropriate technical and organisational protection measures, and those measures were applied to the personal data affected by the personal data breach***, in particular those that render the personal data unintelligible to any person who is not authorised to access it, such as encryption;*

The only cost of a lost device, in this hardware encrypted case, is the piece of hardware that needs to be replaced and the potential data loss in lack of a backup.

On the other hand, an unencrypted USB flash drive that contained a patient journal, a customer list, or employee assessments for example, would need to be reported directly to the relevant data protection authority.

The legislative pressure should lead to a spike in reported cases. The pressure that will be put on an organization subsequent to reporting a breach will likely be significant and "clean up" costs and efforts will be significant and involve more than IT.

In the past lost portable storage devices have often not been reported to the authorities. We know this as the cases of reported devices are far less then what users state when surveyed about lost portable storage. In a Ponemon study, it was found that 65% of users do not report lost USB flash drives.[7]

Unreported breaches should soon be a thing of the past as the GDPR enforces "the right to know when you've been hacked". Organizations are now required to tell regulators about a personal data breach "not later than 72 hours after having become aware of it" or risk fines. This notification is mandatory, per **Article 33**:

"In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours after having become aware of it**, notify the personal data breach to the supervisory authority competent in accordance with Article 55, unless the personal data breach is unlikely to result in a risk to the rights and freedoms of natural persons..." [8][9]

[7] http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf
[8] http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679
[9] http://www.privacy-regulation.eu/en/33.htm

ENSURING COMPLIANCE FOR PORTABLE STORAGE DEVICES

One promise of the GDPR is to simplify the legislative landscape for a business that has customers in Europe. As of June 2013, there is globally a total of 99 national data privacy laws with more laws pending.[10] However it should be noted that there still might be minor local variations depending on which country's authority is the governing one. Germany is one of the countries that is looking to make adjustments.[10]

The GDPR extrapolates and draws from current data protection legislation work in the EU and will be a dominating legislation for the future. A professional Data Protection Officer might say that there is not much that is surprising in what an organization must achieve to handle citizens data correctly. The more surprising part of the GDPR is that the consequences will be much direr if they don't.

Instead of detailing exactly which technology must be used in each area, the GDPR specifies these in general terms, found in **Article 32 - Security of processing:**

1. 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 the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate:

(a) The pseudonymisation ***and encryption of personal data;***

(b) ***The ability to ensure the ongoing confidentiality, integrity, availability and resilience of processing systems and services processing personal data;***

(c) The ability to restore the availability and access to personal data in a timely manner in the event of a physical or technical incident;

(d) ***A process for regularly testing, assessing and evaluating the effectiveness of technical and organisational measures for ensuring the security of the processing.***

...

[10] http://www.hldataprotection.com/2017/01/articles/international-eu-privacy/german-government-presents-revised-draft-gdpr-implementation-bill/

CHECKLIST FOR GDPR COMPLIANCE FOR PORTABLE DATA STORAGE

DataLocker is a global expert within encryption and portable data storage and is well aware of what is the current status of the available technology on the market and knows what legislators and courts can and should expect from data controllers in terms of safeguards and procedures. DataLocker is an instant, cost-effective way to comply with HIPAA, SOX, DHS Initiatives, NRC, GLB and any other directive that requires data encryption such as the GDPR.

DataLocker's recommendation to achieve compliance with the GDPR for portable storage is to implement a solution that:

- Protects all stored data with automatic encryption and strong passwords. (Article 32 1a) This measure releases the organization from the need to report a lost or stolen device as the risk of causing a risk to data subjects rights is unlikely, as per Article 34.
- Only relies on hardware encrypted USB flash drives. Regular USB flash drives can be software encrypted but there is no way to ensure the integrity of the software encryption as the software can be removed from the standard drive, causing non-compliance with Article 32 1b.
- Manages the hardware encrypted devices to comply with Article 32 1d. Placing the device under management ensures that it is possible to show a proof of compliance through the management console.
- Locks down USBs to only allow the certified hardware encrypted USB drives with the means of a port control software.
- Ensures that only authorized staff have the rights to transport data. This step mitigates against insider threat which can be a data breach source.
- Keeps track of which data is transferred onto encrypted portable media. To ensure that the organization can take appropriate action if a device goes missing: Is the data relevant under GDPR? Is further action needed?
- Can permanently erase any and all copies of a data subjects stored information, also known as the right to erasure. This ability is also important when insider threats and employee termination are considered.[11]

For further information and an implementation best practices of portable data storage we recommend our white paper: 7 Steps to Solve the Problems with USB Drives, this paper and more materials are available for download from https://safeconsole.com/whitepaper/

[11] http://www.privacy-regulation.eu/en/17.htm

SUMMARY

- The GDPR will bring a swift end to the relaxed practice of using insecure portable data storage within organizations on 25 May 2018.
- The fines and consequences and EU track record of issuing large fines will mean that the costs of implementing a solid portable storage solution far outweighs exposing an organization to risk of non compliance.
- All organizations (EU, UK, global) that handle any EU citizens data can be fined under the GDPR.
- Centrally managed hardware encrypted portable storage that provides audit trail capabilities is the recommended solution.

ABOUT US

DataLocker provides encrypted external storage, cloud encryption and central management solutions to thousands of government, military and enterprise clients around the world under the DataLocker, Sentry, SafeConsole, and IronKey EMS brand names. Learn more at datalocker.com

KEYWORDS

Data subjects - the persons which personal data is handled

Data controller - the organization processing the personal data of data subjects

GDPR - General Data Protection Regulations

RESOURCES

The full GDPR legislation from the EU law website:
http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32016R0679

The GDPR legislation in an easier to digest formatting with table of contents and internal hyperlinks:
http://www.privacy-regulation.eu

SAFECONSOLE.COM

UNITED STATES
1-913-310-9088
sales@safeconsole.com

To find your local SafeConsole Reseller
please visit datalocker.com for more information.