blancco technology group

12-STEP ACTION PLAN

TO PREPARE FOR EU GDPR COMPLIANCE BY 2018

1 Conduct Internal Audit

Conduct an internal audit of all data and asset management policies currently in place. Analyze and identify weaknesses and gaps that would leave your organization vulnerable to non-compliance with EU GDPR.

2 Create Written Documentation

Create and maintain a detailed register of all physical, virtual and logical places where data is held (including corporate, customers, employees and third party suppliers/vendors). Distribute and communicate all items in this list with all internal departments and stakeholders.

3 Remove Data Securely

Securely erase data from electronics and IT equipment using a certified data erasure solution that adheres to legally required overwriting standards, such as HMG Infosec and DoD 5220.22.M. Make sure the solution is approved by government agencies and bodies like NATO, Department of Defense, CESG, TUV SUD and DIPCOG, just to name a few.

4 Provide Proof of Data Removal

Respond to customer inquiries in writing and show verifiable, physical proof of how and where customer data is removed if/when it is outdated or irrelevant.

5 Deliver Customer Communications

Publish and inform customers regularly and repeatedly about data processing methods and tools used. Publish and inform customers in writing of their right to withdraw consent to use/store their data. If and when any changes are made to data processing and management methods, publish and inform customers in writing.

6 Incorporate Mobile Device Management

If employees use mobile devices for work (BYOD program), create and communicate data retention and BYOD resale policies to all employees. Make sure to create separate plans for "Choose Your Own Device" and corporate-owned devices.

7 Collect Data Responsibly

Set clear definitions for all types and levels of profiling implemented by your organization.

8 Drive Cross-Department Collaboration

Work with other departments across the entire organization to support their specific business needs/goals in relation to data collection, storage and removal.

9 Implement Education & Training

Build and distribute ongoing training (verbal and written) for internal employees across the entire organization outlining breach scenarios and causes, recordkeeping/monitoring best practices and an overview of proper (and improper) data removal methods. Create a culture of security across the entire organization, regardless of individual roles/functions.

10 Appoint Data Protection Officer

Identify and appoint an internal team member as your organization's dedicated Internal Data Protection Officer (DPO). This person should be in charge of implementing operational systems and IT asset management workflows, while also staying up to date with announcements and suggestions made by the ICO and other governing bodies.

11 Monitor Risk Management

Create a comprehensive risk management plan that includes management of data across the entire lifecycle – from creation to storage to transfer to removal. This should include third party suppliers/vendors that may be used by your organization.

12 Develop Incidence Response Plan

Develop a written incident plan (crisis response) that can be enacted if/when data breaches occur. This should include customer response messaging, media response messaging, maximum response times, expected timelines and an outline of all involved parties and their specific crisis response roles/functions.

Proactively planning for the removal of data helps organizations meet "right to be forgotten" requirements, while also decreasing the chances of being investigated and fined by the Supervisory Authorities.

DOWNLOAD FULL RESEARCH STUDY

LEARN ABOUT OUR DATA ERASURE SOLUTIONS