Inhalt

1. Datenschutz und Informationelle Selbstbestimmung

1983 haben die Richter am Bundesverfassungsgericht im sogenannten „Volkszählungsurteil“ das Recht auf informationelle Selbstbestimmung definiert. Sie leiteten dieses neue Grundrecht ab aus den bestehenden Grundrechten in Art.2 Grundgesetz „Jeder hat das Recht auf freie Entfaltung seiner Persönlichkeit.“ und Art.1 Grundgesetz „Die Würde des Menschen ist unantastbar“. Die Richter formulierten das Recht folgendermaßen: „Das Grundrecht gewährleistet insoweit die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen“. Dies war zwar nicht das erste Auftauchen von Datenschutz, aber der Meilenstein, der Datenschutz im Interesse der Bevölkerung verankerte.

Der Hintergrund der Klage war, dass viele Bürger und Bürgerinnen nicht mit der vom Staat vorgenommenen Datenerfassung im Rahmen der damaligen Volkszählung einverstanden waren und Verfassungsbeschwerde eingelegt hatten. Im Rahmen der elektronischen Datenverarbeitung können viel mehr Daten verarbeitet und miteinander verknüpft werden, als dies vorher möglich war. Mit den heutigen Möglichkeiten ist noch einmal deutlich mehr möglich an Informationsgewinnung über einzelne Personen.

Die Europäische Union hat sich zum Datenschutz als Grundrecht im Jahr 2009 in der Charta der Europäischen Grundrechte bekannt und durch die Datenschutz-Grundverordnung einen ab dem 25. Mai 2018 europaweit geltenden und weitgehend einheitlichen Rechtsrahmen für die Verarbeitung personenbezogener Daten geschaffen.

Anders als der Name vermuten lässt, geht es somit nicht um den Schutz der Daten an sich, sondern um den Schutz des Individuums im Zusammenhang mit der Verarbeitung von Daten durch den Staat und Private, die Rückschlüsse auf persönliche, soziale und wirtschaftliche Verhältnisse der einzelnen Person zulassen. Der gesetzliche Schutz ist nötig, weil die Einzelperson sich gegen den Staat und verarbeitende Unternehmen sonst kaum gegen unerwünschte Verarbeitungen zur Wehr setzen könnte. Dies zeigt sich eindrücklich an der Dominanz von einigen wenigen Internetgiganten, deren Hauptgeschäftsmodell die Verknüpfung und Vermarktung von Informationen über Einzelpersonen ist. Der Bedarf an diesem Grundrecht besteht somit heute mehr denn je, wobei auch die besonderen Erfordernisse einer modernen Informationsgesellschaft beachtet werden müssen. Die Aufgabe des Datenschutzes ist somit nicht das Rad der Zeit zurückzudrehen, sondern den Menschen (wieder) mehr Kontrolle und somit mehr Souveränität im Umgang mit ihren persönlichen Daten zu geben.

2. Grundsätze der Verarbeitung personenbezogener Daten

Die folgenden sechs Grundsätze der Verarbeitung personenbezogener Daten müssen bei jeder Verarbeitung personenbezogener Daten eingehalten werden:

Rechtmäßigkeit:
Jede Verarbeitung personenbezogener Daten benötigt eine Legitimation (dazu später mehr!) Das heißt: jede Verarbeitung personenbezogener Daten ist untersagt, es sei denn, sie ist gesetzlich oder durch ausdrückliche Einwilligung der betroffenen Person erlaubt!

Zweckbindung:
Die Verarbeitung von personenbezogenen Daten ist immer mit einem bestimmten Zweck verknüpft, z.B.

- Bewerbungsverfahren auf einen Studienplatz,
- Konkretes Forschungsvorhaben,
- Studierendenverwaltung,
- Durchführung eines Beschäftigungsverhältnisses.

Erst wenn der Zweck oder mehrere Zwecke der Verarbeitung festgelegt sind, kann überprüft werden, ob die Datenverarbeitung genau zu diesem/n Zweck/en gesetzlich oder durch Einwilligung der Betroffenen erlaubt ist (also rechtmäßig ist). Die Zweckfestlegung hat aber noch eine weitere Funktion: an die/den festgelegte/n Zwecke ist die weitere Verarbeitung der Daten grundsätzlich gebunden. Somit dürfen die vorhandenen Daten nicht einfach so für einen anderen Zweck verarbeitet werden. Nur wenn die Verarbeitung für den anderen Zweck explizit erlaubt ist oder die betreffende Person in diese andere Verarbeitung eingewilligt hat, darf dies erfolgen. So müssen z.B. die im Rahmen der Bewerbung auf den Studienplatz angegebenen Daten nicht noch einmal neu für die Immatrikulation angegeben werden, weil die Hochschule laut Gesetz die Bewerbungsdaten für die Immatrikulation nutzen darf. Der oder die Betroffene muss nur noch die ergänzenden Informationen angeben.

Datensparsamkeit:

Es sollen nur die personenbezogenen Daten verarbeitet werden, die erforderlich sind, um die Verarbeitung durchführen zu können. Beispiel: Die Erfassung der Teilnahme an einer Lehrveranstaltung z.B. durch eine Teilnehmerliste ist nur dann erforderlich, wenn eine in der Prüfungsordnung verankerte Anwesenheitspflicht existiert.

Richtigkeit:
Personenbezogene Daten müssen richtig, aktuell und vollständig sein. Dies muss der für die Datenverarbeitung Verantwortliche sicherstellen.

- Wenn in der Prüfungsakte Angaben zu Prüfungen fehlen, unvollständig oder falsch sind, ist ein Anspruch auf Vervollständigung und Korrektur auszuführen.
  Ist z.B. durch einen Schreibfehler die Note falsch in die Prüfungsakte aufgenommen worden, besteht ein Anspruch auf Korrektur.
  Der Korrekturanspruch aus dem Datenschutzrecht gilt aber nicht für die Bewertung selbst.
- Ihnen fällt auf, dass Ihre Anschrift falsch hinterlegt wurde. Auch in diesem Fall haben Sie einen Anspruch auf Korrektur der falschen Anschrift.

Speicherbegrenzung:
Wenn personenbezogene Daten nicht mehr gebraucht werden, z.B. weil die Verarbeitung erfolgreich durchgeführt wurde, müssen sie gelöscht werden.

- Alte Bankverbindungen bei Lastschriften werden nicht mehr benötigt, wenn eine neue mitgeteilt wurde.
- Alte Anschriften werden nicht mehr benötigt.

Vertraulichkeit und Integrität:
Wenn personenbezogene Daten verarbeitet werden, muss sichergestellt werden, dass niemand außer den zur Verarbeitung befugten Personen und die Betroffenen selbst die Daten sehen können. Gleiches gilt für die Möglichkeit zur Veränderung der Daten.

Im Hinblick auf die Einhaltung der genannten Grundsätze besteht eine Rechenschaftspflicht der Hochschule. Es reicht somit nicht aus, dass die Grundsätze eingehalten werden. Die Hochschule muss dies nachweisen können und hierfür prüffähige Dokumentationen führen und bereithalten.

Transparenz
Jede betroffene Person soll Informationen über die Verarbeitung erhalten und wissen, warum welche Daten von ihr verarbeitet werden.

2.1 Was sind denn jetzt personenbezogene Daten?

Alle auf eine einzelne Person beziehbare Daten. Entscheidend ist dabei, ob man selbst oder unter Zuhilfenahme von Informationen Dritter (Internet- und andere Anbieter, Ergebnisse polizeilicher Ermittlungen) oder anderer sachlichen Informationen (Kennzeichen) die betreffende Person zweifelsfrei identifizieren kann.

Beispiele:

- Name, Vorname (u.U. nur in Zusammenhang mit weiteren Daten wie z.B. Geburtsdatum)
- Kreditkartennummer, IBAN (Kreditkartenunternehmen, Bank)
- Telefonnummer (Selbst über Inverssuche oder über den Telefonanbieter)
- Pseudonyme wie Matrikelnummer, Kfz-Kennzeichen, Chipkartennummer, Personalnummer, ID, Benutzername, und alle weiteren Merkmale, die sich über eine bestehende Zuordnungstabelle einer Person zuordnen lassen
- Foto, das verwendet werden könnte, um eine Person aus einer Gruppe zu identifizieren
- Blutprobe (enthält die DNA der Person, mit der sie sich zumeist eindeutig identifizieren lässt)
- IP-Adresse (ggf. z.B. zusammen mit dem Zeitpunkt der Nutzung über den Internet-Anbieter auf eine bestimmte Person beziehbar)

Der Personenbezug erfasst auch alle weiteren Daten, die mit diesem identifizierenden Merkmal verbunden sind, so dass mit dem Merkmal der gesamte Datensatz einen Personenbezug aufweist.

Beispiel:

- Das Geburtsdatum alleine ist kein personenbezogenes Datum. Wird es jedoch mit Vor- und Nachname der betroffenen Person verknüpft, trägt es sogar zur Identifizierbarkeit der betreffenden Person bei. Folglich ist der gesamte Datensatz personenbezogen.

Aber auch andere Daten können einen Personenbezug aufweisen, insbesondere wenn sich aus einer Verknüpfung mehrerer Informationen eine Person identifizieren lässt:

Beispiele:

- Der erste Kanzler der BRD war verheiratet. Hier ergibt sich aus der Verknüpfung und dem dazugehörigen Allgemeinwissen, dass es sich dabei um Konrad Adenauer handelt.
- Der Rektor der Universität Musterstadt ordnete am 10.09.2008 an... Auch hier ergibt sich der Personenbezug aus der Verknüpfung von Funktion und Zeitpunkt und der öffentlichen Verfügbarkeit der Information, welche Person die Funktion zu dieser Zeit bekleidet hat.

Wird eine sehr kleine Gruppe unter 5 Personen betrachtet, kann ein besonders herausstechendes Merkmal (Kennzeichen) zu einem Personenbezug führen.

Beispiel:

- Ein Studiengang hat nur 4 Studierende. Zu diesem Studiengang wird neben den Leistungen nur das Alter der teilnehmenden Studierenden zu statistischen Zwecken dargestellt. Wenn nun z.B. eine Person deutlich älter ist, können die Leistungen dieser Person eindeutig von Personen zugeordnet werden, die diese Gruppe kennen.

Es gibt natürlich auch Daten, die grundsätzlich keinen Personenbezug aufweisen, insbesondere wenn sie ohne jeglichen Kontext auftauchen:

Beispiele:

- Gehalt, insbesondere bei Tarifverträgen. Im Einzelfall (insbesondere bei Besoldungsgruppen, denen nur wenige Personen angehören) kann aber über das Gehalt und die geringe Größe der Gruppe (siehe eben) ein Personenbezug hergestellt werden.
- Geburtsjahr

2.2 Optional – Schutzbedarf von personenbezogenen Daten

Es gibt auch besondere Kategorien personenbezogener Daten. Diese sind gesetzlich besonders geschützt.
Auch andere personenbezogene Daten können sehr sensibel sein und verlangen einen hohen Schutzbedarf.

Bei den besonderen Kategorien personenbezogener Daten handelt sich um Daten aus denen folgendes hervorgeht:

- Rassische und ethnische Herkunft
- Politische Meinung
- Religiöse oder weltanschauliche Überzeugungen
- Gewerkschaftszugehörigkeit
- Genetische und biometrische Daten (Blutprobe, Fingerabdrücke)
- Gesundheitsdaten
- Daten zum Sexualleben oder der sexuellen Orientierung.

Neben den besonderen Kategorien von personenbezogenen Daten gibt es weitere Informationen, die einem besonderen grundrechtlichen Schutz unterliegen:

- Inhalte aus nichtöffentlichen Konversationen (Schutz des nichtöffentlich gesprochenen Wortes): z.B. darf man den Inhalt einer Unterredung nicht einfach heimlich aufzeichnen.
  Hierbei handelt es sich sogar um eine Straftat.
- Fernmelde- und Postgeheimnis: Die Inhalte von Postsendungen und aus Kommunikationsverbindungen unterliegen einem besonderen Schutz. Unter Umständen kann man sich strafbar machen, wenn man Inhalte abhört und diese Dritten weitergibt. Geschützt sind vom Fernmeldegeheimnis auch die Informationen wer mit wem wann wie lange und von welchem Ort kommuniziert hat [16]. Das gilt auch für private E-Mails und für E-Mails einer personenbezogenen Hochschul-E-Mailadresse wenn auch die private Nutzung erlaubt ist.
- Bilder (Recht am eigenen Bild): Ohne Einverständnis der betroffenen Person dürfen Bilder nicht einfach verbreitet werden. Das gilt übrigens auch für soziale Medien. Ausnahmen gibt es für Bilder der Zeitgeschichte, Bilder in denen Landschaften oder sonstige Örtlichkeiten im Vordergrund stehen, Bilder von Versammlungen und für die Kunst.

Die genannten Daten und Informationen sind besonders geschützt. Für sie gelten besondere Anforderungen an die Rechtmäßigkeit der Verarbeitung. Bitte wenden Sie sich bei Umgang mit solchen Daten im Zweifel an den Datenschutzbeauftragten/die Datenschutzbeauftragte.

3. Gesetzliche Grundlagen

Weil die Verarbeitung personenbezogener Daten grundsätzlich verboten ist, ist es wichtig zu prüfen, ob im konkreten Fall eine der folgenden gesetzlichen Erlaubnisse nach Art. 6 Abs. 1 DSGVO greift:

1) Die Verarbeitung personenbezogener Daten ist für die Erfüllung eines Vertrages, den die von den Daten betroffene Person geschlossen hat oder für vorvertragliche Maßnahmen, die die von den Daten betroffene Person angefragt hat, erforderlich, z. B.:

- Beschäftigungsverhältnis
- Bestellung beim Lieferservice
- Eröffnung Bankkonto
- Teilnahme an einem Gewinnspiel

2) Der Verantwortliche unterliegt einer rechtlichen Verpflichtung, die Daten zu verarbeiten:

- Pflicht zur Meldung von Daten über Beschäftigte und Studierende an die Krankenkasse
- Anschrift und Personendaten bei der Kfz-Anmeldung
- Identifikationsdaten bei der Aktivierung einer SIM-Karte

3) Die Verarbeitung erfolgt für die Wahrnehmung einer Aufgabe im öffentlichen Interesse. Hierunter fallen im Prinzip alle im Landeshochschulgesetz genannten Aufgaben der Hochschule. Die der Hochschule übertragenen Aufgaben sind in § 3 HG Abs. 2- 7 NRW definiert. Die Hochschule darf die zur Wahrnehmung dieser Aufgaben erforderlichen Daten verarbeiten, z.B.:

- Bewerbung und Einschreibung an der Hochschule
- Prüfungsverwaltung
- Drittmittelverwaltung bei Forschungsprojekten

4) Die betroffene Person hat in die Datenverarbeitung eingewilligt (dazu im Einzelnen auch unter 3.2). Dann dürfen die Daten der Person im Umfang der erteilten Einwilligung verarbeitet werden, z.B.:

- Anmeldung zu einem Newsletter
- Registrierung im Alumni-Netzwerk
- Teilnahme an einem Forschungsvorhaben

5) Der Verantwortliche hat ein berechtigtes Interesse an der Verarbeitung, wobei das Interesse des oder der Betroffenen an seinem oder ihren Grundrechtsschutz nicht überwiegen darf.

Eine Datenverarbeitung aufgrund eines berechtigten Interesses setzt somit immer eine Abwägung im Einzelfall zwischen dem Interesse an der Verarbeitung und den Interessen der Betroffenen voraus. Außerdem ist eine Verarbeitung aufgrund eines berechtigten Interesses gänzlich ausgeschlossen, soweit die Hochschule als Behörde handelt. In der Praxis wird es an der Hochschule Fälle des berechtigten Interesses kaum geben, weil die Hochschule in der Regel die Daten zur Erfüllung ihrer gesetzlichen Aufgaben in Lehre und Forschung verarbeitet (siehe oben Nr. 3). Es verbleiben somit nur wenige Bereiche wie z.B. das Hochschulmarketing und die Wahrnehmung berechtigter

Sicherheitsinteressen übrig, die jeweils nur mittelbar der Aufgabenerfüllung dienen, für die es keine konkreten Erlaubnisnormen gibt und die jeweils eine Abwägung im Einzelfall voraussetzen.

3.1 Die Einwilligung als Rechtsgrundlage mit besonderen Voraussetzungen

Eine Einwilligung wird benötigt, wenn die Verarbeitung von personenbezogenen Daten nicht über eine andere Rechtsgrundlage abgedeckt ist. Eine Einwilligung kann jederzeit – mit Wirkung für die Zukunft – widerrufen werden. Sie ist damit nicht geeignet für Verarbeitungen, denen eine jederzeitige Widerrufsmöglichkeit schaden könnte, weil die Verarbeitung mit dem Widerruf unverzüglich beendet werden muss und bereits gespeicherte personenbezogene Daten zu löschen sind. Auf die Datenverarbeitung angewiesene Dienstleistungen wie z.B. Newsletter können nach erfolgtem Widerruf nicht mehr angeboten werden. Auf diese möglichen Folgen muss der oder die Betroffene bei Erteilung der Einwilligung hingewiesen werden.

Aufgrund der gegebenenfalls weitreichenden Folgen für den oder die Betroffenen unterliegen Einwilligungen besonderen Anforderungen:

- Freiwilligkeit: Dies setzt voraus, dass eine transparente und verständliche Information über den Zweck, die Art (z. B. erheben, speichern etc.) und den Gegenstand (genaue Angabe der personenbezogenen Daten, die verarbeitet werden) der Verarbeitung vor der Einwilligung erfolgt und der oder die Betroffene frei und ohne Zwang sich dafür oder dagegen entscheiden kann. So muss z. B. im Beschäftigungsverhältnis die Freiwilligkeit stets hinterfragt werden, weil ein Beschäftigter oder eine Beschäftigte gegenüber dem Arbeitgeber ggf. nur einwilligt um dessen Erwartungshaltung gerecht zu werden oder weil er oder sie ansonsten Nachteile befürchtet.
- Es gibt keine Formvorgabe. Allerdings muss derjenige, der die Einwilligung einholt, diese im Zweifel auch nachweisen können. Dabei ist z.B. zu beachten, dass Telefongespräche oder das nichtöffentlich gesprochene Wort nicht einfach so zu Beweiszwecken aufgezeichnet werden dürfen. Im Beschäftigungsverhältnis bedarf die Einwilligung in der Regel immer der Schriftform.
- Der Widerruf der Einwilligung muss so einfach sein, wie die Erteilung der Einwilligung selbst. Es darf somit nicht sein, dass eine Einwilligung zwar per Mail erteilt werden kann, der Widerruf dann aber einen eingeschriebenen Brief voraussetzt.
- Der Widerruf ist jederzeit mit Wirkung für die Zukunft möglich. Ein Widerruf kann die Rechtmäßigkeit von in der Vergangenheit erfolgten Verarbeitungen nicht beseitigen. Die einwilligende Person muss hierauf in den Informationen zur Einwilligung hingewiesen werden. Die in der Vergangenheit gespeicherten personenbezogenen Daten sind nach dem Widerruf zu löschen und stehen für die Zukunft nicht mehr zur Verfügung.

3.2 Optional - Gesetze und ihr Verhältnis zueinander

Die Datenschutz-Grundverordnung (DSGVO) ist europaweit direkt anwendbar. Sie gilt als Verordnung unmittelbar in jedem Mitgliedsstaat der EU, daher müssen keine nationalen Gesetze die Verordnung in nationales Recht umsetzen. Trotzdem gibt es weiterhin nationale Regelungen zum Datenschutz. Das liegt darin begründet, dass die DSGVO nicht umsonst Grundverordnung heißt, weil mit ihr eine grundlegende Harmonisierung erfolgt, die nicht alle Spezialmaterien umfassen kann. Deshalb gibt es so genannte „Öffnungsklauseln“ die es den Mitgliedstaaten erlauben, in bestimmten Bereichen durch Anpassungsgesetze zur DSGVO weiterhin eigene Regelungen zu treffen.

Dabei handelt es sich beispielsweise um

- Datenverarbeitung bei Behörden und öffentlichen Stellen der Mitgliedstaaten
- Datenverarbeitung im Rahmen des Beschäftigungsverhältnisses
- Einschränkung der Rechte betroffener Personen (nächster Abschnitt)
- ...

Der deutsche Gesetzgeber hat diese Öffnungsklauseln mit dem neuen Bundesdatenschutzgesetz, sowie auf Landesebene mit den Landesdatenschutzgesetzen genutzt. Die Landesdatenschutzgesetze (DSG NRW in Nordrhein Westfalen) gelten nur für öffentliche Stellen der Länder (inkl. Hochschulen), das Bundesdatenschutzgesetz (BDSG) für öffentliche Stellen des Bundes sowie nichtöffentliche Einrichtungen wie Unternehmen und private Vereine.
Darüber hinaus gibt es für spezielle Materien noch Gesetze mit Regelungen zum Datenschutz, die sich ebenfalls auf die Öffnungsklauseln stützen. Hierbei handelt es sich z.B. um das Landeshochschulgesetz mit Regelungen zur Verarbeitung von Daten durch Hochschulen, das Telekommunikations- Telemedien- Datenschutzgesetz (TTDG) mit Bestimmungen zur Datenverarbeitung von Telekommunikationsanbietern, die Sozialgesetzbücher zur Verarbeitung von Sozialdaten im Rahmen der sozialen Sicherungssysteme.

5. Technische und organisatorische Maßnahmen

Der Verantwortliche muss angemessene technische und organisatorische Schutzmaßnahmen implementieren, um die Sicherheit der Verarbeitung zu gewährleisten.
Die Angemessenheit verlangt hierbei nicht durchgängig den höchstmöglichen Schutz, sondern die Gewährleistung eines dem Risiko angemessenen Schutzes. Hierbei kommt es auf mehrere Faktoren an, wie:

- Art, Umfang, Umstände und Zwecke der Verarbeitung
- Eintrittswahrscheinlichkeiten und Schwere der Risiken
- Stand der Technik
- Implementierungskosten

Beispiele für Maßnahmen:

- Rollen- und Rechtekonzepte
- Verschlüsselung und Pseudonymisierung
- Backup, Redundanz und Lastverteilung
- Notfallpläne
- Audit- und Überprüfungsverfahren

Technische und organisatorische Maßnahmen für die Mobile Arbeit
Der Datenschutz steht Mobiler Arbeit nicht entgegen. Aufgrund der Flexibilität des Arbeitsortes und des möglicherweise notwendigen Transportes von dienstlichen Unterlagen sind jedoch besondere technische und organisatorische Maßnahmen erforderlich, um die Persönlichkeitsrechte der Menschen, deren Daten in der Mobilen Arbeit verarbeitet werden, zu schützen. Dabei gilt: je sensibler die verarbeiteten personenbezogenen Daten sind, desto stärker sind sie zu schützen. Die Entscheidung trifft der Dienstvorgesetzte in Abstimmung mit den MitarbeiterInnen. Technische Maßnahmen bei der mobilen Arbeit können sein:

- clean desk nach Ende des Arbeitstages;
- Sperrung des mobilen Gerätes bei Verlassen des Arbeitsplatzes;
- Telefongespräche/Videokonferenzen nur dort, wo unbefugte Personen nicht mithören können;
- Sichtschutzfolie auf Bildschirmfläche;
- Anbindung an das Hochschulnetz mit verschlüsselter VPN Verbindung nach Stand der Technik;
- Datenspeicherung nur auf über die VPN-Verbindung erreichbaren Netzlaufwerke der Hochschule;
- keine Nutzung öffentlicher Wi-Fi-Hotspots;
- Mobiles Arbeiten nur an von dem Dienstherrn vorkonfigurierten Dienstrechnern/mobilen Geräten;
- Nutzung Dienstrechner nur zu dienstlichen Zwecken;
- kein Anschluss privater USB-Sticks an Dienstrechner;
- Transport des mobilen Gerätes nur in gesperrtem Zustand;
- Dokumentenausdruck nur an dem Büroarbeitsplatz;
- Notwendige Papierunterlagen nur in verschlossenem Behältnis transportieren;
- Transport der notwendigen Papierunterlagen ohne Unterbrechung des Weges von/zum Mobilen Arbeitsort (keine Zwischenstopps zum Einkaufen/Tanken etc.);

- Entsorgung von Papierunterlagen nur am Büroarbeitsplatz oder an dem Mobilen Arbeitsort durch Aktenvernichter mit mind. Sicherheitsstufe 5 nach DIN 66399;
- Schulung/Informationen der MitarbeiterInnen über die datenschutzrechtlichen und IT sicherheitstechnischen Regelungen mobiles Arbeiten;
- Keine Weiterleitung von privaten/dienstlichen E-Mails an dienstliche/privaten E-Mail-Konten.

5.1 Verletzung des Schutzes personenbezogener Daten

Sollte eine Verletzung des Schutzes personenbezogener Daten bekannt werden, so muss dies gemeldet werden. Zunächst muss eine interne Meldung erfolgen. Dann wird dort entschieden, ob die Datenschutz-Aufsichtsbehörde und zusätzlich die von der Schutzverletzung (oder auch Datenpanne) betroffenen Personen direkt zu informieren sind.

Beispiele für Schutzverletzungen:

- Ein unverschlüsselter Datenträger mit Prüfungsergebnissen oder personenbezogenen Forschungsinterviews geht verloren.
- Eine unverschlüsselte E-Mail mit Prüfungsdaten wird versehentlich an einen falschen Empfänger oder eine falsche Empfängerin geschickt.
- Durch einen Fehler sind die Daten von Studierenden auf einer Datenbank nicht geschützt und durch Person im Internet einsehbar
- Eine für diese personenbezogenen Daten unbefugte Person kann den Bildschirm eines Sachbearbeiters oder einer Sachbearbeiterin einsehen, während diese(r) personenbezogene Daten verarbeitet (z.B. in der Bahn, aber auch im Büro ist dies möglich)
- Zugangskennungen zu Systemen, mit denen personenbezogene Daten verarbeitet werden, werden Dritten bekannt

6. Ansprechpartner und Datenschutzmanagement

Es obliegt dem oder der DSB, die Einhaltung der gesetzlichen Vorgaben zur Verarbeitung personenbezogener Daten intern zu beobachten und zu kontrollieren.
Da der oder die DSB sich schlecht selbst kontrollieren kann, müssen andere Stellen innerhalb der Organisation den Datenschutz umsetzen. Der oder die DSB unterstützt diese datenverarbeitenden Stellen in der Organisation beratend. Außerdem ist er oder sie Ansprechpartner für betroffene Personen und die Datenschutz-Aufsichtsbehörde.

Die Gesamtverantwortung für die Umsetzung des Datenschutzes in einer Organisation trägt deren Leitung, also das Präsidium der Hochschule Bochum. Da dieses jedoch nicht alle Verarbeitungen in der Hochschule überblicken kann, müssen die jeweils fachlich für die jeweilige Verarbeitung verantwortlichen Personen einbezogen werden. Um eine nachhaltige und inhaltlich richtige Umsetzung zu gewährleisten, müssen Strukturen zur Unterstützung und Beratung geschaffen werden. Neben dem oder der behördlichen Datenschutzbeauftragten kann dies z.B. eine zentrale Beratungsstelle zu technischen oder rechtlichen Fragestellungen sein.

Zudem können Datenschutzkoordinatoren und -koordinatorinnen als dezentrale Stellen mit fachlichem Hintergrundwissen Teil dieser Struktur sein. Diese Koordinatoren können die vielen kleinen Fragen der Beschäftigten klären und als erste Ansprechstelle bereitstehen. Für alle schwierigen und rechtlich komplexen Fragen ist der oder die Datenschutzbeauftragte zuständig. Die Koordinatoren dienen dem oder der Datenschutzbeauftragten zudem als Gesprächspartner für datenschutzrechtliche Strukturen in den Bereichen und helfen ihm oder ihr, datenschutzrechtliche Vorgaben in den Bereichen umzusetzen.

7. Zusammenarbeit mit Dritten

Besondere Vorschriften gelten, wenn personenbezogene Daten - für deren Verarbeitung die Hochschule verantwortlich ist - im Auftrag der Hochschule von Externen verarbeitet werden und die Verarbeitung bei den Externen weisungsgebunden erfolgt. Dies ist z.B. der Fall, wenn ein Softwareprodukt beschafft wird, das auf einem Server des Anbieters gespeichert ist und von der Hochschule über eine Cloud genutzt wird. Das Dienstleistungsunternehmen darf mit diesen Echtdaten nicht machen was er will, sondern muss den Anordnungen der Hochschule Folge leisten. Auch eine Auftragsverarbeitung liegt z.B. vor, wenn ein Copyshop mit der Versendung von Einladungen beauftragt wird und dieser hierfür eine Liste mit Namen und Anschriften erhält. Zwar erledigt er diesen Auftrag selbständig, unterliegt in Bezug auf die Verarbeitung dieser Daten aber ebenfalls den Weisungen der Hochschule als Auftraggeber. Es gelten die folgenden Anforderungen:

- Es muss eine schriftliche Vereinbarung zur Auftragsdatenverarbeitung zwischen der Hochschule und der externen Stelle abgeschlossen werden. Dieses Auftragsdatenverarbeitungsvertrag wird in der Hochschule Bochum durch die Datenschutzbeauftragte geprüft und unterzeichnet. Es existiert ein Mustervertrag, der grundsätzlich für alle Beschaffungsvorgänge zu verwenden ist. Im besonderen Einzelfall akzeptiert die Hochschule auch die Vertragsmuster des Vertragspartners, die sodann von der Datenschutzbeauftragten geprüft werden.
- Es muss eine weisungsabhängige Verarbeitung durch den Dritten erfolgen. Ist dies nicht der Fall und besteht ein gemeinsames Interesse der Verarbeitung, besteht gegebenenfalls eine gemeinsame Verarbeitung. Dies kommt häufig in Forschungsprojekten vor, da hier oft gemeinsam Daten aufbereitet werden oder ein Forschungspartner dies für alle vornimmt. Hier handelt es sich nicht um eine Zuarbeit, sondern um ein arbeitsteiliges Vorgehen und somit in der Regel um gemeinsame Verarbeitungen mehrerer Verantwortlicher. Auch in diesen Fällen ist ein Vertrag erforderlich, der die Verteilung der Verantwortlichkeiten regelt.
- Auftragsverarbeiter müssen so ausgewählt werden, dass sie „hinreichend Garantien dafür bieten, dass geeignete technische und organisatorische Maßnahmen so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen [der DSGVO] erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet“. Dasselbe gilt für ggf. von ihm beauftragte weitere Auftragsverarbeiter. Die Qualität der Garantien muss der Verantwortliche festlegen. Dabei gilt: Je sensibler die Daten bzw. je größer das Risiko der betroffenen Personen bei einer Datenpanne, desto höhere Anforderungen sind an die Garantien zu stellen. So kann es in einem Fall ausreichen, dass der Auftragsverarbeiter die bei ihm getroffenen Sicherheitsmaßnahmen plausibel nachweisen kann, während in einem anderen Fall ISO 27.000 ff-Zertifikate für Technik und Organisation zu verlangen sind.

8. Zusammenfassung

- Jede Stelle innerhalb der Hochschule, die für Prozesse der Verarbeitung personenbezogener Daten verantwortlich ist, muss die Einhaltung der datenschutzrechtlichen Vorgaben der DSGVO sicherstellen.
- Dazu gehört an erster Stelle die Festlegung der Rechtsgrundlage in Bezug auf den Zweck der Datenverarbeitung. Denn ohne Rechtsgrundlage bzw. ggf. ohne Einwilligung darf die Verarbeitung gar nicht erfolgen.
- Dazu gehört aber auch die Prüfung, ob alle Daten auch erforderlich sind, denn es dürfen nur Daten verarbeitet werden, die zur Erfüllung des Zwecks auch erforderlich sind und auch nur solange, wie es erforderlich ist.
- Zu den Pflichten bei der Verarbeitung personenbezogener Daten gehört auch die Information der Betroffenen gem. Art. 13 und 14 DSGVO.
- Zu regeln ist außerdem, dass nur die Personen Zugriff auf die Daten erhalten, die diesen im Rahmen der Erfüllung des festgelegten Zwecks auch brauchen.
- Auch müssen die nötigen Informationen für das Verzeichnis von Verarbeitungstätigkeiten nach Art. 30 DSGVO im Rahmen der für die Hochschule noch festzulegenden Verfahrensweise bereitgestellt werden.
- Es sollte auch schon bei der Einführung von Verfahren festgelegt werden, wie ggf. die Meldepflichten bei Datenschutzverletzungen nach Art. 33 und 34 DSGVO sichergestellt werden.
- Schließlich sind ausreichende technische und organisatorische Maßnahmen gem. Art. 24 und Art. 32 DSGVO festzulegen und zu dokumentieren, um die Sicherheit der Verarbeitung zu gewährleisten.
- Weiterhin sollte schon bei der Einführung von Verfahren festgelegt werden, wie ggf. die weiteren Betroffenenrechte (Art. 15 bis Art. 23 DSGVO) sichergestellt werden.
- Es ist sicherzustellen, dass bei Auftragsverarbeitung und bei gemeinsamer Verantwortung die nötigen Verträge geschlossen werden.
- Werden bei einer Auftragsverarbeitung, einer gemeinsamen Verarbeitung oder einer Übermittlung aufgrund einer anderen Grundlage Daten außerhalb der EU verarbeitet, ist eine besondere Prüfung der Zulässigkeit dieser Verarbeitung außerhalb des Geltungsbereichs der DSGVO erforderlich.
- **Datenschutz schützt nicht Daten, sondern Personen!**