Provided by: ***Marshall & Sterling Insurance***

Key Facts About the **GDPR**

WHAT RIGHTS DOES THE GENERAL DATA PROTECTION REGULATION GIVE INDIVIDUALS?

- **Right to be informed:** Organizations must be transparent about how they use personal data
- **Right of access:** Individuals have the right to access their personal data
- **Right to rectification:** Individuals have the right to have their personal data rectified (for example, if it's inaccurate or incomplete)
- **Right to erasure:** Individuals have the 'right to be forgotten'—meaning, they have the right to have their data deleted
- **Right to restrict processing:** Individuals have the right to block or suppress processing of personal data
- **Right to data portability:** Individuals have the right to obtain and reuse their personal data for their own purposes across different services
- **Right to object:** Individuals have the right to object to processing of their personal data
- **Rights in relation to automated decision making and profiling**

HOW MUCH CAN I GET FINED?

- **€10 million (roughly £8 million) or 2% of your annual turnover—whichever is higher**—for not keeping proper records, violating data breach notification requirements, failing to appoint a data protection officer when necessary and more
- **€20 million (roughly £16 million) or 4% of your annual turnover—whichever is higher**—for violating the basic principles for processing, ignoring data subjects' rights, incorrectly transferring personal data and more

WHAT QUALIFIES AS PERSONAL DATA?

Any information that can directly or indirectly identify a person, such as:

- Name, identification number, location data or an online identifier
- Factors specific to a person's physical, physiological, genetic, mental, economic, cultural or social identity

If you're unsure whether something is personal data, the best practice is to treat it as such.

RISK INSIGHTS

Marshall & Sterling INSURANCE
LEEDS ◆ SARATOGA SPRINGS
www.marshallsterling.com/leeds

Lorraine Emerick, Vice President
lemerick@marshallsterling.com

EU General Data Protection Regulation

USA companies need to be prepared for any customers they may have in the EU that request removal of any information stored pertaining to them.

The European Union's new General Data Protection Regulation (GDPR) becomes effective on May 25, 2018. The European Union (EU) enacted these rules to create uniform data protection rules for all member states. In its view, a unified set of rules and standards would allow EU citizens more control over their personal information. The new rule will also have a global impact on any company that offers goods or services to EU residents or monitors their behavior (e.g., tracking their buying habits). The ruling will impact U.S. firms that have interests, holdings and customers on European soil.

Although the proposed rules should make it easier for non-European companies to comply with the regulations, there are severe penalties for noncompliance. Potential fines could be as high as €20 million or 4 percent of annual turnover—whichever is greater.

According to a recent study from Veritas Technologies, 86 percent of organizations worldwide are concerned that a failure to adhere to the GDPR could have a major negative impact on their business. Furthermore, 47 percent of organizations around the world have major doubts that they will meet the compliance deadline.

Data protection reform takes place through the following two instruments:

- The GDPR
- The Data Protection Directive

The GDPR

The GDPR enables individuals to better control their personal data, regardless of where this data is sent, stored or processed. The GDPR has four provisions, which provide the following:

- **More access to personal data:** Individuals will have more information on how their data is processed (this information must be provided in a clear and understandable way).

Under the GDPR, a business can retain personal data if it is still being used for the original purpose at the time of collection. However, the data must be deleted when it is no longer needed for that same purpose.

- **A right to data portability:** It will be easier for individuals to transmit their personal data between service providers.
- **A right to be forgotten:** Individuals have a right to have their personal data erased if there is no legitimate ground for retaining the data.
- **The right for individuals to know when their information has been hacked:** The GDPR creates an obligation for those who gather, store or process

personal data to notify their respective national supervisory authority of any data breaches that put them at risk.

Data Protection Directive

The Data Protection Directive applies to the police and criminal justice sectors. The directive was adopted to protect the personal data of victims, witnesses and suspects in a criminal investigation or law enforcement action.

The directive also facilitates the sharing of information and cross-border cooperation to combat crime and terrorism.

Impact on Businesses

The reforms create a more efficient business environment by cutting red tape and reducing the costs many businesses must endure if they process personal data across borders. Businesses may be able to capitalize on simpler, clearer and more unified standards as they restore or maintain consumer trust.

The reforms also make new data protection standards extraterritorial by requiring all businesses to comply while they do business in an EU member state. This ensures that all players within the EU are bound by the same rules, regardless of where they are established.

In addition, the rules streamline data safety by creating one central, single supervisory authority in each member state. It also promotes a risk-based approach to compliance requirements, recognizing that businesses should have different obligations and operate under standards that more accurately represent the particular risk associated with their data processing.

Finally, the new rules call for data processors to implement data protection safeguards from the early stages of product and service development to ensure that data protection becomes the norm—by design and by default. This includes appointing a data protection officer (DPO) responsible for data protection compliance. Organizations must appoint a DPO if they are a public authority, if they carry out large-scale systematic monitoring of individuals, or if they carry out large-scale processing of special categories of data or data relating to criminal convictions and offenses.

Impact on Employers

Employers process a large amount of personal data from their employees. Often, processing employee information is necessary to comply with employment law and to provide adequate benefits. However, many organizations lack a mechanism to determine which data should be saved or deleted based on its value.

Under the GDPR, a business can retain personal data if it is still being used for the purpose originally notified to the individual at the time of collection. However, the business must delete personal data when it is no longer needed for that same purpose. For this reason, employers should evaluate how the GDPR affects their personal data processing practices, policies and procedures. In particular, employers should consider whether they've obtained consent for a specific purpose and delineate when and how this consent may lapse.

Preparing for the GDPR

Although the GDPR does not come into effect until 2018, businesses can take action now to prepare and ensure compliance. The following checklist is from the Information Commissioner's Office (ICO) in the United Kingdom, but can be applied to U.S. businesses:

1. **Awareness:** Ensure that all decision-makers and key people in your organization are aware of the GDPR and appreciate its impact.
2. **Information you hold:** Document what personal data you hold, where it came from and whom you share it with. Also, organize an information audit.
3. **Communication of privacy information:** Review your current privacy notices and put a plan in place for making any necessary GDPR changes.

4. **Individuals' rights:** Check your procedures to ensure they cover all the rights individuals have, including how you would delete personal data or provide data electronically and in a commonly used format.
5. **Subject access requests:** Update your procedures and plan how you will handle requests within the new time frames and provide any extra information.
6. **Legal basis for processing personal data:** Look at the various types of data processing you carry out, and identify and document your legal basis for doing so.
7. **Consent:** Review how you are seeking, obtaining and recording consent and whether you need to make any changes.
8. **Children:** Think about putting systems in place to verify individuals' ages and to gather parental or guardian consent for the data processing activity.
9. **Data breaches:** Ensure you have the right procedures in place to detect, report and investigate data breaches.
10. **Data protection by design and data protection impact assessments:** Familiarize yourself with the guidance the ICO has produced on privacy impact assessments, and work out how and when to implement them.
11. **Data protection officers:** Designate a DPO, if required, or someone to be responsible for data protection compliance, and assess where this role will sit within your organization's structure and governance arrangements.
12. **International:** If your organization operates internationally, you should determine which data protection supervisory authority you fall under.

For a more detailed overview of your responsibilities under the GDPR, consult the ICO's guide for organizations located here: https://ico.org.uk/for-organisations/data-protection-reform/overview-of-the-gdpr. For more information on protecting your business and ensuring compliance, contact Marshall & Sterling Insurance today.

Marshall & Sterling INSURANCE
LEEDS ◆ SARATOGA SPRINGS
www.marshallsterling.com/leeds

Lorraine Emerick, Vice President
lemerick@marshallsterling.com

RISK INSIGHTS