Report of the GDPR Focus Group

The Focus Group

The GDPR Focus Group was formed in late 2019 on the initiative of members primarily from the German user community. Christian Hänger, Mannheim University, then an IGeLU Steering Committee member, agreed to chair the group, whose first meeting took place on November 29, 2019. The group consisted of IGeLU community members and Ex Libris representatives. It was charged with discussion of the impact of relevant GDPR articles (15, 16, 17, 18, 20) on the Data Controller responsibility of Ex Libris customers, and to recommend changes to the Ex Libris software that could improve the customers' ability to fulfill this responsibility.

After a quiet period following Mr. Hänger's departure from IGeLU, the GDPR Focus Group resumed its work in winter/spring 2021, with a different cast that has completed the work that forms the basis of this report. Group members in this final phase were:

- Erez Shabo, Ex Libris
- Itai Veltzman, Ex Libris
- Mathias Kratzer, Bayerische Staatsbibliothek (BSB), Munich
- Michael Voss - for HBZ Köln
- François Renaville – Université de Liège, Liège
- Audun Skorstad – UNIT, Trondheim
- Ole Holm, Royal Danish Library, Copenhagen
- Knut Anton Bøckman, Royal Danish Library, Copenhagen (SC Liaison and coordinator of the Focus Group)

The group has met repeatedly online, and discussed the following GDPR Articles:

- Article 15: "Right of access by the data subject"
- Article 16: "Right to rectification"
- Article 17: "Right to erasure ('right to be forgotten')"
- Article 18: "Right to restriction of processing"
- Article 20: "Right to data portability"

General considerations

Before presenting the recommendations for action, and how they apply to the particular articles, some general observations from the group are in place in order to set the framework for the group's activities.

(A) **The Data Controller** is the institution. Thus, protection of personal data, and compliance with GDPR demands, is solely the responsibility of the institution. The aim of the focus group is to find ways that make it **as easy as possible for the institution to fulfil its responsibilities** as concerns handling of personal data stored or processed in Ex Libris Products.

(B) GDPR is an opportunity: Regulations for personal data protection are subject to national legislation, which varies greatly. With GDPR, a framework is created for regulations on a European scale. With this alignment, it becomes realistic, in a global software system, to develop tools or methods to specifically facilitate the institutions' fulfilling of their personal data protection responsibilities.

(C) **The Data Subject**, in the discussions and recommendations of the focus group, is the end-user (or patron) of the library. In focusing on end-user data, the group recognizes that handling of staff user data is governed by other, more context-specific employer/employee contracts and regulations. They were considered as too varied and complicated to result in general tools and methods.

(D) **Kinds of data:** In our discussions and recommendations, the group has deliberately focused on personal data that is stored in databases and processed by the system. Data that is stored temporarily and deleted automatically in order to secure system performance and maintenance (e.g., logfiles kept for 90 days before deletion) are not considered.

(E) The aim of the Task Force was **cross-product,** covering data protection tasks for institutions using any Ex Libris product. In the discussion and recommendations, we have, however, focused on products on Ex Libris' Higher-Education Platform, as the platform is characterized by extensive re-use of data for several different products. This makes it a natural focus point for discussion of personal data protection, but it also provides a relatively easy access for a comprehensive control and handling of the data. Current products on the Higher-Education Platform are Alma, Primo VE, Leganto, Esploro, and Rialto. Product Working Groups for other

products should regard the recommendations set forth for Higher-Ed Platform products as general recommendations, and discuss how they apply or need to be modified for their product.

(F) While for some of the articles it seems very unlikely that a claim of these rights will ever be raised against a library, the institution has a legal obligation to fulfill them if a claim *is*raised. Consequently, a tool or a method for doing so needs to be in place.

(G) The Focus Group recognizes that in many cases, there are already tools or methods available that only need minor adjustments or repurposing.

Main recommendations

1. Ex Libris should work to develop a tool that easily and securely delivers an end-user's personal data stored in the system to the end-user upon his or her request. Ideally, this would be a service available to authenticated users through the end-user interface (Discovery solutions, Reading List solutions, etc.). Users would be authenticated by the regular method selected by the institution. In order to protect the data privacy of end users, we would generally recommend using a two-factor solution for authentication. Such a tool would be of substantial help in many of the situations envisioned in the GDPR articles, notably 15 and 20.
2. Additional tools should be available for staff in order to fulfill data responsibilities on systems without an end-user authenticated interface, e.g., data stored in Sandboxes. Cloud Apps or other API-based tools could provide a model for this. (Article 15)
3. Anonymization of historical personal data should be the default setting, from which institutions must be able to actively divert if legal regulations or contractual assignments require them to keep personal data for a longer time. (Article 17)
4. To fulfill legal or contractual assignments on retaining historical personal data, institutions need a way to indicate specific data areas (as impacted by system workflow) where process data needs to remain personally identifiable for an extended time, thus preventing deletion of required data even at the end-user's request. (Article 17)
5. A method by which an end-user account can be temporarily set to locked/inactive such that its data is no longer processed need to be put in place. (Article 18)
6. The IGeLU community - through the Product Working Groups – should consider the recommendations and this report, and discuss how it applies to the specific products. Feedback should be brought to the SC.

Application to each GDPR article

In this section, the plain text of the considered GDPR articles is presented, followed by a brief summary of the main discussion points of the Focus Group, and finally a set of recommendations for handling each of them.

Article 15: "Right of access by the data subject"

1. The data subject shall have the right to obtain from the controller confirmation as to whether or not personal data concerning him or her are being processed, and, where that is the case, access to the personal data and the following information:
(a) the purposes of the processing;

(b) the categories of personal data concerned;
(c) the recipients or categories of recipient to whom the personal data have been or will be disclosed, in particular recipients in third countries or international organisations;
(d) where possible, the envisaged period for which the personal data will be stored, or, if not possible, the criteria used to determine that period;
(e) the existence of the right to request from the controller rectification or erasure of personal data or restriction of processing of personal data concerning the data subject or to object to such processing;
(f) the right to lodge a complaint with a supervisory authority;
(g) where the personal data are not collected from the data subject, any available information as to their source;
(h) the existence of automated decision-making, including profiling, referred to in Article 22(1) and (4) and, at least in those cases, meaningful information about the logic involved, as well as the significance and the envisaged consequences of such processing for the data subject.
2. Where personal data are transferred to a third country or to an international organisation, the data subject shall have the right to be informed of the appropriate safeguards pursuant to Article 46 relating to the transfer.
3. The controller shall provide a copy of the personal data undergoing processing. For any further copies requested by the data subject, the controller may charge a reasonable fee based on administrative costs. Where the data subject makes the request by electronic means, and unless otherwise requested by the data subject, the information shall be provided in a commonly used electronic form.
4. The right to obtain a copy referred to in paragraph 3 shall not adversely affect the rights and freedoms of others.

Main points of discussion

- Users have the right to request a copy of their personal data available in Ex Libris systems. Personal data is a whole lot and providing ARC or Analytics reports do not cover all personal data: information like Primo/Summon history search, alerts, and favourites are not available to the library. And yet, according to the GDPR, the user has the right to get this information. There could be an option button in the MyAccount that could allow patrons to request a copy of their personal data available in Ex Libris systems.
- We should keep in mind that users mustn't have to worry about the different Ex Libris systems used at the library. They should have the possibility to create a single access request or opt-out decision that would be valid for all Ex Libris systems. This requires some interface and interaction between Ex Libris systems.
- Anonymization should be enabled by default in sandboxes. If not, personal data stored in Sandboxes should also be requestable by the user.

Recommendation:

For Higher-Education Platform products, the tools envisioned in **Main recommendations Item 1 and 2** would provide sufficient support for the institution to fulfil its responsibilities for this article. For other products, a more piecemeal approach may need to be taken, to be determined by the relevant Product Working Groups.

Article 16: "Right to rectification"

The data subject shall have the right to obtain from the controller without undue delay the rectification of inaccurate personal data concerning him or her. Taking into account the purposes of

the processing, the data subject shall have the right to have incomplete personal data completed, including by means of providing a supplementary statement.

Main points of discussion

In order to enable customers to fulfil such a request for rectification we would need Ex Libris products to provide functionality that allows the institution/staff to correct/complete the subject's personal data at one single place in the particular product.
Example: If a patron requests the correction of her or his personal data stored in Alma it should be possible to perform the correction at one single place in Alma such that it affects each and every of the other occurrences within Alma.
The group discussed at some length if such changes should be prevented from propagating automatically to any other Ex Libris products connected to Alma. Any such propagation, the reasoning goes, should rather be part of the institution's internal workflow for processing a patron's request for correction of her/his personal data. This would raise issues when different products reuse the same user data. This is notably the case with Higher-Education Platform products, but not exclusively so. For example, a non-VE version of Primo directly employs the user data as the underlying LMS, be it Aleph or Alma, and so when data are corrected there, it will also appear as corrected in Primo. It is not technically a question of propagation, as the data are not stored in Primo, but the effect would be the same. The group decided to leave the issue of propagation out of the recommendations.
The group noted that in many cases, an institution will control its end-user data in an external system (e.g., SIS) and the Alma (or other ILS) data are derivative of the data stored in the external system. In such cases, the rectification of personal data will of course happen in the master system and propagate to Alma (or other ILS) by API updates or synchronization profile.

Recommendation

Current functionality for rectification of end user data is sufficient and sufficiently efficient for institutions' fulfilling this responsibility, the group finds.

Article 17: "Right to erasure ('right to be forgotten')"

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:
(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;
(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;
(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);
(d) the personal data have been unlawfully processed;
(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;
(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).
2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers

which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.
3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:
(a) for exercising the right of freedom of expression and information;
(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);
(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or
(e) for the establishment, exercise or defence of legal claims.

Main points of discussion

Concerning this article, the discussion focused not so much on the ability to delete user data from the system, as this is readily available in current products. In Alma, there is even the distinction between deleting users and purging users, where the latter function keeps anonymized statistics data for users that are removed from the system.
Rather, the discussion centred on how it would be possible to prevent data from being deleted, if other legal regulations or contractual assignments demand that they be retained. Clearly, there are technical and transactional "live data" that already prevent the deletion of a user record – e.g., active loans, an unpaid fee, etc. However, other regulations than GDPR may put legal obligations on an institution to retain also historical data over a prolonged time – e.g., to keep track of financial transactions (say, payment of fees) for a period of 5-7 years. In such cases it would be optimal to have configurations available in the product for the institution to be able to codify such restrictions, to prevent the deletion of archival data that the institution is required to retain.
A less optimal alternative could be a method for easy export of such data – in this case the required data could be retained by the institution outside of the Ex Libris product, even if the user data are removed from the library system at the request of the data subject.

Recommendation

The main purpose of this article is fulfilled by existing functionality to delete or purge user records, however, the group wants to recommend a change of default for Anonymization of archival data, as set forth in **Main recommendations Item 3**.
The need to have the right to erasure counterbalanced by other legal or contractual assignments, results in the **Main recommendations Item 4**, laid out in more detail below.

For these cases Ex Libris systems shall provide functionality such that

a) the institution can **generally flag personal data areas** as being necessary to fulfil a legal or contractual assignment of the institution;
b) the institution can **define areas impacted by workflows** of legal or contractual assignment
c) the institution can **delete all occurrences** of personal data of the requesting data subject which is either not necessary to fulfil a legal or contractual assignment or not involved in a yet unaccomplished workflow impacting a data area flagged as being necessary to fulfil a legal or contractual assignment of the institution;
d) the institution is notified of any yet unaccomplished workflows that involve personal data of the requesting data subject stored in an area flagged as being necessary to fulfil a legal or contractual assignment of the institution.

The data that needs to be retained even after the partial deletion referred to in point c) could be kept in the system or, alternatively, readily exported for separate storage, as discussed above.

Article 18: "Right to restriction of processing"

The data subject shall have the right to obtain from the controller restriction of processing where one of the following applies:
(a) the accuracy of the personal data is contested by the data subject, for a period enabling the controller to verify the accuracy of the personal data;
(b) the processing is unlawful and the data subject opposes the erasure of the personal data and requests the restriction of their use instead;
(c) the controller no longer needs the personal data for the purposes of the processing, but they are required by the data subject for the establishment, exercise or defence of legal claims;
(d) the data subject has objected to processing pursuant to Article 21(1) pending the verification whether the legitimate grounds of the controller override those of the data subject.

Main points of discussion

The conditions for the application of this right are restricted to cases where a data subject wants purportedly inaccurate or unlawful personal data retained by the institution in order to be used as evidence in a legal case against the institution. While this situation may seem unlikely in a library setting, the institution is legally bound to comply, and therefore needs to be prepared.
The discussion also settled that the article does not grant the end-user the right to opt out of selective processes; it is a question of "freezing in place" all of the data subject's personal data for a limited time and under specific circumstances. Similarly, not all data processing can be stopped, if legal or contractual assignments depend on their continuation, e.g., processing of active loans/fees.
The main point is that in cases such as these, should they arise, the user's data should **not** be deleted, but temporarily be "frozen". Therefore, the solution suggested by Ex Libris in the GDPR handling document, is inappropriate.

Recommendations

a) Institutions would be supported in fulfilling their responsibility towards this article by **Main recommendations Item 5:** a method by which a user record may be temporarily locked or set to inactive, and its data prevented from processing. A number of steps could be taken to obtain this goal, including assigning such user records to a separate user group, that would allow filtering out of reports, search and require special staff instructions. The steps need to be enacted temporarily so they can be removed, when the issue is resolved.
b) Ex Libris should rectify their recommendation in the "What you need to know about addressing GDPR Data Subject Rights in Alma" document, as deletion is explicitly not called for.
c) For each specific product, the Product Working Groups should encourage institutions to report how well (or badly) they are served by current tools and solutions should cases like this arise, and how often they do.

Article 20: "Right to data portability"

1. The data subject shall have the right to receive the personal data concerning him or her, which he or she has provided to a controller, in a structured, commonly used and machine-readable format and have the right to transmit those data to another controller without hindrance from the controller to which the personal data have been provided, where:
(a) the processing is based on consent pursuant to point (a) of Article 6(1) or point (a) of Article 9(2) or on a contract pursuant to point (b) of Article 6(1); and
(b) the processing is carried out by automated means.
2. In exercising his or her right to data portability pursuant to paragraph 1, the data subject shall have the right to have the personal data transmitted directly from one controller to another, where technically feasible.
3. The exercise of the right referred to in paragraph 1 of this Article shall be without prejudice to Article 17. That right shall not apply to processing necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller.
4. The right referred to in paragraph 1 shall not adversely affect the rights and freedoms of others.

Main points of discussion

The practical relevance in the library world became a point of discussion for this article as well. The more obvious use case is, e.g., the portability of data from one mobile physical workout app to another. Nonetheless, as with the previous articles, library institutions are data controllers too, and need to be able to respond to demands rising from these rights.
The group found that most of the recommendations set forth in Article 15 would also support the concerns raised by Article 20. If the end-user can retrieve all one's user data, it can also be imported into another format. The main additional issue here is that data should be available in some kind of machine-readable format.
The group also found that relevant data for possible portability to another system would be:

- Saved searches
- Saved documents
- Search history (if available; i.e., enabled by the insitution)
- Loans, requests and fees history (if available, i.e., not anonymized)

Given the cross-product nature of these data types, we would expect a solution to be available first in Higher-Education Platform products.
A self-service option from the My Account page for authenticated end users (like for Article 15) would be preferable.

Recommendation

Ex Libris shall provide patrons with the option to request data related to:

- Patron activity history (Loans, requests and fees)
- Saved searches, search history, and saved documents in Discovery and Reading list solutions

The data shall be supplied as a file in a machine-readable format (.csv) to the patron

Conclusion

The GDPR Focus Group has discussed the needs and concerns regarding Ex Libris Products when it comes to institutions' obligations towards GDPR regulations. It is unequivocally the responsibility of the institution – the Ex Libris Customer – to fulfill the responsibilities arising from the rights of the Data Subject in these articles. The aim of the recommendations set forth in this document is to make

the Ex Libris products better products for the customers, in providing support for tasks that the institutions need to perform in order to fulfill their responsibilities.
The Focus Group has aimed to keep a cross-product perspective in discussions and recommendations, as the rights of the data subject is towards the data controller, not towards specific products. Often though, the examples have been taken from Alma, as this often is the central storage of personal data, and by extension, the other products on the Higher-Education Platform. The main recommendations are meant to be cross-product, as far as they apply to each.
We encourage the Product Working Groups to discuss the recommendations 1-5 and to what extent, they are relevant for “their” product. The details of the solution for each product should be discussed between the Product Working Group and the Ex Libris Product Management.