



covering IT needs for professional societies

COVR B.V.B.A.

# GDPR COMPLIANCE OF CMOFFICE AND CMHOST WEB APPLICATIONS

**Author: Pol Van de Perre**

Last updated: May 8, 2018

---

## INTRODUCTION

This document is a status-update of COVR's previous document "Roadmap to GDPR compliance of cmOffice and cmHost Web application". The previous document identified many areas where our software was already GDPR compliant, and several requirements where the software did not yet provide features to comply with GDPR. This current document shows the updated status as of 1 May 2018.

---

## 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.

---

## DETAILED COMPLIANCE INDICATIONS

Colour codes used in this table:

<i>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.</i>	
<i>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.</i>	
<i>New feature added to cmOffice and/or the relevant cmHost Web page.</i>	

## GDPR compliance of cmOffice and cmHost web applications

Excerpt from detailed guidance	Current compliance
<p>2. Information you hold</p> <p><i>“The GDPR requires you to maintain records of your processing activities”</i></p>	<p>As of version 2.80, cmOffice provides log files of all changes to records.</p> <p>The log files report:</p> <ul style="list-style-type: none"> <li>• which operator made a change (including changes made by the “end customer”, i.e. member, congress attendee, etc.)</li> <li>• When the change was made</li> <li>• What the old information was before the change</li> <li>• The revised information after the change</li> </ul> <p>COVR will also be adding a logging feature which lists exports made by operator.</p>
<p>3. Communicating privacy information</p> <p><i>“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.”</i></p>	<p>All cmHost web applications which collect information and interact with cmOffice include provisions to publish a privacy notice.</p> <p>The content of these privacy notices can be fully configured with cmConfigurationmanager.</p> <p>An acknowledgement checkbox can be configured to appear with each privacy notice.</p> <p>Processes can be made conditional to having received confirmation to the acknowledgement.</p>

## GDPR compliance of cmOffice and cmHost web applications

4. Individuals' rights	
4.a. the right to be informed	<p>All individuals or companies with a record in cmOffice can <b>consult</b> all information stored on them in their online profile via the Relation manager.</p> <p>This includes personal information (name, address, etc), profile information collected) as well as transactional data (membership history, meetings attended, etc.)</p>
4.b. the right of access	<p>All individuals or companies with a record in cmOffice can <b>access</b> all information stored on them in their online profile via the Relation manager</p>
4.c. the right of rectification	<p>All individuals or companies with a record in cmOffice can <b>update</b> 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.</p>
4.d. the right to erasure	<p>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</p>
4.e. the right to restrict processing	<p>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.</p> <p><i>"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."</i></p>

## GDPR compliance of cmOffice and cmHost web applications

	<p>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, CRM, CMS applications etc) are used,</p> <ul style="list-style-type: none"> <li>• and these provide user-specific content based on “processing” readers’ behaviour, or</li> <li>• when marketing campaigns are based on e-mail read-statistics</li> </ul> <p>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.</p>
<p>4.f. the right to data portability</p> <p><i>“You will need to provide the personal data in a structured commonly used and machine-readable form free of charge”</i></p>	<p>A new feature “Download data” has been added to the cmHost Relation Manager. This allows for a button and descriptive text to be placed in the relation manager web page, by which a user can initiate a download of all data which is stored about him/her in cmOffice.</p> <p>This download includes name and contact info, profiles, membership data, event registration data and submitted abstract data.</p> <p>This data is provided in an JSON file, which is a machine-readable format – as required for GDPR portability purposes.</p>
<p>4.g. the right to object</p> <p>The 12-step document does not elaborate on this requirement. The actual DGPR guidance lists these</p>	<p>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 generated messaging in all cmHost</p>

## GDPR compliance of cmOffice and cmHost web applications

<p>relevant paragraphs:</p> <p>(3) <i>“Where the data subject objects to processing for direct marketing purposes, the personal data shall no longer be processed for such purposes”</i></p> <p>(4) <i>“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”</i></p>	<p>applications can be configured to include this information.</p> <p>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.</p>
<p>4.h. the right not to be subject to automated individual decision-making, including profiling</p>	<p>cmOffice and the cmHost web applications do not include any functionality for automatic profiling and subsequent automated decision making.</p> <p>These can only be achieved with third party tools.</p> <p>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.</p> <p>If an association is using these tools, then the consent box can be placed in the relation manager. Automatically instructing a 3<sup>rd</sup> party application not to process based on the consent status would require a custom integration.</p>
<p>5. Subject access requests</p> <p><i>“In most cases you will not be able to charge for complying with a request.</i></p> <ul style="list-style-type: none"> <li><i>• You will have a month to comply, rather than the current 40 days.</i></li> </ul>	<p>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</p>

## GDPR compliance of cmOffice and cmHost web applications

<ul style="list-style-type: none"> <li><i>You can refuse or charge for requests that are manifestly unfounded or excessive.</i></li> <li><i>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.”</i></li> </ul>	<p>Standard e-mails and on-screen notifications can be configured to tell individuals how to use these features</p> <p>Only in areas 4.e and 4.g an automated response cannot be accommodated, but it can be processed manually by staff.</p>
<p>6. Lawful basis for processing personal data</p> <p><i>“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.”</i></p>	<p>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.</p>
<p>7. Consent</p> <p><i>“Consent must be freely given, specific, informed and unambiguous. There must be a positive opt-in”</i></p> <p><i>“You will need to have simple ways for people to withdraw consent”</i></p>	<p>Consent check-boxes can be included on all cmHost web forms where data is collected</p> <p>Users can access consent check-boxes at any time to withdraw consent.</p>
<p>8. Children</p> <p><i>“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.”</i></p>	<p>Given the nature of associations’ activities, no services will in practice be made available to children. Hence parental guardian consent is not applicable.</p> <p>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).</p>
<p>9. Data breaches</p>	

## GDPR compliance of cmOffice and cmHost web applications

<p><i>“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.”</i></p>	<p>Of the criteria “<i>detect, report and investigate</i>”, the latter two are on the policies and procedures level. Detection is on the systems base.</p> <p>Most detection mechanisms are not applicable on an application level (cmHost pages /cmOffice) but on the server infrastructure. If hosting is managed by COVR and adequate range of protection and intrusion prevention systems are included.</p> <p>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</p>
--	--

### 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
<p>Centralised management of opt-outs for direct marketing.</p> <p>The GDPR specifies “<i>It shall be as easy to withdraw as to give consent</i>”.</p> <p>This implies that given consents by a user should be easy to find, and hence be centralized.</p>	<p>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).</p> <p>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.</p>



## GDPR compliance of cmOffice and cmHost web applications

<p>Data retention management.</p> <p>To minimize vulnerabilities in case of security breaches you must have procedures in place to discard unused and no longer relevant user data.</p> <p>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.</p>	<p>cmOffice includes a feature to delete unused relation records.</p> <p>This features allows:</p> <ul style="list-style-type: none"> <li>• Selecting relation records based on activity/inactivity over a given time-period</li> <li>• Mass deleting the selected relation records.</li> </ul>
<p>Central log of database access.</p> <p>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.</p>	<p>As of version 2.84 cmOffice keeps records of which operators logged in to the database at what time.</p> <p>This log can be consulted by users with the proper access rights.</p>