Verfahrensverzeichnis gemäß § 7 LDSG

Stand: 21.10.2013

I. Verfahren (Bezeichnung): IServ-Portalserver

Aktenzeichen: 11.2013 neues Verfahren ◉ Änderung ○

☑ Das Verfahren ist zur Einsichtnahme bestimmt (§ 7 Abs. 4 LDSG)

1. Name und Anschrift der Daten verarbeitenden Stelle

1.1 Name und Anschrift

Goethe-Gemeinschaftsschule, Hansastraße 25-27, 24118 Kiel

1.2 Organisationskennziffer, Amt, Abteilung, ggf. Sachgebiet

Schulleitung

2. Zweckbestimmung und Rechtsgrundlage der Datenverarbeitung

2.1 Zweckbestimmung

IServ ist eine Schulplattform im pädagogischen Netz der Schule und beinhaltet Komponenten zur

- Schulorganisation, z. B. Kalender, Adressbuch, Fileserver, Infobildschirm
- Administration nahezu aller IT-Komponenten innerhalb des pädagogischen Netzes der Schule, z. B.
  - Rechnerverwaltung mit Softwareverteilung,
  - Benutzer- und Benutzergruppenverwaltung inklusive der Rechte- und Berechtigungsverwaltung
- Kommunikation, z. B. E-Mail, Chat, Forum, News

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

2.2 Rechtsgrundlage (ggf. nach Art der Datenverarbeitung unterscheiden)

Die Verarbeitung personenbezogener Daten ist zulässig soweit der Betroffene bzw. deren erziehungsberechtigten Personen eingewilligt haben.

Schriftliche Einwilligungserklärungen gemäß § 12 LDSG sind einzuholen und zu dokumentieren.

3. Art der gespeicherten Daten

lfd. Nr.	
1	Für jeden Benutzer werden gespeichert: • Vorname • Nachname • Spitzname (selbst gewählt) • farbliche Darstellungen / Markierungen (selbst gewählt) • Account (Format: vorname.nachname) • Passwort (als Prüfsumme) • interne E-Mail-Adresse (Format: vorname.nachname@meineschule.de) • Homeverzeichnis • Terminverwaltung • Erstellungsdatum • Zeitstempel • Name des Erstellers • Letzter Login • Gruppenmitgliedschaften (z. B. Klassen oder Kurse) • persönliche Einstellungen • Inhalte der Kommunikation in z. B. E-Mail, Chat, Foren • beliebige Dateien, z. B. Dokumente, Bilder, Videos • IP-Adresse • Informationen zu http- und smtp-Anfragen • Informationen zu Raumbuchungen • Informationen zu Klausurplänen • Druckaufträge • Druckguthaben Alle Anmeldeversuche am Server werden mit IP-Adresse und Zeitstempel protokolliert.

4. Kreis der Betroffenen

lfd. Nr.	
1	Alle Benutzer des Servers (Schüler, Lehrer, Administratoren)

5. Art der regelmäßig zu übermittelnder Daten, deren Empfänger sowie Art und Herkunft regelmäßig empfangener Daten

5.1 Übermittlung an Stellen außerhalb der Mitgliedstaaten der Europäischen Union

x	nein	☐	ja	(aufgeführt in Punkt 5.2)

5.2 Empfänger der Daten

lfd. Nr. aus 3.	Empfänger
1	entfällt

5.3 Herkunft der Daten

lfd. Nr. aus 3.	Herkunft
1	entfällt

6. Zugriffsberechtigte Personen oder Personengruppen

lfd. Nr. 3.	
1	Alle Benutzer des Servers (Schüler, Lehrer, Administratoren) entsprechend der schulindividuellen erteilten Gruppenberechtigungen

7. Auftragsdatenverarbeitung

Supportleistung im Rahmen von Backup/Restore durch die Firmen:

- IServ GmbH, Bültenweg 73, 38106 Braunschweig
- Reese IT System & Service GmbH, Preetzer Chaussee 55, 24222 Schwentinental

Verträge zur Auftragsdatenverarbeitung gemäß § 17 Landesdatenschutzgesetz (LDSG) bezüglich der IT Systembetreuung für Hardware und Software für den „IServ-Portalserver“ werden jeweils schulindividuell abgeschlossen.

8. Maßnahmen zu Auskunftsansprüchen von Betroffenen nach § 27 LDSG

Maßnahmen zu Auskunftsansprüchen von Betroffenen sind innerhalb von IServ differenziert zu betrachten, zum Teil nicht fest festgelegt. Je Funktion bzw. Modul werden unterschiedliche Betroffenendaten gespeichert.

9. Maßnahmen zur Berichtigung, Löschung, Sperrung und Übermittlung personenbezogener Daten

Maßnahmen zur Berichtigung, Löschung, Sperrung und Übermittlung personenbezogener Daten sind innerhalb von IServ je Funktion bzw. Modul differenziert zu betrachten.

Maßnahmen

Programm	Maßnahmen

IServ-Portalserver – Basisfunktionen	• Maßnahmen zur Berichtigung sind nicht vorgesehen.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Die Informationen von gelöschten Benutzern werden nach 90 Tagen endgültig gelöscht.
	  ○ Die Anmeldeversuche am Server werden für 6 Monate gespeichert.
	  ○ Eine Löschung erfolgt im Dateisystem und in der Datenbank.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: keine

E-Mail	• Berichtigungen sind nachträglich nicht möglich.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ E-Mails werden beim Löschen in den Ordner „Gelöscht“ verschoben. Dort können sie manuell endgültig gelöscht werden. E-Mails älter als 7 Tage im Ordner „Gelöscht“ werden automatisch endgültig gelöscht.
	  ○ E-Mails von gelöschten Benutzern werden ausgeblendet und nach 90 Tagen endgültig gelöscht.
	  ○ Eine Löschung erfolgt im Dateisystem.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche, Mailprogramme per (S)SMTP, POP3(S), IMAP(S)
	
	Das Recht, E-Mails mit anderen Servern auszutauschen, kann gewährt werden.

Foren	• Berichtigungen von Forenbeiträgen können nur vom Anwender selbstständig vorgenommen werden.
	  ○ Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Forenbeiträge werden dauerhaft gespeichert. Benutzer können eigene Forenbeiträge nicht ändern oder löschen. Im Missbrauchsfall können einzelne Forenbeiträge von Administratoren, in diesem speziellen Fall „Moderatoren“, gelöscht werden. Ältere Forenbeiträge werden ausgeblendet und sich nur noch über die Archiv-Ansicht aufrufbar.
	  ○ Forenbeiträge bleiben auch nach Löschung des Autors vollständig erhalten. Gruppenbezogene Foren werden 90 Tage nach Löschen der Gruppe endgültig gelöscht.
	  ○ Eine Löschung erfolgt im Mailserver.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche

Dateien	• Berichtigungen von Daten können nur vom Anwender selbst vorgenommen werden. Andere Personen (z. B. Lehrer oder Administratoren) haben keinen Zugriff auf dessen Daten.

	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Änderungen an persönlichen und gruppenbezogenen Dateien sind jederzeit durch den Benutzer selbst möglich.
	  ○ Die persönlichen Dateien von gelöschten Benutzern werden nach 90 Tagen endgültig gelöscht. Dateien in Gruppenordnern werden 90 Tage nach Löschen der jeweiligen Gruppe endgültig gelöscht.
	  ○ Die Löschung erfolgt im Dateisystem.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche, Windows-Freigabe (SMB), WebDAV, FTP

Aufgaben	• Der Schüler sieht in der Weboberfläche jederzeit den aktuellen Stand seiner Abgabe. Er kann diese bei Änderungen oder Fehlern erneut hochladen und auch wieder löschen. • Maßnahmen zur Sperrung sind nicht vorgesehen. • Verfahren zur Übermittlung: Weboberfläche, Mailprogramme per (S)SMTP, POP3(S), IMAP(S)

Chat	• Berichtigungen sind nur im Chat selber und unmittelbar, allerdings nur nachträglich möglich.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Die Chatprotokolle werden für 3 Monate aufbewahrt.
	  ○ Die Löschung erfolgt im Dateisystem.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche

Adressbuch	• Berichtigungen von Adressbucheinträgen können nur vom Anwender selbst vorgenommen werden.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Änderungen am eigenen Adressbuch und seinem eigenen Kontakt im gemeinsamen Adressbuch sind jederzeit durch den Benutzer selbst möglich.
	  ○ Daten von gelöschten Benutzern werden ausgeblendet und nach 90 Tagen endgültig gelöscht.
	  ○ Eine Löschung erfolgt in der Datenbank.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche

Kalender	• Berichtigungen an Terminen sind im Rahmen der Berechtigungen jederzeit auch nachträglich möglich.

	• Eingetragene Termine können im Rahmen der Berechtigungen gelöscht werden. Eine Sicherheitsabfrage ist zu bestätigen. • Maßnahmen zur Sperrung sind nicht vorgesehen. • Es besteht die Möglichkeit Kalender als ICS-Datei zu im- und exportieren. • Der Kalender v2 unterstützt eine vollständige Synchronisation von Terminen über das CalDAV-Protokoll. • Das Kalendermodul bietet auch eine Funktion zum Abonnieren von externen Kalendern.

Internet	• Maßnahmen zur Berichtigung sind nicht vorgesehen.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Webproxy-Log: 7 Tage.
	  ○ Firewall-Log: 1 Monat
	  ○ Verbleibende Zeitguthaben zur Internetrecherche werden beim Löschen eines Benutzers ausgeblendet und nach 90 Tagen endgültig gelöscht.
	  ○ Eine Löschung erfolgt im Dateisystem.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: keine

Drucken	• Berichtigungen von Druckaufträgen können nur vom Anwender selbst vorgenommen werden.
	• Maßnahmen zur Löschung werden wie folgt beschrieben:
	  ○ Auf dem Server gespeicherte Druckaufträge können jederzeit durch den Benutzer selbst gelöscht werden.
	  ○ Druckaufträge von gelöschten Benutzern nach 90 Tagen endgültig gelöscht.
	  ○ Eine Löschung erfolgt im Dateisystem.
	  ○ Unabhängig davon können Daten noch für längere Zeit auf dem Backupserver vorgehalten werden.
	• Maßnahmen zur Sperrung sind nicht vorgesehen.
	• Verfahren zur Übermittlung: Weboberfläche, gängige Druckprotokolle (z. B. SMB, IPP)

Infobildschirm	• Änderungen der Inhalte von Infobildschirmen sind jederzeit möglich. • Die Löschung der Inhalte von Infobildschirmen ist jederzeit möglich. • Maßnahmen zur Sperrung sind nicht vorgesehen. • Eingestellte Inhalte werden auf dem Bildschirm angezeigt und können jedermann innerhalb der Schule wahrgenommen werden.
Buchungen	• Änderungen von Buchungen sind jederzeit möglich. • Die Löschung von Buchungen ist jederzeit möglich. • Maßnahmen zur Sperrung sind nicht vorgesehen. • Die Übermittlung der Buchungen ist nicht vorgesehen.

Klausurplan	• Änderungen am Klausurplan sind jederzeit möglich. • Die Löschung von Klausuren ist jederzeit möglich. • Maßnahmen zur Sperrung sind nicht vorgesehen. • Die Klausuren der nächsten 14 Tage werden auf dem IDesk der betroffenen Schüler angezeigt.

10. Allgemeine Beschreibung der nach den §§ 5 und 6 LDSG zur Einhaltung der Datensicherheit getroffenen Maßnahmen

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 den sechs Datensicherheits- und Datenschutz-Schutzzielen, die nachfolgend mit den für dieses Verfahren wichtigsten Maßnahmen aufgeführt werden.

11. Datenschutzrechtliche Beurteilung

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

- IServ läuft im Dauerbetrieb 24/7. Zeitliche Zugriffsbeschränkungen gibt es nicht.
- Die Daten werden täglich gesichert.
- Das Verfahren IServ wird auf einem separaten Backupserver im Netzwerk gesichert und kann vor dort aus wiederhergestellt werden.

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

- Für das Verfahren gelten die allgemeinen Zutritts-, 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 ausschließlich über Benutzeraccount 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 Fernwartungsauftragdatennehmer 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).

Transparenz (die automatisierte Verarbeitung von Daten kann mit zumutbarem Aufwand geplant, nachvollzogen, überprüft und bewertet werden):

- Die Dokumentation des IServ-Portalservers mit Weboberfläche, des Benutzerbereiches und der Administratoren, die Beschreibung der Module, die Einbindung der Windowsrechner sowie die Installation und Konfiguration ist dokumentiert unter http://iserv.eu/doc/.

Intervenierbarkeit (die Daten verarbeitende Stelle kann nachweisen, dass sie den Betrieb ihrer informationstechnischen Systeme steuernd beherrscht):

- Der in der Schule ansässige Systemadministrator kann sämtliche Einlogmöglichkeiten für Teilnehmer und Fernwartungsauftragdatennehmer jederzeit von jedem Ort sperren.
- Die zuständigen Systemadministratoren sind in der Verwendung des Verfahrens geschult.

Nicht-Verkettbarkeit (es kann sichergestellt werden, dass Daten nur zu dem Zweck automatisiert verarbeitet werden, zu dem sie erhoben wurden):

- Die Anwendung wird auf einem dedizierten Server betrieben, der nur zu diesem Zweck betrieben wird.

12. Freigabe

Kiel, 26.11.2013	
Ort, Datum	Unterschrift