GDPR and How it Affects You

There are a new set of European Laws that will take effect in May. These new regulations will have major ramifications for businesses around the globe.

What is the GDPR?

The European Union has enacted a new set of laws entitled the General Data Protection Regulations or GDPR for short. These laws were approved in April 2016 and go into effect in May 2018. Under the GDPR EU citizens have the right to choose how their personal data is used and stored. Their personal info will be treated with the same sensitivity as their Credit Card information or Social Security number. The GDPR is replacing the EU Data Protection Directive with stricter rules on how a business should handle consumer's personal information.

What the New Laws Mean for EU Citizens

Under the GDPR EU citizens will have more control than ever over their personal information. Personal data includes but is not limited to a name, a photo, an email address, bank details, posts on social media, medical information, or an IP address. Anything that can be used to directly or indirectly refer to a person.

Under the GDPR, individuals have:

- ✓ **The Right to Access** – This means that an individual has the right to know what data has been collected, if it is being used and how it is being used. This information is free of charge unless the request is deemed repetitive, excessive or unfounded.
- ✓ **The Right to be Forgotten** – A citizen has the right to request that their data be removed from a company's business systems. A business is subject to either remove the data in a timely manner or justifiably inform the individual why they cannot.
- ✓ **The Right to Data Portability** – Individuals have the right to receive their personal information in a format suitable for the easy transfer to another service provider (i.e. insurance information). It must happen in a commonly used and machine readable format.
- ✓ **The Right to be Informed** – Consumers have to opt in for their data to be gathered, and consent must be freely given rather than implied.
- ✓ **The Right to Have Correct Information** – This ensures that individuals can have their data updated if it is out of date, incomplete or incorrect.
- ✓ **The Right to Restrict Processing** – Individuals can request that their data is not used for processing. Their information will remain in your business system but cannot be used.
- ✓ **The Right to Object** – Is the right to not have their data used for the purpose of direct marketing. If a company receives this request than they must immediately cease all data processing of said individual. This right must be expressed in clear language at the time that communication starts.
- ✓ **The Right to be Notified** – An individual has the right to be informed of a data breach that compromises their personal data within 3 days of the company's awareness of said breach.

What the New Laws Mean for Businesses

When the regulation takes effect in May 2018 all European Union businesses must be under GDPR compliance. In addition, any company that does business in one of the 28 member states of the European Union will be subject to these laws.

In the age of the GDPR businesses will have to be more careful in how they collect personal information. Previously you could pre-check boxes in online forms to imply a user's consent to your marketing communications. Not anymore, you will have to write in clear and easy to understand language exactly what you will send them and that they have the right to retract this information at any time.

Do you ever trade business cards? With GDPR you will no longer be able to just enter the information from a business card into your business system. You will need some sort of evidence that you have received explicit permission to enter the individual's information into your business system.

Implications for U.S. Businesses

At this point you may be thinking that the U.S. is in the clear, especially since they are not a member of the EU. However, there are serious implications that this new regulation has for U.S. businesses. Any U.S. company that handles the personal information of an EU citizen will be responsible to comply with the GDPR regulation. A financial transaction doesn't have to take place for the extended scope of the law to kick in. If your organization collects any "personal data" which is EU-speak for what we in the U.S. call personally identifiable information (PII) then you will be required to comply with the GDPR.

When do these Regulations take Effect?

The GDPR laws take effect on May 25, 2018. Meaning your business needs to be ready with these changes prior to that date. Organizations must prove that consent was given in any case where an individual objects to receiving the communication. This means that any data held, must have an audit trail that is time stamped and reporting information that details what the contact opted into and how.

What is the Consequence for Non-compliance?

There are two different levels of fines for businesses that don't comply with the new regulation, the severity of the case will determine what fine the offending business is imposed. For less severe cases the max penalty is 2% of annual global revenue for the most recently completed year or 10 million euros whichever is higher. For more severe cases those numbers increase to 4% of annual global turnover or 20 million Euros.

What can my Business do to Prepare?

There are several steps your business can take right now to make sure you are GDPR compliant.

1. **Organize your Data**

   Find out where the personal data in your business comes from and figure out all the ways you utilize that data. Also, find all the places your data is currently located, who all can access it and if there are any risks to the data. If your business has any information that is not used anymore or is considered irrelevant, then consider removing it. The GDPR encourages that you are more disciplined in what data you collect and use. When cleaning up your data ask yourself if it is something you really need to keep, in the long run keeping your database clean will save you time and money.

2. **Review your Data Collecting Processes**

The GDPR contains tight rules about data collection. EU citizens have to explicitly express consent to the acquisition and processing of their data. Having pre-checked boxes on questionnaires and other forms of implied consent (for example business cards) will no longer be enough. Every form you create to collect personal information will need to be written in easy to understand language. It will also need to be completely clear what your company intends to do with the collected data. It will need to be as easy for the customer to retract the data as it was to originally collect the data. In addition, all company privacy statements and disclosure agreements will have to be reviewed and altered as needed.

3. **Create New Methods for Handling Personal Data**

Special care has to be made to ensure that your data is always handled in a professional GDPR compliant way. Your company will need to create a strategy for how to handle all data situations, including:

- ✓ How will we go about getting explicit consent from the customer?
- ✓ What is the process for a person who wants their data removed?
- ✓ How do we ensure that the customer's data is actually completely deleted from our information systems?
- ✓ How will you go about transferring data to another company should the customer request it?
- ✓ What is the plan if there is a data breach?

4. **Protect your Data from Breaches**

Your business will need to create and implement new procedures to protect the data from potential breaches. This means putting various security measures in place. But also being proactive if a breach ever does occur. Letting the affected individuals and the authorities know quickly is a recommended best practice in the event that a data breach occurs. In fact the GDPR requires that a data breach be reported to the Information Commissioners Office within 72 hours of the breach. Your business might outsource some or all of your data collection to an outside firm. This does not make you exempt from liability, so it is essential to check with them to make sure that their data is compliant.

How NAV can Help

All of this information can seem a little overwhelming. But the fact of the matter is it doesn't have to be. Microsoft Dynamics NAV can be used to make your business system GDPR complaint. One of the strengths of Dynamics NAV is that it is simple to modify the source code to make a customized experience for its users. We can customize Dynamics NAV to make your business GDPR compliant.

If you have any additional questions or would like additional information on how to get your business ready for GDPR Compliance, please contact us via the information below.