CHUBB®

EU General Data Protection Regulation (GDPR)

What to know about GDPR: A Guide for North American Companies

How Chubb can help you mitigate your cyber risk

CHUBB®

What to know about GDPR

The new GDPR aims to set out a single set of rules across the European Union. It harmonizes national data protection laws, is mandatory, and covers changes in technology and in society that have occurred over the past two decades.

It is designed to ensure that companies that hold personal data of EU citizens are responsible and accountable for that data, regardless of where on the globe those companies are located.

The scope of the Regulation, among other things, includes:

Regulation of **consent** to process personal data and explicit consent to process special categories of data (e.g. data concerning health).

Effective date:
May 25, 2018

Extra emphasis on the responsibility of **data processors** versus data controllers.

- The data controller:
  Broadly defined as the person, company or agency who "determines the purpose and means" of processing data.
- The data processor:
  Broadly defined as the person, company or agency that processes the personal data on behalf of the controller.

GDPR Regulation

Right to **data portability**

Timely notification of data breaches to data protection authorities and to data subjects without undue delay.

The right to **'erase'** and **'be forgotten.'**

The need for data protection **impact assessments** for high risk processing activities.

New sanctions including **fines** up to a maximum of €20m or 4% of global turnover, **warnings** by data protection authorities and **audits**.

> How Chubb can help you mitigate your cyber risk

What to know about GDPR

Article 32: Security of Processing - The Regulation's Fundamental Change to EU Privacy Law

The EU has always had a measure of privacy regulation by which to abide. The GDPR not only fleshed out these already established privacy principles, but added a new security element to create a protection obligation, which is focused on the secure handling of the data and not just the risk from its disclosure. In fact, the legislation doesn't require an actual loss or unauthorized disclosure of data for a fine to be levied. Fines can be triggered if the requirements of the Regulation haven't been complied with, something that can be discovered during the investigation of a suspected breach or by a procedural audit by a data protection authority such as the Information Commissioner's Office (ICO).

Requirements of the Regulation are risk based rather than prescriptive.

Data controllers and data processors are both categorically responsible for implementing "appropriate technical and organizational measures to ensure a level of security appropriate to the risk." As well as the dual responsibility, it is worth noting that this covers organizational measures (policy/procedure/ training, etc.) as well as technological protection

Certain clauses within Article 32 expand further on what is required in relation to the 'measures' taken to secure risk.

1. Encryption

The wording of the clause suggests that both the controller and the processer will be expected to ensure a level of security appropriate to the risk including, among other things, data encryption. For high risk processing activities, controllers will need to ensure a risk assessment is undertaken, including assessment of security measures such as encryption.

2. Processing systems and services

Duties now extend beyond the protection of data to include infrastructure. Processors now must provide controllers with sufficient guarantees to implement appropriate technical and organizational measures. In other words, processors have to ensure their infrastructure, equipment and information flows are continually available and that provision of service is maintained.

Threats such as DDoS and ransomware can cause an interruption to the service. Unavailability of personal data is now considered to be a breach that might trigger sanctions similar to loss or unauthorized disclosure of data.

Data processors will need to ensure their security is sufficiently robust to protect against these kinds of threats. This will include a proper risk assessment and evaluation of current controls.

> How Chubb can help you mitigate your cyber risk

What to know about GDPR

3. Restoring availability and access in a timely manner in the event of a physical or technical incident

Key phrases are included in this section of the regulation. The phrase **Restore** introduces the need for resilience of the system and possibly the provision of a back-up site to ensure continuity of service.

Use of the phrase **"in a timely manner,"** suggests that it is important for the controller to consider all possible consequences of a breach. Consideration would need to be given to the impact on individuals and possible needs of consumers and private individuals accessing data, not just to commercial needs.

By mentioning both a physical and a technical incident, responsibility then widens beyond cyber attacks to fire, flood, breakdown and other standard perils. And these considerations need to

4. Testing and evaluating technical and organizational measures

This part of the Regulation suggests that risk assessment becomes necessary to establish the need for the measures, and that testing confirms the effectiveness of them.

Summary

The requirements of GDPR go beyond protection of personal data:

- Risk assessment beyond Data Privacy Impact Assessment
- The need to ensure a level of security appropriate to the risk including, among other things, data encryption
- Redundancy/resiliency of systems is now mandated
- Disaster recovery planning with the "timeliness" element considered
- Testing and ongoing evaluation of all security measures, both organizational and technical

> How Chubb can help you mitigate your cyber risk

How Chubb can help you mitigate your cyber risk

How Chubb can help you mitigate your cyber risk

Who is Chubb's Cyber ERM coverage right for?

Chubb's Cyber Enterprise Risk Management (Cyber ERM) can help protect organizations of any size against a range of cyber-related incidents.

How does Cyber ERM work?

Chubb's Cyber ERM uses a three-pronged approach to help protect organizations from loss due to data breaches, data corruption, ransomware attacks, and other cyber risk. The three pillars of our Cyber ERM approach are:

1. **Loss Mitigation Services:** We provide policyholders with access to the tools and resources needed to address and gauge key areas of cyber security risks before an event occurs.

2. **Risk Transfer Services:** With our first-in-class claims service, we are there to walk side by side with our policyholders during a cyber incident and carry the burden of the risk when we can.

3. **Incident Response Services:** We partner with a diverse team of experts in the legal, computer forensics, notification, call center, public relations, fraud consultation, credit monitoring, and identity-restoration services areas to help organizations limit exposure to a loss when a cyber incident occurs.

Types of Coverage Available

Cyber ERM provides options to address both third-party liability and first-party losses. We help potential insureds consider and address the growing cyber and data privacy risks that all companies face today.

Third-party liability coverage protects the insured for liability resulting from the loss of personal and corporate confidential information of third parties.

First-party coverage is designed to minimize the effects of a cyber event to the policyholders and provide a level of protection for the policyholder.

Why choose Chubb?

Chubb has been a global leader in insuring cyber security risks since 1998 and has helped notify more than 500 million individuals of a privacy breach. This premier coverage is backed by the financial strength of Chubb's A++ balance sheet. Our holistic approach to cyber coverage and careful analysis of proprietary data allows us to implement coverage that protects your entire enterprise.

> Learn more about Chubb's Cyber ERM

Contact us

Visit www.chubb.com/cyber to learn more about Chubb's offerings and to contact your local underwriter.

Chubb. Insured.℠

14-01-1285 (Ed. 07/18)