OEF Communications Team 2019 Report

OEF Communications Team Accomplishments since Chapter 2018:

1) Upgraded the OEF website to be entirely protected by digital certificates and encryption. This will help prevent any third party impersonation of the OEF web site, keep communications secure, and provide additional regulatory compliance.

2) Drafted a policy statement on OEF compliance with the EU's General Data Protection Regulation (GDPR). (see section on GDPR)

3) Trello was piloted as a collaboration tool. It was found to be very useful.

4) Evaluated Wild Apricot's newsletter publishing capabilities and found it not to be very useful.

Limitations:

1) Resources - In spite of having some good technology and technology management skill sets in the team, it was difficult to provide the concerted effort needed to implement technology solutions. The team was able to perform well on collaborative efforts like defining policies, requirements, and content. Some additional organisational thought needs to be given as to how best to staff activities involving the "hands on" tasks of technology development and implementation.

2) While the team did come up with useful recommendations. In the end, we could not complete many implementation plans for many of them because of the uncertainty of the OEF's continued use of Wild Apricot. The team understands the problems associated with Wild Apricot's lock in with AfiniPay. However, we felt the need to park our enhancement recommendations until a long term technology platform replacement is selected for the OEF. We did not do any work to address Wild Apricot replacement.

Actionable Recommendations for the Order:

1) This policy statement is to be accepted by the OEF Council and if they deem it necessary by OEF by-laws, approved by the membership at the Chapter meeting. Basically we need to say that it is the policy of the OEF that we will comply with the EU's *General Data Protection Regulation* (GDPR). This compliance then becomes a guiding principle for all OEF committees and activities. (see attached GDPR write up)

2) The GDPR *Data Protection Officer* (DPO) for the OEF should be the OEF Council Secretary. This would give appropriate management visibility and tracking of any official correspondence. The Secretary could then involve the Communication Team or other appropriate individuals in the resolution of any particular issue.

3) Our work indicated the need for an OEF data privacy policy. This goes beyond the web site and should address how all of our siblings deal with all of our data, in all of the places that data exists. A sample policy is attached.

Functional Requirements for the new technology platform to replace Wild Apricot:

1) The OEF web site should have a GDPR privacy policy statement similar to other Franciscan web sites (see examples in the Trello workspace)

2) Typically, organisations require an annual affirmation of understanding personal responsibility for data privacy by members/volunteers/employees. This could be tied into an annual request to review and update personal information on the OEF member directory. (see: OEF data privacy policy).

3) Add Google Map of Individual Ministries to OEF Web site along the lines of what has been piloted by Brother Jacoba.
It is a useful tool for explaining who we are, what we do , and where we are.
It is free form enough to represent siblings short descriptions in their own words.
It is generic enough to allow members to be reasonable anonymous.

4) As it is the official system of record for OEF member information, the Wild Apricot database should contain all of the key demographic information pertaining to a sibling's relationship with the order. While we have the most commonly used ones (birth date, profession date, etc.), there are others which we are not currently capturing (e.g. date of death, release from vows, readmission to order, etc.). Currently "Formation Counselor" is tracked. However we are not tracking rule reporting relationships. This should be added.

5) Wild Apricot has a mobile phone app for IPhones and Androids that allows members to interact with events and directory information. The app has been around for a while and have been through multiple released. (https://gethelp.wildapricot.com/en/articles/9-mobile-support#memberapp) We would need to determine which of the mobil features to allow, what directory information would be accessible, and that our personal opt-out features are in place. Phone app support should be considered in the selection of the new technology platform.

6) Members should be able to logon and view their own OEF member record in its entirety and also change any of the user maintainable fields. Data quality concerns may require that this function is performed via a developed web page rather than the default Wild Apricot web or app. The reasons for this are two fold: 1) we may need specific descriptive language to help the sibling to properly understand the intent of a field 2) some fields should not be typed in free form if they can be made to refer to an edited pick list. For example: state, country, OEF regional affiliation, OEF Formation Counsellor, and OEF Rule Reporting Companion are all items which need to be selected from edited lists and not typed in free form.

7) Users of the web site will be annually prompted to validate their web access. This will include: A) the option of updating their member maintained directory information - or acknowledging that it is correct and B) affirming the personal data privacy statement
We can use E-Mail to send a reminder and include a link to the validation page. We could also have the web site redirect registered users to the validation page if they have not already validated in the past 12 month.

8) There are some siblings who have more accurate contact information on Google Groups than they do in Wild Apricot. As a result, we have not been able to move the publication and distribution of the OEF Newsletter and Devotional. The new technology platform should address this.

General Data Protection Regulation (GDPR)

The General Data Protection Regulation (GDPR) is Europe's new framework for data protection laws. is designed to unify / "harmonise" data privacy requirements across the European Union (EU). Any organisation that processes the information of EU Data Subjects – which include end users, customers and employees – needs to address compliance with the key GDPR data protection requirements.

GDPR specifies eight rights for individuals. These include allowing people to have easier access to the data that companies hold about them, a new fines regime and a clear responsibility for organisations to obtain the consent of people about whom they collect information.

For example: Perhaps you have noticed many web sites suddenly giving you pop-up notifications telling you that they use “cookies” and inviting you to read and acknowledge the “cookie” policy. Those sites are beginning their enforcement of GDPR and ePrivacy Directive (ePR) compliance of the requirement that website owners must obtain and store cookie consents from their visitors from the EU. Notice also, that the web sites are extending this consumer protection more universally to both EU and other citizens. Through this consistency of site administration policy, even users who are not legally entitled to protection still enjoy the privacy protections awarded to EU citizens.

Why GDPR

Passed in May 2016, the European Union (EU) General Data Protection Regulation (GDPR) replaces the minimum standards of the Data Protection Directive, a 21-year-old system that allowed the 28 EU member states to set their own data privacy and security rules relating to the information of EU subjects. Under the earlier directive, the force and power of the laws varied across the continent. Not so after GDPR went into effect May 25, 2018. Under GDPR, organisations are subject to new, uniform data protection requirements—or could potentially face hefty fines. So what factors played into GDPR’s passage?

- ***Changes in users and data.*** The number, types and actions of users are constantly increasing. The same is true with data. The types and amount of information organisations collect and store is skyrocketing. Critical information should be protected, but often it’s unknown where the data resides, who can access it, when they can access it or what happens once it’s accessed.
- ***Changes in data access and processing.*** The cloud, social networking, smart cards, and an array of digital and mobile devices flung open the door to data security threats. Aware of this globally changed landscape, the EU enacted regulations that recognise that “the protection of natural persons in relation to the processing of personal data is a fundamental right.”

Impacts of GDPR

While Europe has long been highly concerned with privacy, in other parts of the world it can seem that concerns are low and regulatory oversight is lax. However, GDPR makes such inattention risky for any company collecting personal data on people located in the EU or for any organisation doing business in the EU. For these organisations, GDPR compliance is mandatory and its reach is global. Regardless of where data is sent, processed or stored, GDPR requires that personal information be protected. Its underlying goal is to award greater control and transparency over one’s own personal data.

To achieve this control, GDPR includes two key components:

- ***Noncompliance:*** Potential administrative fines up to EUR20 million (nearly USD22.3 million) or up to 4 percent of the total worldwide annual sales volume/revenue for the preceding financial year, whichever is higher.
- ***Notification:*** Upon detecting a data breach, a company should notify the supervisory authority “without undue delay and, where feasible, not later than 72 hours after having become aware of it.”

In layperson's terms, compliance with GDPR is enforced with the potential for substantial impact on the bottom line and a substantial demand on security and IT operations.

OEF Call to Action

Naturally GDPR compliance impacts the OEF. There are two reasons for this:

- The OEF is an international organisation and its on-line presence contains personal information about OEF members and contacts in the EU (e.g., Brothers Peddie and Dunnigan - Note: Post BREXIT Brother Peddie will not be a EU citizen, however Britain has already adopted its own "me too" version of GDPR). This can also include information about financial contributions and transactions such as chapter meetings.

- More importantly, the lack of appropriate mandatory regulation in the US does not morally disconnect the OEF from compliance with the leading practice as established in the industry and implemented by the EU through GDPR - why would we not?

While the GDPR contains 99 specific articles setting out the rights of individuals and obligations placed on organisations covered by the regulation, it is not necessary that the OEF be deeply conversant in all of these. Fortunately, much of the technical work of a compliant infrastructure is already provided for OEF by its technology vendor - Wild Apricot. This still requires that the OEF is aware GDPR policy and properly executes its role in configuring and administering our Wild Apricot domain.

Key Wild Apricot GDPR capabilities include:

Consent Collection
- In Wild Apricot's role as a GDPR *Data Controller* everyone has to agree to our terms of use in order to use our service. They can opt-out or delete their accounts at anytime.
- In Wild Apricot's GDPR role as a *Data Processor* it is the obligation of the GDPR *Data Controller* (i.e., OEF) to ensure that they have collected consent and made clear that personal data is being collected for the purposes served by the Wild Apricot platform. This is accomplished by appropriate configuration and use of Wild Apricot's pre-established *consent fields*.

Right to access / Right to portability
- Wild Apricot clients can access their personal data at anytime, and we can export it to them upon request.
- OEF's Wild Apricot administrators can access, edit and export their own and member data at anytime. Individual members can also access and edit their own profiles (not yet fully configured by OEF).

Right to Erasure / Opt-out
- Wild Apricot Clients can opt out and cancel their accounts as needed, and we can also delete their accounts upon request, see "canceling your account".
- Site administrators can delete any of their member and contact records.

Notification in the event of a Data Breach
- Wild Apricot will notify account owners within the required 72hrs in the case of a data breach.

The OEF has an additional piece of technology infrastructure provided by WordPress. This is used for certain static content on the OEF web site. WordPress has released a statement of intent for GDPR compliance. WordPress has added a number of new GDPR privacy features in its *WordPress 4.9.6 Privacy and Maintenance Release*. In addition, a number of independent vendors within the WordPress ecosystem have begun to deliver GDPR compliant plug-in solutions.

OEF Next Steps

Fortunately, as indicated above, the OEF is well positioned to respond to GDPR at minimum cost provided appropriate awareness, planning, and operational controls are in place.

The OEF Communications Committee has the following recommendations:

1) The OEF Communications Committee proceeds on an operational level to insure that the technical steps are taken for GDPR compliance with our technology vendors and in our OEF administration of that technology. This will be approached for the time being as an acceptance of GDPR as an industry leading practice.
2) The OEF should institute a management directive to formally require GDPR compliance as the policy of the order. This would establish an on-going organisational policy which will provide a formal GDPR compliance endorsement by the Order and would apply to any related activity, whether or not it was within the boundaries of the current OEF Communications Committee. It is left to the OEF Council to determine the wording and appropriate governance mechanism in which to articulate the OEF's GDPR compliance policy.

Sample OEF Data Privacy Policy Statement

Our evangelical Counsels of Chasity and Obedience call on us to be faithful to each other and submit ourselves respectfully. In this spirit, the OEF Leadership Council has implemented a policy of annual reading and affirmation of our OEF Data Privacy Policy. This policy defined how professed, novices, inquirers, associates, and friends of the order all respect and protect that data that belongs to or is entrusted to the OEF.

“OEF Public” refers to data that has been publish by the OEF for use by the general public. This typically includes information distributed by the OEF in channels including: press releases, the OEF public Facebook page, the unrestricted pages on OEFFranciscans.org.

“OEF Confidential” refers to data that is only intended for OEF internal use. This includes data like: OEF internal meeting minutes, drafts of governance documents, personal rules, personal rule reports, donor information, the OEF membership directory, the OEF member listserv/blog/ GoogleGroup, discussions held at OEF Chapters and local events, and restricted pages on OEFFranciscans.org and ooef.wildapricot.org.

The use of OEF Confidential information is further constrained. You may only use the information for its intended purpose. For example: 1) information about financial donors is typically restricted to use by the OEF Treasurer and 2) documents shared by inquirers and novices is typically restricted to the Formation team.

The OEF does not retain personal information that is prohibited by regulations or leading practices. For example, the OEF conforms to restrictions on collecting credit card numbers, social service / tax ids / individual date of birth.

The OEF does not retain personal information when the need for holding that data has passed. If for valid reasons, you copy OEF Confidential information (e.g. your hardcopies of material or OEF contact information in your smartphone) you are required to protect this information, restrict it to your on OEF related use, and delete it when the need for it is gone.

If you are unsure if a particular document or piece of information is OEF Public or OEF Private, ask the OEF Leadership Council.

If you observe what you consider to be a possible breach in OEF Data Privacy Policy, inform the OEF Leadership Council.