**Vorlage zur Erstellung eines Verzeichnisses der Verarbeitungstätigkeiten nach Art. 30 EU-DSGVO**

|  |  |  |  |
| --- | --- | --- | --- |
| **Nr.** |  | **Inhalt** | **Erläuterungen / Hinweise zum Ausfüllen** |
| 1 | Namen und Kontaktdaten des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen sowie des Datenschutzbeauftragten |  | Der Verantwortliche ist nach Art. 4, Nr. 7 EU-DSGVO die Stelle, die alleine oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogene Daten entscheidet. Dies ist in der Regel die Schule. Daneben sind die Kontaktdaten des Datenschutzbeauftragten anzugeben.  Anzugeben sind:   * Name und dienstliche Anschrift der Stelle * Name des Verantwortlichen (Schulleiter), ggf. E-Mail-Adresse und Telefonnummer * Name und dienstliche Anschrift des Datenschutzbeauftragten, ggf. E-Mail-Adresse und Telefonnummer   Hinweis: Eine Auftragsdatenverarbeitung nach Art. 28 EU-DSGVO ändert nichts an der Rolle des Verantwortlichen. |
| 2 | Zweck der Verarbeitung |  | Der Zweck der Datenverarbeitung ist so ausführlich und präzise wie möglich zu benennen. Überlegen Sie, aus **welchen Gründen** und zu **welchen Zwecken** Ihrer Stelle personenbezogene Daten verarbeitet.  Dies ist eine sehr wichtige und zentrale Stelle des Verzeichnisses. Es sind stest alle Zwecke anzugeben, aufgrund deren die Verarbeitung von personenbezogenen Daten erfolgt.  So ist z. B. bei der Verarbeitung von personenbezogenen Daten von Schülerinnen und Schülern sowie von deren Erziehungsberechtigten in der Regel als übergeordneter Zweck der Erziehungs- und Bildungsauftrag der Schule und Verwaltungs- oder Fürsorgeaufgaben zu nennen, aber auch die einzelnen Zwecke wie die Verwaltung des Schülers oder die Zeugniserstellung. Bei Lehrkräften sind es meist Zwecke wie die Personalverwaltung oder/und die Unterrichtsorganisation.  Ferner ist der besondere Zweck für die Verarbeitung besonderer Kategorien personenbezogener Daten, z. B. Religionszugehörigkeit, anzugeben. |
| 3 | Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten |  | Es ist darzustellen, welche Personen (z.B. Schüler, deren Erziehungsberechtigte, das Lehrpersonal, Lieferanten, Personal des Schulträgers, usw.) betroffen sind und welche Datenarten von diesen betroffenen Personen verarbeitet werden.  Es wird eine tabellarische Darstellung empfohlen.  Es geht nicht darum, jedes einzelne im automatisierten Verfahren gespeicherte Datenfeld aufzuführen. Vielmehr sind sachlich zusammengehörende Datenfelder zu sinnvollen Gruppen zusammenzufassen und diese Datenarten dann allgemein verständlich zu benennen. Beispiele dafür sind:   * Ordnungsmerkmal (z. B. Personennummer) * Familienname * Vorname * Geburtstag   Einzelmerkmale wie etwa "Postleitzahl", "Wohnort", "Straße" und "Hausnummer" können dabei zu einem Sammelmerkmal, in diesem Falle "Postanschrift", zusammengefasst werden. Bei der Bildung von Sammelmerkmalen ist allerdings darauf zu achten, dass diese noch aussagekräftig bleiben. Die Kunst besteht also darin, den richtigen Konkretisierungsgrad zu finden. Einerseits dürfen die Begriffe, die die Art der gespeicherten Daten beschreiben, nicht zu allgemein sein, weil sonst die Transparenz über den Umfang der Datenspeicherung verloren ginge. Die Aussagekraft von Begriffen wie "Personalien" oder "Vermögensverhältnisse" wäre recht begrenzt. Andererseits sollten die gewählten Begriffe so flexibel sein, dass nicht jede kleine Änderung am automatisierten Verfahren eine Änderung am Verfahrensverzeichnis nach sich zieht.  Eine Auflistung der in einer Schule grundsätzlich in zulässiger Weis zu verarbeitenden personenbezogenen Daten von Schülerinnen und Schülern, deren Erziehungsberechtigten und dem Lehrpersonal finden Sie in der Verwaltungsvorschrift "Datenschutz an öffentlichen Schulen“. |
| 4 | Kategorien von Empfängern (auch andere Lehrkräfte der eigenen Schule), gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen |  | Empfänger ist nach Art 4. Nr. 9 EU-DSGVO jede natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, der personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Empfänger können bspw. Stellen der Schulaufsicht, andere Schulen oder andere Behörden sein.  Empfänger ist auch immer der Dienstleister, der z. B. das Rechenzentrum oder eine Cloudlösung betreibt. |
| 5 | Gegebenenfalls Übermittlungen von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Art. 49 Abs. 1 UAbs. 2 EU-DSGVO genannten Datenübermittlungen die Dokumentierung geeigneter Garantien |  | Darzustellen ist, welche personenbezogenen Daten an solche Stellen übermittelt werden, sofern eine solche Übermittlung tatsächlich im Verfahren erfolgt.  Ferner sind die geeigneten Garantien darzustellen. Diese finden Sie in Artikel 46 EU-DSGVO:  Die geeigneten Garantien können, ohne dass hierzu eine besondere Genehmigung einer Aufsichtsbehörde erforderlich wäre, bestehen in  a) einem rechtlich bindenden und durchsetzbaren Dokument zwischen den Behörden oder öffentlichen Stellen,  b) verbindlichen internen Datenschutzvorschriften gemäß Art. 47 EU-DSGVO,  c) Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 EU-DSGVO erlassen werden,  d) von einer Aufsichtsbehörde angenommenen Standarddatenschutzklauseln, die von der Kommission gemäß dem Prüfverfahren nach Art. 93 Abs. 2 EU-DSGVO genehmigt wurden,  e) genehmigten Verhaltensregeln gemäß Art. 40 EU-DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen, oder  f) einem genehmigten Zertifizierungsmechanismus gemäß Art. 42 EU-DSGVO zusammen mit rechtsverbindlichen und durchsetzbaren Verpflichtungen des Verantwortlichen oder des Auftragsverarbeiters in dem Drittland zur Anwendung der geeigneten Garantien, einschließlich in Bezug auf die Rechte der betroffenen Personen.  Vorbehaltlich der Genehmigung durch die zuständige Aufsichtsbehörde können die geeigneten Garantien auch insbesondere bestehen in  a) Vertragsklauseln, die zwischen dem Verantwortlichen oder dem Auftragsverarbeiter und dem Verantwortlichen, dem Auftragsverarbeiter oder dem Empfänger der personenbezogenen Daten im Drittland oder der internationalen Organisation vereinbart wurden,  b) Bestimmungen, die in Verwaltungsvereinbarungen zwischen Behörden oder öffentlichen Stellen aufzunehmen sind und durchsetzbare und wirksame Rechte für die betroffenen Personen einschließen. |
| 6 | Vorgesehene Löschfristen der verschiedenen Datenkategorien |  | Wer personenbezogene Daten verarbeitet, muss - beginnend mit der erstmaligen Speicherung von Daten - festlegen, wann welche Datenarten zu löschen sind.  Die Regelungen hierzu befinden sich auch in der mit der Verwaltungsvorschrift "Datenschutz an öffentlichen Schulen" in den Abschnitten zu den Daten der jeweiligen Personengruppen. Es ist aber immer die Zeit anzugeben, nach denen die Daten an Ihrer Stelle gelöscht werden. |
| 7 | Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen gemäß Art. 32 Abs. 1 EU-DSGVO |  | Jede Stelle muss unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs , der Umstände und der Zwecke der Verarbeitung, sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen geeignete technischen und organisatorischen Maßnahmen treffen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.  Diese Maßnahmen schließen insbesondere Folgendes ein:   1. Die Pseudonymisierung und Verschlüsselung personenbezogener Daten. 2. Die Fähigkeit, die Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung auf Dauer sicherzustellen:   Dies umfasst - je nach Erforderlichkeit im Einzelfall - Maßnahmen der Zutrittskontrolle, der Zugriffskontrolle, der Benutzerkontrolle, der Eingabekontrolle, der Organisationskontrolle, ferner den Einsatz von Authentifizierungsverfahren und Verschlüsselungstechnologien (besonders wenn die Daten übermittelt werden).  Empfohlen, wird, zu jedem der Punkte Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste darzustellen, wie diese umgesetzt wurden.  Dabei helfen die folgenden Aspekte:  -Maßnahmen, die geeignet sind, Unbefugten den Zugang zu Datenverarbeitungsanlagen zu verwehren: Es ist also die räumliche Situation zu beschreiben, in denen sich Datenverarbeitungsgeräte befinden.  Empfehlungen: Unbefugte Personen sollen nicht in die Nähe von Datenverarbeitungsanlagen gelangen bzw. diese beobachten und dabei von Daten Kenntnis nehmen können. Der Rechner zur Verarbeitung personenbezogener Daten an Schulen sollte daher, sofern es die räumliche Situation der Schule zulässt, in einem besonderen, abschließbaren Raum stehen, zu dem nur bestimmte Personen Zutritt haben. Bei Abwesenheit der Zugangsberechtigten ist der Rechner abzuschalten und der Raum abzuschließen. Rechner zur Verarbeitung personenbezogener Daten an Schulen können aus organisatorischen Gründen oft nicht in einem besonderen, abgetrennten Raum untergebracht werden, sondern stehen im Schulsekretariat, das für viele Personen zugänglich ist. Es ist in diesem Fall zu gewährleisten, dass diese keinen Einblick auf den Bildschirm haben, die vom Drucker ausgegebenen Daten nicht einsehen und die Tastatur nicht bedienen können. Soweit bei Abwesenheit der Zugangsberechtigten ein Abschließen des Raumes nicht möglich ist, muss der Rechner gesondert gesichert sein.  -Maßnahmen, die geeignet sind, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können. Soweit das zu beschreibende Verfahren verschiedene Benutzergruppen mit unterschiedlichen Rechten kennt, sollte diese hier dargestellt werden. Es ist folglich darzustellen, welche Benutzergruppe oder Rolle (z.B. Schulleiter, Klassenlehrer, Fachlehrer, Sekretariat usw.) welche Zugriffsrechte (z. B. nur lesend, schreiben, verändern, Administratorrechte usw.) hat. Weiterhin ist das verwendete Filesystem (z. B. NTFS) zu nennen und, soweit relevant, der jeweilige Zugriff auf verwendete Verzeichnisse (z. B. individuelle Ablagen, Ablagen für Gruppenverzeichnisse, Ablagen für Daten der Anwendungsprogramme). -Maßnahmen, die geeignet sind, zu verhindern, dass Datenverarbeitungssysteme mit Hilfe von Einrichtungen zur Datenübertragung von Unbefugten genutzt werden können. Ein Zugriff auf personenbezogene Daten sollte nur möglich sein durch die Verwendung eines persönlichen Accounts (Benutzername und Passwort). Es sollte hier insbesondere der Passwortschutz beschrieben werden, so z. B. die im Betriebssystem eingestellten Passwortkonventionen wie Mindestlänge, Höchstalter, Sperrung nach wie viel Fehlversuchen oder Passwort-Historie im Einzelnen bezeichnet werden (etwa durch Screen-Shots). Damit Passwörter nicht durch systematische Versuche gefunden werden können, sollte das Programm die Passworteingabe nach mehrmaligen Fehlversuchen selbsttätig sperren. -Maßnahmen, die geeignet sind, zu gewährleisten, dass nachträglich überprüft und festgestellt werden kann, welche Daten zu welcher Zeit von wem in Datenverarbeitungssysteme eingegeben worden sind.  Es ist darzustellen, wie Erfassung oder Veränderungen von Daten festgehalten werden, damit man diese später kontrollieren kann. In der Regel erfolgt diese über eine automatisierte Protokollierung der o.g. Angaben. -Maßnahmen, die geeignet sind, zu gewährleisten, dass überprüft und festgestellt werden kann, an welche Stellen Daten durch Einrichtungen zur Datenübertragung übermittelt werden können. Hier geht es um die Kontrolle von Rechnern, die über das Internet oder andere Netze Daten übermitteln können. Falls das Verfahren eine verschlüsselte Datenübermittlung bietet (z.B. den Service „https“) oder eine Übermittlung nur über ein geschütztes Intranet erfolgt, wäre dies hier darstellen. Sofern über die lokalen Netze auch E-Mails ausgetauscht oder im Internet gesurft werden soll, sind im Verfahrensverzeichnis eines Mailprogrammes oder eines Internetbrowsers auch die dafür vorgesehenen Sicherheitsmaßnahmen zu beschreiben. -Maßnahmen, die geeignet sind, zu gewährleisten, dass bei der Übertragung von Daten sowie beim Transport von Datenträgern die Daten nicht unbefugt gelesen, kopiert, verändert oder gelöscht werden können.  Hier sind Maßnahmen wie z. B. die Verschlüsselung von Daten bei einem Transport auf einem USB-Stick oder der Transport in einem versiegelten Umschlag zu nennen. -Maßnahmen, die geeignet sind, die innerbehördliche oder innerbetriebliche Organisation so zu gestalten, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Die Gesamtverantwortung für die ordnungsgemäße Verarbeitung personenbezogener Daten trägt der Schulleiter. Die Verarbeitung personenbezogener Daten muss in der Schule mit klaren Zuständigkeiten durchsichtig organisiert sein. Die ergriffenen Maßnahmen sind hier zu beschreiben. So sollte z. B. benannt und beschrieben werden:   * Die verantwortlichen Personen für die IT-Technik der Schule * Wie wird der Zugang zum Internet, falls das beschriebene Verfahren einen benötigt, verwaltet? * Organisatorische Anweisungen zur Datensicherung * Wie erfolgt die Beauftragung der Reparatur defekter Geräte und die vorherige Sicherung der Daten? * Wie erfolgt die Vergabe von personenbezogenen Kennwörtern? * Gibt es Regelmäßige Kontrollen? * Gibt es eine Nutzungsordnung? * Aufgabenbeschreibung Netzwerkberater * Gibt es Schulung der Mitarbeiter an der Schule? * Gibt es eine Person, die die Aufgaben des behördlichen Datenschutzbeauftragten wahrnimmt? Empfehlung: Unterlagen wie zum Beispiel Dienstanweisungen oder eine Nutzungsordnung können als Anlage beigefügt werden, so dass darauf verwiesen werden kann.  1. Die Fähigkeit, die Verfügbarkeit der personenbezogenen Daten und den Zugang zu ihnen bei einem physischen oder technischen Zwischenfall rasch wiederherzustellen: Darunter sind insbesondere Maßnahmen der Verfügbarkeitskontrolle zu verstehen, wie eine Datensicherung durch Backups, aber auch die redundante Ausgestaltung verschiedener Komponenten wie z. B. Festplatten. 2. ein Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit   Es wird empfohlen, zu jedem dieser Punkte in konkreter, detaillierter und nachvollziehbarer Weise darzustellen, wie diese umgesetzt wurden. Beschreiben Sie bitte alle Maßnahmen, die in Ihrer Stelle für die Sicherung von personenbezogenen Daten getroffen werden.  Folgende beispielhaft erwähnte Aspekte mögen verdeutlichen, welche Detaillierung dabei empfehlenswert ist: Unzulänglich wäre etwa, wenn beispielsweise im Zusammenhang mit den Maßnahmen der Zugriffskontrolle, die einen unberechtigten Zugriff auf personenbezogene Daten verhindern sollen, nur Stichwörter wie "Passwortschutz", "differenzierte Zugriffsberechtigungen" oder "Dienstanweisung" genannt würden. Diese Maßnahmen sind zwar allesamt notwendig, jedoch sind dafür unterschiedlichste Realisierungsmöglichkeiten vorstellbar, die letztlich ein ganz unterschiedliches Sicherheitsniveau gewährleisten. Es muss daher erkennbar sein, **wie** die Realisierung jeweils erfolgt. |
| 8 | Einhaltung der Grundsätze für die Verarbeitung personenbezogener Daten nach Art 5. EU-DSGVO | | Aus Gründen der gesetzlich vorgeschriebenen Rechenschaftspflicht wird empfohlen, in dem Verzeichnis auch die Umsetzung der datenschutzrechtlichen Grundprinzipien zu dokumentieren. |
| 8.1 | Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz |  | Es ist die Rechtsgrundlage genau anzugeben (einschlägiges Gesetz unter Nennung des §) oder Einwilligung.  Eine Rechtsgrundlage muss vorhanden sein oder eine Einwilligung vorliegen, die Verarbeitung muss für Betroffene nachvollziehbar sein.  Nach Art. 6 Abs. 1 EU-DSGVO ist die Verarbeitung personenbezogener Daten u. a. zulässig, wenn die EU-DSGVO oder eine andere Rechtsvorschrift sie erlaubt oder der Betroffene eingewilligt hat.  Im Verzeichnis der Verarbeitungstätigkeiten ist daher zu dokumentieren, ob die Verarbeitung aufgrund einer Rechtsvorschrift (z. B. bei der Verarbeitung von Schülerstammdaten) oder einer Einwilligung (z. B. wenn es um Schülerfotos geht) erfolgt. Es können, wie bei manchen Schulverwaltungsprogrammen die auch Fotos enthalten, auch beide Zulässigkeitsgründe anzugeben sein. Daher muss in solchen Fällen die Rechtsgrundlage auch nach Datenarten getrennt angegeben werden. Bei Schülerfotos ist dann zu erwähnen, dass diese auf Grund einer Einwilligung des Schülers oder, bei unter 16-jährigen, der Erziehungsberechtigten erfolgt. Bei den Stammdaten des Schülers ist hingegen die Rechtsgrundlage § 1 Schulgesetz in Verbindung mit Art. 6 Abs. 1 lit c EU-DSGVO in Verbindung mit der Verwaltungsvorschrift "Datenschutz an öffentlichen Schulen" zu nennen.  Als Rechtsgrundlage der Verarbeitung von personenbezogenen Daten von Lehrkräften sind in der Regel § 1 Schulgesetz in Verbindung mit Art. 88 EU-DSGVO und § 50 Beamtenstatusgesetz und die Verwaltungsvorschrift "Datenschutz an öffentlichen Schulen" zu nennen. Im Falle einer Verarbeitung von besonderen Kategorien personenbezogener Daten wie Religionszugehörigkeit usw. etc.) muss die hierfür spezifische Rechtsgrundlage genannt werden.  Es ist ferner darzustellen, auf welche Weise transparente Information, Kommunikation und Modalitäten für die Ausübung der Rechte der betroffenen Personen gemäß Art. 12 EU-DSGVO umgesetzt wurden.  Insbesondere:   * Informationspflicht bei der Erhebung (Art. 13 und 14) * Auskunftsrecht der betroffenen Person (Art. 15) * Rechte auf Berichtigung, Löschung, Einschränkung der Verarbeitung, Mitteilungspflicht im Zusammenhang mit einer Berichtigung oder Löschung, Datenübertragbarkeit, Widerspruchsrecht, Recht zu automatisierte Entscheidung im Einzelfall (Art. 16 bis 22) * Recht auf Benachrichtigung bei einer Datenschutzverletzung (Art. 34). |
| 8.2 | Zweckbindung |  | Festlegung eines eindeutigen, legitimen Zwecks, keine Weiterverarbeitung zu anderen, widersprechenden Zwecken.  Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 2 „Zwecke der Verarbeitung“. |
| 8.3 | Datenminimierung |  | Nur erforderliche Daten dürfen im erforderlichen Umfang verarbeitet werden.  Die Umsetzung ist darzustellen. |
| 8.4 | Richtigkeit |  | Daten müssen sachlich richtig und ggf. aktuell sein. Eine Löschung, Berichtigung muss realisierbar und ggf. realisiert sein.  Die Umsetzung ist darzustellen. |
| 8.5 | Speicherbegrenzung |  | In Bezug auf Umfang und zeitl. Speicherung, falls möglich: anonymisiert, pseudonymisiert.  Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 6 „Löschfristen“. |
| 8.6 | Integrität und Vertraulichkeit |  | Geeignete techn.-org. Datenschutzmaßnahmen müssen getroffen werden.  Siehe Verzeichnis der Verarbeitungstätigkeit Nr. 7, „Beschreibung der techn.-org. Maßnahmen“. |

Weitere Hinweise:

Für jede einzelne Verarbeitungsart (also z.B. für Schulverwaltungssoftware, Stundenplansoftware, Kontaktverwaltung, Schüler- oder Personalakten usw.) sind die o. g. Angaben zu machen.

Die Angaben sind so konkret und detailliert zu machen, dass eine kundige Person in der Lage ist, diese nachzuvollziehen.

Dieses Verzeichnis ist vor der ersten Verarbeitung personenbezogener Daten zu erstellen.