ML Luetolf
Xaraya Development Group

EU Data Protection Compliant Users Module

Status of this Memo

This document specifies a Xaraya Best Current Practices for the Xaraya Community, and requests discussion and suggestions for improvements. Distribution of this memo is unlimited.

Copyright Notice

Abstract

This RFC describes a possible Xaraya users module that complies with the EU Directive on Data Protection.

The proposed modifications to the current users module involve giving the user the ability to control how his/her personal data is displayed, and to remove his/her personal data from the site.

Table of Contents

1. Introduction

This document proposes certain changes to the Xaraya source code to make the users module compliant with the EU directive on data protection. This does not imply that Xaraya sites without these changes cannot comply with the directive. The changes proposed simply make it easier to do so, primarily by giving the users enhanced functionality concerning the data they submit.

The directive is quite complex and, depending on the type and purpose of the data collected, can be quite onerous. The changes proposed in this document purport to take into account common situations encountered by most organizations that will run Xaraya. With this in mind, what follows is a simplified summary of the major points of the directive that will be used to define the requirements of a compliant users module.

For special situations the directive in its entirety may need to be taken into account. The directive can be found here: http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection.html[1]

1.1 Implications of the Directive

For the purpose at hand the directive distinguishes between the following subjects (we take subject to mean a natural or legal person):

- Data Subject: the natural person whose personal data is the object of the directive.
- Controller: the subject that determines the purposes and means of the processing of personal data.
- Processor: the subject that processes personal data on behalf of the controller.
- Recipient: the subject to whom data are disclosed.

The directive distinguishes between data collected from the user and data about the user collected from other sources. For our purpose only the former is relevant, i.e. data submitted by users registering on a site. The directive applies to any and all processing of personal data, with some exceptions. Exempted are a number of national or EU institutions themselves (!), and strictly personal or household uses of personal data.

The directive distinguishes between data collected from the user and data about the user collected from other sources. For our purpose only the former is relevant, i.e. data submitted by users registering on a site. While we can make a module EU compliant, this does not necessarily mean that any use of the module is necessarily legal in all cases. National legislation may supercede the directive. What may be allowed by the directive, e.g. processing of personal data "revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership" with the user's consent, may be prohibited by national law. Such considerations are excluded from this document.

Also excluded from this discussion is the obligation that a site may or may not have to notify a supervisory authority as described by the directive. [section IX]

The directive distinguishes between data collected from the user and data about the user collected from other sources. For our purpose only the former is relevant, i.e. data submitted by users registering on a site.

1.2 Main Points

1. The user must give his/her unambiguous consent to the processing of his/her personal data.
2. The user must be told to what end the data will be used.
3. The user must be told whether submitting the data is mandatory or not, and the consequences of submitting or not submitting the data.
4. The user must be told who the recipients of the data will be.
5. The user must have the right to access and modify the data.
6. The user has the right to object at any time to the processing of the data. Accordingly "Where there is a

[1] http://www.privacy.org/pi/intl_orgs/ec/final_EU_Data_Protection..html

justified objection, the processing instigated by the controller may no longer involve those data".

2. List of Requirements for the EU Compliant Module

For the purpose of this document we will take the Controller/Processor to mean the owner of a Xaraya site, or any administrator of the site (as long as the administrator has the access rights to view, modify, delete or publish personal data). The Data Subject is any user that has registered and submitted personal data. The personal data is any information relating to the user.

- Controller, Processor = Administrator
- Data Subject, Recipient = User

Translating the above rights to a community oriented CMS environment, they can be summarized as:

- The user can grant or waive consent that his/her data be collected.
- The user can modify his/her data at any time.
- The user can remove his/her data (or ask that it be removed) at any time.

The "processing" of user data for the purposes of this proposal can be defined as the processing that occurs in Xaraya's users module through the xarAPI. Compliance in this module will automatically extend compliance to any other module that uses the xaruserapi and xaradminapi functions of the users module.

Strictly speaking, the rights above go a bit further than the letter of the directive in that the user is not just given the right to object, but also the right to implement his/her objection (by unregistering).

EU compliant users modules are therefore solutions that implement these 3 rights. Two such proposals are described below.

3. Solution Proposal 1: Simple Compliance

3.1 Example: P2 Masonic Lodge

Having been attacked in the press, P2 is opening a Xaraya site to convince the public that they're just a social club with funny hats and really not out to control the Italian government. Being something of a secretive organization, registrations will be vetted and the members' list is only accessible to registered members. Within the restricted members' area, however, information such as name, secret code name and ICQ number is made available to all fellow members. Members who resign from the lodge are keen to have their data removed from the site, so as to avoid possible future lawsuits.

3.2 Overview

As concerns consent and removal this is an all or nothing proposition. Those rights are applied to the user data as a whole.

- Consent: is given when the user registers.
- Modification: the user can modify his/her data in the user account area.
- Removal: the user can "unregister", and his/her data will be removed.

3.3 Database Tables

No change required.

3.4 Code that will need to be rewritten

- Consent: Appropriate statements concerning rights and obligations under the EU directive can be inserted under the terms and conditions as currently implemented.
- Modification: As currently implemented.
- Removal: Add an additional button "Unregister" to the user account area. Clicking displays a confirmation page explaining that all data will be removed and the user unregistered. Confirmation deletes the user's entry in the relevant tables. (see Open Issue B)

4. Solution Proposal 2: Differentiated Compliance

4.1 Example: AC Milan Football Club

AC Milan, which has done quite well in the Champion's League lately, is opening a Xaraya site with up to date information about the Club and its players, including a feedback area. The members' list is public and contains such basic information as name and telephone number. The owner of AC Milan, Silvio Berlusconi, is also Prime Minister of Italy. While he is interested in getting feedback on what fans think about the Club and having his secretary field calls on his business number, he'd rather make his private number available only to the site's admins, to avoid crank political calls on the government's upcoming budget.

4.2 Overview

In this solution the functionality is applied to single data elements, rather than the user data as a whole. The site administrator can define a subset of the user data as mandatory. For this subset this solution is the same as the previous one (i.e. an all or nothing proposition). The remaining data fields are user optional. The user can define each of these fields as visible to the recipients or not.

The site administrator:

- Can define variable registration data fields (xar_user_property table). (current)
- Can define for each data field whether it is to be mandatory (i.e. requires data to be entered) or not. (new)
- Can define for each data field whether its visibility is user optional or not. (new)

The user:

- Can consent to the visible fields as a whole. (current)
- Can define the user optional data fields visible or not at any time. (new)
- Can modify the data at any time. (current)
- Can unregister from the site at any time. (new)

The possible recipients for user data depend on the visibility setting and are either administrators or users (="All Groups"). (see Open Issues D)

4.3 Database Tables

Add the following database fields:

```
        Table xar_user_property:
        Field Name           Type          Contains
        xar_prop_mandatory    boolean       True = field must contain a non-null
value
        xar_prop_visible      boolean       True = field visibility can be set by
user

        Table xar_users:
        Field Name           Type          Contains
        xar_fields_visible    varchar 255   1-dim array consisting of the
xar_prop_id
                                           of all xar_user_property fields set
visible
```

4.4 Code that will need to be rewritten

1. Add appropriate code for xar_prop_mandatory and xar_prop_visible fields to the functions

users_admin_newvar() in xaradmin.php. The same for updating or deleting entries to xar_user_property.

2. Add a checkbox to each user definable field in users_user_new() and users_user_modify() in xaruser.php in the users module that lets the user define whether the field will be visible or not. Same thing for when the user modifies the personal data.
3. Modify function users_userapi_getall and users_userapi_get in xaruserapi.php to select those fields included in the xar_fields_visible array.
4. If the xar_prop_mandatory field is set true the user must enter a value upon registering or modifying his/her data. If no value is entered an error message is generated and the page re-presented.
5. Create the "unregister" functionality as described above.

5. Appendix - Open Issues

5.1 Currently hard-coded fields

The approach described above could be extended to include all user fields. This would mean merging most of the xar_users table fields (except: uid, username, pass) into the xar_user-property table, thereby allowing the admin complete freedom in deciding which user fields will be user optional.

In practice, however, this probably doesn't make sense. A minimum of mandatory user fields will always be necessary simply to make it possible to do something meaningful. The currently chosen fields seem to be a sensible minimalist choice (exception: url?) that will no doubt work in most cases.

5.2 Removal of Users

When a user unregisters, his/her data can either be inactivated or physically deleted. Inactivation could be implemented through an additional boolean field in the xar_users table, which would be checked by the appropriate api functions in the users module whenever getting data.

Another approach would be to combine the inactivation with whatever variable (xar_active in xar_userblocks? [check this]) drives the visibility of the user in the members list, as they are really different aspects of the same property.

On the face of it inactivation complies with the directive (there would be no further processing of the data), and may be the wiser choice, as authorities will probably continue to put in place regulation requiring certain data to be archived for extended periods. On the other hand it isn't clear that Xaraya needs to address such requirements (rather than, say, the ISP the site runs on). The EU directive does not cover this area, and it is beyond the scope of this document.

5.3 Overlap with allowinvisible

Xaraya allows for the functionality that the user can be set invisible in user view. This flag could be redefined so as to allow or not the EU compliant functionality, i.e. allowing the user to define his/her user fields as visible or invisible. A separate EU flag could be also created. The latter is the preferred solution.

5.4 Admin can set user fields to visible per group

Rather than stipulate that the field xar_prop_visible be a boolean, and therefore the recipients are either admins or users, a more general solution would be:

```
        Table xar_user_property:
        Field Name          Type          Contains
        xar_prop_visible     integer       xar_gid of the group that the property
field
                                          is visible to.

        Table xar_users:
        Field Name          Type          Contains
        xar_fields_visible   varchar 255   2-dim array consisting of the
xar_prop_id
                                          of all xar_user_property fields to be
visible
                                          and the xar_gid of the group each
property field
                                          is visible to.
```

If a group is deleted, any corresponding entries in xar_fields_visible must be changed to the xar_gid of the admins. The admins group cannot be deleted.

Creating an easy to use interface for this solution would be more complicated, as it probably involves either a scheme with multiple dropdowns or having the user input a list of group names (with the appropriate parsing for errors).

While situations can be imagined in which this functionality might be useful, they probably won't apply to the majority of Xaraya sites.

Author's Address

Marc Luetolf
Xaraya Development Group
EMail: mfl@netspan.ch
URI: http://www.xaraya.com

Intellectual Property Statement

The DDF takes no position regarding the validity or scope of any Intellectual Property Rights or other rights that might be claimed to pertain to the implementation or use of the technology described in this document or the extent to which any license under such rights might or might not be available; nor does it represent that it has made any independent effort to identify any such rights. Information on the DDF's procedures with respect to rights in standards-track and standards-related documentation can be found in RFC-0.

The DDF invites any interested party to bring to its attention any copyrights, patents or patent applications, or other proprietary rights which may cover technology that may be required to practice this standard. Please address the information to the DDF Board of Directors.

Acknowledgement

Funding for the RFC Editor function is provided by the DDF