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

Every company doing business in the European Union has some challenges ahead. [1]

IAPP President and CEO J. Trevor Hughes

Concerns for any EU or globally active entity

The European Union's General Data Protection Regulation (GDPR) means that organizations, that handle EU citizens data face fines of up to €20 million or 4% of their global annual turnover if they are found non-compliant.[2]

"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.[3]

The GDPR and portable data storage

This paper focuses on the implications of the GDPR on portable data storage. The GDPR spans all aspects of business and will in general mean that companies will need a broad approach to ensure compliance. However, the risks associated with portable storage means that considering the practical implementation aspects of this area from the onset has a value.

[1]http://www.prnewswire.com/news-releases/iapp--truste-launch-gdpr-assessment-solution-to-help-companies-prepare-for-strict-new-eu-privacy-requirements-300245065.html
[2] http://www.consilium.europa.eu/en/press/press-releases/2015/12/18-data-protection/
[3]http://searchcio.techtarget.com/news/4500267769/New-EU-data-protection-legislation-will-challenge-US-IT-execs

Report data breaches to authorities within 72 hours

In the past lost portable storage devices have 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.[4]

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." This notification won't be required if the breach is "unlikely to result in a risk for the rights and freedoms of individual." [5] An unencrypted USB flash drive that contained a patient journal or customer list would need to be reported directly to the relevant data protection authority. The legislative pressure should lead to a spike in reported cases.

The GDPR is approved - deadline approaching rapidly

It is high time to start preparing for the GDPR. The Information Commissioner in the UK Christopher Graham issued a call for organizations to begin their preparations for the forthcoming EU data protection reforms in March of 2016.[6] The GDPR will come into full effect in 2018. The legislation has won formal approval by the European parliament by a vast majority, so the countdown to the deadline has begun.[7] The new legislation will replace the EU Data Protection Act that dates back to beginnings of the Internet in 1995.

The ICO has put together the most relevant resource of any of the EU country authorities at http://dpreform.org.uk/. Here you can find a 12 step guide that provides a very good overview of the work ahead.[8] IAPP has also produced guidelines and will be hosting conferences dedicated to GDPR work.[9]

[4] http://media.kingston.com/pdfs/Ponemon/Ponemon_research_EMEA_summary_UK_1111.pdf
[5] http://blogs.wsj.com/law/2015/12/16/the-eu-data-privacy-agreement-what-we-know-and-dont/
[6]https://ico.org.uk/about-the-ico/news-and-events/news-and-blogs/2016/03/20-million-reasons-for-organisations-to-get-eu-data-reforms-right/
[7]https://www.theguardian.com/technology/2016/apr/14/european-parliament-approve-tougher-data-privacy-rules
[8] https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf
[9]https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-1-data-security-and-breach-notification/

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]

The GDPR extrapolates and draws from current data protection legislation work in the EU and will be a dominating legislation for the future. A 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 which technology must be used in each area, the GDPR uses a general term phrased as: "**Data controllers must implement appropriate security measures**"[11]. This can be translated into meaning that organizations should protect data at a level that is achievable with current technology at a reasonable cost and effort. If this can't be achieved organizations should consider not exposing or collecting the data at all.

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's recommendation to achieve compliance with the GDPR is to implement a solution that:

- Protects all stored data with automatic encryption and strong passwords. This measure practically 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.
- 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?
- Only allows access to the data in approved territories. A transborder data flow is a transfer of personal data to a recipient who or which is subject to a foreign

[10] https://papers.ssrn.com/sol3/Data_Integrity_Notice.cfm?abid=2280875
[11] http://www.consilium.europa.eu/en/press/press-releases/2015/06/15-jha-data-protection/

jurisdiction.[12] Transborder data flows will be subject to additional restrictions under the GDPR.[13]

- Can permanently erase any and all copies of a data subjects stored information, also known as the right to be forgotten. [14] This ability is also important when insider threats are consider.

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/whitepapers/

Summary

- The GDPR will bring a swift end to the relaxed practice of using unsecure portable data storage within organizations.
- 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 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 Regulation

[12] http://www.echr.coe.int/Documents/Handbook_data_protection_ENG.pdf
[13] https://iapp.org/news/a/top-10-operational-impacts-of-the-gdpr-part-4-cross-border-data-transfers/
[14] https://dpreformdotorgdotuk.files.wordpress.com/2016/03/preparing-for-the-gdpr-12-steps.pdf

Resources

Final draft of the GDPR - full text:
http://online.wsj.com/public/resources/documents/2015_1216_gdpr.pdf