Data Privacy Protection

(Trans-Atlantic Data Privacy)

Scott Macdonald
VP, EBSCO Security and Privacy Governance

April 2022

Agenda

- Overview
  - GDPR
  - Common Security and Privacy Framework Controls
- EBSCO's Approach to Data Minimization
  - Institutional-Level Access (Non-Personalized)
  - Personalized User Privacy Experience (New eHost UI)
  - Anonymized Privacy Configurations
- Trans-Atlantic Data Privacy Framework
  - Standard Contractual Clauses (SCCs)
- Way Ahead
- Questions

Common Security & Privacy Frameworks

Wikimedia: Structure Paris les Halles

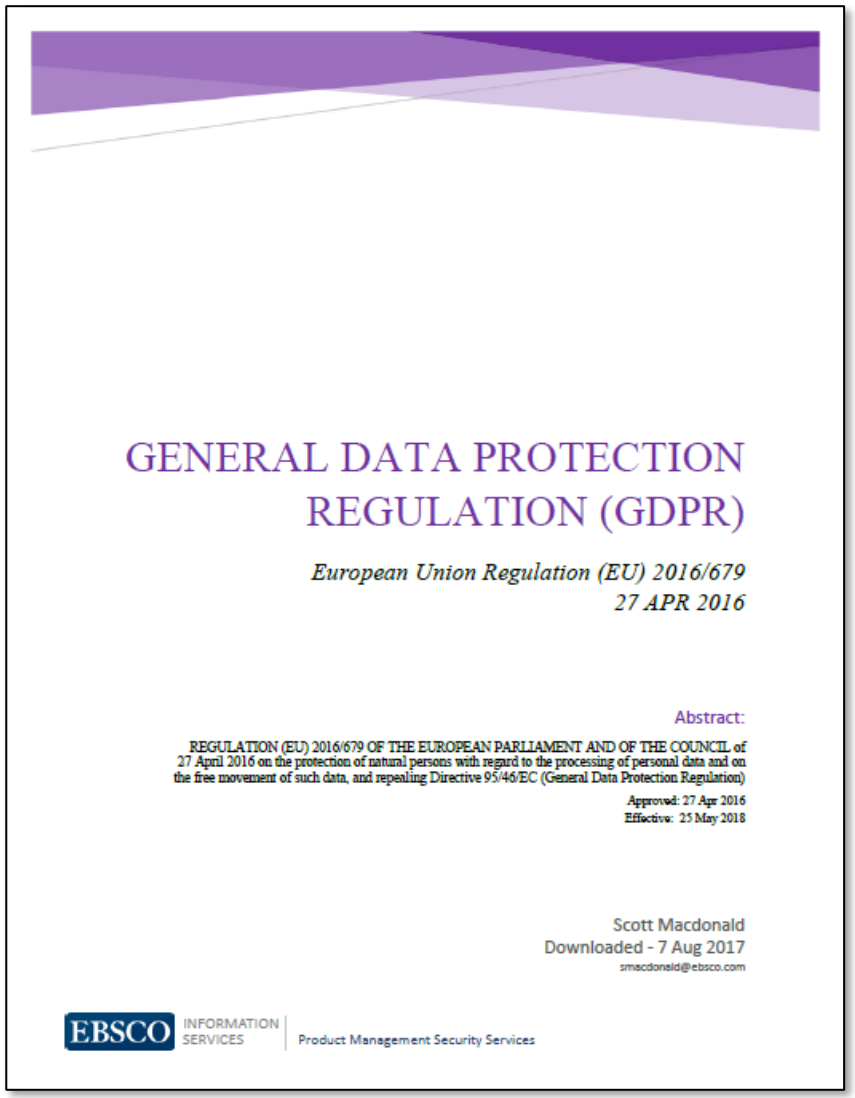
- General Data Protection Regulation (GDPR)
- Privacy Shield / Privacy Shield
- ISO 27001 - Information Security Management System (ISMS)
- ISO 27701 - Privacy extension to ISO 27001 ("Privacy Information Management System")
- ISO 27017- Information Security for Cloud Services
- ISO 27018 - PII Protection in Public Cloud

Common structure to security and privacy governance and transparency

EU General Data Protection Regulation (GDPR)

- **Regulation (EU) 2016/679**
  - Adopted 27 Apr 2016
  - Effective 25 May 2018
- **Single set of rules**
  - Use Consent
  - Right to access
  - Right to Be Forgotten
  - Data Portability
  - Privacy By Design

EU General Data Protection Regulation (GDPR)



GENERAL DATA PROTECTION REGULATION (GDPR)

European Union Regulation (EU) 2016/679
27 APR 2016

Abstract:

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Approved: 27 Apr 2016
Effective: 25 May 2018

Scott Macdonald
Downloaded - 7 Aug 2017
smacdonald@ebsco.com

EBSCO INFORMATION SERVICES | Product Management Security Services

- **Article 6:** *Consent to Processing*
- **Article 12:** *Clarity of Information*
- **Article 15:** *Right of Access*
- **Article 17:** *Right of Erasure*
- **Article 19:** *Right to Notification*
- **Article 20:** *Data Portability*
- **Article 25/32:** *Data Protection*
- **Article 33/34:** *Data Breaches*

Data Privacy Control and Minimization | EBSCO's Approach

- EBSCO Information Services does not and will not sell Personal Information to third parties for a business or commercial purpose
- EBSCO recognizes the following Data Subject Access Rights:

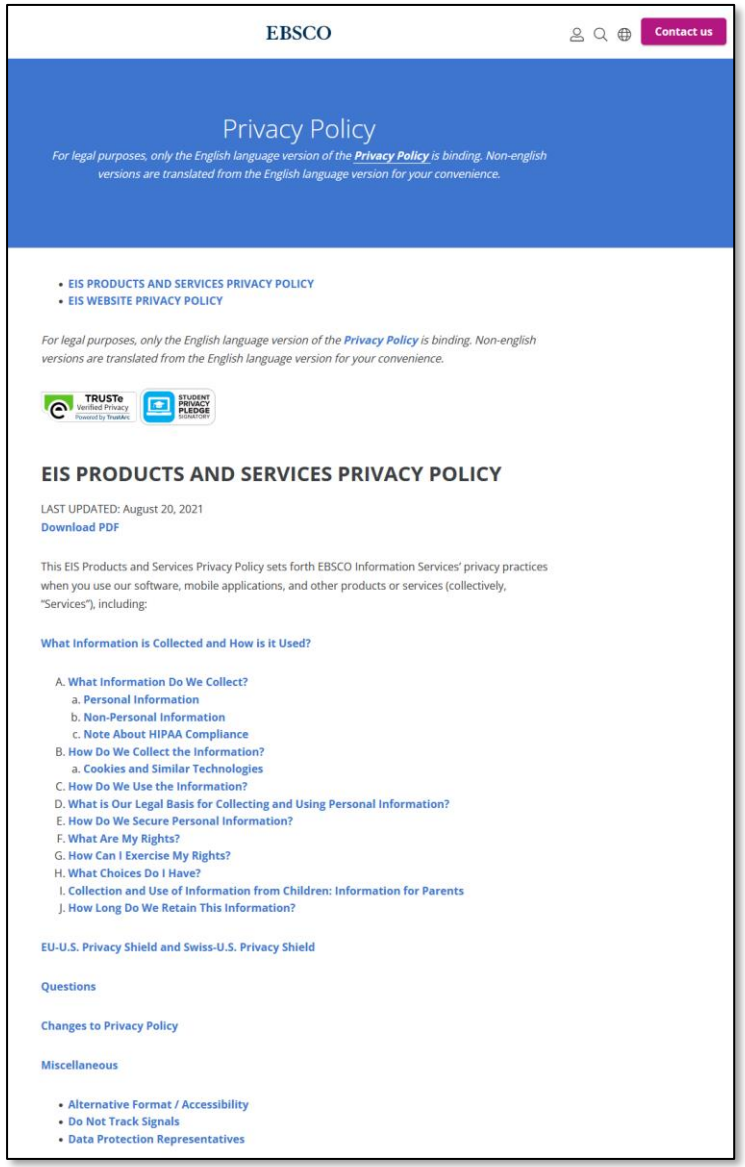
  - *Right to be Informed*
  - *Right to Access*
  - *Right to Rectification*
  - *Right to Restrict Processing*
  - *Right to Data Portability*
  - *Right to Object or Opt-out*
  - *Right to Withdraw Consent*
  - *Right to Erasure or Deletion*
  - *Right to Non-discrimination*
  - *Right to not be Subject to Automated Decision Making*
  - *Right to Lodge a Complaint*

Data Privacy Control and Minimization | EBSCO's Approach

- Empower Customer and User Patrons to access and directly control their own data quickly and easily
- Enable Customer Administrators with the ability to restrict Personalization
- Individuals can make Subject Access Rights at any time
- Strike a balance between User Control and User Experience
- EBSCO has provided a secure, online self-service system that provides an individual with direct access to his or her information

EBSCO is processing a very limited set of personal data ... certainly when compared to Social Media applications, etc and has a very clear approach on how to manage data privacy while providing a valuable User Patron experience

EBSCO Privacy Policy



EBSCO

Contact us

Privacy Policy

*For legal purposes, only the English language version of the **Privacy Policy** is binding. Non-english versions are translated from the English language version for your convenience.*

- EIS PRODUCTS AND SERVICES PRIVACY POLICY
- EIS WEBSITE PRIVACY POLICY

*For legal purposes, only the English language version of the **Privacy Policy** is binding. Non-english versions are translated from the English language version for your convenience.*

TRUSTe Verified Privacy Powered by TrustArc | STUDENT PRIVACY PLEDGE SIGNATORY

EIS PRODUCTS AND SERVICES PRIVACY POLICY

LAST UPDATED: August 20, 2021

Download PDF

This EIS Products and Services Privacy Policy sets forth EBSCO Information Services' privacy practices when you use our software, mobile applications, and other products or services (collectively, "Services"), including:

What Information is Collected and How is it Used?

A. What Information Do We Collect?
   a. Personal Information
   b. Non-Personal Information
   c. Note About HIPAA Compliance
B. How Do We Collect the Information?
   a. Cookies and Similar Technologies
C. How Do We Use the Information?
D. What is Our Legal Basis for Collecting and Using Personal Information?
E. How Do We Secure Personal Information?
F. What Are My Rights?
G. How Can I Exercise My Rights?
H. What Choices Do I Have?
I. Collection and Use of Information from Children: Information for Parents
J. How Long Do We Retain This Information?

EU-U.S. Privacy Shield and Swiss-U.S. Privacy Shield

Questions

Changes to Privacy Policy

Miscellaneous

- Alternative Format / Accessibility
- Do Not Track Signals
- Data Protection Representatives

- What Information Do We Collect?
- Personal Information
- Non-Personal Information
- How Do We Collect the Information?
- Cookies and Similar Technologies
- How Do We Use the Information?
- What is Our Legal Basis for Collecting and Using Personal Information?
- How Do We Secure Personal Information?
- What Are My Rights?
- How Can I Exercise My Rights?
- What Choices Do I Have?
- How Long Do We Retain This Information?

https://www.ebsco.com/company/privacy-policy

EBSCO's Privacy Policy ensures User Patrons are able to provide "Informed Consent"

EBSCO Connect | Frequently Asked Questions (GDPR)

Q: What is EBSCO doing to address the Schrems decision and the invalidation of Privacy Shield?

The opinion issued by the Court of Justice of the European Union (CJEU) invalidating the EU-US Privacy Shield (Decision 2016/1250) triggered an immediate re-assessment of transfers of personal information between the EU and the United States by all global companies, including EBSCO. *Personal information protected by GDPR that is collected by any of EBSCO's companies and transferred to the United States either directly or via onward transfer is made pursuant to Standard Contractual Clauses (SCCs) instead of reliance on Privacy Shield.* EBSCO is closely following this opinion as its impact on EBSCO and its customers continues to develop. EBSCO will continue to adhere to the privacy practices outlined in its Privacy Policy with respect to data it collects.

For information collected under the Privacy Shield prior to *Schrems*, EBSCO must continue to adhere to the Privacy Shield principals, and such commitment remains referenced in our Privacy Policy. Although we no longer rely on Privacy Shield as an adequacy mechanism for cross-border transfer, *EBSCO continues to value annual certifications to its privacy principals and our independent third-party assessments of our privacy program performed by TrustArc.*

https://connect.ebsco.com/s/article/General-Data-Protection-Regulation-GDPR-Frequently-Asked-Questions?language=en_US

EBSCO Connect | Frequently Asked Questions (GDPR)

Q: Is EBSCO a processor or controller for customer and end user personal information?

EBSCO is *a joint controller of end user personal information* for all products and services other than FOLIO hosting services. *This end user information is provided to EBSCO directly from the data subject and pursuant to the contractual relationship with the customer.* Joint controllers jointly determine the purposes and means of processing. EBSCO collects end user consent at the point of collection and allows end users the ability to access and request deletion of this data in our account preference center. As a joint controller, the customer still retains certain rights with respect to the end user data, such as the ability to request deletion and in some cases, access usage reports related to its end users. *End Users do not enter personal data directly into FOLIO Hosting Services so there are no grounds for EBSCO to be classified as a "Joint Controller" in this case.*

EBSCO is *a processor of customer-provided personal information* and all personal information collected in connection with our FOLIO hosting services, processing such personal information on behalf of the customer as data controller when the customer is purchasing or using EBSCO products and services. EBSCO's customers act as the data controller for any personal data the customer provides to EBSCO in connection with their use of EBSCO's products and services. The data controller determines the purposes and means of processing personal data, while the data processor processes data on behalf of the data controller.

https://connect.ebsco.com/s/article/General-Data-Protection-Regulation-GDPR-Frequently-Asked-Questions?language=en_US

EBSCO Connect | Frequently Asked Questions (GDPR)

Q: Does EBSCO offer a data protection addendum?

Yes. EBSCO's form data protection addendum (DPA) *addresses our obligations with respect to personal data we collect as a processor and joint from the EEA, EU, and UK to the US*. This DPA is available for all of our customers for whom we pr*controller and for transfers of data* ocess personal information.

Q: What privacy controls have been implemented for end users?

EBSCO has enabled *a set of privacy controls that will allow end users of EBSCOHost databases and eBooks, Flipster digital journals and EDS Discovery Service to manage their personal information, including the ability to remove their information from EBSCO's services at any time.* Any user creating a new personal account (MyEBSCO Folder, Personal User Account, DynaMed Personal User Account) will be provided privacy policy information and must complete the account creation process. Users with existing accounts or acccounts created in an automated fashion through Single Sign On integration with the institutional active user directory will also be prompted to read the policy the first time they log in after these new privacy controls become available. *Users who do not wish to adhere to the privacy policy have the ability to use the Forget Me option and have their account removed from EBSCO's system. Accounts that are removed are not recoverable.*

https://connect.ebsco.com/s/article/General-Data-Protection-Regulation-GDPR-Frequently-Asked-Questions?language=en_US

Agenda

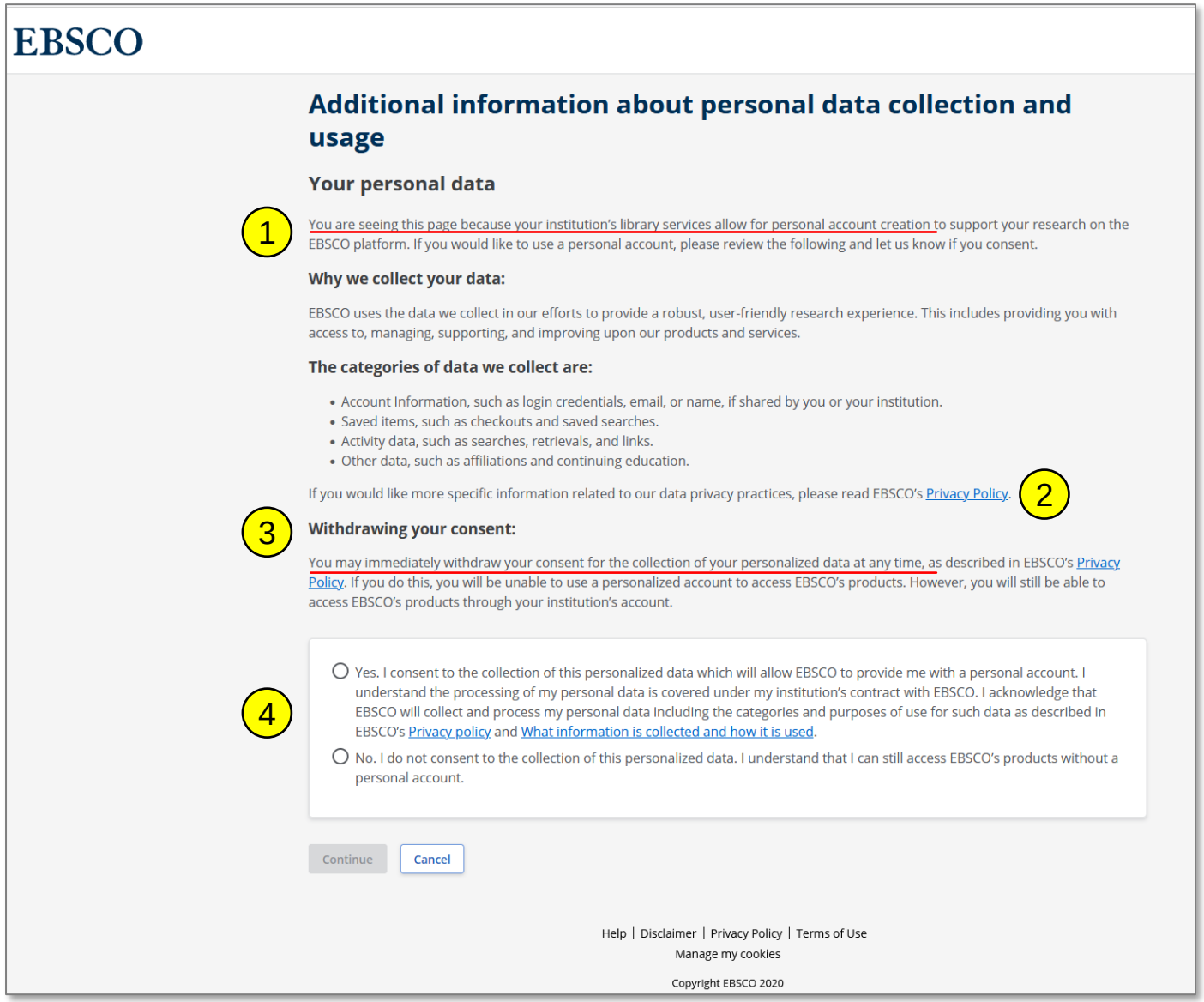
- Overview
  - GDPR
  - Common Security and Privacy Framework Controls
- EBSCO's Approach to Data Minimization
  - Institutional-Level Access (Non-Personalized)
  - Personalized User Privacy Experience (New eHost UI)
  - Anonymized Privacy Configurations
- Trans-Atlantic Data Privacy Framework
  - Standard Contractual Clauses (SCCs)
- Way Ahead
- Questions

Data Minimization and Transfer of Data Outside of EU

- As an EBSCO customer, is it possible to use EBSCO library systems without any transfer of personal data outside of EU?
  - There are several ways for User Patrons to access EBSCO products
  - **Institutional-Level:** EBSCO provides GDPR-compliant products with no advanced configuration required ... Administrators can set Account Personalization to "Off"
  - **Personalized (with DSAR):** EBSCO also provides a full set of Data Subject Access Request functions directly within our products/platform
  - **Pseudo-Anonymized (with DSAR):** Additional configuration (network proxies and SSO/Federated Identity) are recommended as best practices for User Patrons to use personalized features while minimizing User Personal Information
    - Can provide pseudonomous identifiers (Example: ahf8543w0_da3ryrYYisyd8)

EBSCO provides a spectrum of tools and recommended configurations to enable Customer User Data Privacy, such as "Institutional-Level" (No Personalization), Personalization (with Direct User Control), and integration tooling that enables pseudonymization.

Personalized User Privacy Experience (New eHost UI)



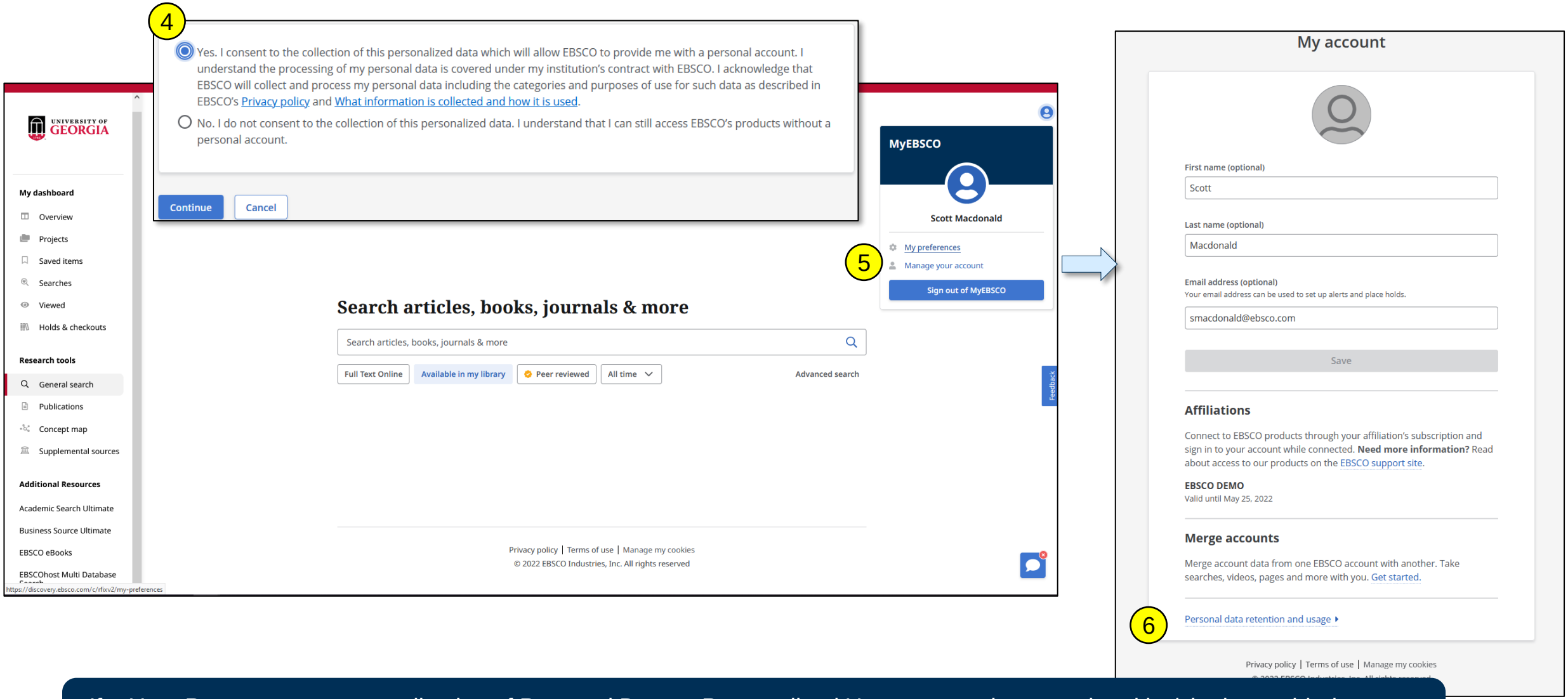
1. Customer Administrators are given the choice of enabling/disabling Personalization

2. EBSCO's detailed Privacy Policy is provided within the consent prompt should a User Patron wish to review prior to decision.
   https://www.ebsco.com/company/privacy-policy#prod_shields

3. User Patrons are advised of their rights to revoke consent at any time

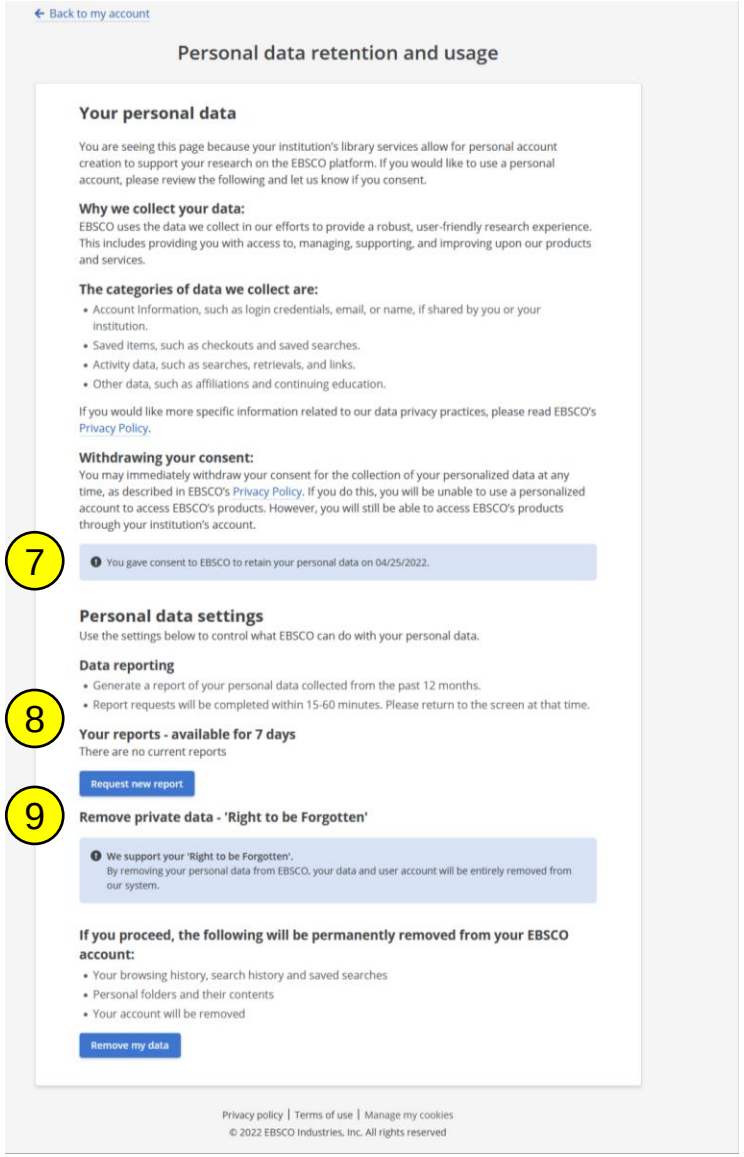
4. New Users are immediately prompted for consent to collection of some Personal Information

Personalized User Privacy Experience (New eHost UI) ... contd.

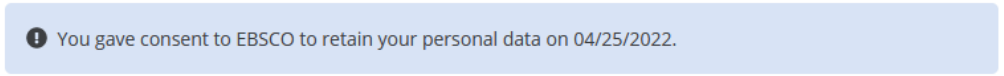


If a User Patron consents to collection of Personal Data, a Personalized User account is created and he/she is provided access to additional "Personal data Retention and Usage" management controls ...

Personal Data Retention and Usage

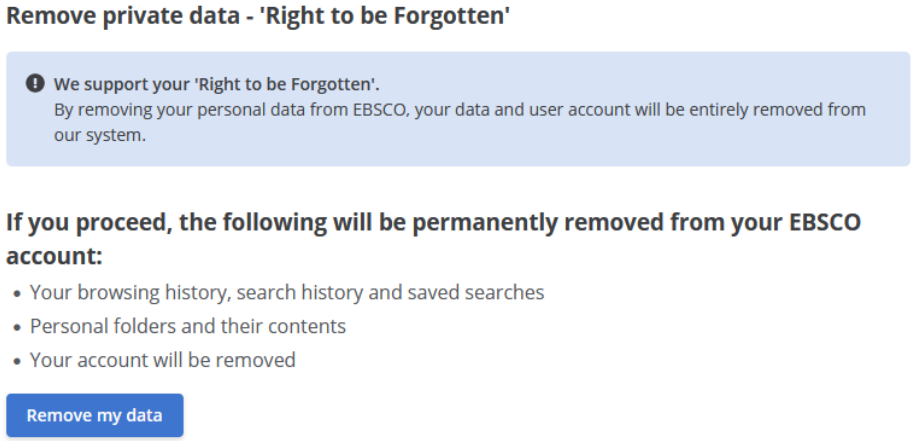


7 User Patrons are provided their date of last consent

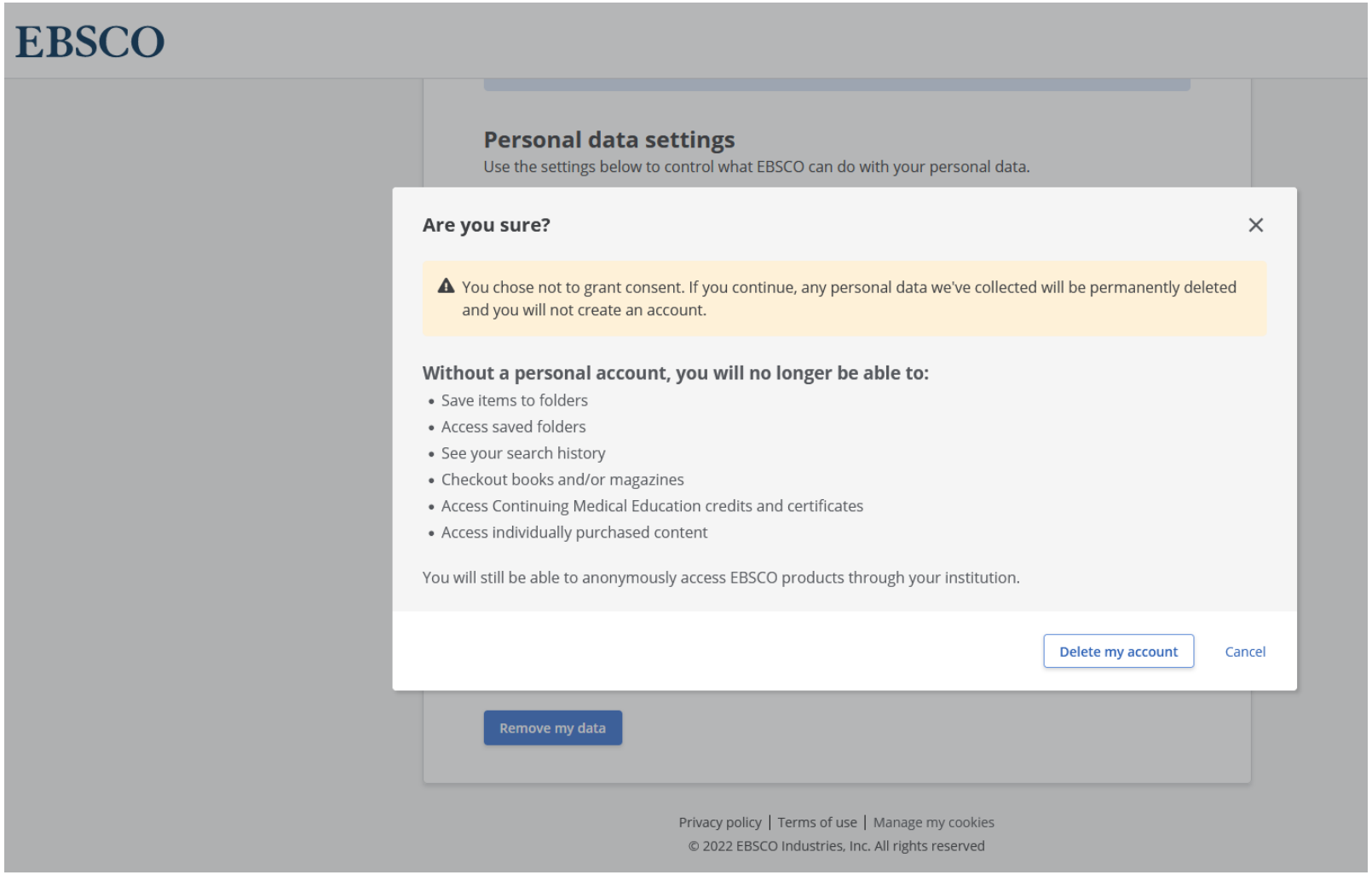


8 User Patrons are empowered to exercise their "Right to Access" by generating an "On-demand" report listing Personal Data collected on a subject within the previous 12 months.

9 User Patrons are empowered to exercise their "Right to Withdraw Consent"



Personal Data Retention and Usage ... Contd.



The Data Anonymization process is final and cannot be reversed

Single Sign-On (SSO) | Federated Identity

- The only attribute that is truly required when using a Single Sign-On (SSO) capability is a persistent, unique identifier which is maintained by the Customer Organization
  - Individual Users can access personalization features while preserving their privacy as their unique ID is linked to encrypted attribute data which is passed with their consent from their organization to the EBSCO platform.
  - The extent to which Personal Information can be associated with this unique identifier is maintained under the direct control of the Customer organization, not the SSO provider, nor EBSCO products or services
  - This can be any attribute of the organization's choosing, though it must exist on all user accounts and be unique to each individual user account.
- This attribute is how an SSO service provider identifies an individual user for the purposes of authentication and personalization.
- The ability of individual users to Personalize their accounts in order to leverage additional product functionality remains at the discretion of the Customer Organization Administrator

Best practice for advanced identity management is the use of a Single Sign-On (SSO) | Federated Identity capability

Agenda

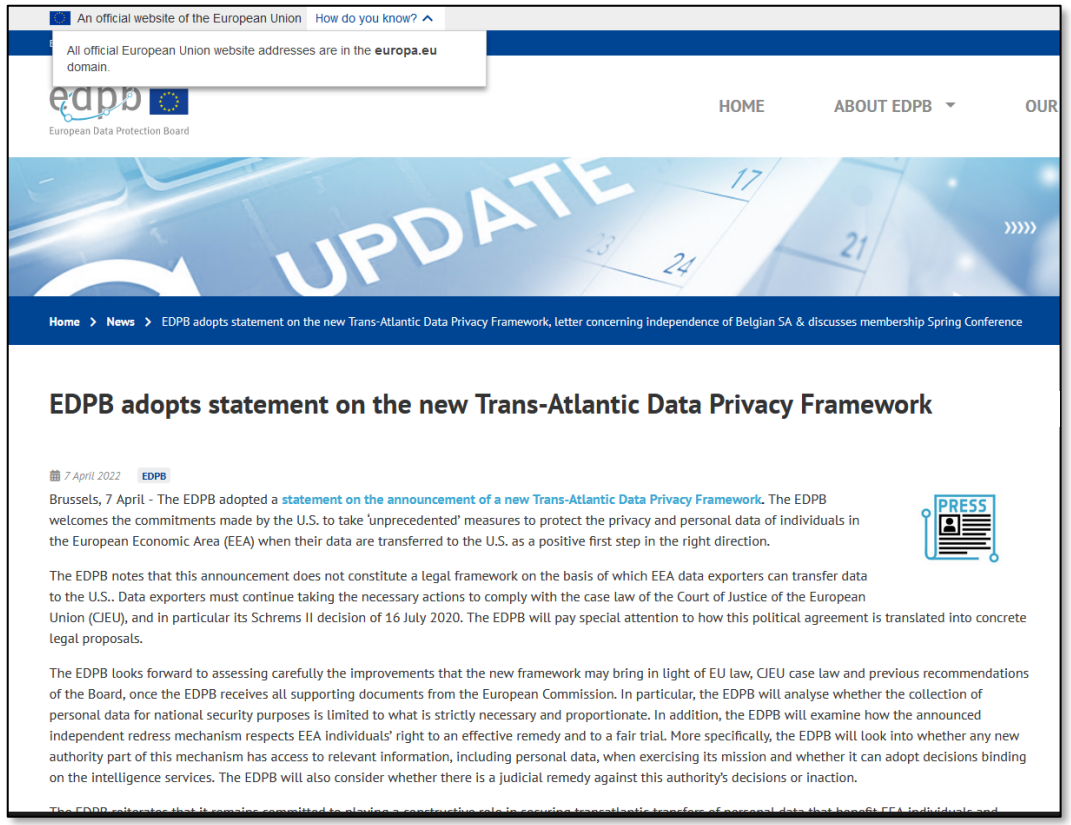
- Overview
  - GDPR
  - Common Security and Privacy Framework Controls
- EBSCO's Approach to Data Minimization
  - Institutional-Level Access (Non-Personalized)
  - Personalized User Privacy Experience (New eHost UI)
  - Anonymized Privacy Configurations
- Trans-Atlantic Data Privacy Framework
  - Standard Contractual Clauses (SCCs)
- Way Ahead
- Questions

Trans-Atlantic Data Transfer | Considerations

- Can you elaborate on the work on the principles for a new Trans-Atlantic Data Privacy Framework?
- How is EBSCO prioritizing this work? Which measures are EBSCO preparing in order to comply with the new framework?

https://ec.europa.eu/commission/presscorner/detail/en/ip_22_2087

European Data Protection Board (EDPB) Response



- EDPB notes that this announcement does *not constitute a legal framework*
- Data exporters must continue taking the necessary actions to comply with the case law of the Court of Justice of the European Union (CJEU), *and in particular its Schrems II decision of 16 July 2020.*
- The EDPB will pay special attention to how this political agreement is translated into concrete legal proposals. In particular the EDPB will consider ...
  - Collection of personal data for national security purposes
  - Independent redress mechanisms & EEA Individuals' rights
  - Whether any new authority part of this mechanism can adopt decisions binding on the intelligence services.
  - Whether there is a judicial remedy against this authority's decisions or inaction.

Standard Contractual Clauses

In order for EU-members to use SCCs, companies must ensure that the recipient country has the same data protection as the EU. As EU sees it, this makes it hard, or impossible, to use SCCs, with U.S. companies. Can you please comment on that?

- According to the GDPR, the “pre-approved” Standard Contractual Clauses ensure appropriate data protection safeguards can be used as a ground for data transfers from the EU to third countries.
- The European Commission has issued modernised standard contractual clauses under the GDPR (4 Jun 2021)
- Until 27 December 2022, controllers and processors can continue to rely on those earlier SCCs for contracts that were concluded before 27 September 2021, provided that the processing operations that are the subject matter of the contract remain unchanged.

Key Partners in our Privacy Empowerment efforts ...

OpenAthens

- Fine-grained privacy controls
- Enabled through SSO and Identity services

TrustArc
Privacy Compliance

- 3rd-Party Privacy Compliance
- Privacy Shield attestation

osano

- GDPR-compliant preference management for machine tokens (cookies)
- Best of breed approach for New UI

OneTrust
PRIVACY, SECURITY & GOVERNANCE

- GDPR-compliant DSAR management
- Data Mapping
- Compliance Documentation

Way Ahead ...

Wikimedia: Structure Paris les Halles

- General Data Protection Regulation (GDPR)
- Privacy Shield / Privacy Shield
- ISO 27001 - Information Security Management System (ISMS)
- ISO 27701 - Privacy extension to ISO 27001 ("Privacy Information Management System")
- ISO 27017- Information Security for Cloud Services
- ISO 27018 - PII Protection in Public Cloud

Continue to invest in Security & Privacy Governance Frameworks and Appropriate Controls implementation

Questions ?

Thank you