Koha og GDPR

Magnus Enger
CTO, Libriotech AS
Lund, 16. oktober 2019

I Am Not A Lawyer!

Hovedprinsipper i GDPR

- Lovlig, rettferdig og gjennomsiktig
- Formålsbegrensning
- **Dataminimering**
- Riktighet
- **Lagringsbegrensning**
- Integritet, konfidensialitet og tilgjengelighet
- Ansvarlighet

Dataminimering

- Prinsippet om dataminimering innebærer å **begrense mengden innsamlede personopplysninger til det som er nødvendig for å realisere formålet med innsamlingen**. Dersom personopplysninger ikke er nødvendige for å oppnå formålet, skal man heller ikke samle dem inn.

Magnus Enger (1)
Amtmann Theisens vei 21
Bodø 8009, Norge
magnus@enger.priv.no
Intet telefonnummer lagret.
Kategori: Aministrator (ADMIN)
Hjemmebibliotek: Vårt bibliotek
Lånernummer: 1
Oppdatert den 14/10/2019 10:00

Utlån
Detaljer
Gebyrer
Rutingslister
Sirkulasjonshistorikk
Reservasjonshistorikk
Endringslogg
Meddelelser
Statistikk

Magnus Enger (1)

Kontaktinformasjon

Rediger

Amtmann Theisens vei 21
Bodø 8009, Norge

Primær e-post:	magnus@enger.priv.no
Kjønn:	Mann

Innstillinger for meldinger til lånerne

Rediger

	Dager på forhånd	E-post:	Kun sammendrag
Forfalt lån	-	☑	☐
Forhåndsvarsel	3	☑	☐
Reservert eksemplar tilgjengelig	-	☑	-
Innlevering	-	☑	-
Utlån	-	☑	-

Bibliotekbruk

Kortnummer:	1
Lånernummer:	1
Kategori:	Aministrator (ADMIN)
Registreringsdato:	18/06/2011
Utløpsdato:	18/09/2094
Bibliotek:	Vårt bibliotek
Innstilling for personvern:	Standard
Vis utlån for garantist	Nei
Brukernavn:	magnus
Passord:	*******

Alternativ adresse

Alternativ kontakt

Lagringsbegrensning

- Prinsippet om lagringsbegrensning innebærer at **personopplysninger skal slettes eller anonymiseres når de ikke lenger er nødvendige for formålet de ble innhentet for**.

Magnus Enger (1)
Amtmann Theisens vei 21
Bodø 8009, Norge
magnus@enger.priv.no
Intet telefonnummer lagret.
Kategori: Aministrator (ADMIN)
Hjemmebibliotek: Vårt bibliotek
Lånernummer: 1
Oppdatert den 14/10/2019 10:00

Utlån
Detaljer
Gebyrer
Rutingslister
Sirkulasjonshistorikk
Reservasjonshistorikk
Endringslogg
Meddelelser
Statistikk
Kjøpsforslag

Rediger | Endre passord | Duplikat | Skriv ut | Søk for å reservere | Legg til melding | Mer

Forny låner
Angi tillatelser
Slett
Eksporter strekkoder som er levert inn i dag

Magnus Enger (1)

Kontaktinformasjon

Amtmann Theisens vei 21
Bodø 8009, Norge

Primær e-post:	magnus@enger.priv.no
Kjønn:	Mann

Innstillinger for meldinger til lånerne

Rediger

	Dager på forhånd	E-post:	Kun sammendrag
Forfalt lån	-	☑	☐
Forhåndsvarsel	3	☑	☐
Reservert eksemplar tilgjengelig	-	☑	-
Innlevering	-	☑	-
Utlån	-	☑	-

kbruk

Kortnummer:	1
Lånernummer:	1
Kategori:	Aministrator (ADMIN)
Registreringsdato:	18/06/2011
Utløpsdato:	18/09/2094
Bibliotek:	Vårt bibliotek
Innstilling for personvern:	Standard
Vis utlån for garantist	Nei
Brukernavn:	magnus
Passord:	*******

Alternativ adresse

Alternativ kontakt

1 Utlån | Gebyrer og satser | 0 Reservasjoner | Restriksjoner

Vis utlån

Vis alltid aktive utlån umiddelbart ☐

Når en låner «slettes» i Koha...

- ...overføres alle data til database-tabellen `deleted_borrowers`
- ...men de vises ikke noe sted
- ...og det finnes ingen verktøy for å ta dem helt bort

GDPR - hva skjer i Koha?

https://wiki.koha-community.org/wiki/Improve_data_protection_and_patron_privacy

9	Prio 2		Administration	Staff client should not be publicly accessed, even the access to login form should be restricted.	form is always shown - koha database user could log in in every case, or somebody could try to guess the password.	deny all IP and just white list IPs which could access ▪ Two factor auth for staff client?
10	Prio 2		Patrons data portability	We need one tool to export all patron related data in machine readable format at least CSV Art 20	We can export patron data from tools via staff client, but without all related data. We can print some data, but that is not machine readable.	Bug 20028 - Export all patron related data as one file
11	Prio 2		Cookies	Do we need one of those "This site uses cookies, click here to agree" thingies? [marcelr: AFAIK we only use functional cookies in Koha. And those do not need a banner.]		
12	Prio 2	BSZ	Cookies	Maintaining documentation about the use of cookies in Koha (description of use, storage duration, values)	DONE Use of Cookies and DOC1 in Coding Guidelines	
13	Prio 3		Privacy statement/Agreement	We need a way of presenting a privacy statement/agreement that outlines all the private information that is being collected by the system and what the institution will do with that data. The agreement must be explicitly accepted by a self-registered user and a record of that acceptance must be stored (potencially as a log entry - Art 7 the consent can be undone and a checkbox is ok if this is clear). For users that are created administratinvely, I guess the agreement can be presented and accepted by other means (e.g. paper). Art 6.1.a	DONE Bug 20819 - GDPR: Add a consent field for processing personal data in account menu and self-registration Introduced in Koha 18.11.	
14	Prio 4		Apache access logs	Can correlate an IP address (which is usually PII) with records viewed	Having a strict by default logrotate policy or something could be good	
15	Prio 1		old_reserves	old_reserves keeps the link to borrowers until the borrower is deleted. Need a way to anonymize.	Needs investigation on how best to implement it: new script or enhance existing.	*Bug 19008 - More database cleanups (statistics, deleted catalog, deleted patrons, old issues, old reserves, item transfers)
16			Fines	When a fine is paid, information like "paid for by (Patron name and barcode) DATE TIME" is added to items.paidfor. It is unclear why this information is stored, and there is no way to (periodically) clean it. See Bug 19919 for some discussion around this.	DONE Bug 19919 makes Koha stop using items.paidfor. This fix will be in Koha 19.11.	
17	TBD	Marcel	Request account deletion	Art 17 - Right to erasure "Right to be forgotten"	See bug 20819. I propose to add a consent tab in opac-user and also a pref GDPR_Policy. If you set the pref to Enforced, you can only continue after login when you give your consent. A refusal is interpreted as a request to unsubscribe.	Bug 20819 - GDPR: Add a consent field for processing personal data in account menu and self-registration

Hva har vi?

- «Privacy» for lånere
- misc/cronjobs/batch_anonymise.pl
  - Bare gamle lån i tabellen `old_issues`
- misc/cronjobs/cleanup_database.pl
  - Bug 19008 - More database cleanups
  - Men dette dekker fortsatt ikke alle behovene

GDPR_Policy + PrivacyPolicyURL

Introdusert i Koha 18.11.

«[GDPR_Policy] enables a GDPR consent form to appear on the OPAC when a patron attempts to login. If this preference is set as **Enforced** then when a patron attempts to log into the OPAC a GDPR consent form be presented to them. The patron will have to provide consent to the library's GDPR policy before they can gain access to their account details. If the patron does not consent to the GDPR policy they will be logged out of their account. If the preference is set to **Permissive** then the patron will be presented with the GDPR consent form but they will not be required to give consent to access their patron account.»

https://koha-community.org/manual/19.05/en/html/systempreferences.html#gdpr-policy

Viktige lenker kan plasseres her

ditt sammendrag
dine gebyrer
dine personopplysninger
dine samtykker
dine tagger
endre passordet
din lesehistorikk

For at du skal kunne fortsette å være logget inn trenger vi ditt samtykke til at vi behandler dine persondata som spesifisert i "EU General Data Protection Regulation" av 25. mai 2018.

Vennligst lagre ditt samtykke nedenfor, eller logg ut. På forhånd takk!

Dine samtykker

GDPR-samtykker

- Jeg har lestRetningslinjer for behandling av persondata og samtykker til deres behandling av mine persondata som beskrevet.
  - ○ Ja, jeg samtykker.
  - ○ Nei, jeg gir ikke mitt samtykke. Vennligst fjern min konto innen rimelig tid.

Lagre

Hva trenger vi?

- Verktøy for å oppfylle kravene
- Verktøy som kan hjelpe bibliotekene å dokumentere at de oppfyller kravene
- En cronjobb som settes opp på Koha-serveren av en leverandør gir veldig lite valgmuligheter og innsikt...

Forslag...

- En rydde-cronjobb som alltid er aktiv*
- Ett grafisk grensesnitt for å slå på hva som skal ryddes og når
  - Systempreferanser
  - Eget grensesnitt, som inkluderer feedback på om ryddingen fungerer
- Bibliotekene må definere behov - og finansiere :-)

* = Ihvertfall om man installerer Koha med Debian-pakkene

«State of GDPR»

En Koha-plugin for å vise hvordan et bibliotek ligger an i forhold til sletting og anonymisering av data.

Versjon 0.0.1

https://github.com/Libriotech/koha-plugin-stateofgdpr

State of GDPR

Deleted borrowers

Number of deleted borrowers in the "deletedborrowers" table: 1236.

Oldest: 2017-11-10 01:24:07

Newest: 2019-10-07 13:35:59

Tables: borrowers, deletedborrowers

State of GDPR

Deleted borrowers | **Gender** | Privacy

Gender

You are tracking the gender of:

- 15623 current patrons
- 1102 deleted patrons

Tables: borrowers, deletedborrowers

State of GDPR

Deleted borrowers | Gender | **Privacy** | Old loans | Last borrower | Old reserves

Privacy

These are the privacy settings of you current patrons.

You have set the syspref OPACPrivacy to 0, which means that patrons can't change their own privacy i

"Default privacy" is the privacy setting of the patron category the patron belongs to.

"Actual privacy" is the actual privacy setting of a patron.

Category	Code	Default privacy	Actual privacy	Number of patrons
Barn	BARN	default	default	4333
Barn	BARN	default	never	2
Bibliotekarie	BIB	default	forever	1
Bibliotekarie	BIB	default	default	34
Bibliotek övriga	BIBOVR	default	default	25
Boken kommer	BKO	forever	forever	17
Boken kommer	BKO	forever	never	1
Dagbarnvårdare	DAGBV	default	default	5
Deposition	DEPOSITION	default	default	2
Förskolor	FORSKOLA	default	default	137
Förskolor	FORSKOLA	default	never	1
Fritidshem	FRITIDSHEM	default	default	17
Grundskola	GRUNDSKOLA	default	default	157

State of GDPR

Deleted borrowers | Gender | Privacy | **Old loans** | Last borrower | Old reserves

Old loans

You have 580227 old loans. 561429 of these have been anonymized. That is 96.7602334948219%.

The oldest non-anonymized loan is from 2016-06-08 11:42:10.

The loans that have not been anonymized are distributed among your patron categories as follows:

Category	Code	Default privacy	Number of loans
Barn	BARN	default	439
Bibliotekarie	BIB	default	116
Bibliotek övriga	BIBOVR	default	2
Boken kommer	BKO	forever	2159
Förskolor	FORSKOLA	default	33
Grundskola	GRUNDSKOLA	default	89
Hederslåntagare	HEDERLANT	default	17
Internlån	INTERN	default	2
Övrigt	OVRIGT	default	7
Personal Kulturhuset	PERSOVR	default	1
Talboken kommer	TK	forever	5625
Talbokslåntagare	TL	forever	7205
Vuxen	VUXEN	default	2904

Tables: old_issues

State of GDPR

Deleted borrowers | Gender | Privacy | Old loans | **Last borrower** | Old reserves | Statistics | Messages | Misc | TODO

Last borrower

The syspref StoreLastBorrower is set to 1 (on). You are tracking the last borrower for 67614 items. The oldest return you are tracking was made on 2017-11-10 09:02:27.

Tables: items_last_borrower

State of GDPR

Deleted borrowers | Gender | Privacy | Old loans | Last borrower | **Old reserves**

Old reserves

You have 37777 old reserves. 0 of these have been anonymized. That is 0%.

The oldest non-anonymized reserve is from 2016-03-22 09:12:25.

Year	Count
2016	37
2017	2363
2018	18609
2019	16420

Tables: old_reserves

State of GDPR

Deleted borrowers | Gender | Privacy | Old loans | Last borrower | Old reserves | **Statistics** | Messages | Misc | TOD

Statistics

Anonymized

These are entries in the statistics table where the borrowernumber-field is equal to the borrowernumber of the anonymous patron, or empty.

Type	Count
localuse	4
return	321194

Non-anonymized

These are entries in the statistics table where the borrowernumber-field is non-empty and not equal to the borrowernumber of the anonymous patron.

Type	Count
issue	567926
localuse	31
onsite_checkout	2
payment	4252
renew	326967
return	579164
writeoff	10783

Age of non-anonymized entries:

Year	Count
2016	247118
2017	440978
2018	446849
2019	354181

Tables: statistics

State of GDPR

Deleted borrowers | Gender | Privacy | Old loans | Last borrower | Old reserves | Statistics | **Mess**

Messages

There are 336585 old messages that have not been anonymized. The oldest such message is from 2016-02-10 09:59:03.

Age of non-anonymized messages:

Year	Count
2016	45086
2017	96983
2018	105558
2019	87336

Tables: message_queue

State of GDPR

Deleted borrowers | Gender | Privacy

TODO

- Logs
- Fines
- Patron consent (see Koha bug 20819)

Rapporter

- Gir tilgang til alle data som finnes i Koha sin database
- Vi burde ha...
  - Mulighet for å flagge rapporter som sensitive
  - En rettighet for å se sensitive rapporter
  - https://bugs.koha-community.org/bugzilla3/show_bug.cgi?id=20026

Google Analytics?

- Bør vi hjelpe Google å samle inn data om brukerne våre?
- Det finnes alternativer
  - Matomo: matomo.org

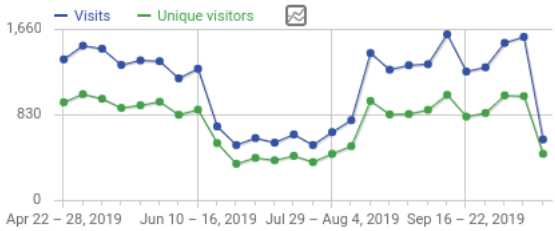
matomo

Dashboard | All Websites | Tag Manager

FROM 2019-10-14 TO 2019-10-20 | ALL VISITS | DASHBOARD

- Dashboard
  - Oversikt for magnusenger
- Visitors
- Behaviour
- Acquisition
- Goals

Visits Over Time

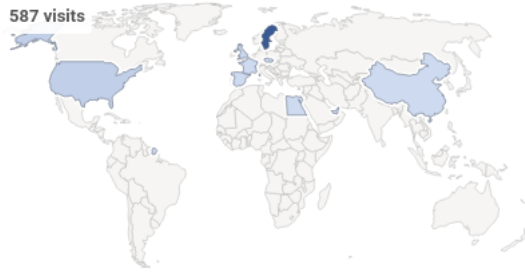


Websites

WEBSITE	VISITS
[redacted]	160
[redacted]	1
www.superstart.se	1

1–3 of 3

Visitor Map



Countries | World-Wide | Visits

Visits in Real-time

DATE	VISITS	ACTIONS
Last 24 hours	249	1,283
Last 30 minutes	9	43

Wednesday, October 16, - 09:37:10 (1 min 53s)

iOS

Search Engines

SEARCH ENGINE	VISITS
Bing	12
Google	12
DuckDuckGo	2

Browsers

BROWSER	VISITS
Mobile Safari	187
Chrome	109
Chrome Mobile	94

Spørsmål?

Magnus Enger, Libriotech AS
magnus@libriotech.no