stealthbits
NOW PART OF netwrix

EXECUTIVE BRIEF

AN INTRODUCTION TO EU GDPR COMPLIANCE

THE ORIGINS OF THE EU GDPR

For many, April 14th will go down in history as the day the world (well, Europe anyway) woke up and realized the importance of data privacy laws designed for the 21st Century. The EU GDPR – European Union, General Data Protection Regulation – repeals the 1995 EU Data Protective Directive (Directive 95/46/EC), after four years of discussion and legal wrangling. Finally, a DP directive intended to deal with the issues of a modern, mobile and connected society.

216 PAGES OF LEGISLATION

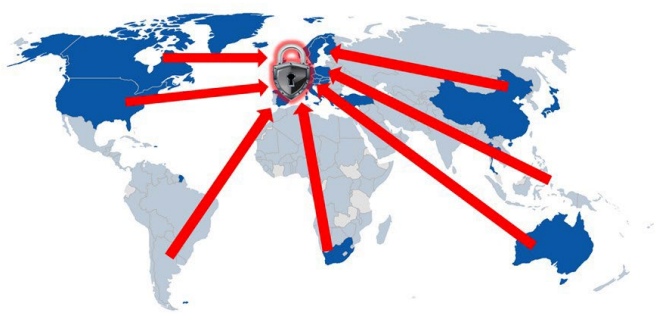
For anyone interested in trawling through all 216 pages of the Interinstitutional File, here's a direct link to the downloadable pdf:

http://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CONSIL:ST_5419_2016_INIT&from=EN

For those who don't, see the bottom of page 3 for the highlights.

NOT IN THE EU? WHY CARE ABOUT THE EU GDPR?

- Do you offer goods or services in the EU zone?
- Do you offer goods or services to an EU Member State?
- Do you monitor the behaviour of an EU Citizen?



If you answered yes to one or more of these questions, then you need to be in compliance and will likely need to employ a representative in the EU. Previous legislation did not require this – including the Safe Harbour.

20 MILLION REASONS TO CARE

Under the previous United Kingdom Data Protection Act, the maximum fine for a data breach was approximately €644k / $729k / £500k. Not small change to most, but barely a scratch on the surface to companies with billion-dollar annual turn overs.

And herein lies the reason why every business that trades in or with the EU truly needs to care.

Under EU GDPR the maximum fine for transgression is a whopping:

€20 M | $22.5M | £15.5M

Again not peanuts to most, but still not earth shattering to the billion-dollar revenue

business. So, this is why under EU GDPR there is an 'or' and that 'or' is:

4% of Annual GLOBAL revenue
Whichever figure is higher!

YOU HAVE UNTIL MAY 25TH, 2018 TO BECOME COMPLIANT

But now is the time to start considering where your

organization sits.

- Will it be subject to EU GDPR?
- Are you compliant?
- What actions are needed to be compliant?

...HERE ARE THE HIGHLIGHTS (WITH A LITTLE PARAPHRASING)

- **Clear and affirmative consent** must be provided for the processing of private data. All consent documentation must be laid out in simple terms – no confusing jargon and lawyer speak.
- An EU citizen shall have **greater control** of their personal data.
- **The right to be forgotten:** If an individual no longer wants their data to be processed, they can ask the holding company to permanently erase it.
- **Businesses will be responsible** for notifying an individual that they have or are collecting, along with **why and to what end**.
- If a company (the Controller) has any hosted infrastructure (IaaS, PaaS, SaaS) and there is a breach on the hosted infrastructure (of the Processor). **The liability will now be classed as shared responsibility.**
- DPO – Data Protection Officer. If the Controller is involved in 'regular and systematic monitoring of data subjects on a large scale', or processes 'special categories of personal data' then **they MUST appoint a DPO**.
- Controllers must adopt, if they haven't already, a risk-based approach. If any activity could be classed as higher risk, then **comprehensive privacy impact assessments must be undertaken.**
- All efforts must be made to **minimize a breach of data**.
- Data Controllers are required to **report any data breach within 72 hours** of the incident becoming apparent. The exception is if it may present a risk to the rights of the data subject(s) involved.
- **Regular internal and supply chain audits are required** to ensure processes are fit for purpose.
- A data controller must be able to **provide a data subject a copy of their personal data**, in a format suitable for processing by another data controller – for example; you should be able to take your email, documents etc from one provider to another.

NEXT STEPS

Schedule a demo
stealthbits.com/demo

Download a free trial
stealthbits.com/free-trial

Contact us
info@stealthbits.com

IDENTIFY THREATS. SECURE DATA. REDUCE RISK.

Stealthbits Technologies, Inc. is a customer-driven cybersecurity software company focused on protecting an organization's sensitive data and the credentials attackers use to steal that data. By removing inappropriate data access, enforcing security policy, and detecting advanced threats, our highly innovative and infinitely flexible platform delivers real protection that reduces security risk, fulfills compliance requirements, and decreases operational expense.

stealthbits
NOW PART OF netwrix