COVR B.V.B.A.

ROADMAP TO GDPR COMPLIANCE OF CMOFFICE AND CMHOST WEB APPLICATIONS

Author: Pol Van de Perre

Last updated: October 31, 2017

INTRODUCTION

This document outlines the current GDPR compliance level of cmOffice and the suite of cmHost Web Applications and the processes they enable. Additionally, it also lists the planned developments to add currently unavailable functionality.

SCOPE & BOUNDARIES OF THIS DOCUMENT

In addition to using systems which provide all features to work in a GDPR compliant way, organisations must also put in place policies and procedures which define how staff should treat customer data. While we are fully willing to participate in discussions regarding policy and procedure development, this particular document focuses solely on requirements which impact cmOffice and cmHost Web Applications.

Additionally, the impact of GDPR on general IT infrastructure (server security, hosting, network security, etc) is not covered in this document. COVR will be issuing GDPR statements regarding its services in those areas separately.

SOURCES USED FOR THIS DOCUMENT

Using the actual EU GDPR 88-page regulation as a starting point would not keep this document brief and useful. Instead, we have looked for concise-yet complete guidance documents. The 12-step approach followed below is extracted from "Preparing for General Data Protection Regulation – 12 steps to take now". This document is written by the UK Information Commissioner's Office (ico.org.uk). Even though the UK is preparing for the Brexit, the ICO has stressed that the UK's approach towards data protection will stay in line with EU regulations. Hence these UK recommendations also serve as practical guidance outside the UK.

12 AREAS OF GDPR COMPLIANCE

The table below lists 12 areas of GDPR compliance and provides a high-level indication whether the specific requirements for that area impact software. More precisely whether they impact use of cmOffice and the cmHost web applications.

Areas where "No" is indicated are of course equally important for an association's compliance, but these are met through establishing the proper policies, procedures and internal documentation.

GDPR Area	*Software impact?*
1. Awareness *You should make sure that decision makers and key people in your organisation are aware that the law is changing to the GDPR. They need to appreciate the impact this is likely to have.*	*No*
2. Information you hold *You should document what personal data you hold, where it came from and who you share it with. You may need to organise an information audit.*	*Yes*
3. Communicating privacy information *You should review your current privacy notices and put a plan in place for making any necessary changes in time for GDPR implementation.*	*Yes*
4. Individuals' rights *You should 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.*	*Yes*
5. Subject access requests *You should update your procedures and plan how you will handle requests within the new timescales and provide any additional information.*	*Yes*
6. Lawful basis for processing personal data *You should identify the lawful basis for your processing activity in the GDPR, document it and update your privacy notice to explain it.*	*Yes*
7. Consent *You should review how you seek, record and manage consent and whether you need to make any changes. Refresh existing consents now if they don't meet the GDPR standard.*	*Yes*
8. Children *You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity.*	*Yes*
9. Data breaches *You should make sure you have the right procedures in place to detect, report and investigate a personal data breach.*	*Yes*
10. Data Protection by Design and Data Protection Impact Assessments *You should familiarise yourself now with the ICO's code of practice on Privacy Impact Assessments as well as the latest guidance from the Article 29 Working Party, and work out how and when to implement them in your organisation.*	*No*

11. Data Protection Officers *You should designate someone to take responsibility for data protection compliance and assess where this role will sit within your organisation's structure and governance arrangements. You should consider whether you are required to formally designate a Data Protection Officer.*	*No*
12. International *If your organisation operates in more than one EU member state (ie you carry out cross-border processing), you should determine your lead data protection supervisory authority. Article 29 Working Party guidelines will help you do this.*	*No*

DETAILED COMPLIANCE INDICATIONS

For the areas where an impact on systems is indicated (the green sections above), the table below shows more concrete requirements and:

- A brief description of how complying to the requirement can currently be achieved with COVR's software tools
- An indication of planned new functionality to accommodate compliance.

Colour codes used in this table:

The software complies with GDPR requirements in this area. Specific configuration effort might be needed to fully leverage all features and to ensure that a specific client-implementation is GDPR compliant.	
The software has the necessary features to comply, but integration with other systems will require custom development to ensure GDPR compliance of the integrated solution.	
The software does not (yet) have the features to accommodate GDPR requirements in this area.	

Excerpt from detailed guidance	**Current compliance**
2. Information you hold *"The GDPR requires you to maintain records of your processing activities"*	As of version 2.80, cmOffice provides log files of all changes to records. The log files report: • which operator made a change (including changes made by the "end customer", i.e. member, congress attendee, etc.) • When the change was made • What the old information was before the change • The revised information after the change COVR will also be adding a logging feature which lists exports made by operator.
3. Communicating privacy information *"When you collect personal data you currently have to give people certain information, such as your identity and how you intend to use their information. This is usually done through a privacy notice. Under the GDPR there are some additional things you will have to tell people. For example, you will need to explain your lawful basis for processing the data, your data retention periods and that individuals have a right to complain if they think there is a problem with the way you are handling their data. The GDPR requires the information to be provided in concise, easy to understand and clear language."*	All cmHost web applications which collect information and interact with cmOffice include provisions to publish a privacy notice. The content of these privacy notices can be fully configured with cmConfigurationmanager. An acknowledgement checkbox can be configured to appear with each privacy notice. Processes can be made conditional to having received confirmation to the acknowledgement.

4. Individuals' rights	
4.a. the right to be informed	All individuals or companies with a record in cmOffice can **consult** all information stored on them in their online profile via the Relation manager. This includes personal information (name, address, etc), profile information collected) as well as transactional data (membership history, meetings attended, etc.)
4.b. the right of access	All individuals or companies with a record in cmOffice can **access** all information stored on them in their online profile via the Relation manager
4.c. the right of rectification	All individuals or companies with a record in cmOffice can **update** the personal and profile information stored on them in their online profile via the Relation manager. They cannot update transactional information. However they can approach the association should they wish for certain transaction data to be altered. The decision (how) to accommodate such a request is on an organizational policy level. As a back office data processing system cmOffice allows deletion and alteration of processing records.
4.d. the right to erasure	As of version 2.83 of cmOffice, a feature to request deletion of a user record has been added. This is accessible via the online Relation Manager
4.e. the right to restrict processing *"where the processing is based on the individual's consent or for the performance of a contract; and when processing is carried out by automated means."*	Collecting consents and preferences can be achieved by configuring profiles. These profiles can then be made available online for users to indicate their preference or give/revoke consent.

	With regards to the second condition; cmOffice itself does not carry out automated processing (beyond user-initiated processes such as registration, abstract submissions, etc.) However, if third party applications (e-mail marketing suites, CMS applications etc) are used, • and these provide user-specific content based on "processing" readers' behaviour, or • when marketing campaigns are based on e-mail read-statistics then fully complying with GDPR would require an integration between these applications and cmOffice, so that users can select not to be subject of these processing activities. This will always require a tailor-made solution. Hence it is impossible for COVR to provide this "out of the box". But the architecture of cmOffice is based on standards which make these integrations possible.
4.f. the right to data portability *"You will need to provide the personal data in a structured commonly used and machine-readable form free of charge"*	There is currently no feature for a user to initiate a process which collects all personal data and makes this available. COVR's development roadmap includes a feature which will: • Provide a feature for a user to request this via the online relation manager. • Intiate a process in cmOffice to create an XML file (or collection of XML files) which contains all data stored for the user. • Return that data to the user. The expected release of this feature is by Q2 2018
4.g. the right to object The 12-step document does not elaborate on this requirement. The	Complying with paragraph 4 lies on a policy level and is achieved by providing the proper information to the user upon first contact. On-screen and e-mail

actual DGPR guidance lists these relevant paragraphs: (3) *"Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes"* (4) *"At the latest at the time of the first communication with the data subject, the right referred to in paragraphs 1 and 2 shall be explicitly brought to the attention of the data subject and shall be presented clearly and separately from any other information"*	generated messaging in all cmHost applications can be configured to include this information. Complying with paragraph 3, from an IT systems level requires the same functionality as described in 4.e. and can only be made possible through the envisioned custom developments.
4.h. the right not to be subject to automated individual decision-making, including profiling	cmOffice and the cmHost web applications do not include any functionality for automatic profiling and subsequent automated decision making. These can only be achieved with third party tools. If an association is not using any of these tools, then this can be described in the privacy statement. In that case there is no need for users to indicate preferences or consent. If an association is using these tools, then the consent box can be placed in the relation manager. Automatically instructing a 3rd party application not to process based on the consent status would require a custom integration.
5. Subject access requests *"In most cases you will not be able to charge for complying with a request.*	Most cases where individuals can request actions are covered in self-service options such as accessing or changing information and profile data and granting or revoking consents. In these cases, fulfilling the request is automated and instantly

• *You will have a month to comply, rather than the current 40 days.* • *You can refuse or charge for requests that are manifestly unfounded or excessive.* • *If you refuse a request, you must tell the individual why and that they have the right to complain to the supervisory authority and to a judicial remedy. You must do this without undue delay and at the latest, within one month."*	Standard e-mails and on-screen notifications can be configured to tell individuals how to use these features Only in areas 4.e and 4.g an automated response cannot be accommodated, but it can be processed manually by staff.
6. Lawful basis for processing personal data *"You will also have to explain your lawful basis for processing personal data in your privacy notice and when you answer a subject access request."*	While the authoring of the texts to be displayed is on a policy basis, the actual displaying of the privacy notice can be accomplished with cmConfigurationmanager in all cmHost web applications. Collecting acknowledgement of the privacy notice is also fully supported.
7. Consent *"Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in"* *"You will need to have simple ways for people to withdraw consent"*	Consent check-boxes can be included on all cmHost web forms where data is collected Users can access consent check-boxes at any time to withdraw consent.
8. Children *"You should start thinking now about whether you need to put systems in place to verify individuals' ages and to obtain parental or guardian consent for any data processing activity."*	Given the nature of associations' activities, no services will in practice be made available to children. Hence parental guardian consent is not applicable. cmOffice can be configured to take age-requirements into account for sign-up or for purchasing of items and services. This way, access by minors can be prevented (unless with wrongful intent).

9. Data breaches *"You should make sure you have the right procedures in place to detect, report and investigate a personal data breach. You should put procedures in place to effectively detect, report and investigate a personal data breach."*	Of the criteria *"detect, report and investigate*", the latter two are on the policies and procedures level. Detection is on the systems base. Most detection mechanisms are not applicable on an application level (cmHost pages /cmOfiice) but on the server infrastructure. If hosting is managed by COVR and adequate range of protection and intrusion prevention systems are included. Communication between cmHost web pages (on the user's PC and cmOffice) is protected by use of https (secure socket layer) and user identifiers are protected by use of SHA (Secure Hash Algorithm) encryption

ADDITIONAL GDPR REQUIREMENTS

In addition to the recommendations from the UK ICO 12-steps to compliance document, the items below (posing requirements on software systems) have also come to our attention. This table indicates the compliance level of cmOffice and the cmHost applications in for these.

Requirement	**Current compliance**
Centralised management of opt-outs for direct marketing. The GDPR specifies *"It shall be as easy to withdraw as to give consent".* This implies that given consents by a user should be easy to find, and hence be centralized.	Opt-in and out preferences are stored in profiles in cmOffice can be made available as check-boxes in cmHost web pages (or in integrated CMS applications such as Sitecore). Creating a centralised page which shows all available lists, and which allows users to review and update their subscriptions at all times, is possible but requires custom development by COVR.

Data retention management. To minimize vulnerabilities in case of security breaches you must have procedures in place to discard unused and no longer relevant user data. While complying could be achieved through manual processing, in practice the only cost-efficient way to achieve this is through a feature in the database.	cmOffice currently does not have a feature to delete unused records. COVR's development roadmap includes a feature which will: • Allow selecting relation records based on x years of inactivity • Allow mass deleting the selected records. The expected release of this feature is by Q2 2018
Central log of database access. To monitor data access and processing by operator, and to trace operator activities to ensure adherence to policies, it is advised to log and store access by operator.	COVR will be adding a logging feature which provides information of which operators logged in to cmOffice at what time. The expected release of this feature is by Q2 2018