Die Umsetzung der Datenschutzgrundverordnung (DSGVO) in meiner Bibliothek

Eine Schritt-für-Schritt-Anleitung

Ansprechpersonen:

Barbara Gruber, Martina Stadler, Martin Stieber

Version: 1, 25.04.2018

BÜCHEREIVERBAND ÖSTERREICHS

bvö

Inhaltsverzeichnis

Einleitung

Datenschutz betrifft uns alle – auch wir als Privatpersonen möchten gerne wissen, was mit unseren persönlichen Daten passiert, wo diese gespeichert werden und selbst entscheiden können, ob diese geändert oder gelöscht werden sollen.

Bibliotheken haben in Ihrem Betrieb viele personenbezogene Daten, die es zu schützen gilt. Daher ist die DSGVO auch für Bibliotheken anzuwenden.

In dieser Anleitung versuchen wir möglichst praxisnah darzustellen, wie Sie die Vorgaben der DSGVO umsetzen können.

A. Wie komme ich zu einem Verarbeitungsverzeichnis?

Schritt 1: Wo verwenden wir personenbezogene Daten?

Wozu brauche ich das?

Dieses Verarbeitungsverzeichnis muss die Bibliothek vorweisen, sollte die Datenschutzbehörde kontrollieren oder eine Person Auskunft über die Verwendung ihrer Daten einfordern (Recht auf Auskunft).

Was ist zu tun?

Laden Sie sich das Verarbeitungsverzeichnis des BVÖ herunter:
https://www.bvoe.at/serviceangebote/dsgvo

Füllen Sie als erstes die Felder für den Verantwortlichen, den Kontakt und die zuständige Person aus. Lassen Sie sich vom Umfang der Tabelle nicht abschrecken – wichtig sind in diesem ersten Schritt die **ersten vier Spalten**. Denken Sie darüber nach, ob die hier beschriebenen Anwendungen auch in Ihrer Bibliothek vorkommen. Streichen Sie Datenanwendungen, die in Ihrer Bibliothek nicht vorkommen und ergänzen Sie weitere Anwendungsfälle.

> *Wenn in ihrer Bibliothek Datenanwendungen vorkommen, die in anderen Bibliotheken ebenfalls auftreten können, melden Sie uns diese bitte zurück – wir adaptieren dann die Liste.*

Erläuterungen zu den einzelnen Spalten:

- Name der Anwendung
- Zweck der Anwendung: Eine möglichst kurze und prägnante Beschreibung der Datenanwendung, damit Unbeteiligte sich davon ein Bild machen können.
- Datenkategorien: Welche Daten (oder Datenarten) sind für diese Verarbeitung in Verwendung. (Achten Sie in Folge darauf, dass Sie dann auch nur diese verwenden.)
- Betroffenenkreis: Um die Daten welcher Personen handelt es sich? In den meisten Fällen werden die NutzerInnen (N) betroffen sein, beachten Sie aber, dass Sie auch Daten der MitarbeiterInnen und externer Personen (AutorInnen, Lieferanten usw.) verwalten.

Wir arbeiten an einer Erläuterung zu den einzelnen Datenanwendungen, die Beispiele und weiterführende Überlegungen beinhaltet. Auch hierfür nehmen wir gerne Anregungen entgegen, die wir nach und nach einarbeiten.

Schritt 2: Welche Personen greifen auf welche Daten zu? Was ist der rechtliche Rahmen dafür?

Wozu brauche ich das?

Die DSGVO sieht vor, dass nur Daten erhoben werden dürfen, die für die angegebene Verarbeitung notwendig sind und für die eine rechtliche Grundlage vorliegt. Außerdem gilt auch, dass so wenige Personen wie möglich (sowohl intern als auch extern), Zugriff auf personenbezogene Daten haben sollen.

Was ist zu tun?

Wenden Sie sich nun den nächsten Spalten im Verzeichnis der Datenanwendungen zu.

Unter „Zugriff von“ definieren Sie interne Personengruppen die Zugriff auf die jeweiligen Daten haben (müssen). In der Vorlage sind in fast allen Fällen die Bibliotheksleitung (BL) und die MitarbeiterInnen (MA) genannt. Klären Sie intern die Abläufe und definieren Sie, wer welche Berechtigungen haben darf.

Unter „Empfänger“ sind Personengruppen angeführt, an die Daten zur Verarbeitung weitergegeben werden oder die aufgrund ihrer Tätigkeit Zugriff auf Daten haben.

In der Spalte „Rechtsgrundlage“ adaptieren Sie bitte, auf Basis welcher Vereinbarung oder gesetzlichen Vorgabe die Daten gespeichert werden dürfen. In den meisten Fällen wird es die Benutzungsordnung sein.

Kommen wir nun zur Spalte mit der Bezeichnung „Sensible Daten“. Als sensible Daten bezeichnet man besonders schutzwürdige Daten, mit denen äußerst sorgsam umgegangen werden muss. Dazu gehören zum Beispiel Gesundheitsdaten, politische oder religiöse Überzeugungen, sexuelle Orientierung. In der Tabelle finden Sie eine Spalte mit der Bezeichnung „Sensible Daten“. Setzen Sie ein „J“ für ja, wenn Sie sensible Daten verarbeiten. In der Vorlage ist zum Beispiel die Lesehistorie als solches gekennzeichnet, da anhand der entliehenen Bücher Rückschlüsse auf politische Überzeugungen, Krankheiten etc. möglich sein könnten.

Schritt 3: Wie lange speichern wir personenbezogene Daten?

In der Spalte „Speicherdauer“ tragen Sie ein, wie lange die jeweiligen Daten gespeichert werden (dürfen) bzw. wann diese wieder gelöscht werden müssen. Wichtig ist, dass personenbezogene Daten so kurz wie möglich aber so lange wie nötig gespeichert werden dürfen.

Wozu brauche ich das?

Gerade im digitalen Bereich tendieren viele dazu, Daten anzuhäufen, da es die Speicherkapazitäten zulassen. Sehen Sie diesen Punkt des Verarbeitungsverzeichnisses als Mittel, um regelmäßig gezielt auszusortieren. Vergessen Sie dabei aber nicht auf Ihre Unterlagen in Papierform.

Schritt 4: Welche Maßnahmen setze ich in meiner Bibliothek zum Schutz dieser Daten?

Wozu brauche ich das?

Sie haben Verantwortung für die Daten, die Ihnen die BenutzerInnen, MitarbeiterInnen und andere Personen anvertrauen. Überlegen Sie deshalb, was Sie tun können, um diese Daten zu schützen und vor unbefugtem Zugriff zu sichern.

Man unterscheidet zwischen organisatorischen und technischen Maßnahmen. Diese müssen nach aktuellem Stand der Technik getroffen werden und sicherstellen, dass die Daten verfügbar und nach einem technischen Zwischenfall rasch wiederherstellbar sind. Ein wichtiger Punkt ist auch die Unterweisung der MitarbeiterInnen für den Umgang mit personenbezogenen Daten.

a. Organisatorische Maßnahmen

Regelungen über den Zutritt zu Räumlichkeiten

Stellen Sie sicher, dass die Räumlichkeiten der Bibliothek für die Öffentlichkeit nur zu den Öffnungszeiten oder zu entsprechenden Veranstaltungen mit Publikumsbetrieb zugänglich (unversperrt) sind. Außerhalb der Öffnungszeiten muss sichergestellt werden, dass diese nur von berechtigten Personen, die einen Schlüssel oder eine Zutrittsberechtigung erhalten haben, betreten werden können. Ein Verlust, Diebstahl oder ähnliches ist dem Verantwortlichen umgehend zu melden. Räumlichkeiten, in denen personenbezogene Daten aufbewahrt werden, sind vor unbefugtem Betreten zu schützen. Das gilt auch für einen Serverraum und ein Archiv.

Regelung über den Zugriff auf Dokumente und Unterlagen in Papierform

Dokumente mit personenbezogenen Daten (z. B. die unterschriebene Benutzungserklärung, Rechnungen, Honorarnoten, Unterlagen zur Ausbildung der MitarbeiterInnen,…) sind in verschlossenen Aktenordnern oder Aktenschränken für Unbefugte unzugänglich aufzubewahren.

Werden Unterlagen mit personenbezogenen Daten ausgedruckt, ist außerdem zu beachten, dass während der Öffnungszeiten ein Drucker verwendet wird, der nicht im Publikumsbereich steht. Das betrifft u.a. Mahnschreiben etc…

Entsorgung von Dokumenten / Benutzungserklärungen

Sorgen Sie dafür, dass alle personenbezogenen Daten durch die Entsorgung unlesbar gemacht werden (Schreddern). Verwenden Sie diese auf keinen Fall als „Schmierpapier“. Nehmen Sie die Dokumente nur dann zur Entsorgung mit nach Hause, wenn Sie garantieren können, dass dort keine Verletzung des Datenschutzes passieren kann.

b. Technische Maßnahmen

Technische Maßnahmen zum Sichern von Arbeitsplatzrechnern

Sichern Sie die Arbeitsplatzrechner mit entsprechenden Passwörtern (am besten mit unterschiedlichen Benutzeraccounts für alle Teammitglieder, die die Hierarchie mit unterschiedlichen Rechten für Leitung/Administratoren/Teammitglieder abbilden). Achten Sie auf ein geeignetes, sicheres Passwort (entsprechende Länge, keine Wörter).

Empfohlen wird auch, dass sich bei Verlassen des Arbeitsplatzes nach wenigen Minuten eine Bildschirmsperre aktiviert, die ein erneutes Eingeben des Passworts nötig macht.

Regelmäßige Sicherheits-Updates des Betriebssystems und Aktualisierung des Virenschutz sind dringend anzuraten.

Sicherer Umgang mit personenbezogenen Daten im Bibliotheksprogramm

Auch für den Einstieg in das Bibliotheksprogramm sollten Sie Passwörter mit entsprechenden Zugriffsrechten vergeben. MitarbeiterInnen sollen nur soweit auf jene personenbezogenen Daten zugreifen können, die sie für ihre Arbeit in der Bibliothek benötigen.

Falls Sie statistische Auswertungen vornehmen, sorgen Sie für Pseudonymisierung und Anonymisierung der Daten.

Umgang mit E-Mail

Auch für das E-Mail-Programm brauchen Sie ein Passwort. Die offizielle Bibliotheks-E-Mail-Adresse sollte nicht für privaten E-Mailverkehr verwendet werden. E-Mail-Verkehr ist grundsätzlich zu verschlüsseln. Fragen Sie gegebenenfalls einen Computer-Spezialisten, ob eine Verschlüsselung schon umgesetzt bzw. umsetzbar ist.

Umgang mit Speichermedien (USB-Sticks, externen Festplatten etc.)

Wenn Sie personenbezogene Daten auf externen Speichermedien speichern, stellen Sie sicher, dass die Speichermedien für Außenstehende unzugänglich sind. Dasselbe gilt auch für die Verwahrung von Sicherungskopien und Datenträgern außerhalb der Bibliotheksräumlichkeiten.

Werden die Datenträger für Back-Ups genutzt, sorgen Sie dafür, dass die Daten verschlüsselt aufbewahrt werden.

Sicherer Umgang mit mobilen Endgeräten (Tablet, Mobiltelefon etc.)

Sichern Sie Ihre Geräte mit einem Passwort und einer Bildschirmsperre, sofern personenbezogene Daten darauf gespeichert sind. Der Speicher des Gerätes muss verschlüsselt sein, so wie die Datenübertragung. Verlust, Diebstahl etc. ist sofort dem Verantwortlichen zu melden.

Umgang mit privaten Endgeräten (Home Office am privaten PC, Tablet, Mobiltelefon etc.)

Das Verarbeiten von personenbezogenen Daten auf privaten Endgeräten ist nur nach Genehmigung des Verantwortlichen erlaubt. Es gelten dieselben Sicherheitsbestimmungen wie im Punkt „Sicherer Umgang mit mobilen Endgeräten (Tablet, Mobiltelefon etc.)“ beschrieben.

WLAN/Netzwerkdosen

Stellt die Bibliothek öffentliches WLAN zur Verfügung, muss dieses so gesichert sein, dass kein Zugriff auf das Bibliotheksnetzwerk und somit auf die dort gespeicherten personenbezogenen Daten möglich ist.

Achten Sie darauf, dass auch die Netzwerkdosen im Publikumsbereich entweder deaktiviert sind oder keinen Zugriff auf im Netzwerk gespeicherte Daten ermöglichen.

Entsorgung von ausgeschiedenen Geräten

Sorgen Sie dafür, dass alle personenbezogenen Daten vor Entsorgung fachgerecht gelöscht oder unlesbar gemacht werden (Schreddern). Beim Tausch von Rechnern und Servern ist gegebenenfalls mit der Computerfirma eine Vereinbarung zu treffen.

c. Belehrungspflicht für MitarbeiterInnen

Mitarbeiterschulungen

Sensibilisieren Sie ihre MitarbeiterInnen für das Thema Datenschutz und stellen Sie sicher, dass jede/r weiß wie in der Bibliothek mit personenbezogenen Daten umzugehen ist. Das beginnt bei der Ausstellung der Leser-/Benutzungserklärung, die unzugänglich aufzubewahren ist und reicht bis zum Versenden von E-Mails an BenutzerInnen, das nicht ohne Zustimmung der Person erfolgen darf. Auch für ehrenamtliche MitarbeiterInnen ist es ratsam, sich mit Unterschrift bestätigen zu lassen, dass eine entsprechende Unterweisung stattgefunden hat.

Nutzung von Kommunikationsmitteln

Legen Sie Regeln für die Nutzung von privaten Geräten für dienstliche Zwecke fest und geben Sie diese an die MitarbeiterInnen weiter. Insbesondere ist sicherzustellen, dass diverse (Social-Media-) Apps nicht auf personenbezogene Daten aus dem Arbeitsumfeld (Telefonbuch) können.

Sehr wichtig ist auch, dass eventuelle datenschutzrechtlich relevante Vorfälle oder Sicherheitsverstöße (Datenlecks, Virenbefall, Verlust, Diebstahl) sofort an die Bibliothek (den Verantwortlichen) gemeldet werden.

Umgang mit Passwörtern

Regeln Sie, wie häufig die MitarbeiterInnen ihre Passwörter aktualisieren müssen und wie die Passwörter nicht aufbewahrt werden sollen (in der Schreibtischlade, unter der Tastatur, …)

Löschen der Passwörtern, E-Mails und Ordner von ehemaligen MitarbeiterInnen

Vereinbaren Sie mit Ihren MitarbeiterInnen, welche persönlichen Daten diese beim Ausscheiden vom Bibliotheksserver/-rechner zu löschen haben – und welche Daten für die anderen MitarbeiterInnen zugänglich gespeichert werden müssen.

Achten Sie nach dem Ausscheiden einer MitarbeiterIn, dass innerhalb einer angebrachten Zeitspanne dann die Zugänge (PW) aber auch die E-Mails und persönliche Ordner gelöscht werden.

Sichere Nutzung des Internets

Weisen Sie Ihre MitarbeiterInnen darauf hin, dass sie bei der Benützung von Online-Services achtsam mit personenbezogenen Daten umgehen sollen.

Benutzerrichtlinie für den Arbeitsplatz

MitarbeiterInnen haben beim Verlassen ihres Arbeitsplatzes dafür zu sorgen, dass keine Unterlagen mit personenbezogenen Daten oder Passwörtern für andere einsichtig sind.

Geheimhaltungsvereinbarung

Vereinbaren Sie mit Ihren MitarbeiterInnen schriftlich eine Geheimhaltungspflicht und bewahren Sie diese auf.

Umgang mit persönlichen Lesedaten von BenutzerInnen/Lesehistorie

Um eine Lesehistorie für BenutzerInnen zu speichern braucht es unbedingt eine Einwilligungserklärung. Diese kann bereits bei Einschreibung mit Hilfe der Benutzungserklärung eingeholt werden und muss aufbewahrt werden. Die Lesehistorie und weitere persönliche Daten dürfen nicht an andere BenutzerInnen/Personen weiter gegeben werden.

d. Sonstiges

Umgang mit dem „Recht auf Auskunft“

Definieren Sie, wie die MitarbeiterInnen vorzugehen haben, wenn eine Anfrage zur Auskunft, Richtigstellung oder Löschung von Daten an sie herangetragen wird.

Überprüfung der Einhaltung

Der Verantwortliche prüft regelmäßig die für die Bibliothek festgelegten organisatorischen und technischen Maßnahmen.

B. Praktische Anwendung in der Bibliothek

Sie sollten nun ein fertiges Verarbeitungsverzeichnis haben, das **alle** Datenanwendungen Ihrer Bibliothek aufzeigt. Legen Sie diese so ab (digital oder ausgedruckt), dass Sie es jederzeit wiederfinden und bei Bedarf ändern können.

Mitarbeiterbelehrung

Informieren Sie alle Teammitglieder über die wesentlichen Punkte DSGVO-konformer Bibliotheksarbeit. Welche Daten werden verarbeitet? Wer darf was damit tun? Weisen Sie darauf hin, dass MitarbeiterInnen ihrerseits Recht auf Schutz ihrer personenbezogenen Daten haben.

Lassen Sie Ihre MitarbeiterInnen eine entsprechende Geheimhaltungsvereinbarung unterzeichnen.

Geben Sie keine Auskunft über persönliche Daten an andere Personen weiter ohne eine entsprechende Einwilligungserklärung.

Erstellen Sie sich eine Checkliste dafür, wie Sie mit gewissen Daten umgehen – wie gehen Sie mit Passwörtern um, welcher Drucker darf für den Ausdruck von Mahnungen etc. verwendet werden, welche Unterlagen müssen versperrt werden etc.

Löschen von Daten

Löschen Sie Daten, deren Speicherdauer bereits überschritten wurde. Halten Sie sich dabei an die von Ihnen selbst festgelegten Vorgaben aus dem Verarbeitungsverzeichnis bzw. an die entsprechenden gesetzlichen Vorgaben (Finanzdaten 7 Jahre, urheberrechtlich relevante Vereinbarungen 30 Jahre, Empfehlung für Daten inaktiver LeserInnen: 3 Jahre ab Rückgabe des letzten Mediums für etwaige Schadenersatzforderungen).

Löschen Sie E-Mail-Kontos und persönliche Ordner von ehemaligen MitarbeiterInnen, falls das noch nicht passiert ist.

Leser-Erklärung

Überarbeiten Sie Ihre Leser-Erklärung, um sie DSGVO-konform zu machen (Eine Vorlage für die Leser-Erklärung befindet sich noch in Erstellung und wird zur Verfügung gestellt.). Sie können die Vorlage des BVÖ verwenden oder Teile entnehmen, um Ihre bereits vorhandene Leser-Erklärung anzupassen.

Zwingend enthalten müssen folgende Punkte sein:

- Datenschutzerklärung
- Recht auf Widerruf, Löschung und Auskunft

Fakultativ:

- Einwilligungserklärung für Newletter
- Einwilligungserklärung für Ausleihhistorie
- Einwilligungserklärung für NutzerInnen-Fotos zur Verarbeitung in der Bibliothekssoftware

Benutzungsordnung

Überprüfen Sie die Benutzungsordnung. Achten Sie darauf, dass alle Datenanwendungen die im Rahmen des Verleihbetriebs vorkommen, auch in der Benutzungsordnung erwähnt sind.

C. Checkliste DSGVO

Die folgende Checkliste ermöglicht es Ihnen, Punkte, die Sie bereits erledigt haben, abzuhaken, um so den Überblick zu bewahren.

- ☐ **Rücksprache mit Ihrem Träger:** Bevor Sie Maßnahmen ergreifen, kann eine Rücksprache mit Ihrem Träger nützlich sein. Möglicherweise gibt es von seiner Seite Vorgaben zur Umsetzung der DSGVO.
- ☐ **Verarbeitungsverzeichnis anlegen**
- ☐ **Leser-Erklärung anpassen oder neu erstellen**
- ☐ **Benutzungsordnung überprüfen**
- ☐ **Falls vorhanden: Einwilligungserklärungen für Newsletter etc. anpassen**
- ☐ **Organisatorische und technische Maßnahmen treffen**
- ☐ **Mitarbeiterbelehrung**
- ☐ **Löschen von Daten, deren Speicherdauer überschritten wurde**
- ☐ **Datenschutzerklärung auf der Website anpassen**
- ☐ **Auftragsverarbeiter-Vertrag erstellen**
- ☐ **Recht auf Auskunft:** Ich bin vorbereitet, wenn NutzerInnen oder die Datenschutzbehörde von dem Recht auf Auskunft Gebrauch machen bzw. eine Überprüfung stattfindet?