

Verzeichnis der Verarbeitungstätigkeiten LAS:eR

Nr. 12

beim betrieblichen Datenschutzbeauftragten
(Artikel 30 DSGVO)

Inhalt

Inhalt.....	1
1 Historie.....	2
2 Einleitung	2
3 Beteiligte Personen	2
4 Verantwortliche Stelle	3
4.1 Angaben zur verantwortliche Stelle	3
4.2 Vertretung/Ansprechpartner	3
4.3 Behördlicher Datenschutzbeauftragter	4
5 Beschreibung des Verfahrens	5
5.1 Angaben zum automatisierten Verfahren.....	5
5.1.1 Allgemeine Bezeichnung des Verfahrens.....	5
5.1.2 Aufgaben, zu deren Erfüllung die personenbezogenen Daten verarbeitet oder genutzt werden.....	6
5.1.3 Rechtsgrundlage, Zweckbestimmung der Verarbeitung.....	7
5.2 Beschreibung der betroffenen Personengruppen.....	7
5.3 Art der gespeicherten Daten oder Datenkategorien.....	8
5.4 Empfänger, denen die Daten mitgeteilt werden.....	9
5.5 Regelfristen für die Löschung der Daten	9
5.6 Festlegung des Schutzbedarfs/Risikoanalyse	10
5.7 Weitere Angaben	10
5.8 Geplante Datenübermittlung in Drittstaaten	10
5.9 Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)	11
6 Sicherheit der Verarbeitung.....	11
6.1 Mittel der Verarbeitung	11
6.2 IT-Sicherheit (Art. 30 Abs. 1 g DSGVO)	12

6.3	Angabe der zugriffsberechtigten Personen (möglichst Funktionsbeschreibungen und keine Beschäftigtenamen):.....	13
6.4	Information der Betroffenen (Art. 12 ff DSGVO).....	13
7	Überwachung.....	14

1 Historie

Version	Datum	Autor	Beschreibung
1.0	03.07.2018	Michael Nelißen, Daniel Rupp	Initiales Dokument
1.1	13.12.2019	Michael Nelißen, Daniel Rupp	Aktualisierung
1.2	27.11.2020	Michael Nelißen, Daniel Rupp	Aktualisierung

2 Einleitung

Die rechtliche Notwendigkeit für die im Verzeichnissesverzeichnis geforderten Angaben ergibt sich aus Art. 30 DSGVO.

3 Beteiligte Personen

Position	Name	Mail	Telefon
Datenschutzbeauftragter	Michael Nelißen	datenschutz@hbz-nrw.de	0221/40075-137
Externer Datenschutzberater	RA Thomas Feil	feil@recht-freundlich.de	0511/473906-0

4 Verantwortliche Stelle

4.1 Angaben zur verantwortliche Stelle

1.1 Name	Hochschulbibliothekszentrum des Landes NRW im folgenden hbz
1.2 Straße	Jülicher Straße 6
1.3 PLZ/Ort	50674 Köln
1.4 Telefon	+49-221-40075-0
Telefax	+49-221-40075-169
1.5 E-Mail-Adresse	
1.6 Internetadresse	www.hbz-nrw.de

4.2 Vertretung/Ansprechpartner

2.1 Leitung	Dr. Silke Schomburg
2.2 IT-Leitung	Uwe Wank
2.3 Gruppenleitung	Michaela Selbach

4.3 Behördlicher Datenschutzbeauftragter

1.1 Name	Michael Nellißen
1.2 Straße	Jülicher Straße 6
1.3 PLZ/Ort	50674 Köln
1.4 Telefon/Telefax	+49-221-40075-137
1.5 E-Mail-Adresse	datenschutz@hbz-nrw.de
1.6 Internetadresse	www.hbz-nrw.de

- ☐ Datenschutz-Folgeabschätzung
- ☐ Erstmalige Beschreibung eines automatisierten Verfahrens nach DSGVO
- ☐ Auftragsverarbeitung
- ☒ Änderung des Verzeichnis der Verarbeitungstätigkeit vom 03.07.2018, lfd. Nr.: 12
- ☐ Fehlanzeige zur Erfassung von Verarbeitungstätigkeiten
- ☐ Abmeldung bestehender Verarbeitung

5 Beschreibung des Verfahrens

5.1 Angaben zum automatisierten Verfahren

(Art. 30 Abs. 1 DSGVO)

Das hbz bietet mit LAS:eR (Lizenz-Administrationssystem für eRessourcen) ein bundesweit einsetzbares, mandantenfähiges System als Software-as-a-Service-Dienstleistung (SaaS) an, welches das Management elektronischer Ressourcen auf lokaler, regionaler und nationaler Ebene unterstützt und konsortiale Verhandlungsführer und Bibliotheken von den entsprechenden Verwaltungsaufgaben entlastet.

Dazu werden für die Nutzer Konten eingerichtet und für diese Name, Vorname, Institutionszuordnung und Kontaktdaten hinterlegt. Über dieses Konto erhält der Nutzer Zugriff auf die Daten zu elektronischen Ressourcen, die für seine Institution freigegeben sind. Darüber hinaus funktioniert LAS:eR im Sinne eines Adressbuchs, d.h. Nutzer können Kontaktdaten zu dienstlichen Kontakten, die im Zuge der Verwaltung der elektronischen Ressourcen anfallen, in LAS:eR hinterlegt werden.

Die personenbezogenen Daten, sowohl der Kontodaten wie auch der Kontaktdaten zu dienstlichen Kontakten im Sinne eines Adressbuchs, sind für die LAS:eR-interne Verwaltung notwendig. Exporte von LAS:eR-Daten über Schnittstellen sind lediglich für nicht-personenbezogene Daten möglich.

5.1.1 Allgemeine Bezeichnung des Verfahrens

LAS:eR

Betrieb eines nationalen „Electronic Resource Management System“, eines System für Bibliotheken und Konsortialstellen zur Verwaltung von Lizenzen zu erworbenen elektronischen Ressourcen (E-Journals, E-Books, Datenbanken etc.)

5.1.2 Aufgaben, zu deren Erfüllung die personenbezogenen Daten verarbeitet oder genutzt werden

lfd. Nr. (entspr. lfd. Nr. in 5.3.)	Aufgabe
1	Interne Datenbank-ID, Kontoname und Passwort werden zur Verwaltung des LAS:eR-Nutzers benötigt.
2	Der Name und Vorname der LAS:eR-Nutzer oder der LAS:eR-Administratoren werden von Super-Administratoren des hbz bzw. von Institutions-Administratoren der jeweiligen Institution zum Anlegen eines LAS:eR-Nutzer-Accounts benötigt.
3	Nutzer arbeiten in LAS:eR im Rahmen einer oder mehrerer Institutionszuordnungen, wodurch ihre Sicht- und Bearbeitungsrechte gesteuert werden.
4	Die Kontaktinformationen (Institution, E-Mail-Adresse, dienstl. Telefonnr., dienstl. Faxnummer, evtl. Kürzel) der LAS:eR-Nutzer oder der LAS:eR-Administratoren werden vom Institutionsübergreifenden Super-Administrator der Gruppe „Digitale Inhalte“ und/oder vom Institutions-Administratoren der jeweiligen Institution zum Anlegen eines LAS:eR-Nutzer-Accounts benötigt.
5-7	Name, Vorname, Institutionszuordnung und Adressen von Kontaktpersonen dienen dazu, in Form eines Adressbuches bzw. einer Kontaktseite Kontakte zu verwalten.
8	Die Logdateien werden von Super-Administratoren des hbz ausschließlich zur Fehleranalyse genutzt.

5.1.3 Rechtsgrundlage, Zweckbestimmung der Verarbeitung, (Art. 30 Abs. 1 b DSGVO)

Rechtsgrundlage

a) Auftragsdatenverarbeitung mit den Bibliotheken (Artikel 28 DSGVO)

b) Einzelauftrag LAS:eR (Artikel 6 DSGVO, Abs. 1b)

Zweckbestimmung

LAS:eR wird zur Verwaltung elektronischer Ressourcen genutzt. Dazu können Lizenzen, Lizenzverträge und Finanzierungen für eine Bibliothek angelegt, mit E-Ressourcen-Paketen verknüpft und Aufgaben, Dokumente etc. erstellt werden.

Um die genannten Zwecke nutzen zu können, ist eine persönliche Anmeldung erforderlich.

5.2 Beschreibung der betroffenen Personengruppen (Art. 30 Abs. 1 c DSGVO)

lfd. Nr. (entspr. Nr. in 5.3.)	Personengruppe
1-4, 8	Beschäftigte aus Bibliotheken bzw. Konsortialstellen sowie des hbz, die LAS:eR nutzen (LAS:eR-Nutzer und -Administratoren)
5-7	Ansprechpartner von Einrichtungen, die von LAS:eR-Nutzern verwaltet werden (im Sinne eines Adressbuchs bzw. einer Kontaktseite)

5.3 Art der gespeicherten Daten oder Datenkategorien (Art. 30 Abs. 1 c DSGVO)

Lfd. Nr.	Bezeichnung der Daten/Kategorien (aussagekräftige Oberbegriffe, z.B. Namen, Anschriften; keine Angaben von Feldnummern des Datensatzes, sind ausreichend.)	Beschreibung
1	Benutzer-ID und Zugangsdaten	Interne Datenbank-ID zur Identifikation der Nutzer, Kontoname und Passwort.
2	Name / Vorname Nutzer	Name und Vorname der LAS:eR-Nutzer oder der LAS:eR-Administratoren. Dient der Anzeige des angemeldeten Nutzerkontos.
3	Institutionszuordnung Nutzer	Angabe der Institutionen, der ein Nutzer zugeordnet ist. Der Nutzer arbeitet im System immer im Kontext einer dieser Institutionen, für die er Lizenzen verwaltet.
4	Kontaktinformationen Nutzer	E-Mail-Adresse der LAS:eR-Nutzer oder der LAS:eR-Administratoren. Die Kontaktdaten dienen bei entsprechender Einstellung zum Versenden von Benachrichtigungen aus dem System heraus.
5	Name / Vorname Ansprechpartner	Dient der Anzeige eines Ansprechpartners für dienstliche Kontakte im Sinne eines Adressbuchs bzw. auf Einrichtungsprofilen, die für konsortiale Systemnutzer freigegeben sind.
6	Institutionszuordnung Ansprechpartner	Die Institution, der ein Ansprechpartner in einer bestimmten Funktion angehört.
7	Kontaktinformationen Ansprechpartner	E-Mail-Adresse, Telefonnummer, Faxnummer der in LAS:eR gepflegten Ansprechpartnern. Sie dienen zur dienstlichen Kontaktaufnahme im Sinne eines Adressbuchs bzw. über Einrichtungsprofile, die für konsortiale Systemnutzer freigegeben sind.
8	Logdateien	Serverseitige Logdateien der Systemereignisse.

5.4 Empfänger, denen die Daten mitgeteilt werden (Art. 30 Abs. 1 d DSGVO)

Lfd. Nr. (entspr. Nr. in 5.3.)	Empfänger
1-4	Super-Administratoren des hbz, die mit der Verwaltung der Nutzerkonten beschäftigt sind. Institutions-Administratoren der jeweiligen Institution, die die Nutzer dieser Institution verwalten.
5-7	Nutzer des Systems, für deren Einrichtung die genannten Kontaktdaten verwaltet werden, sowie Nutzer des Systems, die als konsortiale Nutzer Zugriff auf die Kontakte auf dem Einrichtungsprofil der jeweiligen Einrichtung erhalten.
8	Super-Administratoren des hbz zur Fehleranalyse.

5.5 Regelfristen für die Löschung der Daten (Art. 30 Abs. 1 f DSGVO)

Lfd. Nr. (entspr. Nr. in 5.3.)	Löschfrist
1-4	Löschanträge für Benutzerkonten können jederzeit an die auf der Homepage genannte Mail-Adresse laser@hbz-nrw.de bzw. laser_support@hbz-nrw.de geschickt werden. Die Daten der Nutzerkonten werden daraufhin gelöscht bzw. anonymisiert. Nutzer, die zwei Jahre inaktiv waren, werden automatisiert gelöscht bzw. anonymisiert. Mit einer Löschung des eigenen Profils durch den Nutzer selbst wird das Nutzerkonto direkt gelöscht bzw. anonymisiert.
5-7	Die Löschung von nicht mehr genutzten Kontaktdaten erfolgt nach Nutzungsende der die Kontaktdaten pflegenden Einrichtung, d.h. nach Kündigung der LAS:eR-Nutzung laut Vertrag, innerhalb von 6 Monaten.
8	Per Lösch- oder Anonymisierungsskript nach 3 Monaten.

5.6 Festlegung des Schutzbedarfs/Risikoanalyse

Ifd. Nr. (entspr. Nr. in 5.3.)	Schutzklasse	Bemerkung
1	A	Schutzklasse A, da als Kontodaten nur ein Kontoname, eine dienstliche Mailadresse, ein frei gewähltes Passwort sowie eine interne Datenbank-ID anfallen.
2-4	A	ebenfalls Schutzklasse A, da neben Vor- und Nachnamen nur dienstliche Informationen wie Einrichtungszugehörigkeit, dienstliche Telefon- oder Faxnummer bzw. dienstliche Mailadresse gespeichert werden.
5-7	A	ebenfalls Schutzklasse A, da neben Vor- und Nachnamen nur dienstliche Kontaktinformationen wie Einrichtungszugehörigkeit, dienstliche Telefon- oder Faxnummer bzw. dienstliche Mailadresse gespeichert werden.
8	A	Ebenfalls Schutzklasse A, da lediglich der Kontoname und die Institutionszugehörigkeit (1 und 3) protokolliert wird.

5.7 Weitere Angaben

(z.B. Verarbeitung: Auftragnehmer; bei Verfahrensänderung: Unterschied zum bisherigen Verfahren)

5.8 Geplante Datenübermittlung in Drittstaaten

(Art. 30 Abs. 1 e DSGVO)

5.9 Verarbeitung besonderer Kategorien personenbezogener Daten (Art. 9 DSGVO)

6 Sicherheit der Verarbeitung

6.1 Mittel der Verarbeitung

Welche Software oder Systeme werden für die Verarbeitung eingesetzt (Eigenentwickelte/individuelle Software; Standardsoftware; Cloud-Services)?

- Client-Server-Verfahren
- Client (Datenendgerät): Terminal/Netz-PC (ohne Laufwerke/Festplatten) sowie PC (Arbeitsplatz-rechner/Workstation)
- Client-Server-Kommunikation erfolgt über ein offenes Netz
- Datenspeicherung erfolgt auf Server innerhalb der Behörde (hbz)
- Eingesetzte Software (einschließlich Standardverfahren)

Name	Version/Stand/Datum
SuSe Linux	Enterprise Server 15 (x86_64)
Apache Tomcat	9.0.0.M9
Elastic Search	7.5.0 / 25.11.2020
Java SE Runtime	1.8.0_252
Grails	2.5.6 (3.3.11 geplant)
PostgreSQL	11.5 / 25.11.2020
Individuelle Softwareentwicklung: LAS:eR	1.6.5 / 25.11.2020

6.2 IT-Sicherheit (Art. 30 Abs. 1 g DSGVO)

Allgemeine Beschreibung der Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung.

Vertraulichkeit

- Zutrittskontrolle: Der Server steht in einem abgeschlossenen Raum, zu dem nur die Rechenzentrumsbeschäftigte Zugang haben. Außerdem ist jeder einzelne Flur des hbz durch Sicherheits- bzw. Codeschloss gesichert. Nachts sind die Flure durch eine Alarmanlage mit Bewegungsmeldern gesichert. Ferner gibt es einen Sicherheitsdienst
- Benutzerkontrolle: durch Passworteingabe zur Legitimation.
- Zugriffskontrolle: Es werden unterschiedliche Berechtigungen vergeben.

Integrität

- Vermeidung unbefugter oder zufälliger Datenverarbeitung: Die Daten liegen innerhalb einer Datenbank, die nur vom Nutzer der Anwendung beschrieben werden kann.
- Aktualität: Die Software verarbeitet die Daten, die ihr bekannt sind. Für die Aktualität der anwendungsspezifischen Profile etc. ist der Anwender verantwortlich.

Verfügbarkeit

- Der Datenbestand liegt innerhalb der von der Anwendung verwalteten Datenbank vor. Der Software erlaubt das gezielte Auffinden bestimmter, gesuchter Datensätze.
- IEs erfolgen tägliche Backups.
- Die Kommunikation zwischen Nutzer und dem Web-Server ist durchgehend verschlüsselt.

Authentizität

- Dokumentation der Ursprungsdaten und ihrer Herkunft: Die personenbezogenen Daten werden vom Nutzer erzeugt. Damit sind auch die Verarbeitungsschritte nachvollziehbar.

Revisionsfähigkeit

- Siehe dazu die Angaben unter Authentizität.

Transparenz

- Dokumentation ist vorhanden: Dokumentation nach Inbetriebnahme des Systems

6.3 Angabe der zugriffsberechtigten Personen (möglichst Funktionsbeschreibungen und keine Beschäftigtenamen):

(Bitte erläutern Sie kurz den Prozess zur Erlangung und Verwaltung der Berechtigungen oder benennen Sie das detaillierte Berechtigungskonzept)

lfd. Nr. (entspr. Nr. in 5.3.)	zugriffsberechtigte Personen
1, 3	LAS:eR-Nutzer des entsprechenden Kontos selbst sowie Administratoren, die Nutzerkonten anlegen und entfernen sowie Zugriffsberechtigungen vergeben und entziehen können.
2, 4	LAS:eR-Nutzer des entsprechenden Kontos selbst. Ein Zugriff durch Administratoren ist nach Genehmigung der entsprechenden LAS:eR-Nutzer möglich.
5-7	LAS:eR-Nutzer einer konkreten Einrichtung, die den Ansprechpartner anlegen, Institutionen zuordnen und löschen können. Ein Zugriff durch Administratoren ist nach Genehmigung der entsprechenden LAS:eR-Nutzer möglich. Zudem für die Kontaktdaten, die von den Nutzern einer konkreten Einrichtung auf deren Einrichtungsprofil gestellt werden, Leseberechtigung für konsortiale Nutzer von LAS:eR.

6.4 Information der Betroffenen (Art. 12 ff DSGVO)

Wie und wo werden den Betroffenen, deren Daten verarbeitet werden, die Pflichtinformationen über die Datenverarbeitung zugänglich gemacht?

Die Bibliothek belehrt ihre Mitarbeiterinnen und Mitarbeiter, die LAS:eR-Nutzer sind, gemäß Artikel 13 DSGVO und ebenso die Mitarbeiterinnen und Mitarbeiter als Ansprechpartner der Institutionen, die von ihren LAS:eR-Nutzer verwaltet werden.

7 Überwachung

Gemäß Art. 39 DSGVO gehört es zu den Aufgaben des betrieblichen Datenschutzbeauftragten, die Einhaltung der Datenschutz-Grundverordnung sowie anderer Datenschutzvorschriften zu überwachen. Nachfolgend sind die dazu notwendigen Überwachungsmaßnahmen im Einzelnen dokumentiert.

1. Vorgang geprüft Datum: 10.12.20 Namenszeichen: [Signature]
2. Datenschutzfolgeabschätzung erforderlich ☐ Ja ☒ Nein
3. Ergebnis der Datenschutzfolgeabschätzung: _____
4. Konsultation der Aufsichtsbehörde erforderlich: _____ Nein _____
5. Angestoßenen Maßnahmen:

Verantwortlicher: _____

Frist: _____

Datenverarbeitende Stelle

Hochschulbibliothekszentrum des Landes
NRW

Jülicher Straße 6

50674 Köln

Behördlicher Datenschutzbeauftragter

Michael Nelißen

14.12.2020 i.V. C. Baier
Datum Unterschrift

14.12.2020 M. Nelißen
Datum Unterschrift