Datenschutzrecht nach der DSGVO

Rechtsgrundlage für die Erlassung der Verordnung ist der Art. 16 AEUV in Verbindung mit Art 8 GRC.
Ziel ist die Vereinheitlichung des Datenschutzes in der EU gerade auch bei grenzüberschreitenden Aktivitäten.
Wirksamkeitsbeginn ist der 25.5.2018.

I. Sachlicher Anwendungsbereich

Die DSGVO ist anwendbar für ganz oder teilweise automatisierte und nichtautomatisierte Verarbeitung personenbezogener Daten. Nichtautomatisierte Verarbeitungen unterliegen allerdings nur dann dem Schutz der VO, wenn sie in einem Dateisystem gespeichert werden, also eine strukturierte Sammlung vorliegt.

Personenbezogene Daten: alle Informationen, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. Gilt nicht für Verstorbene, es sei denn die Mitgliedsstaaten treffen hier eigene Regelungen. Der Schutz ist nicht auf Unionsbürger beschränkt. Juristische Personen sind allerdings nicht umfasst (In Ö bisher nach dem DSG2000 schon)

Verarbeitung: Erheben, Erfassen, die Organisation, Ordnen, Speichern, Auslesen, Abfragen, Verwenden, Weitergeben, Verarbeiten, Bereitstellen, Abgleichen, Verknüpfen, Löschen.
Ein einzelner Schritt reicht bereits aus, dass die DSGVO anwendbar ist.

Datei: jede strukturierte Sammlung (technologieneutral). Nicht umfasst ist aber z.B. ein Akt. Ausgenommen sind rein persönliche oder familiäre Tätigkeiten (soziale Netze), Fragen der Staatssicherheit und teilweise Handlungen in der Strafverfolgung.

II. Persönlicher Anwendungsbereich

1. Der Verantwortliche hat eine Niederlassung in der EU
2. Hat der Verantwortliche keine Niederlassung in der EU, dann gilt die DSGVO, wenn
   - Waren für Unionsbürger angeboten werden
   - Verhalten von Unionsbürgern beobachtet werden soll.

III. Wann liegen personenbezogenen Daten vor?

1. Verarbeitungskomponente: Frage nach voll- oder teilweise automatisierten oder nichtautomatisierten Daten
2. Inhaltskomponente: Liegen Daten vor, die sich auf einen Menschen beziehen, oder mit einem Menschen in Verbindung gebracht werden können.
3. Identitätskontrolle: Ist ein Mensch identifiziert oder identifizierbar?
   Damit scheiden absolut anonyme Daten (lassen sich auf keinen Menschen beziehen; Mensch ist nicht identifizierbar; Informationen sind so anonymisiert, dass kein Mensch identifizierbar ist) ebenso aus wie relativ anonyme Daten (nach menschlichem Ermessen gilt es als unwahrscheinlich, dass die Daten zu einer bestimmten Person in Verbindung gesetzt werden können) aus.

IV. Grundsätze der Verarbeitung personenbezogener Daten

Sind der sachliche und der persönliche Anwendungsbereich gegeben, so ist das Vorliegen der allgemeinen Grundsätze für die Verarbeitung personenbezogener Daten zu prüfen:

1. Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz:
   -Transparenz: präzise, leicht zugängliche Information für den Betroffenen
   -Rechtmäßigkeit: zulässige Rechtsgrundlage für die Verarbeitung
   -Treu und Glauben: setzt voraus, dass der Betroffene in der Lage ist, vom Vorhandensein einer Verarbeitung zu erfahren und ordnungsgemäß und umfassend über die Bedingungen der Erhebungen informiert wird.
2. Zweckbindungsgrundsatz: Der Erhebungszweck muss festgelegt sein. Daten dürfen nur für diesen Zweck erhoben und verarbeitet werden. Geht man darüber hinaus, so bleiben aber Maßnahmen der Verschlüsselung oder Pseudonymisierung.
3. Datenminimierung: nur sachlich relevante Daten dürfen erhoben werden.
4. Integrität und Vertraulichkeit: Angemessene Datensicherheit und Datenintegrität muss gewährleistet sein.
5. Rechenschaftspflicht: Der Verantwortliche steht für die Einhaltung der Grundsätze ein.

Rechtmäßigkeit der Datenverarbeitung:

1. Einwilligung des Betroffenen für einen oder mehrere Zwecke; Diese Einwilligung muss ohne Zwang und in Kenntnis der Sachlage erfolgen. Stillschweigen, bereits angekreuzte Kästchen oder Untätigkeit sind keine Einwilligung. Einwilligungen können jederzeit ex nunc widerrufen werden.
   Minderjährige können ab 16 eine solche Einwilligung abgeben (kann von den MS bis auf 13 gesenkt werden). Davor müssen die Eltern zustimmen, was der Verantwortliche sicherzustellen hat. (Wie bleibt offen)
2. Vorliegen eines Vertrags oder die Erforderlichkeit der Durchführung vorvertraglicher Maßnahmen auf Anfrage des Betroffenen
3. Vorliegen einer rechtlichen Verpflichtung des Verantwortlichen
4. Schutz lebenswichtiger Interessen der betroffenen Person oder eines anderen Menschen
5. Aufgaben, die im öffentlichen Interesse liegen oder in Ausübung öffentlicher Gewalt erfolgen, die dem Verantwortlichen übertragen wurden.
6. Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten, sofern nicht Interesse oder Grundrechte der betroffenen Person überwiegen.

V. Betroffenenrechte

1. Transparenz: Informationen sind präzise, leicht zugänglich und verständlich sowie in klarer und einfacher Sprache abgefasst und gegebenenfalls durch visuelle Elemente unterstützt.
2. Informationen sind schriftlich (auch elektronisch) und unentgeltlich zu erteilen (außer bei exzessivem Missbrauch)
   Ist unklar, ob der Fragesteller die betreffende Person ist, so kann ein Nachweis der Identität verlangt werden.
3. Informationen sind unverzüglich zu erteilen

VI. Der Auftragsverarbeiter (Dienstleister)

Der Auftragsverarbeiter ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet.
Der Auftragsverarbeiter entscheidet selbst nicht über den Zweck und die Mittel.
Geht er über den vereinbarten Zweck hinaus, so wird er selbst zum Verantwortlichen mit allen rechtlichen Konsequenzen.

Für Auftragsverarbeiter gelten dieselben Grundsätze zur Verarbeitung personenbezogener Daten wie für den Verantwortlichen.
Der Auftragsverarbeiter muss schon vor seiner Auswahl garantieren, dass er geeignete technische und organisatorische Maßnahmen trifft, um die Datenverarbeitung nach den Grundsätzen der DSGVO zu gewährleisten

Im Vertrag zwischen Verantwortlichem und Auftragsverarbeiter muss enthalten sein:

- Gegenstand des Vertrags und Dauer der Verarbeitung
- Art und Zweck der Datenverarbeitung
- Art der personenbezogenen Daten
- Kategorien der betroffenen Daten
- Pflichten und Rechte des Verantwortlichen
- Verschwiegenheitsverpflichtung
- Verpflichtung zu Sicherungsmaßnahmen
- Unterstützungspflicht bei Betroffenenrechten
- Pflichte zur Pseudonymisierung und Anonymisierung
- Regelung über das, was nach Vertragsablauf mit den Daten geschehen soll (Rückgabe; Löschung)
- Überprüfungsrecht des Verantwortlichen

Subauftragsverarbeiter bedürfen der ausdrücklichen Genehmigung durch den Verantwortlichen.

„Hauptberufliche" Auftragsverarbeiter haben einen Datenschutzbeauftragten zu bestellen.

Sowohl der Verantwortliche als auch der Auftragsverarbeiter haben ein Verzeichnis zu führen, in dem alle Verarbeitungstätigkeiten aufgenommen sind.
Ausnahmen:
Der Betrieb hat weniger als 250 Mitarbeiter

a) Und es besteht kein Risiko für die Rechte des Betroffenen
b) Und die Tätigkeit wird nur gelegentlich ausgeübt
c) Oder es liegen keine besonderen Datenkategorien vor (wahrscheinlich sensible Daten).

VIII. Datensicherheit und Datenverlust

Die DSGVO fordert folgende Maßnahmen:

- Risikoanalyse
- Gewährleistung der Vertraulichkeit, Vollständigkeit, Verfügbarkeit und Belastbarkeit der IT-Systeme
- Falls nötig Pseudonymisierung oder Verschlüsselung der personenbezogenen Daten
- Einführung eines Notfallmanagements zur Wiederherstellung der Daten in Folge eines physischen oder technischen Problems
- Audit-Prozess zur Überprüfung der Sicherheitsmaßnahmen

IX. Vorgangsweise & Problemfälle

1. Erstellen eines Verarbeitungsverzeichnisses: Zuerst erhebt man am besten, welchen Geschäftsfeldern nachgegangen wird, für die personenbezogene Daten gespeichert werden.
   z.B.: Entlehnung physischer Bestände: Welche Daten werden benötigt und welche Handlungen werden mit diesen Daten vorgenommen
2. Auf welcher Grundlage speichern wir die Daten, die wir für die Verarbeitungen nach Z 1 gesammelt haben.
   Hier kommen für uns vier relevante Grundlagen in Frage:
   a) Rechtliche Verpflichtung
   b) Vertrag

c) Zustimmung
d) Berechtigtes Interesse

3. Vor allem die Benutzerdaten bedürfen hier einer genaueren Betrachtung:
   a) Studierende: Hier lässt sich argumentieren, dass eine Universitätsbibliothek eine rechtliche Verpflichtung hat, die Studierenden des eigenen Hauses mit Information zu versorgen. Außerdem sind die relevanten personenbezogenen Daten ohnedies bereits von der Universität erhoben worden und werden nur innerhalb des Unternehmens weitergegeben.
   Studierende anderer Bildungseinrichtungen (andere Uni; FH; etc.) werden dadurch aber nicht erfasst. Da mit diesen auch kein vertragliches Verhältnis besteht (ein Leihvertrag kann ja erst abgeschlossen werden, wenn die Daten bereits vorhanden sind) muss hier eine Zustimmung eingeholt werden.
   Studierende, die das Studium beenden, müssen danach, wenn sie zu externen Benutzern werden, eine Zustimmungserklärung abgeben.
   b) Mitarbeiterinnen und Mitarbeiter der Universität:
   Diese Personen stehen in einem vertraglichen Verhältnis zur Universität (mit Ausnahme der Beamten). Die bibliotheksrelevanten Daten können daher m.E. ohne ausdrückliche Zustimmung von uns übernommen werden, wenn die Universität alle Mitarbeiter darüber in Kenntnis setzt.
   Problematisch ist allerdings, dass viele Dienstverhältnisse an Universitäten auf recht kurze Zeit angelegt sind. Diesem Umstand muss entweder im Dienstvertrag Rechnung getragen werden, oder es muss von diesen Personen eine Zustimmung eingeholt werden.
   c) Externe: Diese Personengruppe steht weder in einer rechtlichen noch einer vertraglichen Beziehung zur Universität, weshalb hier jedenfalls eine Zustimmungserklärung einzuholen ist.
4. Zustimmungserklärung: Ein immanenter Grundsatz der DSGVO ist jener der Datenminimierung. Deshalb ist die Zustimmungserklärung so zu formulieren, dass möglichst wenige Daten erhoben und verarbeitet werden. Dem Unterzeichner muss klar sein, wozu hier zugestimmt wird.
   Besonders wichtig scheint mir hier ein möglichst einheitliches Vorgehen in der Frage, wie lange die Daten nach Ausscheiden aus der Institution oder bei Inaktivität gespeichert bleiben, zu sein. Ich empfehle den Universitäten sich hier abzustimmen!
5. Fernleihe: Nach dem Grundsatz der Datenminimierung sind nur Daten weiterzugeben, die für die Geschäftsbesorgung notwendig sind. Die empfangende Bibliothek würde somit zum Auftragsverarbeiter.
   Ich sehe grundsätzlich keine Notwendigkeit der Weitergabe der Entlehnerdaten, da die Haftung für Verlust oder Beschädigung bei der entlehnenden Bibliothek liegt und diese sich im Innenverhältnis schadlos halten wird.
6. Entlehnhistorie: Nach dem Grundsatz der Datenminimierung ist die Speicherung der Entlehnhistorie nicht vertretbar, es sei denn, es liegt eine Zustimmung vor. Es ist m.E. nicht vertretbar eine solche Zustimmung in die Datenschutzerklärung zu schreiben und die generelle Benutzbarkeit der Bibliothek davon abhängig zu machen. Es empfiehlt sich hier ExLibris zu drängen, eine individuelle Aktivierbarkeit dieser Funktion zu programmieren.
   Die Entlehnhistorie ist nur so lange aufzuheben, wie es für die Bearbeitung notwendig ist. Es kann z.B. durchaus mit bis zu zwei Wochen argumentiert werden, wenn Rückstellungen in einer Magazinsbibliothek etwas dauern und man Exemplare auf Beschädigungen überprüfen will.
   Eine weitere Speicherung dieser Daten beispielsweise aus statistischen Gründen ist nur anonymisiert zulässig.
7. Gebührenvorgänge: Gebührenvorgänge sollten so lange aufgehoben werden, wie dies gesetzlich vorgeschrieben oder notwendig ist. In der Regel werden hier sieben Jahre anzusetzen sein. Dies kann aber auch im Buchhaltungssystem der jeweiligen Universität erfolgen
8. Schenkungen: Bilden ein vertragliches Verhältnis. Hier können die Daten aus vertraglichem und rechtlichem Grund aufbewahrt werden. Ich meine, dass hier die reguläre Verjährungsfrist von 30 Jahren zum Tragen kommt.

9. Lieferantendaten: Innerhalb einer Institution ist das Speichern von Lieferantendaten kein Problem und auf Grund einer Vertrages erlaubt (Vorvertrag genügt). Das Problem, dass Lieferantendaten jeder Institution auch für andere Institutionen einsehbar sind, sollte ja mit dem Start der NZ in Alma behoben sein.
10. Archivfragen: Universitätsarchive sind darauf ausgelegt, Daten langfristig aufzubewahren.
    a) Studierende: Die Daten derjenigen Studierenden, die einen akadamischen Grad verliehen bekommen haben, sind jedenfalls aufzubewahren, da die rechtliche Verpflichtung besteht, den positiven Studienerfolg nachweisen zu können.
    Schwieriger ist dies bei Studierenden, die nicht abgeschlossen haben. Hier kann nur das berechtigte Interesse der Universität ins Treffen geführt werden, diese Daten zu archivieren. In diesem Fall muss das Interesse des Archivs zumindest gleichrangig sein mit den Datenschutzinteressen der archivierten Person.
    Jedenfalls ist der Grundsatz der Datenminimierung zu beachten. Daraus folgt, dass in beiden Fällen darauf zu schauen ist, welche Daten für spätere Forschungszwecke relevant sind. Nur diese dürfen archiviert werden.
    Mitarbeiterinnen: die Archivierung von Mitarbeiterdaten kann sozialrechtlich geboten sein. Ansonsten kann auch hier berechtigtes Interesse geltend gemacht werden unter Berücksichtigung der Datenminimierung.