Protecting your data and reputation under GDPR

How to protect data throughout the entire technology lifecycle

BY SERDAR BANKACI

INTRODUCTION: NEW RULES

On May 25, 2018, the European Union General Data Protection Regulation, also known as GDPR, went into effect. This was one of the most comprehensive overhauls of data privacy laws the world has seen. It is expected that this will be the model for future data privacy laws.

Under GDPR, data liability will be reach beyond basic data protections and exposure. Companies will be required to ensure robust data protection for and absolute destruction of data from end-of-life equipment, including computers, servers, tablets, phones and other data-containing devices.

Legal liabilities for not meeting and documenting appropriate methods can result in irreparable harm to brands, significant civil liability and other penalties, which can be as high as 4% of global annual revenue or €20M.

While GDPR may be new, end-of-life IT asset management is not. By ensuring they have a compliant cradle-to-grave IT asset management and security plan, companies can rest assured that they are protected. The first step in this process is partnering with responsible service providers, vendors and IT asset disposition (ITAD) companies.

Experienced ITAD companies can help you evaluate your current process and improve it. GDPR is only one piece of the puzzle. With no federal e-waste law and many states having their own e-waste laws, companies need help navigating these murky waters.

GDPR IN A NUTSHELL

GDPR is designed to protect the privacy and data of European citizens. GDPR has wide-reaching applications, applying to any business that collects or handles the personal data of European citizens. With nearly all business

transactions taking place online and no physical storefronts, nearly all major companies are affected by GDPR.

If your business meets any of the following criteria, GDPR applies to you:

- It has a physical business presence in an EU country.
- It collects, stores or processes the personal data of EU citizens, regardless of physical location.
- It provides data-related services to companies that handle EU citizens' data.

WHAT CONSTITUTES PERSONAL DATA?

The GDPR applies to 'personal data,' meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier. This definition provides for a wide range of personal identifiers to constitute personal data, including name, identification number, location data or online identifier, reflecting changes in technology and the way organizations collect information about people.

LIABILITY UNDER GDPR

One of the most unique aspects of GDPR is that it creates a shared liability between the companies that collect the data and any data processor. For example, your company hires an ITAD company that fails to destroy your data. Under GDPR, both your company and the ITAD company can be subject to liability. Under GDPR, a company needs to vet its partners, vendors and ITAD providers carefully.

Organizations can be fined up to 4% of annual global turnover or €20 million for breaching GDPR. This is the maximum fine that can be imposed for the most serious infringements, e.g., not having sufficient customer consent to process data or violating the core of Privacy by Design concepts.

There is a tiered approach to fines, e.g., a company can be fined 2% for not having its records in order (article 28), not notifying the supervising authority and data subject about a breach, or not conducting impact assessment. It is important to note that these rules apply to both controllers and processors, meaning 'clouds' are not exempt from GDPR enforcement.

What is the difference between a data processor and a data controller? A controller is the entity that determines the purposes, conditions and means of the processing of personal data, while the processor is an entity that processes personal data on behalf of the controller.

THE ITAD PROCESS AND GDPR

ITAD vendors specialize in the process of disposition of IT assets. Enterprises with end-of-life, off-lease or obsolete equipment must consider whether the items should be resold or recycled. Dumping used IT assets in landfills can be illegal in any state.

ITAD exists in response to several considerations: Nearly all devices contain data, which means that storage devices must be securely wiped and documented. IT assets cannot just be put into the trash; damage to the environment and fines may result from improperly recycled equipment. And with different privacy and e-waste laws in various states, companies have difficulty understanding their responsibility in each state.

Practical applications for end-of-life equipment management:

- Find a reputable ITAD provider. Any reputable ITAD provider will be R2 certified and have cyber liability insurance.
- Establish a written end-of-life asset SOP that outlines both recycling and data destruction.
- Document the serial numbers of equipment and hard drives. ■

CyberCrunch is an innovator when it comes to data destruction and e-waste recycling, finding previously untapped value in e-waste that allows it to provide customers with the best service possible. Based in Pittsburgh, the company serves Fortune 1000 companies across the country with solutions that include data destruction, IT asset disposal and e-waste compliance. The company, which is R2 certified, fully insured and a member of the National Association for Information Destruction (NAID), handles clients' IT assets and sensitive data per the highest industry standards.