

# GDPR Focus Group

Report on Activities and Recommendations

IGeLU 2021, August 25

# Group members

- Erez Shabo, Ex Libris
- Itai Veltzman, Ex Libris
- Mathias Kratzer, Bayerische Staatsbibliothek (BSB), Munich
- Michael Voss - for HBZ Köln
- François Renaville – University of 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)

# General observations

- The Data Controller is the institution (not Ex Libris)
- The Data Subject is the end user
- GDPR is an opportunity to improve products' personal data handling
- The Focus Group is cross-product (but starts with the Higher-Ed platform)
- Main focus has been on data stored in databases, not temp data.
- The unlikelihood of a data request does not preclude a requirement for its fulfillment
- In many cases, there are already tools and methods available

# Work and activities

- The group started its work in November 2019
- The current members of the group have met regularly (online) through winter and spring of 2021 to finish the work.
- The impact of each of the relevant articles (15, 16, 17, 18, 20) has been assessed, and possible solutions discussed.

# GDPR Articles considered

- Article 15: *Right of access by the data subject*
  - "I want to know what data you have on me."
- Article 16: *Right to rectification*
  - "The data you have on me must be corrected."
- Article 17: *Right to erasure ('right to be forgotten')*
  - "I want my data deleted from your system"
- Article 18: *Right to restriction of processing*
  - "You hold my data illegally, and you may not process them, nor delete them, while I prepare legal steps against you."
- Article 20: *Right to data portability*
  - "I want to use my data created in your system in another system."

# 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. (Articles 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)

# Main recommendations, cont'd

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. 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)

# Main recommendations, end.

5. To fulfill legal or contractual assignments on retaining archival 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)

(This recognizes that GDPR is not the only regulation institutions must comply with.)



# Conclusion and further actions

- Data handling is the responsibility of the institution, but ExLibris products can be improved to facilitate this task.
- Already, tools and methods are available for some (but not all) tasks, but further development can make them easier to use.
- The IGeLU community - through the Product Working Groups – should consider the recommendations and the discussions summarized in this report, and then discuss how it applies to the specific products. Feedback should be brought to the SC.