GDPR and the Golden Rule

Director of Technology, Faith Ministries
Reprinted from *MinistryTech Magazine*

I know what you're thinking. You've received numerous emails over the past few months about GDPR and you are sick of hearing about it. Seeing GDPR one more time makes you want to scream. I'm with you. I've gotten emails about GDPR from companies I have no record of ever interacting with, and I'm a geek so I keep track.

While traveling around the past few months since GDPR went into effect on May 25, 2018, I've been amazed at the number of questions folks are asking about it and the astonishing lack of information there is about it, especially as GDPR relates to churches and ministries. In an attempt to narrow the knowledge gap here is my best effort to tackle the GDPR issue, specifically how it relates to churches and ministries. Please note, I'm not an attorney, I don't even play one on TV, so while I've done my research it is always good to ask your legal counsel to sign off on any plans or changes you may have or plan to implement in response to GDPR.

What is GDPR?
GDPR stands for General Data Protection Regulation. It was passed by the European Union to provide their citizens with more control over their personal data and to determine what those they've given their personal data to can do with it. In many ways, it could stand for Golden Data Protection Rule, one with a biblical worldview could sum up GDPR as the Golden Rule of Data, treating others data the same way you want your data treated.

The law also provides a few specific provisions for EU citizens. First, what is considered personal data is defined. Second, EU citizens can request their data be completely removed or can only be used for certain purposes. For example, you can contact me using my data but you cannot send me ads using my data. Third, organizations operating in the EU have to report any data breaches within 72 hours.

Reading what GDPR does you can understand why it was written. It took Equifax weeks to notify the world they had been hacked, GDPR addresses that. Your data on Facebook makes you the product, not the customer and you have no control over what Facebook does with your data, GDPR addresses that.

How does this affect those not in the European Union?
This is the biggest question surrounding GDPR and one the entire planet is struggling to understand. The European Union has 500 million citizens, so they have the ability to push their agenda a bit. The challenge for organizations operating worldwide is the EU has set the strictest of standards, so do you operate with multiple policies concerning data collection and use based on where the individual lives, or do you work off GDPR since that ensures the most people will be

covered by your policies. If you don't fully understand, you aren't alone.

Some companies in response have stopped operating in the EU until they can figure this out. The issue is they operate in the EU and are storing data for EU citizens. GDPR states how you should do that if you meet both qualifications.

Enforcement
This is where the world of international law gets complicated. While GDPR tells you how you can/should store and use the information of its citizens, it cannot be enforced on organizations that do not have a physical presence in the EU. Let's take Facebook for example; they have a large, lucrative presence in the EU. They have data centers, offices, etc in the EU. The EU is able to enforce GDPR because Facebook has a physical presence there. In other words, there is a location that can be seized, personnel that can be arrested, and executives that can be taken to court.

For organizations that do not have a physical presence in the EU, this does not apply. There is no office or data center or person they can hold accountable and the EU is not able to enforce its laws on those outside the EU, for example, in North America. That's how international borders work.

Blah, blah, blah. How does this Impact Churches?
If you've skimmed the first part of this, that's fine but this is the part in which to pay close attention. At its heart, the GDPR legislation is about being a good steward of data. While data can mean many things from name, address, phone number to t-shirt size and food allergies, it is important for us to remember in the church world: data means people and people mean souls. We did not need GDPR to tell us to be good stewards of the people our ministries serve.

The Bible tells us to be good stewards (1 Corinthians 4:2), the Bible also tells us to obey the authority (Romans 13), including governments, placed over us. In this case, it seems the EU is telling those who operate in the EU to do what the Bible says and be good stewards of data.

GDPR requires a few things I would hope churches around the globe are already doing:

1. If your data is breached, report it within 72 hours. Even without GDPR, every church should have a data breach plan and procedure in place and want to be open and honest when mistakes happen. The church is the last place that should try to cover it up for weeks or months.
2. If a user wants you to remove them from your database, remove them. Even without GDPR, every church should have a procedure to remove a record from their database if someone does not want any of their information stored within your organization.
3. If a user wants you to email them prayer requests but nothing else, honor their request. Even without GDPR, you should be able to send folks what they want and not require them to get everything you send out. There is a difference between sending out prayer requests and fundraising requests. Do you allow folks to determine how you use their data?

I'm sure by now some of you are wondering about financial data. What happens when someone gives you money and then wants to be totally removed? In the US you are required to keep a record of financial transactions for 7 years. Even without GDPR, if someone wants to be removed, but they've given you money, do you have a procedure to remove them while still keeping the

financial record for 7 years and then removing them completely when the 7 years are up?

Most churches don't have a physical presence in the EU so there isn't an issue here but what happens if you do have a presence in the EU and someone from the EU gave you money and then wanted to be removed from your database? The principle is to apply donor intent; they don't want to be in your database so you treat them as if they weren't there by removing everything you can until you can remove their record entirely.

While there may be several legal and international law issues at play here, I believe the core concept is not a legal one but one of ministry integrity. We should not have needed GDPR to tell us how to care for the data those we minister to have entrusted to us.

FAQ

1. We support missionaries or other ministries that operate in the EU and have a physical presence there; do we fall under GDPR?
    - No, the organization you support in the EU that has a physical presence there does fall under GDPR but you as an individual or organization supporting them do not.
2. Should churches have data access and user rights policies?
    - Yes, even if in a basic format a policy showing who gets access to your data, for what purposes, and how you handle the data you've been given is important. It is also important to note how you handle requests for removal from your databases and/or email lists. With everyone talking about GDPR, you may find a guest or two asking if you have any data policies before they give you their children's allergies when they check their kids in some Sunday.
3. Should anyone lose sleep over this?
    - No, what we are talking about here is Golden Rule stuff. If you are losing sleep over GDPR then there are probably bigger issues to address in how you handle user data.
4. Is this really new?
    - No, in 1995 the EU had a privacy policy called Data Protection Directive. It expired when GDPR was enacted. In many ways, GDPR further refines and enhances privacy and data protection provisions that have been around since 1995.
5. What counts as data?
    - This is harder to answer because there is admittedly some subjectivity here. The obvious name, address, phone number, email address, SSN, picture, etc are pieces of data that can be used to positively identify a person. Recently an EU court ruled that under certain circumstances an IP address can also be considered personal data and is therefore subject to GDPR.
6. If we take signups and collect data on our website, do we need to make changes for GDPR?
    - Only if you have a physical presence in the EU.

Next Steps

1. If your church or ministries do not have a data access and management policy, then get one. Even a basic policy and procedure for how you handle user data and requests is important and shows you've thought about it and care about it.
2. This is not an IT issue nor should this be dumped on the IT team. While IT clearly has a role in

data management, they should not be the decision makers. GDPR requires organizations operating in the EU to have a privacy compliance officer. This can be a new employee or a role added to an existing employee. While churches and ministries may not need a privacy compliance officer the concept of having someone constantly checking to make sure you are being good stewards of data and coordinating data stewardship across ministry and church departments and silos is valid.

3. Get legal counsel. If you operate in the EU or are concerned you might, it would be wise to consult with a licensed attorney with experience in this area. Don't try to figure it out on your own. The EU is intent on enforcing GDPR and no church or ministry should want to be on their radar.

The Golden Rule comes from Matthew 7:12 and Luke 6:31. "Do unto others as you would have them do unto you." This applies to how individuals relate to each other in person and online, and to how organizations treat each other and those they serve. Whether we are talking about money, data, time, or talent the Golden Rule is more than just a rule or ideology from long ago; it is the Word of God.

Jonathan Smith is the Director of Technology at Faith Ministries in Lafayette, IN. You can reach Jonathan at jsmith@faithlafayette.org and follow him on Twitter @JonathanESmith.