WHITE PAPER

The GDPR and New York Department of Financial Services Data Protection Regulations

Compliance-driven cybersecurity has arrived in Europe and the United States.

The General Data Protection Regulation, or GDPR, is the European Union's new data protection rule that comes with a broader set of mandates, stricter penalties, and applies beyond the boundaries of Europe. The GDPR applies to any business that has personal data of EU data subjects no matter where in the world a business is based or systems are located.

In the U.S., the State of New York Department of Financial Services has implemented similar, but not identical, regulations that impose strict rules around breach notification, cybersecurity planning, compliance verification and cybersecurity staffing.

A company does not need to be breached to be the subject to an enforcement action under the GDPR or NY DFS. Failing to comply is enough to trigger penalties.

The GDPR and NY DFS changes cybersecurity enforcement

On 25 May 2018, European Union regulators begin to enforce the GDPR. Enforcement of New York DFS 23 NYCRR Part 500 is already underway.

Under the GDPR, fines of up to 10 million EUR or 2 percent (2%) of an organization's annual, global sales revenue - whichever is greater – can be assessed for failing to ensure security. Fines for more severe infractions, repeat infractions, or failing to comply with an order under the GDPR may result in fines up to 20 million EUR or four percent (4%) annual global sales.

Under DFS 23 NYCRR Part 500, companies that are attacked must notify DFS within 72 hours of any breach that could impact the business or its customers; maintain written cybersecurity plans, conduct annual penetration tests (in some cases) and twice-a-year vulnerability assessments. Compliance certifications are required to be filed each year with the Department.

The GDPR requires the appointment of a Data Protection Officer: the NY DFS requires the appointment of a Chief Information Security Officer.

A number of recent high profile cyberattacks are good examples of circumstances where the GDPR and/or NY DFS regulations could have led to enforcement actions if the breaches had occurred later in 2018:

Company	Records Breached	Basis for Action
Equifax	Est 156+ million	Failing to patch known flaws
Uber	57 million	Failing to patch known flaws; failing to disclose breach; failing to notify
Under Armor /MyFitnessPal App	Est 150 million	Failing to ensure security
Saks 5th Ave / Lord & Taylor	Est 5 million	Failing to ensure security
Panera Bread	Est. 37 million	Failing to patch known flaws; failing to notify
Delta Air Lines / Sears / Best Buy	Unknown	Failing to ensure security

In the case of Equifax, it is estimated the company would face the maximum GDPR fine based on 2016 revenue – of approximately $125 million dollars.

Waratek
Dublin Office
8 Harcourt Street
Dublin, Ireland

US Office
117 Towne Lake Pkwy, Ste 210
Woodstock, GA 30188

waratek.com