Verzeichnis von Verarbeitungstätigkeiten des Verantwortlichen

Angaben zum Verantwortlichen (Art. 30 Abs. 1 lit. a DSGVO)

Angaben zum Verantwortlichen
Name der Schule: Berufskolleg Ostvest
Name der Schulleiterin oder des Schulleiters: OStD'in Juliane Brüggemann
Straße: Hans-Böckler-Straße 2
Postleitzahl und Ort: 45711 Datteln
Telefon: 02363 378-0
E-Mail-Adresse: mail@bk-ostvest.de

Angaben zur Person des Datenschutzbeauftragten **(Art. 37 ff. DS-GVO oder § 38 Abs. 1 BDSG neu)**
Anrede: Herr
Titel:
Name: S. Keßler
Funktion: Datenschutzbeauftragter des Kreises Recklinghausen
Telefon: 02361/53-4428
E-Mail-Adresse: S.Kessler@kreis-re.de

Verzeichnis von Verarbeitungstätigkeiten

Angaben zur Verarbeitungstätigkeit und zur Verantwortlichkeit (Art. 30 Abs. 1 lit. b DSGVO)

1. Bezeichnung der Verarbeitungstätigkeit: IServ Schulserver

Angaben zur Verarbeitungstätigkeit

2. Zwecke der Verarbeitungen/der Verarbeitungstätigkeit

IServ ist eine Lern- und Kommunikationslösung für den Einsatz im pädagogischen Netzwerk Ihrer Schule. Dabei bietet IServ Komponenten in folgenden Bereichen:

- Organisation, z. B. Kalender, Adressbuch, Fileserver und Infobildschirm
- Netzwerk, z. B. Rechnerverwaltung mit Softwareverteilung, WLAN und Internetfreigabe
- Kommunikation, z. B. E-Mail, Messenger, Forum, Videokonferenz und News
- Unterricht, z. B. Aufgaben, Klausurmodus, Texte

IServ bildet die technische Basis für ein modernes IT-gestütztes Lehren und Lernen in der Schule und ist geeignet für jeden Schultyp.

3. Rechtsgrundlage der Verarbeitungen/der Verarbeitungstätigkeit

Die Verarbeitung der personenbezogenen Daten ist durch die DSGVO, das BDSG-neu, die Landesdatenschutzgesetze und das Schulgesetz §§ 120-122 geregelt.

Die Verarbeitung sonstiger personenbezogener Daten ist zulässig, soweit der Betroffene bzw. deren erziehungsberechtigten Personen eingewilligt haben (Art 6 Abs 1 lit a DSGVO). Schriftliche Einwilligungserklärungen sind einzuholen und zu dokumentieren.

4. Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DSGVO)

Betroffen sind alle Benutzer, die einen Account besitzen.

Art der gespeicherten Daten

Zu jedem Benutzer werden folgende Daten gespeichert:

- Vorname
- Nachname
- Spitzname (Sofern von Benutzer selbst eingegeben)
- farbliche Darstellungen (von Benutzer selbst festgelegt)
- Account im Format vorname.nachname
- Passwort als Prüfsumme

Stand 28.5.2020

- interne E-Mail-Adresse (Account@domain)
- das persönliche Verzeichnis samt Dateien wie Bilder, Dokumente, Videos und andere
- Termine
- Datum der Erstellung des Benutzers
- Zeitstempel
- Letzter Login
- Gruppenmitgliedschaften, z.B. Klassen und Kurse
- persönliche Einstellungen
- Inhalte der Kommunikation aus E-Mail, Chat, Foren, usw.
- IP-Adresse
- Informationen zu http und smtp Anfragen, Raumbuchungen, Klausurplänen
- Druckaufträge und Druckguthaben

Sämtliche Anmeldeversuche am Server werden mit IP-Adresse und Zeitstempel protokolliert.

Die aktuelle Liste finden Sie unter: https://iserv.eu/doc/privacy/general/#art-der-gespeicherten-daten

5. Kategorien von Empfängern, denen die Daten offengelegt worden sind oder noch offengelegt werden (Art. 30 Abs. 1 lit. d DSGVO)

Berechtigte Mitarbeiter der IServ GmbH, Bültenweg 73, 38106 Braunschweig

Im Rahmen von vertraglich vereinbarten Supportleistung werden bei Kundenaufträgen Daten Drittfirmen (Unterauftragnehmern) offengelegt. Die entsprechenden Firmen sind dem IServ-Auftragsverarbeitungsvertrag zu entnehmen

Verträge zur Auftragsverarbeitung gemäß Art 28 DSGV- bezüglich der IT Systembetreuung für Hardware und Software für den IServ Schulserver werden jeweils schulindividuell abgeschlossen.

Schulen haben die Möglichkeit, Fernwartungsmodule von Ihren Servern nach eigenem Ermessen zu entfernen.

6. Datenübermittlungen in Drittländer (Art. 30 Abs. 1 e DSGVO)

Ja

Nein

7. Vorgesehene Fristen für die Löschung der verschiedenen Datenkategorien (Art. 30 Abs. 1 lit. f DSGVO)

Die Nutzer haben in der Regel Einsicht in ihre eigenen Daten und können diese nach eigenem Ermessen löschen.

Eine genaue Aufstellung der Datenkategorien nach Modul finden Sie in der Verfahrensbeschreibung unter https://iserv.eu/doc/privacy/process-description/. Weiterhin gibt es diverse Logdateien zur Fehleranalyse und Aufklärung von Missbrauchsfällen, die nach gewissen Fristen automatisch gelöscht werden, bei personenbezogenen Daten in der Regel 7 Tagen. Näher Informationen zu den Speicherfristen bei Logdateien finden Sie unter https://iserv.eu/doc/privacy/logfiles/.

Die Informationen von gelöschten Benutzern werden nach 90 Tagen endgültig gelöscht. - Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.

8. Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO)

Die für dieses Verfahren eingesetzte Technik ist in die Netzwerkinfrastruktur der Schule eingebunden. Zur Sicherstellung der Datensicherheit und des Datenschutzes werden in der Schule technische und organisatorische Maßnahmen getroffen. Sie orientieren sich an Datensicherheits- und Datenschutz-Schutzzielen, die nachfolgend mit den für dieses Verfahren wichtigsten Maßnahmen aufgeführt werden.

Datenschutzrechtliche Beurteilung

Vertraulichkeit (es können nur die Personen auf die entsprechenden Daten zugreifen, die auch die Berechtigungen dafür besitzen):

- Für das Verfahren gelten die allgemeinen Zugangs- und Zugriffsregelungen der Schule.
- Innerhalb des Verfahrens wird durch eine dokumentierte Berechtigungsvergabe sichergestellt, dass nur berechtigte Personen auf die Datenbestände zugreifen dürfen. Der Server wird über einen DSL-Anschluss angewählt und beinhaltet eine Firewall. Die Anmeldung erfolgt über Benutzer-Account und Passwort.

Integrität (innerhalb einer bestimmten Zeit ist sichergestellt, dass die Daten nicht verändert wurden):

- Auf Server und Backupserver haben nur die technischen Administratoren dieses Systems bzw. die Fernwartungs-Auftragsverarbeiter Zugriff. Sie stellen sicher, dass das Betriebssystem regelmäßig aktualisiert wird (Schutz vor Veränderung der Daten durch Angriffe oder unberechtigten Zugriff).
- Innerhalb des Verfahrens haben nur die fachliche Administration dieses Verfahrens und die Personen, die die Datenpflege betreiben, Zugriff auf die Datenbestände (Schutz vor Veränderung durch unberechtigten Zugriff).

Verfügbarkeit / Belastbarkeit (innerhalb einer bestimmten Zeit ist sichergestellt, dass auf die entsprechenden Daten zugegriffen werden kann):

- Der IServ Schulserver läuft im Dauerbetrieb. Es gibt keine zeitlichen Zugriffsbeschränkungen.
- Die Daten werden täglich gesichert.
- Das System wird auf einem separaten Backupserver im Netzwerk gesichert und kann

vor dort aus wiederhergestellt werden.
- Pseudonymisierung und Verschlüsselung personenbezogener Daten obliegen der Schule.

Erläuterungen

Nr. 1	Eindeutige Bezeichnung der dokumentierten Verarbeitung/der Verarbeitungstätigkeit auf Grundlage eines Fachprozesses. Es sollte eine im Unternehmen geläufige Bezeichnung des Fachprozesses gewählt werden. Beispiele: • Allgemeine Kundenverwaltung • Customer-Relationship-Management (CRM)
Nr. 2	Nach der Unternehmensorganisation für die konkrete Verarbeitungstätigkeit verantwortlicher Fachbereich/verantwortliche Führungskraft (*sofern möglich und sinnvoll, zumindest als Funktionsbezeichnung*)
Nr. 3	Falls mehrere Verantwortliche gemeinsam für die Verarbeitungstätigkeiten verantwortlich sind, bspw. innerhalb einer Unternehmensgruppe, sind hier Name und Kontaktdaten des/der weiteren Verantwortlichen anzugeben (Firma/ladungsfähige Anschrift; Art. 30 Abs. 1 Lit. a DSGVO, Art. 26 Abs. 1 DSGVO)
Nr. 4	Beispiele: • Verarbeitungstätigkeit: „Allgemeine Kundenverwaltung“; verfolgte Zweckbestimmungen: „Auftragsbearbeitung, Buchhaltung und Inkasso“ • Verarbeitungstätigkeit: „Customer-Relationship-Management“; verfolgte Zweckbestimmungen: „Dokumentation und Verwaltung von Kundenbeziehungen, Marketing, Neukundenakquise, Kundenbindungsmaßnahmen, Kundenberatung, Beschwerdemanagement, Kündigungsprozess“ Eine Verarbeitungstätigkeit kann mehrere Teil-Geschäftsprozesse zusammenfassen. Dementsprechend kann eine Verarbeitung auch mehrere Zwecke umfassen, dass auch mehrere Zweckbestimmungen angegeben werden können. Die erforderliche Detailtiefe hängt von der Geschäftstätigkeit des Verantwortlichen ab. Es können neben dem Fachprozess auch begleitende mitarbeiterbezogene Unterstützungsprozesse vorliegen wie z.B. zur Personalführung/-einsatzplanung. Diese können entweder als Teil einer anderen Verarbeitung, oder als eigene Verarbeitung beschrieben sein.
Nr. 5	Die Nennung der einschlägigen Rechtsgrundlage ist für Accountability-Pflichten und die Gewährleistung von transparenzpflichten ggü. betroffenen Personen notwendig.
Nr. 6	Beschreibung der Kategorien betroffener Personen und der Kategorien personenbezogener Daten (Art. 30 Abs. 1 lit. c DSGVO)
Nr. 6.1	Als betroffene Personengruppen kommen beispielsweise Kunden, Interessenten, Arbeitnehmer, Schuldner, Versicherungsnehmer usw. in Betracht.
Nr. 6.2	Den einzelnen Personengruppen sind die jeweils auf sie bezogenen verwendeten Daten oder Datenkategorien zuzuordnen. Damit sind keine personenbezogenen

	Daten, sondern "Datenbezeichnungen"/Datenkategorien gemeint (z.B. „Adresse“, „Geburtsdatum“, „Bankverbindung“). Werden solche Datenkategorien angegeben, s- müssen diese s- konkret wie möglich sein. Nicht ausreichend, da zu allgemein, sind etwa Angaben wie „Kundendaten“ oder Ähnliches. Beispiele: • Kunden: Adressdaten, Kontaktkoordinaten (einschl. Telefon-, Fax-und E-Mail-Daten), Geburtsdatum, Vertragsdaten, Bonitätsdaten, Betreuungsinformationen einschließl. Kundenentwicklung, Produkt- bzw. Vertragsinteresse, Statistikdaten, Abrechnungs- und Leistungsdaten, Bankverbindung • Beschäftigtendaten (Lohn und Gehalt): Kontaktdaten, Bankverbindung, Sozialversicherungsdaten, etc.
Nr. 7	Empfängerkategorien sind insbesondere am Prozess beteiligte weitere Stellen des Unternehmens/Konzerns oder andere Gruppen von Personen oder Stellen, die Daten – ggf. über Schnittstellen – erhalten z.B. in den Prozess eingebundene weitere Fachabteilungen, Vertragspartner, Kunden, Behörden, Versicherungen, Auftragsverarbeiter (z.B. Dienstleistungsrechenzentrum, Call-Center, Datenvernichter, Anwendungsentwicklung, Cloud Service Provider) usw.
Nr. 8	Drittländer sind solche außerhalb der EU/des EWR Beispiele für internationale Organisationen: Institutionen der UNO, der EU -------- *Start optional* ------- - Geeignete Garantien beim Empfänger sind grds. erforderlich, falls für den kein Angemessenheitsbeschluss der EU-Kommission gem. Art. 45 Abs. 3 DSGVO vorliegt. Solche Garantien können gem. Art. 46 DSGVO- durch verbindliche interne Datenschutzvorschriften (BCR) oder EU-Standardverträge erbracht werden. -------- *Ende optional* ------- Liegt keine der genannten Garantien vor, sind hier andere getroffene Garantien zu dokumentieren (Art. 49 Abs. 1. UAbs. 2 DSGVO)
Nr. 9	Anzugeben sind hier die konkreten Aufbewahrungs-/Löschfristen, die in Verarbeitungstätigkeiten implementiert sind, bezogen auf einzelne Verarbeitungsschritte, falls unterschiedlich. Soweit diese in einem Löschkonzept dokumentiert sind, reicht der konkrete Verweis auf das vorhandene und in der Verarbeitungstätigkeit umgesetzte Löschkonzept aus.
Nr. 10	Allgemeine Beschreibung der technischen und organisatorischen Maßnahmen (Art. 30 Abs. 1 lit. g i.V.m. Art. 32 Abs. 1 DSGVO)
Nr. 10.1	Optional kann an dieser Stelle eine knappe Beschreibung der technischen Infrastruktur wie der technischen und organisatorischen Sicherheitsmaßnahmen angegeben werden, um ein besseres Verständnis der allgemeinen Beschreibung der technischen und organisatorischen Maßnahmen (siehe 10.2.) zu ermöglichen.
Nr. 10.2	Soweit sich die technischen und organisatorischen Maßnahmen schon aus vorhandenen Sicherheitsrichtlinien/Konzepten/Zertifizierungen ergeben, ist ein konkreter Verweis hierauf ausreichend. Insbesondere sind hier Abweichungen zu einem übergreifenden Sicherheitskonzept zu dokumentieren. Wenn eine Datenschutz-Folgenabschätzung für die Verarbeitung hohe Risiken ausweist, sind die zur Bewältigung dieser Risiken getroffenen Sicherheitsvorkehrungen für die

	Verarbeitung in der Datenschutz-Folgenabschätzung zu dokumentieren. (Art. 35 Abs. 7 lit. d DSGVO). Ein Verweis auf das Vorhandensein einer Datenschutz-Folgenabschätzung ist eine sinnvolle optionale Angabe (siehe unten).
Optional	Im Hinblick auf die vielfältigen Nachweispflichten, denen das Unternehmen im Datenschutz unterliegt, kann es sinnvoll sein, weitere Aspekte zur Verarbeitungstätigkeit zu dokumentieren. Diese sind nur intern zu verwenden. Zu diesen zusätzlichen Dokumentationen, die sinnvollerweise hier erfolgen, gehören z. B. • Angaben zur Zusammenstellung der Informationspflichten (insbes. Art. 13,14 DSGVO) • Verträge mit Dienstleistern (Art. 28 DSGVO) • Vereinbarungen zur gemeinsamen Verantwortung (Art. 26 DSGVO) • Eine Bewertung der Risiken der Verarbeitungstätigkeit für die Rechte und Freiheiten natürlicher Personen • durchgeführte Datenschutzfolgeabschätzungen zur Verarbeitungstätigkeit oder einzelnen Verarbeitungsschritten (Art. 35 DSGVO)