Dieses Dokument informiert Sie darüber, welche Daten die einzelnen Module in IServ verarbeiten. Wir bemühen uns durch regelmäßige Prüfung und Aktualisierung. Die Liste ist alphabetisch sortiert, eventuelle Zusammenhänge sind in jedem Modul dokumentiert. Den personenbezogenen Daten ist jeweils ein Absatz gewidmet, sensible Daten sind ebenso separat je Modul Thema.
Bitte entnehmen Sie die Daten für die von Ihrer Schule ausgewählten Module.
Der Datenschutzbeauftragte der Schule ist grundsätzlich bei der Anwendung der Softwareprodukte einzubinden, dieser muss ggf. Risiken in den jeweiligen Anwendung erkennen.

PS: Informationen zu den Möglichkeiten der Module finden Sie unter https://www.iserv.de/doc/modules/

Inhaltsangabe

Adressbuch

Das Adressbuch spaltet sich in zwei Teile auf. Das „normale“ Adressbuch ist auf allen Server mit dem E-Mail-Modul installiert. Das gemeinsame Adressbuch ist aktuell noch auf allen Bestandsservern installiert. Es wurde aus dem Adressbuch herausgezogen und für die nahe Zukunft abgekündigt.

Welche personenbezogenen Daten werden verarbeitet?

Das Adressbuch bietet die Möglichkeit, eigene Kontakte anzulegen. Die Eingabe der Daten erfolgt ausschließlich durch den Nutzer.

Folgende Felder stehen dabei zur Verfügung:
Titel, Vorname, Nachname, Firma, Geburtstag, Nickname (nur zur Begrüßung in IServ verwendet), Klasse, Anschrift, Kontaktmöglichkeiten (Telefon, Handy, Fax, E-Mail, Homepage), Messenger-Dienste (ICQ, Jabber, MSN, Skype), Notizen und ein Foto.

Beim gemeinsamen Adressbuch können die oben genannten Informationen vom Nutzer selbst in ein schul-öffentliches Adressbuch eingetragen werden. Die Eingaben sind bis auf den Namen alle nicht verpflichtend. Der Nutzer kann nur seinen eigenen Eintrag bearbeiten. Zusätzlich zu den genannten Feldern wird die Option angeboten, sich selbst aus dem gemeinsamen Adressbuch auszublenden.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Es können nur vom Nutzer sensible Daten in Form von personenbezogenen Daten eingegeben werden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Beim gemeinsamen Adressbuch wird ein großer Warnhinweis vor dem Bearbeiten des eigenen Eintrags ausgegeben, dass die Daten schulöffentlich zu finden sind.

Wer muss Zugriff auf diese Daten haben?

Auf die Kontakte im eigenen Adressbuch hat nur der jeweilige Nutzer Zugriff.

Beim gemeinsamen Adressbuch haben alle Benutzer des Servers Zugriff auf diese Daten. Daher ist die Eingabe auch komplett freiwillig und nicht verpflichtend.

Sind alle Felder wirklich notwendig?

Beim Adressbuch sind die Felder für eine sinnvolle Nutzung erforderlich, jeder kann seine Daten hier eintragen, es ist nicht verpflichtend. Zudem wird gerade geprüft, ob alle Zugangsdaten noch notwendig sind, die Medien sind teils veraltet.

Beim gemeinsamen Adressbuch ist die Notwendigkeit nicht gegeben. Darum wird das Modul, wie oben bereits erläutert, eingestellt.

Werden Daten an Dritte weitergegeben und warum?

Nein. Es ist nur dem User möglich, seine eigenen Daten weiterzugeben.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Daten im eigenen Adressbuch und der Eintrag im gemeinsamen Adressbuch werden mit dem endgültigen Löschen des Nutzers entfernt. Ausblenden kann der User die Daten selbst.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

IServ bietet eine neuerdings sehr eingeschränkte Autovervollständigung für beispielsweise E-Mail-Adressen. Diese Autovervollständigung greift auf die Daten des eigenen Adressbuchs zurück.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Beim gemeinsamen Adressbuch kann der Nutzer Daten über sich veröffentlichen, die nicht veröffentlicht werden sollten. Da es sich hier größtenteils um Kinder handelt, muss hier eine Sensibilisierung stattfinden, solange das gemeinsame Adressbuch noch existiert.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Teilnehmer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Anbindung an Niedersächsische Bildungs-Cloud

Welche personenbezogenen Daten werden verarbeitet?

Das Modul synchronisiert Daten mit einer Zentralinstanz, die die Anbindung an die Niedersächsische Bildungs-Cloud zur Verfügung stellt.

Mandant:

* UUID des Servers
* Domain des Servers
* Letzter Synchronsierungszeitpunkt

Benutzer:

* Benutzername (z.B. max.mustermann)
* Vorname
* Nachname
* Erstellungszeitpunkt und Ersteller
* Löschzeitpunkt und löschender Benutzer
* Status (aktiv, inaktiv, eingeschränkt)
* Passworthash
* Importdaten
* Import ID
  * Zusätzliche Informationen
  * Typ

Gruppe:

* Accountname (z.B. klasse.5a)
* Name (z.B. Klasse 5a)
* Besitzer
* Erstellzeitpunkt und Ersteller
* Löschzeitpunkt und löschender Benutzer
* alle Mitglieder
* alle zugeordneten Rechte
* alle Gruppenmerkmale

Rollen:

* Rollenname
* bereitstellendes Modul, wenn vorhanden
* alle zugeordneten Rechte
* alle zugeordneten Benutzer

Rechte:

* Name
* bereitstellendes Modul
* Titel
* Beschreibung
* Invertierbarkeit

Gruppenmerkmale:

* Name
* bereitstellendes Modul
* Titel
* Beschreibung

Raum:

* Raumname
* Nummer
* Etage
* Ort

Gerät:
* Name
* Raum
* IP
* MAC-Adresse
* Typ
* kontrollierbar (ja/nein)
* Inventarnummer
* Beschreibung
* Internetzugang (ja/nein)
* Besitzer
* zuletzt gesehen

Weitere Details hierzu finden Sie unter:
* https://iserv.de/doc/modules/idm/
* https://iserv.de/doc/privacy/process-description/#nbc-anbindung

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Es werden vom Modul keine sensiblen Daten direkt abgefragt und verarbeitet. Über synchronisierte Gruppenmitgliedschaften sind aber beispielsweise Rückschlüsse auf die Weltanschauung von Benutzern möglich.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Einwilligungs- und Informationspflichten müssen individuell durch die Schulen eingeholt bzw. erfüllt werden. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung. Datenschutzhinweise finden Sie zusätzlich unter https://iserv.de/doc/privacy/process-description/#nbc-anbindung.

Für die Nutzung des Moduls ist ein AV-Vertrag mit der Landesinitiative n-21 notwendig.

Wer muss Zugriff auf diese Daten haben?

Berechtigte Administratoren haben Zugriff auf die Daten zur Systempflege. Außerdem können die Administratoren aus den synchronisierten Daten Felder an externe Anwendungen übergeben. Diese befinden sich außerhalb unseres Einflussbereiches.

Sind alle Felder wirklich notwendig?

Da es sich bei dem Modul um eine Schnittstelle handelt, ist es notwendig, umfangreich Daten zur Verfügung zu stellen, da die angebundenen Anwendungen unterschiedlichste Anwendungsfälle abdecken können. Die weitere Filterung der Daten liegt im Verantwortungsbereich der Landesinitiative n-21 Schulen in Niedersachsen online e.V.

Werden Daten an Dritte weitergegeben und warum?

Die Daten werden zur Anbindung an den Betreiber der Niedersächsische Bildungs-Cloud, die Landesinitiative n-21 Schulen in Niedersachsen online e.V., übermittelt.

Gibt es Löschfristen (automatisch oder empfohlen)?

Es gelten die üblichen Löschfristen. Löschungen auf dem IServ haben eine automatische Löschung auf dem NBC-Server zur Folge.

Sind alle Felder wirklich notwendig?

Da es sich bei dem Modul um eine Schnittstelle handelt, ist es notwendig, die angeforderten Daten zur Verfügung zu stellen, da die angebundenen Anwendungen unterschiedlichste Anwendungsfälle abdecken können. Die weitere Filterung der Daten liegt im Verantwortungsbereich der Landesinitiative n-21 Schulen in Niedersachsen online e.V. (https://www.n-21.de)

Werden Daten an Dritte weitergegeben und warum?

Die Daten werden zur Anbindung an den Betreiber der Niedersächsische Bildungs-Cloud, die Landesinitiative n-21 Schulen in Niedersachsen online e.V., übermittelt. Da hierfür ein AV-Vertrag notwendig ist, handelt es sich nicht um Dritte. Ein Hinweis auf den nötigen AV-Vertrag sollte eingebaut sein...

Gibt es Löschfristen (automatisch oder empfohlen)?

Es gelten die jeweiligen Löschfristen, denn Löschungen auf dem IServ haben eine automatische Löschung auf dem NBC-Server zur Folge.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Nein.
Die Daten werden von externen Anwendungen (siehe AV-Vertrag Bildungscloud) weiter verarbeitet. Zur Synchronisierung mit der Zentralinstanz kommt das IDM-Modul zum Einsatz.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

IServ verarbeitet hier keinerlei Daten, die eine Auswertung oder Profilbildung möglich machen würden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Da in dem Modul umfangreiche Daten an einen Drittanbieter übermittelt werden, ergibt sich ggf. ein erhöhtes Risiko der Kompromittierung von Daten. Bei der Landesinitiative n-21 Schulen in Niedersachsen online e.V. handelt es sich zwar grundsätzlich um einen staatlichen Anbieter, trotzdem erhöhen gerade die externen Anwendungen das Risiko erheblich. Wie oben beschrieben ist dies zu regeln zwischen Schule und n-21.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Die übertragenen Passwort-Hashes entsprechen aktuellen Empfehlungen der Industrie.

Apps

IServ bietet Apps für mobile Endgeräte auf Basis von Apple iOS und Android. Die App verhält sich nach der Anmeldung ähnlich zu einem Webbrowser und speichert keine Daten auf dem lokalen Gerät.

Zusätzlich funktioniert die App als Empfangsmedium für Benachrichtigungen. Dabei werden vom Server Benachrichtigungen über die Apple/Google-Dienste an die Mobilgeräte gesendet. Die Betreiber der Benachrichtigungsdienste sehen nur die Identifikationsnummer einer Benachrichtigung und eine pseudonymisierte Kennung des Accounts, die Inhalte werden direkt zwischen der App und dem jeweiligen IServ Portalserver ausgetauscht.

Darüber hinaus bieten Smartphones vielfältige Funktionen, die personenbezogene Daten mit anderen Apps oder den Herstellern wie Apple und Google teilen, z. B. Cloud-Backups.

Diese werden vom Nutzer selbst konfiguriert und liegen außerhalb des Wirkungskreises des Serverbetreibers.

Welche personenbezogenen Daten werden verarbeitet?

Die Apps nutzen den Benutzernamen und das Passwort für die Authentifizierung. Auf dem Gerät wird dann ein Anmeldeschlüssel gespeichert. Die Zugangsdaten werden nur für die Erstellung des Anmeldeschlüssels benötigt und nicht weiter gespeichert. Weitere Daten erfasst die App nicht.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Nutzung der App auf privaten Smartphones kann durch die Schule erlaubt/verboten werden. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/.

Wer muss Zugriff auf diese Daten haben?

Außer dem User niemand

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Es gelten die Löschfristen der enthaltenen Module. Die App wird nur durch den User selbst gelöscht. Der Zugriff auf die Daten ist zum Ende des Schulbesuchs durch die Schule zu verweigern, die Daten müssen dann gelöscht werden.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine Daten werden in anderen Modulen verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Bei Verlust eines nicht-gesicherten Mobilgeräts könnten Finder auf die Daten im IServ zugreifen, da die Anmeldung für das Gerät gespeichert wird. Es sollte daher Anweisungen zur Nutzung der App geben, bei Verlust umgehend das Passwort zu ändern (Im Dokumentenpaket per Download enthalten).

Welche technischen Maßnahmen schützen diese Daten?

Ggf. Verschlüsselung des Handys, keine automatische Anmeldung

Brockhaus Integration

Welche personenbezogenen Daten werden verarbeitet?

Es werden hier keine personenbezogenen Daten verarbeitet. Das Modul bindet lediglich eine externe Webseite ein.

Datenschutzbestimmungen des Drittanbieters finden Sie unter:
https://brockhaus.de/info/service/datenschutzerklaerung/

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Benutzer haben auf der eingebundenen Webseite die Möglichkeit sich über Datenschutzbestimmungen und Nutzungsbedingungen zu informieren.

Wer muss Zugriff auf diese Daten haben?

-

Sind alle Felder wirklich notwendig?

-

Werden Daten an Dritte weitergegeben und warum?

Das Modul bindet eine spezielle Version der Webseite "brockhaus.de" ein. Durch die Einbindung werden von den Browsern der Benutzer Daten übermittelt. Diese unterliegen den Datenschutzbestimmungen und Nutzungsbedingungen des Anbieters.

Gibt es Löschfristen (automatisch oder empfohlen)?

Nein

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Die App gibt die Daten in den anderen Modulen wie über den Browser aus.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Es bestehen die üblichen Cookie- und Tracking-Risiken wie beim Besuch von allen externen Webseiten.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Das mobile Gerät könnte in unbefugte Hände geraten, sollte daher gesichert sein per Fingerabdruck o.Ä.

Welche technischen Maßnahmen schützen diese Daten?

Es erscheint beim Anwählen ein Hinweis, dass die Daten durch den jeweiligen Seitenanbieter verarbeitet werden. Die App benötigt eine Anmeldung

Buchungen

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer-IDs, Gruppenmitgliedschaften, ausgeführte Aktionen und Buchungszeiten verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein. Es wird im Modul nur der Name des Buchenden ausgegeben.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Buchungen sind eingeschlossen in die allgemeine Einwilligung, IServ nutzen zu können. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/.

Wer muss Zugriff auf diese Daten haben?

Zugriff auf die Daten haben jeweils Benutzer mit den passenden Rechten "Buchungen administrieren", "Buchungen durchführen", "Buchungen einsehen", "Buchungen im Namen anderer Nutzer durchführen" und "Wiederkehrende Buchungen durchführen". Der Zugriff auf einzelne buchbare Objekte kann weiter auf Gruppen eingeschränkt werden. Benutzer mit dem Recht "Buchungen administrieren" haben grundsätzlich Zugriff auf alle im Modul anfallenden Daten.

Sind alle Felder wirklich notwendig?

Ja, ohne diese daten wäre keine Organisation von Buchungen möglich.

Werden Daten an Dritte weitergegeben und warum?

Nicht durch das Programm. Im Rahmen des Organisierens ist es manchmal durchaus notwendig, diese Daten (einzelne Buchungen) Dritten bekannt zu machen.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Aktionen im Modul können zum Versenden von Benachrichtigungen führen, die dann im Kern-Modul weiter verarbeitet werden.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Buchungen sind Rückschlüsse auf die Nutzung von Räumen und Arbeitsmitteln der jeweiligen Benutzer möglich.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Da nur der Buchende selbst als personenbezogenes Datum existiert, ist kaum ein Risiko zu erkennen

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Durch eine feine Einstellung von Rechten und Freigaben kann die Einsicht von Daten auf einen absolut notwendigen Kreis begrenzt werden.

Aufgaben

In diesem Modul können Aufgaben von Benutzern an andere Benutzer gestellt werden, von diesen wieder abgegeben werden inklusive Nachbesprechung. Es werden dabei folgende Benutzergruppen klassifiziert:

Teilnehmer: Einfache Benutzer, die die Aufgabe bearbeiten sollen
Ersteller: Benutzer mit dem Recht Aufgaben zu erstellen.
Verwalter: Benutzer, die verwaltenden Zugriff auf die Aufgabe eines anderen Benutzers erhalten hat.

Verwalter werden jeweils vom Ersteller einer Aufgabe festgelegt und können jederzeit angepasst werden.

Der einfache Arbeitsfluss des Moduls sieht vor, dass eine Aufgabe vom Ersteller angelegt wird und die Teilnehmer diese dann bearbeiten und ihr Ergebnis wieder hochladen. Ersteller und Verwalter können dann optional das Ergebnis mit dem Teilnehmer schriftlich besprechen.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein. Lediglich Bewertungen der abgegebenen Ergebnisse können Inhalt sein

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Das Aufgabenmodul ist Teil der allgemeinen Einwilligung in die Verwendung von IServ. Dieses Dokument soll als detaillierte Information gelten und sollte verfügbar gemacht werden.

Wer muss Zugriff auf diese Daten haben?

Teilnehmer haben Zugriff auf die Aufgabenstellungen und eventuell angehängte Dateien. Dies ist für die Bearbeitung notwendig. Außerdem können die Teilnehmer das Arbeitsergebnis als „Abgabe“ dem Ersteller zur Verfügung stellen.

Ersteller und Verwalter haben den gleichen Zugriff auf die Aufgabe, die Abgaben und die Rückmeldungen.

Teilnehmer können, falls genutzt, dann noch die Rückmeldung von Ersteller / Verwalter für die eigene Abgabe(n) einsehen.

Sind alle Felder wirklich notwendig?

Ja. Dies ist ein Kernmodul für den Unterricht.

Werden Daten an Dritte weitergegeben und warum?

Es ist keine Weitergabe vorgesehen. Werden Dateien dennoch weitergegeben, ist dies in der Verantwortung der Schule zu sehen, sollte ggf. geregelt werden.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht. Die Lehrer werden angehalten, die Aufgaben jeweils zum Schuljahresende zu löschen.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Aktionen im Modul können zum Versenden von Benachrichtigungen führen, die dann im Kern-Modul weiter verarbeitet werden.

Außerdem zeigt eine Informationskachel auf der Startseite live die Aufgaben an, die in den nächsten 14 Tagen bearbeitet werden müssen. Dabei wird nur der Titel der Aufgabe angezeigt. Personenbezogene Daten sind lediglich im Inhalte der Texte möglich.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Für Verwalter und Ersteller besteht die Möglichkeit das Arbeitsverhalten eines Nutzers im Rahmen der eigenen Tätigkeit zu analysieren. Ein Gesamtbild über Aufgaben anderer Ersteller ist nicht möglich. Dieses Modul hat die pädagogische Bewertung als Ziel.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hochgeladen werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich haben nur die Ersteller / Verwalter und Teilnehmer

Zugriff auf die notwendigen Daten. Dabei hat jeder Teilnehmer nur auf die vom ihm erstellten Daten Zugriff. Einen Zugriff auf die Daten anderer Teilnehmer haben die Teilnehmer nicht.

Curriculum

In diesem Modul können Lehrpläne von Benutzern erstellt, eingesehen und verwaltet werden.
Für die Verwendung des Moduls werden drei Berechtigungsstufen unterschieden.

Curriculum einsehen: Benutzer mit diesem Recht dürfen die Planung für alle Bildungsgänge und deren Zeiträume sehen, die Planung der Unterrichtseinheiten nicht.

Zugang zum Material: Benutzer mit diesem Recht dürfen die komplette Planung einsehen.
Curriculum verwalten: Benutzer mit diesem Recht dürfen das komplette Curriculum verwalten und einsehen.

Benutzer ohne eines dieser Rechte haben keinen Zugriff auf das Modul.

Die Rechtevergabe erfolgt durch die Administration im Administrationsbereich.

Der einfache Arbeitsfluss des Moduls sieht vor, dass Bildungsgänge durch einen Benutzer erstellt, verwaltet und geändert werden können. Optional durch Zuordnung eines Teams (Gruppe von Benutzern) können weitere bearbeitende Rechte an Benutzer vergeben werden. Diese sind auch im Nachhinein veränderbar.
In den Bildungsgängen können Lernsituationen, bestehend aus Zeiträumen und Phasen, erfasst werden.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Einwilligungs- und Informationspflichten müssen individuell durch die Kunden (Schulen) eingeholt bzw. erfüllt werden. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung.

Wer muss Zugriff auf diese Daten haben?

Ersteller sowie Benutzer, die dem zugewiesenen Team angehörig sind, haben Zugriff auf die Bildungsgänge sowie Lernsituationen und eventuell angehängte Dateien. Dies ist für die Bearbeitung notwendig.

Ersteller und Benutzer, die dem vom Ersteller zugewiesenen Team angehörig sind, haben den gleichen Zugriff auf Lernsituationen und deren Zeiträume.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die vom Nutzer erzeugten Inhalte bleiben auch nach dem Löschen des Nutzers im System, da diese Daten in der Regel personenübergreifend erstellt und weiter benötigt werden. Die Verknüpfungen zum Nutzer werden bei Löschung entfernt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Aktionen im Modul können zum Versenden von Benachrichtigungen führen, die dann im Kern-Modul weiter verarbeitet werden.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Für Ersteller und Benutzer, die dem zugewiesenen Team angehörig sind, besteht die Möglichkeit das eigene Arbeitsverhalten zu analysieren.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hochgeladen werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich haben nur die Ersteller und Benutzer, die dem optional zugewiesenen Team angehörig sind, Zugriff auf die notwendigen Daten.

Drucken

In diesem Modul können durch Dateiauswahl oder Upload Dateien auf hinterlegten Drucker-Geräten gedruckt werden.

Benutzer: Einfache Benutzer, die Dateien drucken können
Verwalter: Benutzer, die das Recht „Verwaltung von Guthaben“ erhalten haben

Verwalter werden durch die Rechtevergabe im Administrationsbereich festgelegt.

Der einfache Arbeitsfluss des Moduls sieht vor, dass Benutzer Dateien von ihrem Gerät hochladen oder eine bereits dem Benutzer zugängliche Datei aus dem Modul „Dateien“ zum Druck vorbereiten können. Die Datei wird im Modul in einer Vorschau ausgegeben. Dort kann der Druck auf einen von Benutzer ausgewählten Drucker gedruckt werden.

Der Verwalter kann zudem virtuelles Guthaben verwalten und den virtuellen Kontostand aller der im Modul hinterlegten Benutzer einsehen.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Voraussetzung für die Nutzung von IServ ist eine Einwilligung der Verarbeitung der eigenen Daten. Detaillierte Information erlangt man durch dieses Dokument oder die Verfahrensbeschreibung auf der Homepage.

Wer muss Zugriff auf diese Daten haben?

Der Benutzer, der dieses Modul verwendet, hat Zugriff auf die von ihm dem Modul bereitgestellten Dateien.
Verwalter haben Zugriff auf den virtuellen Kontostand aller in dem Modul hinterlegten Benutzer und können Benutzern über Gruppenzuordnung oder Direktzuweisung weiteres Guthaben hinzufügen.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine Daten werden in anderen Modulen verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Für Verwalter besteht die Möglichkeit, das Druckverhalten eines Nutzers im Rahmen des verwendeten virtuellen Kontostandes zu analysieren. Dabei ist die Beobachtung des Guthabens notwendig, ein Protokoll wann welches Guthaben verwendet wird, gibt es nicht.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hochgeladen werden. Ausschlaggebend hierfür ist das jeweilige Schulgesetz des Bundeslandes.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich hat nur der Benutzer Zugriff auf die eigenen Daten. Einen Zugriff auf die Daten anderer Benutzer besteht nicht.

Dateien

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer ID, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Welche sensiblen Daten lt. Art 9 DSGVO verarbeitet?

Derartige Datenarten können nur durch die Nutzer selbst verarbeitet werden, es sind die für das Bundesland geltenden Schulgesetze zu beachten.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Einwilligungs- und Informationspflichten müssen individuell durch die Kunden (Schulen) eingeholt bzw. erfüllt werden. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/.

Wer muss Zugriff auf diese Daten haben?

Zugriff auf die benutzergenerierten Inhalte haben jeweils die Eigentümer der Dateien und ggf. bei Verwendung von Gruppenordnern die Mitglieder und Eigentümer der Gruppe. Auf die Logdateien besteht nur Zugriff durch berechtigte Administratoren.

Sind alle Felder wirklich notwendig?

Ja. Die Felder werden zur Organisation und zum Nachweis von Aktionen im Dateien-Bereich benötigt.

Werden Daten an Dritte weitergegeben und warum?

Eine automatische Weitergabe an Dritte findet nicht statt. Die Daten werden nur durch Freigaben der Benutzer selbst weitergegeben. Ob eine Freigabe notwendig ist, müssen die Benutzer selbst entscheiden.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Dateien werden mit dem Löschen der Benutzer gelöscht. Dateien in Gruppenordnern werden durch das Löschen der Gruppe gelöscht. Logdateien werden 6 Monate zur Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups verlängern.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Benutzergenerierte Inhalte können in andere Module eingebettet oder aus dem berechtigten Dateibereich importiert werden.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Erfassung von Zugriffszeiten wäre es möglich, Rückschlüsse auf die Arbeitszeiten von Benutzern zu ziehen. Die Auswertung von Dateinamen ergibt ggf. auch Ansätze.
Die eigenen Dateien sind aber nur für den User selbst einseh- und auswertbar.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hochgeladen werden. Durch die Windows-Anbindung des Datei-Moduls können auch beispielsweise Browserverläufe und Datenbanken von Passwortmanagern auf dem IServ gespeichert werden. Wir empfehlen, solche Daten zur verschlüsselt zu speichern und auf die dienstliche Nutzung zu beschränken.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Auf dem zu Grunde liegendem Linux-Betriebssystem werden die Dateien mit jeweils getrennten Eigentümern gespeichert und nur bei Bedarf weiteren Benutzern freigegeben.

Edupool

Welche personenbezogenen Daten werden verarbeitet?

Land, Bundesland, Bezirk und Schule des Benutzers, sitzungsspezifische ID, E-Mail-Adresse, Benutzername, Vor- und Nachname, Rollen (Lehrer/Schüler), Gruppenmitgliedschaften sowie die Klassenstufe.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Aus den Gruppenmitgliedschaften sind ggf. Hinweise auf die Weltanschauung abzuleiten.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Informationspflichten müssen individuell durch die Kunden (Schulen) eingeholt bzw. erfüllt werden. Hierzu kann dieses Dokument auch verwendet werden. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/#edupool.

Datenschutzbestimmungen des Anbieters finden Sie unter:
https://niedersachsen.edupool.de/edupool/versions/2.6/images/common/Ant_Impudat.pdf

Wer muss Zugriff auf diese Daten haben?

Berechtigte Administratoren haben auf die Daten zur Systempflege Zugriff.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Da das Modul eine Drittanbieter-Anwendung einbindet, ist die Übertragung zwingend nötig. Die Übertragung erfolgt an das vom Medienzentrum Niedersachsen beauftragte Unternehmen ANTARES PROJECT GmbH.

Gibt es Löschfristen (automatisch oder empfohlen)?

Nein

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Bedingt durch die Authentifizierung per OAuth können Benutzer bei späterer Nutzung der Webseite wiedererkannt werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Es besteht kein weiteres Risiko.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Elternregistrierung

Es gibt die Möglichkeit, zu bestehenden Schülerkonten einen Eltern-Account anlegen zu lassen.

Welche personenbezogenen Daten werden verarbeitet?

Im Eltern-Import übertragene Daten (* = Pflichtangabe): *Name & Vorname, *Import-Id des Kindes bzw. der Kinder, E-Mail-Adresse, Telefonnummer/Handy, Adresse. Die optionalen Daten werden genutzt, um mögliche Duplikate von Nutzer(innen) identifizieren und zusammenführen zu können. * Bei der Eltern-Registrierung muss das Elternteil eine persönliche E-Mail-Adresse und ein Passwort, das verschlüsselt gespeichert wird, angeben.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?
Anhand der Vornamen oder Namen gemeinsamer Elternteile könnten sexuelle Orientierung oder Herkunft der Eltern interpretiert werden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?
Zusammen mit der Einwilligungserklärung erhalten die Eltern die gesetzlichen Informationen.

Wer muss Zugriff auf diese Daten haben?
Die Daten werden beim Anlegen oder Import nur den Admins verfügbar gemacht.
Sind alle Felder wirklich notwendig?
Pflichtfelder sind für die Accountverwaltung notwendig.
Optionale Daten dienen der Identifikation einer Person und werden nur zu diesem Zweck gespeichert.

Werden Daten an Dritte weitergegeben und warum?
Nein

Gibt es Löschfristen (automatisch oder empfohlen)?
Zugänge von Eltern-Accounts, denen keine Kinder zugeordnet sind, werden automatisch gesperrt.
Admins können Eltern-Accounts, denen keine Kinder zugeordnet sind, filtern und löschen.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?
Name, Vorname, Kind-Verknüpfung werden in anderen Modulen genutzt.
Hierzu zählt das Modul Elternbriefe.
Die Mail-Adresse wird für den Login verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?
Eltern können mit ihren Kindern in Verbindung gebracht werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?
Nur Admins haben Zugang zu den erhobenen Daten und dürfen diese nur zu Verwaltungszwecken auf Weisung der Schulleitung, laut Admin-Verpflichtung, nutzen

Welche technischen Maßnahmen schützen diese Daten?
Nur Inhaber der Rolle „Administrator“ haben Zugriff auf die Daten. Die Rollen- und Rechtevergabe obliegt der Schule.

Elternbriefe

Das Modul Elternbriefe ermöglicht es Lehrer(innen) über ihre Schüler(gruppen) mit Eltern in Kontakt zu treten.

Welche personenbezogenen Daten werden verarbeitet?
Name und Vorname von Benutzern,

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Anhand der Vornamen oder Namen gemeinsamer Elternteile könnten sexuelle Orientierung oder Herkunft der Eltern interpretiert werden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?
Zusammen mit der Einwilligungserklärung erhalten die Eltern die gesetzlichen Informationen.

Wer muss Zugriff auf diese Daten haben?
Personen mit der Berechtigung Elternbriefe schreiben zu dürfen, in der Regel Lehrer(innen) und die Schulverwaltung. Die Rechtevergabe obliegt der Schule.

Sind alle Felder wirklich notwendig?
Ja.

Werden Daten an Dritte weitergegeben und warum?
Nein

Gibt es Löschfristen (automatisch oder empfohlen)?
Lehrer(innen) sind Inhaber(innen) der von ihnen verfassten Elternbriefe und können diese und implizit alle zugehörigen Antworten löschen.
Kinder sind die Empfänger der Elternbriefe. Eltern können Elternbriefe über ihre Kinder abrufen.
Eltern können ihre Antworten zu einem Elternbrief löschen
Antworten werden automatisch gelöscht, nachdem das Kind (Empfänger) gelöscht wurde.
Elternbriefe werden automatisch gelöscht, wenn sowohl keine Kinder (Empfänger) mehr existieren, als auch der Inhaber nicht mehr existiert.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?
Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?
Eltern können mit ihren Kindern in Verbindung gebracht werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?
Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer in IServ verarbeitet werden.

Welche technischen Maßnahmen schützen diese Daten?
Nur Inhaber des Rechts "Elternbriefe schreiben" haben Zugriff auf die Daten. Die Rollen- und Rechtevergabe obliegt der Schule.
Eltern sehen nur die, über ihre verknüpften Kinder, an sie adressierten Elternbriefe und die eigenen Antworten.
Die Verknüpfung von Eltern und Kindern obliegt der Schuladministration.

E-Mail

Welche personenbezogenen Daten werden verarbeitet?

Das Modul wird zum Senden und Empfangen von E-Mails verwendet und verarbeitet damit auch alle Informationen, die normalerweise mit einer E-Mail in Verbindung stehen. Dazu zählt die E-Mail-Adresse von Absender und Empfänger, Betreff und Inhalt. Außerdem werden Meta-Informationen, wie Versandzeitpunkt, Verlauf über E-Mail-Server verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nicht durch IServ. Die Inhalte der Mails sind durch die Schule und die Teilnehmer zu verantworten

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?
Das Mailmodul ist Teil der allgemeinen Einwilligung in die Verwendung von IServ. Dieses Dokument soll als detaillierte Information gelten und sollte verfügbar gemacht werden.

Wer muss Zugriff auf diese Daten haben?

Nur der Benutzer hat Zugriff auf seine E-Mails.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Eine automatische Weitergabe an Dritte findet nicht statt. Der Versand von E-Mail-Nachrichten an externe E-Mail-Adresse erzwingt die Weitergabe der gesamten E-Mail-Nachricht an Fremdserver, die nicht den Datenschutzrichtlinien von IServ unterliegen. Das Mailen außerhalb IServs ist ein Recht, dass Gruppen zugewiesen werden kann.

Der Benutzer hat außerdem die Möglichkeit, eine automatische Weiterleitung auf eine beliebige E-Mail-Adresse einzurichten. Ein entsprechender Datenschutzhinweis wird bei der Einstellung angezeigt. Eine Vermischung von privaten und dienstlichen Mails sollte unterbleiben und geregelt sein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Es werden keine E-Mail-Nachrichten automatisch aus den Benutzerkonto entfernt. Es gelten folgende Ausnahmen:

- E-Mails werden beim Löschen zunächst in den Ordner „Papierkorb“ verschoben und dort nach 7 Tagen automatisch endgültig gelöscht. Der Benutzer kann E-Mails im Ordner „Papierkorb“ auch sofort manuell löschen.
- E-Mails, die als Spam erkannt werden, werden automatisch in den Ordner „Unerwünscht“ sortiert und automatisch nach 30 Tagen entfernt.

Sämtliche Inhalte des Moduls werden beim endgültigen Löschen des Benutzers automatisch entfernt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Das Empfangen von E-Mails löst das Versenden von Benachrichtigungen aus, die dann im Kern-Modul weiter verarbeitet werden. Die Benachrichtigungen werden nur dem Empfänger zugestellt, dies kann eine einzelne Person, aber auch eine Gruppe sein.

Außerdem können auf der Startseite die Betreffzeilen der neusten 5 ungelesenen Nachrichten oder nur die Anzahl der ungelesenen Nachrichten angezeigt werden. Die Daten werden live aus dem E-Mail-Modul abgerufen. Eine Zwischenspeicherung findet nicht statt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Da nur der Benutzer selbst Zugriff auf seine E-Mail-Nachrichten hat, ergibt sich keine Möglichkeit der Auswertung oder Profilbildung. Denkbar wäre nur eine Auswertung von Mail-Inhalten und Mengen anderer Teilnehmer, die diese Mails selbst gesendet haben.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer in IServ verarbeitet werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

E-Mail-Nachrichten, die an andere Benutzer des gleichen IServ-Servers gesendet werden, verlassen technisch gesehen nie den Server und werden direkt zugestellt. Die Zustellung zwischen verschiedenen IServ-Servern findet grundsätzlich verschlüsselt statt.

Bei Zustellung von fremden Servern wird der Versand soweit möglich verschlüsselt durchgeführt. Da diese Server nicht der Kontrolle der IServ GmbH unterliegen, ist eine umfassende Verschlüsselung nicht zu garantieren.

Sollen Mails verschlüsselt versendet werden, kann dies über Zip-Dateien oder ein separate Tool realisiert werden.

Fernwartung

Das Modul selbst verarbeitet keine personenbezogenen Daten, gewährt allerdings ausgewählten Mitarbeitern den Zugriff auf die Daten eines Servers. Der Zugriff setzt einen Auftragsverarbeitungsvertrag voraus und wird durchgehend protokolliert.

Welche personenbezogenen Daten werden verarbeitet?

Das Modul selbst verarbeitet keine personenbezogenen Daten.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Diese sollten nach Möglichkeit nicht durch den Verantwortlichen sichtbar gemacht werden, Grenzen sind hier auch durch das jeweilige Schulgesetz gegeben.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Fernwartung geschieht auf Weisung des Verantwortlichen, IServ ist Auftragsverarbeiter, dies sollte den Betroffenen bekannt gemacht werden..

Wer muss Zugriff auf diese Daten haben?

Zugriff auf Daten ist abhängig von der Weisung der Schule.

Sind alle Felder wirklich notwendig?

./.

Werden Daten an Dritte weitergegeben und warum?

Nein, im Extremfall könnte ein Unter-Auftragnehmer hinzugezogen werden.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Protokolle werden zum Ticket gespeichert und mit diesem gelöscht.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine, die Fernwartung findet aber ggf. in anderen Modulen statt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Hier sind die Möglichkeiten durch Regelungen zu Administrator- und Fernwartungsrechten beschränkt und würden Konsequenzen haben.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keines, da die Vorgehensweise durch den AV-Vertrag geregelt ist und Vertraulichkeit vereinbart ist.

Welche technischen Maßnahmen schützen diese Daten?

Nur speziell ausgebildete und namentlich festgelegte Mitarbeiter dürfen Fernwartung machen, deren Name wird im Protokoll festgehalten.

Forum

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Klarname, Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Im Forum muss zwischen 3 Arten unterschieden werden

- Öffentliches Forum**:** Alle Benutzer des IServ haben auf diese Art des Forums uneingeschränkten Zugriff.

- Forum für eine oder mehrere Gruppen**:** Zugriff wird auf bestimmte, zugewiesene Gruppen beschränkt.
- Gruppenforum**:** Zugriff haben nur die Mitglieder der entsprechenden Gruppe.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nicht über definierte Felder. Für die Inhalte sind die Betroffenen selbst bzw. die Schule verantwortlich.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Foren sind über die Einwilligung in die IServ-Nutzung geregelt, die detaillierte Information ist diesem Dokument zu entnehmen.

Wer muss Zugriff auf diese Daten haben?

Zur Identifikation des Erstellers innerhalb der Beiträge des Moduls benötigen alle Benutzer, des dem jeweiligen Benutzer zugesprochenen Foren-Bereiches, Zugriff auf den Benutzernamen des Erstellers.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nicht durch den Hersteller. Es besteht hier die Möglichkeit, Inhalte per Mail an Dritte zu übermitteln.

Gibt es Löschfristen (automatisch oder empfohlen)?

Beim Löschen eines Benutzers wird der Autorenname aus all seinen Forenbeiträgen gelöscht. Der Inhalt der Forenbeiträge bleibt jedoch bei schulöffentlichen Foren dauerhaft und bei gruppenbezogenen über die Lebenszeit der jeweiligen Gruppe erhalten. Das Löschen ganzer Foren ist an Admin-Rechte gebunden.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Beim Erstellen von Beiträgen und Antworten werden Benachrichtigungen ausgelöst, die dem Ersteller sowie abonnierten Benutzern des Beitrages zugestellt werden. Diese werden zu diesem Zweck auch im Kern-Modul weiter verarbeitet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Erstellung von Beiträgen und Abonnements Möglichkeit zu Beiträgen sind Rückschlüsse auf die vom Benutzer interessierten Themenbereiche möglich.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass

besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer erstellt / hochgeladen werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung), Zugang haben nur Moderator und Eingeladene.

Bei mit Gruppenzugehörigkeit gesteuerten Foren können durch Benutzer erstellte Beiträge nur durch Benutzer derselben Gruppe eingesehen werden.

Der Benutzer hat jederzeit die Möglichkeit, den eigenen hinzugefügten Beitrag zu verändern und dem Beitrag angefügte Dateien zu löschen.

Gerätebewerbung

Das Modul Gerätebewerbung ermöglicht es den Nutzern von IServ, Anträge auf Aufnahme ihrer Notebooks oder anderer mobiler Endgeräte in die IServ-Geräteverwaltung zu stellen. Die Anträge werden dann von einem Administrator geprüft und entweder angenommen oder abgelehnt.

Welche personenbezogenen Daten werden verarbeitet?

- Bei der Aufnahme eines Gerätes können diverse Informationen erfasst werden. Hierzu zählt die MAC und IP-Adressen der Netzwerkschnittstellen. Die MAC-Adresse lässt unter Umständen erkennen, um welchen Hersteller bzw. um welchen Gerätetypen es sich handelt.
- Das Gerät wird dem Antragsteller zugeordnet.

In dem Modul werden des Weiteren der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen des Zugrifflogs verarbeitet. Dies betrifft sowohl den Prozess der Antragstellung sowie auch die Verwaltung der Anträge.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Es ist in Arbeit, einen Hinweis bei der Bewerbung auszugeben. Ansonsten ist dieses Dokument zu verwenden.

Wer muss Zugriff auf diese Daten haben?

Das Modul befindet sich im Verwaltungsbereich und ist daher ausschließlich von der Administration zugänglich. Auf Logdateien besteht ebenfalls nur Zugriff durch berechtigte Administratoren. Diese müssen eine Verpflichtung durch die Schule nachweisen können

Der Antragsteller hat keinen Zugriff auf die Daten anderer Benutzer dieses Moduls.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die von Nutzer registrierten Geräte werden mit der Löschung des Nutzers automatisch aus dem System entfernt. Bei Wechsel auf ein anderes Gerät wird das alte zu entfernen.

Logdateien werden 7 Tage zur möglichen Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups auf maximal 6 Monate verlängern.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Das vom Benutzer angegebene Gerät wird mit einer freien IP-Adresse und Zuweisung des entsprechenden Benutzers in das Modul „Geräteverwaltung“ übertragen.

Der Benutzer erhält eine Entscheidung über den Antrag über das Modul „E-Mail“. Dazu wird die interne E-Mail Adresse des Benutzers verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Erfassung der Mac-Adresse können Rückschlüsse auf das Gerätemodell getätigt werden. Durch die Log-Dateien können Rückschlüsse auf die Häufigkeit der Anmeldungen gezogen werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keines außer den Genannten.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).Grundsätzlich hat nur die Administration Zugriff auf die Daten der Antragssteller. Der Zugriff wird durch Rechtevergabe gesteuert.

Gerätesteuerung

Das Modul erlaubt es berechtigten Nutzern, Befehle an Computer im lokalen Netzwerk zu senden. Das Modul „Rechnersperre“ ist dabei eine Erweiterung und erlaubt es Computer so zu sperren, dass eine Nutzung nicht mehr möglich ist.

Keine der zur Verfügung stehenden Funktionen ermöglicht den Zugriff auf die Daten auf dem jeweiligen Computer.

Welche personenbezogenen Daten werden verarbeitet?

- Der Benutzer hat Zugriff auf die für ihn über das Modul „Geräteverwaltung“ angelegten Geräte (Gerätenamen) und dessen zugeordneten Benutzer (Benutzernamen). Der Benutzername des angemeldeten Benutzers wird allerdings nur angezeigt, wenn der berechtigte Nutzer sich im lokalen Netzwerk der Schule befindet. Beim Zugriff aus dem Internet wird diese Information nicht angezeigt.
- Es kann der Klausurmodus gesteuert werden. In diesem Modus sind über die Benutzernamen hinaus auch der Raum und Zuordnung zur Klausur der Benutzer möglich.

In dem Modul werden des Weiteren der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen des Zugrifflogs verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Im Rahmen der Einwilligung zur Nutzung von IServ. Natürlich kann dieses Dokument auch hinzugezogen werden.

Wer muss Zugriff auf diese Daten haben?

Zur Ausübung der Modul-Funktion wird der Zugriff nur den Benutzern gestattet, die mit dem benötigten Recht durch die Administration versehen wurden.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Logdateien werden 7 Tage zur Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups auf maximal 6 Monate verlängern.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Dieses Modul konsumiert Daten vom Modul „Geräteverwaltung“. Durch die Verwendung dieses Moduls kann der Klausurmodus aktiviert werden (s.o.).

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Über die Beobachtung der angemeldeten Benutzer lässt sich eine Auswertung des Arbeitsverhaltens erstellen. Dies kann nur aus dem lokalen Netzwerk der Schule heraus als Administrator geschehen. Dies ist noch ein Grund für die Administratorenverpflichtung.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Kein weiteres als das Genannte.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Die Verwendung des Moduls ist nur mit dazu bestimmter Berechtigung möglich. Für den Klausurmodus hat standardmäßig nur die Gruppe Admins die benötigten Rechte.

Auf die weiteren Logdateien besteht nur Zugriff durch berechtigte Administratoren, der Zugriff ist zu regeln.

Geräteverwaltung

Die Geräteverwaltung speichert Informationen von Geräten, die aufgenommen werden, unabhängig davon, ob es sich dabei um ein privates Gerät oder um ein Gerät der Organisation handelt. Unbekannte Geräte im Netzwerk sind über die Funktion „Unbekannte Geräte“ sichtbar, werden allerdings nicht dauerhaft gespeichert.

Zur Geräteverwaltung zählt auch das Modul „MacOS-Unterstützung“ und ermöglicht die Anmeldung an MacOS-Geräte über das lokale Netzwerk.

Welche personenbezogenen Daten werden verarbeitet?

- Bei der Aufnahme eines Gerätes können diverse Informationen erfasst werden. Hierzu zählt, in welchem Raum sich ein Gerät befindet und welche Position es innerhalb des Raumes das Gerät einnimmt, die Inventarnummer des Gerätes, sowie die MAC und IP-Adressen der Netzwerkschnittstellen. Die MAC-Adresse lässt unter Umständen erkennen, um welchen Hersteller bzw. um welchen Gerätetypen es sich handelt. Weiterhin können über eine Freitextbeschreibung und Schlagwörter („Tags“) Zusatzinformationen hinzugefügt werden. Handelt es sich bei dem Gerät um ein privates Gerät, wird auch ein Benutzer zugeordnet.
- Wenn sich ein Gerät innerhalb der Domäne befindet, kann außerdem festgestellt werden, wer es momentan bedient.

In dem Modul werden des Weiteren der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen des Zugrifflogs verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Geräte werden, sofern nicht Schuleigentum, durch eine Benutzereinwilligung in die Liste aufgenommen. Es werden solche Geräte nur verarbeitet, wenn der Besitzer dies aktiv anmeldet.

Wer muss Zugriff auf diese Daten haben?

Das Modul befindet sich im Verwaltungsbereich und ist daher ausschließlich von der Administration zugänglich.
Auf Logdateien besteht nur Zugriff durch berechtigte Administratoren.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Geräte-Daten, sofern das Gerät einem Benutzer zugewiesen wurde, werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht.
Logdateien werden 7 Tage zur Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups auf maximal 6 Monate verlängern.
Wird eine neues Gerät eines Users eingepflegt, ist zu prüfen, ob ggf. ein anderes dafür gelöscht werden muss.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Die Geräteinformationen sowie zugeordnete Benutzer werden auch im Modul „Gerätesteuerung“, „Mobilgerätesteuerung“ und „Mobilgeräteverwaltung“ verwendet. Des Weiteren werden die im Modul erfassten Informationen für den Betrieb des Netzwerkes verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Möglichkeit der Zuordnung eines Benutzers zu einem Gerät, ist es möglich, dessen Benutzerverhalten anhand der erfassten Zeit „Zuletzt gesehen“ zu analysieren.
Durch die Erfassung der Mac Adresse können Rückschlüsse auf das Gerätemodell getätigt werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keines außer des bereits Genannten

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).
Grundsätzlich hat nur die Administration Zugriff auf das Modul.
Der Zugriff wird durch Rechtevergabe gesteuert. Auch hier greift die Administratoren verpflichtung.

Gruppenansicht

Das Modul Gruppenansicht stellt eine alternative Ansicht von Informationen zur Verfügung. Diese Informationen sind gruppenbasiert. Alle dargestellten Informationen werden von den

jeweiligen Mitgliedern einer Gruppe erfasst und verarbeitet. Diese Daten werden bei Aufruf der Gruppenansicht per Schnittstelle abgefragt und dargestellt. Es werden keine Daten zwischengespeichert.

Welche personenbezogenen Daten werden verarbeitet?

Das Modul verarbeitet keine personenbezogenen Daten.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Es werden keine personenbezogenen Daten verarbeitet.

Wer muss Zugriff auf diese Daten haben?

./.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Nein.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

-

Welche technischen Maßnahmen schützen diese Daten?

-

Gruppenbewerbungen

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, beantragte Gruppe, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen des Zugriffslogs verarbeitet.
Der antragstellende Benutzer kann keine Benutzernamen von anderen Benutzern einsehen.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Verarbeitung entsteht nur auf Veranlassung des Betroffenen.

Wer muss Zugriff auf diese Daten haben?

Nur Benutzer, die über mögliche Gruppenzugehörigkeiten entscheiden sollen, können Namen sowie beantragte Gruppe der Antragsteller einsehen.

Der Zugriff auf den Verwaltungsbereich des Moduls ist durch Vergabe von Rechten beschränkt.

Auf Logdateien besteht nur Zugriff durch berechtigte Administratoren, die diese Daten nur zu angewiesenen Zwecken verwenden dürfen.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Ggf. ist es notwendig, andere Lehrer zu informieren (z.B. den Leiter der Musik-AG, der ein neues Mitglied bekommt)

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht.
Logdateien werden 7 Tage zur Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups auf maximal 6 Monate verlängern.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Der antragstellende Benutzer wird ggf. durch dieses Modul auf eigenen Wunsch hin einer weiteren Gruppe hinzugefügt. Dadurch ergibt sich eine Verwendung in allen Modulen.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Beantragung in Gruppen durch den Antragsteller ist es dem verwaltenden Benutzer möglich, Präferenzen des Beantragenden aus den beantragten Gruppen abzuleiten. Es dürfen daher nur Mitglieder der Administratoren sein.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Die Verarbeitung erfolgt auf Wunsch des Betroffenen.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich haben nur Benutzer mit Berechtigung auf den Verwaltungsbereich des Moduls Zugriff auf die beantragten Gruppen. Diese Gruppe muss so klein wie möglich gehalten werden, unerlaubte Auswertungen müssen untersagt sein.

Import

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul auf dem Server werden die interne ID, der Vor- und Nachname, die IP-Adresse und die Browserkennung verarbeitet.

Das Modul verarbeitet Listen an Daten aus Schulverwaltungsprogrammen. Aus diesen Daten berechnet das Modul direkt die notwendigen Änderungen, um die Benutzerdatenbank von IServ auf den aktuellen Stand der Liste zu bringen. Die Dateien mit den Listen werden nicht gespeichert.

Für die Verwendung des Moduls sind folgende Informationen notwendig: Vorname und Nachname. Die Klasse und die schulinterne ID, Nachnamenzusatz, Gruppen, ein zu vergebenes Passwort für neue Benutzer und ein Hilfsindikator (bei fehlender ID) genutzt werden, um den Import zu komplettieren. Die ID oder der Hilfsindikator wird zur Wiedererkennung bei späteren Importvorgängen verwendet.

Der durchführende Administrator erhält eine Liste aller erstellten Benutzer mit generierten Passwörtern zur Verfügung gestellt.Bei der ersten Anmeldung muss der User ein sicheres Passwort setzen.

Welche sensiblen Daten lt. Art 9 DSGVO verarbeitet?

Die exportierten Dateien aus den Schulverwaltungsprogrammen können sensible Daten nach Art. 9 DSGVO beinhalten. Das Modul kann lediglich die oben genannten Daten verarbeiten. Weitere Informationen werden ignoriert.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Das Importmodul ist Teil der allgemeinen Einwilligung in die Verwendung von IServ. Dieses Dokument soll als detaillierte Information gelten und sollte verfügbar gemacht werden. Nur Personen, die bereits eingewilligt haben, werden importiert.

Wer muss Zugriff auf diese Daten haben?

Die Administratoren, die den Import durchführen, benötigen Zugriff auf die exportierte Liste um den Import durchzuführen. Soll IServ oder der Schulträger / ein betreuendes IT-Unternehmen das übernehmen, ist ein bestehender AV-Vertrag notwendig.

Im weiteren Verlauf haben alle verpflichteten Administratoren Zugriff auf die importierten Informationen über die Benutzerverwaltung von IServ. Sie müssen neue Benutzer händisch einrichten , andere löschen können oder auf Anfrage des Users sein Passwort zurücksetzen können.

Sind alle Felder wirklich notwendig?

IServ versucht mit so wenig Informationen wie möglich einen Import zu ermöglichen. Darum sind auch nur der Vorname und der Nachname Pflichtfelder im Importprozess. Für einen Import sind die Felder Klasse und ID empfohlen, da sie den Wartungsaufwand in späteren Importprozessen deutlich reduzieren.

Werden Daten an Dritte weitergegeben und warum?

Eine Weitergabe der Daten an Dritte findet nicht statt.

Gibt es Löschfristen (automatisch oder empfohlen)?

Zugriffe auf die Weboberfläche von IServ werden für maximal 7 Tage (zzgl. Backups) protokolliert.
Interaktionen mit Videokonferenzen werden für maximal 7 Tage (zzgl. Backups) protokolliert.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Es werden keine erfassten Daten in anderen Modulen verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch das automatische Anpassen von Benutzergruppen können Administratoren gegebenenfalls den Werdegang eines Schüler über die Klassenzugehörigkeit auslesen.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Teilnehmer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Grundsätzlich wird empfohlen die Daten auf einem verschlüsselten Medium zu übertragen oder direkt vom exportierenden Rechner in das Import-Modul zu laden, damit die Daten auf dem Weg zum Modul nicht in falsche Hände geraten.

Die exportierten Dateien des Schulverwaltungsprogramms LUSD sind verschlüsselt. Diese werden vom IServ selbst entschlüsselt und dann verarbeitet. Eine Verlust der Daten auf einem beispielsweise USB-Stick stellt kein Datenschutzrisiko dar.

Messenger

Welche personenbezogenen Daten werden verarbeitet?

Das Modul wird zum Senden und Empfangen von Nachrichten verwendet.
In dem Modul werden der Name, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte und IP-Adressen

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Auf die Inhalte der im Messenger verarbeiteten Texte hat IServ keinen Einfluss, es sollte eine Benutzerordnung geben, die bestimmte Inhalte untersagt. (IServ liefert dazu ein Muster)

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Das Messengermodul ist Teil der allgemeinen Einwilligung in die Verwendung von IServ. Dieses Dokument soll als detaillierte Information gelten und sollte verfügbar gemacht werden.

Wer muss Zugriff auf diese Daten haben?

Benutzer können über die Oberfläche nur auf Nachrichten aus Räumen zugreifen, in denen sie Mitglied sind. Bei Betreten eines Raumes erhalten Benutzer keinen Zugriff auf frühere Nachrichten im Raum. Benutzer mit dem Recht „Meldungen ansehen“ erhalten die Ausschnitte der gemeldeten Konversationen unabhängig davon, ob sie Mitglied im betroffenen Raum sind.

Sind alle Felder wirklich notwendig?

Ja, es sind auch hier nur die absolut notwendigen Felder enthalten, die Unterricht auch ohne persönliche Anwesenheit ermöglichen.

Werden Daten an Dritte weitergegeben und warum?

Eine automatische Weitergabe an Dritte findet nicht statt. Per Mail oder Datei können von den Usern Inhalte auch an Dritte gelangen. Dies sollte nur mit pädagogischer Begründung erlaubt sein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Von bearbeiteten Nachrichten werden auch sämtliche älteren Fassungen zu Dokumentationszwecken gespeichert. Ebenso bleiben vom Benutzer gelöschte Nachrichten im System gespeichert und werden nur ausgeblendet. Einmal gelesene Nachrichten bleiben auch dann erhalten, wenn der Absender-Benutzer gelöscht wurde.
Auf diese Daten hat nur IServ auf Weisung (z.B. bei Strafverfolgung) Zugriff.
Gelöschte Räume und Räume ohne Mitglieder werden nach spätestens 24 Stunden endgültig vom Server gelöscht, also auch zum Schuljahresende.
Eine automatische Lösung ist nicht vorgesehen.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Das Empfangen von E-Mails aus dem Messenger löst das Versenden von Benachrichtigungen aus, die dann im Kern-Modul weiter verarbeitet werden. Die Benachrichtigungen werden nur dem Empfänger zugestellt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Über Beobachtung des Online-Status lässt sich gegebenenfalls ein nicht-genaues Bild über die Aktivität eines Nutzers erstellen. Eine automatische Auswertung findet nicht statt.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer verarbeitet werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Um die Ladegeschwindigkeit zu verbessern, werden ausgewählte Daten, wie zum Beispiel Raumzustände verschlüsselt auf dem Gerät des Endnutzers gespeichert. Nach einem Logout oder nach einer Woche werden die Daten beim nächsten Öffnen neu verschlüsselt. Nicht mehr benötigte Daten werden gelöscht. Bei einem nicht autorisierten Zugriff, wie etwa durch einen anderen Account, werden die Daten invalidiert und vom System gelöscht.

Infobildschirm

Welche personenbezogenen Daten werden verarbeitet?

Eingestellte Inhalte können entweder in der Weboberfläche des IServ Portalservers oder auf Bildschirmen innerhalb der Schule angezeigt. Bei der Anzeige auf Bildschirm sind die Inhalte vor Ort auch für Personen ohne Benutzerkonto einsehbar. Die Inhalte werden nur von verantwortlichen IServ-Nutzern eingestellt.

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.
Ggf. kommen Lehrerkürzel oder in Texten auch Klarnamen zum Einsatz.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Für die Veröffentlichung von Inhalten ist hier die Schule verantwortlich, IServ leitet die Dateien nur weiter.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Daten entsprechen weitestgehend den bisherigen Vertretungsplänen, diese sind für die Abläufe in der Schule notwendig. Dass Daten zu Personen jetzt innerhalb IServs oder schulweit veröffentlicht werden, muss den Personen vorher bekannt gemacht werden.

Wer muss Zugriff auf diese Daten haben?

Abhängig von den Einstellungen des jeweiligen Infobildschirms benötigen alle Benutzer Zugriff auf die Inhalte. Teilweise auch ohne Benutzeranmeldung, dies muss aber explizit eingestellt werden und die Inhalte sind dann nur über eine geheime URL erreichbar.

Änderungen / Aktualisierungen können nur über die Mitglieder der Gruppe Infobildschirm erfolgen.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Über gezielte Weitergabe der URL. Dritte können die Info zudem verarbeiten, sofern Sie Infobildschirme in der Schule einsehen können.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die vom Nutzer erstellten Infobildschirme werden beim endgültigen Löschen des Benutzers ebenfalls entfernt. Für die Aktualität der Inhalte ist die Schule verantwortlich.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Das Modul konsumiert lediglich Inhalte anderer Module zur Anzeige auf Bildschirmen.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hochgeladen werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).
Die Verwaltung von Inhalten in dem Modul erfolgt aus der Gruppe Infobildschirme heraus.

Kalender

Welche personenbezogenen Daten werden verarbeitet?

Das Modul verwendet neben der internen ID auch den Namen und die E-Mail-Adresse des Nutzers. Die ID wird genutzt, um die Daten der Kalenderdaten mit dem Nutzer zu verknüpfen. Der Name und die E-Mail-Adresse werden verwendet, um Termineinladungen zu verschicken.

Die Details der Termine (unter anderem Ort, Start- und Endzeit) stehen neben dem Nutzer auch den eingeladenen Teilnehmern zur Verfügung. Die Details werden im Rahmen der Termineinladung per E-Mail an die Teilnehmer geschickt.

Welche sensiblen Daten lt. Art 9 DSGVO verarbeitet?

Es werden vom Modul keine sensiblen Daten abgefragt und verarbeitet. Werden vom User solche Daten eingestellt (Arzttermine oder Krankheits-Abwesenheiten), so sollte dies nur im eigenen Kalender geschehen und selbst eingerichtete Freigaben für andere im Blick behalten werden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Dieses Dokument sollte den Usern zur Verfügung gestellt werden. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/#kalender.

Wer muss Zugriff auf diese Daten haben?

Zugriff auf die benutzergenerierten Inhalte haben jeweils die Eigentümer der Dateien und ggf. bei Verwendung von Gruppenordnern die Mitglieder und Eigentümer der Gruppe. Auf die Logdateien besteht nur Zugriff durch berechtigte Administratoren oder IServ.

Sind alle Felder wirklich notwendig?

Die Abfrage von Termindetails enthält alle Felder, die einen Termin beschreiben können. Die Daten, die bei der Erstellung von Terminen abgefragt werden, sind bis auf den Titel, Beginn, Ende und dem Kalender alle freiwillig.

Werden Daten an Dritte weitergegeben und warum?

Jeder Benutzer kann den Zugriff auf seine Kalenderdaten durch Freigaben für andere selbst steuern. Termine können an Dritte per Mail oder Einladung weitergegeben werden (Eltern, Behörden) Eine automatische Weitergabe an Dritte findet nicht statt.

Gibt es Löschfristen (automatisch oder empfohlen)?

Zugriffe auf die Weboberfläche von IServ werden für maximal 7 Tage (zzgl. Backups) protokolliert.

Die Daten im Kalender werden nach dem Löschen des Benutzerskontos automatisch gelöscht. Eine automatische Löschung der Termine im Kalender von aktiven Benutzern findet nicht statt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Auf der Startseite werden dem Nutzer die zukünftigen Termine der nächsten 14 Tage aller abonnierten Kalender angezeigt.

Im Modul Gruppenansicht werden die zukünftigen Termine einer Gruppe für die Gruppenmitglieder dargestellt. In beiden Fällen findet keine Speicherung der Daten im jeweiligen Modul statt.

Bei Termineinladungen und -erinnerungen werden Benachrichtigungen ausgelöst, die über das IServ System den jeweiligen Nutzern zugestellt und angezeigt werden. Diese enthalten neben einer Verlinkung auf den Termin auch den Titel, Start- und Endzeitpunkt und den Ort des Termins.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?
Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Jeder Kalender kann freigegeben werden. Dabei kann pro Termin bestimmt werden, welche Informationen weitergegeben werden. Diese Informationen sind dann den freigegebenen Personen zugänglich und können neben dem Tagesablauf potenziell auch den jeweiligen Aufenthaltsort und Tagesabläufe preisgeben. Die Freigabe eines Kalenders ist freiwillig. Im Kalender ist Auswertung auch ein notwendiger Punkt, um z.B. freie gemeinsame Termine zu ermitteln.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Teilnehmer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Klausurmodus

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, vom Benutzer erstellte Daten (Inhalte) und IP-Adressen verarbeitet.

Für die Dauer einer Klausur wird der Besitzer der Klausur mit den Geräten assoziiert. Diese Assoziation wird automatisch nach spätestens 24 Stunden oder durch das Beenden einer Klausur gelöscht.

Die Teilnehmer der Klausur können dem Besitzer über ein eingehängtes Netzlaufwerk Dateien der Klausur übergeben. Der Besitzer der Klausur erhält Vollzugriff zu diesen Dateien. Während der Klausur sind Zugang zu gespeicherten eigenen Dateien und dem Internet ggf. gesperrt. Die Teilnehmer der Klausur haben nach Ende der Klausur keine Möglichkeit, diese Dateien zu verändern oder zu löschen.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein. Die Inhalte der Klausuren (die einzige Möglichkeit für sensible Inhalte) können hier nicht Thema sein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Außer dem Namen und der Klassenzugehörigkeit werden nur die Inhalte der Klausur an den Lehrer weitergegeben, hier ist keine Information notwendig. Die Information ist schon bei den Betroffenen.

Wer muss Zugriff auf diese Daten haben?

Nur der Lehrer, der die Klausur durchführen lässt, hat Zugriff auf die von den Schülern hinterlegten Daten.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein. (Nur bei Vertretungen wg. Krankheit o.ä. ist ein weiterer Lehrer involviert.)

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Aktivierung des Klausurmodus an Windows-Computern in der Schule wird spätestens nach 24 Stunden entfernt. Die erzeugten Daten bleiben dem Ersteller zur Verfügung gestellt und werden nicht automatisch gelöscht.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Die von den Teilnehmern hinterlegten Daten werden durch das Modul „Dateien“ verarbeitet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Die Klausuren selbst sind zum Zwecke der Auswertung erstellt. Durch das Modul selbst ist aber keine Auswertung oder gar ein Profiling möglich.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Die Inhalte der Klausuren obliegen der pädagogischen Verantwortung des Lehrers.

Welche technischen Maßnahmen schützen diese Daten?

Der Zugriff auf die hinterlegten Daten wird durch Berechtigungen gesteuert.

Klausurplan

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

In diesem Modul werden Klassen- oder Klein-Gruppen verarbeitet, der Plan hat den Zweck der Koordination der Termine, es ist keine Extra-Information notwendig, da im äußersten Fall Name und Klassenzugehörigkeit verarbeitet werden.

Wer muss Zugriff auf diese Daten haben?

Nur Benutzer mit entsprechender Berechtigung können die erstellten Pläne einsehen. Die Schüler sehen nur die für sie vorgesehenen Klausuren, sobald sie freigeschaltet sind.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die erstellten Klausuren eines Nutzers werden mit dem endgültigen Löschen des Nutzers entfernt. Eingestellte Sperrungen von Tagen und Zeiträumen blieben erhalten, lediglich die Zuordnung zum gelöschten Benutzer wird entfernt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Das Modul stellt eine Erweiterung für das Modul „Kalender“ zur Verfügung. Über diese Erweiterung werden dem Nutzer die Klausuren als Termine im Kalender dargestellt.

Außerdem werden die Klausuren der nächsten zwei Wochen kompakt für den Nutzer auf der Startseite angezeigt.

Die Anzeige wird bei jedem Aufruf ausgelesen. Eine zusätzliche Speicherung im Kalender oder der Startseite findet nicht statt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Datenschutzrechtlich keines.

Welche technischen Maßnahmen schützen diese Daten?

Grundsätzlich haben nur Benutzer mit bestimmter Berechtigung Zugriff auf das Modul. Die Teilnehmer von Klausuren können nur die sie betreffenden Einträge sehen.

Knowledge-Base

Die IServ-Knowledge-Base stellt eine Plattform zur Verfügung, mit der Sie eine Wissensdatenbank anlegen können. Darin können beliebige Informationen, z. B. Lösungen zu Problemen oder allgemeine Informationen zu Abläufen hinterlegt, definierten Kategorien zugeordnet und über eine Suchfunktion abgerufen werden. Die Definition der Kategorien erfolgt durch die Administration.

Die Kategorien sind einer einzelnen Gruppe zugeordnet. So können Inhalte auf bestimmte Gruppen begrenzt werden.

Der Zugriff auf das Modul kann durch die Administration gesteuert werden.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Detaillierte Information kann diesem Dokument entnommen werden, die hier gespeicherten Inhalte und die dazu gehörenden Daten werden durch die Benutzer selbst eingepflegt.

Wer muss Zugriff auf diese Daten haben?

Ersteller und Benutzer, die durch Gruppenmitgliedschaft berechtigt sind, eine Kategorie einzusehen, haben schreibenden Zugriff auf die erstellten Beiträge. Beiträge können jederzeit gelöscht werden.

Benutzer müssen außerdem das Recht besitzen, das Modul verwenden zu können.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Sinn und Zweck einer Knowledge-Base ist es, Informationen bereitzustellen. Hier ist durch die Schule darauf zu achten, dass interne Vorgaben und die Grenzen durch das Schulgesetz eingehalten werden.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Inhalte bleiben bis zur manuellen Löschung im Modul erhalten. Bei Löschung des Nutzers wird aber die Autoreninformation entfernt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Für Ersteller und Benutzer besteht die Möglichkeit, das Arbeitsverhalten eines Nutzers im Rahmen der eigenen Tätigkeit zu analysieren.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer eingestellt werden.

Welche technischen Maßnahmen schützen diese Daten?

Grundsätzlich haben nur von der Administration berechtigte Benutzer Zugriff auf das Modul. Durch Zugriffssteuerung mittels Kategorien können einzelne Beiträge granularer vor Zugriff von nicht berechtigten Benutzern geschützt werden.

Kurswahlen

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen eines Zugriffslogs verarbeitet. Dieses umfasst sowohl den Prozess der Erstellung und Verwaltung einer Kurswahl als auch die Teilnahme eines Benutzers.

Bei der Erstellung einer Kurswahl, zur Bestimmung der Teilnehmer werden dem Benutzer Gruppen und andere Nutzer vorgeschlagen. Die vorgeschlagenen Einträge sind auf die eigenen Gruppen und deren Mitglieder beschränkt. Die Freigabe für Personen, deren Name vollständig bekannt ist, ist ebenfalls möglich.

Der Benutzername des Erstellers ist im Verwaltungsbereich des Moduls für andere Benutzer sichtbar.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Sie werden zu Kursen vorgeschlagen, können Kurse wählen. Da die dafür verwendeten Daten und der Zweck in der Einwilligung in das Verwenden von IServ enthalten sind, ist hier keine separate Einwilligung notwendig

Wer muss Zugriff auf diese Daten haben?

Der Zugriff auf den Verwaltungsbereich des Moduls ist durch Vergabe von Rechten beschränkt.
Auf Logdateien besteht nur Zugriff durch berechtigte Administratoren.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die erstellen Kurswahlen bleiben auch nach dem Löschen eines Nutzers erhalten. Die Zuordnung zum Nutzer wird allerdings entfernt.

Die Kurswahlen der Nutzer werden mit dem Löschen des Nutzers automatisch entfernt.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Aktionen im Modul können zum Versenden von Benachrichtigungen führen, die dann im Kern-Modul weiter verarbeitet werden.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Im Verwaltungsbereich des Moduls besteht die Möglichkeit die Interessen eines Nutzers im Rahmen der gewählten Kurse zu analysieren.

Durch die vom Teilnehmer gewählten Optionen kann eine Auswertung der Präferenzen des Teilnehmers erfolgen. Dies ist allerdings auch Aufgabe des Moduls.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer eingestellt werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich haben Benutzer mit Berechtigung auf den Verwaltungsbereich des Moduls Zugriff auf die von den Teilnehmern getätigten Wahlen.

Methodenguide (Medienberatung Niedersachsen)

Welche personenbezogenen Daten werden verarbeitet?

Es werden durch das IServ-Modul keine personenbezogenen Daten verarbeitet. Das Modul bindet lediglich eine externe Webseite ein.

Datenschutzbestimmungen des Drittanbieters finden Sie unter:
https://www.methodenguide.de/basic/datenschutz/

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Benutzer haben auf der eingebundenen Webseite die Möglichkeit sich über Datenschutzbestimmungen und Nutzungsbedingungen zu informieren. Beim Wechseln auf diese Seite wird der Nutzer über den Wechsel des Anbieters informiert

Wer muss Zugriff auf diese Daten haben?

-

Sind alle Felder wirklich notwendig?

-

Werden Daten an Dritte weitergegeben und warum?

Das Modul bindet eine spezielle Version der Webseite "methodenguide.de" ein. Durch die Einbindung werden von den Browsern der Benutzer Daten übermittelt.

Gibt es Löschfristen (automatisch oder empfohlen)?

-

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

-

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Dies ergibt sich aus den Datenschutzhinweisen der Seite.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

s.o.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

MUNDO

Welche personenbezogenen Daten werden verarbeitet?

Es werden durch dieses IServ-Modul keine personenbezogenen Daten verarbeitet. Das Modul bindet lediglich eine externe Webseite ein.

Datenschutzbestimmungen des Drittanbieters finden Sie unter: https://mundo.schule/data-protection

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Benutzer haben auf der eingebundenen Webseite die Möglichkeit sich über Datenschutzbestimmungen und Nutzungsbedingungen zu informieren. Es erfolgt vorab ein Hinweis, dass man zu einer externen Seite wechelt.

Wer muss Zugriff auf diese Daten haben?

-

Sind alle Felder wirklich notwendig?

-

Werden Daten an Dritte weitergegeben und warum?

Das Modul bindet die Webseite "mundo.schule" ein. Durch die Einbindung werden von den Browsern der Benutzer Daten übermittelt. Diese unterliegen den Datenschutzbestimmungen und Nutzungsbedingungen des Anbieters.

Gibt es Löschfristen (automatisch oder empfohlen)?

-

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

-

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Es bestehen die üblichen Risiken wie beim Besuch von externen Webseiten.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Es besteht kein wesentliches zusätzliches Risiko.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

News

Das Modul ermöglicht es berechtigten Nutzern, Text-Inhalte bestimmten Benutzergruppen zur Verfügung zu stellen.

Kommende Neuerung: Zukünftig wird das Modul allen Nutzern die Änderungsprotokolle für den IServ Portalserver anzeigen.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Nur die personenbezogenen Daten der Ersteller der News werden verarbeitet, was aus redaktioneller Sicht und zu Zwecken der Protokollierung notwendig ist.

Wer muss Zugriff auf diese Daten haben?

Das Einsehen der erfassten Inhalte durch andere Benutzer kann vom Ersteller durch Auswahl von berechtigten Gruppen eingeschränkt werden.

Beiträge ohne Gruppenangabe sind von allen Benutzern des Servers intern einsehbar.

Andere Benutzer, mit Berechtigung News-Beiträge zu erstellen, sind in der Lage, ihre Inhalte einzusehen und zu bearbeiten.

Der Administrator kann optional einzelne News-Kategorien als RSS-Feed im Internet veröffentlichen oder RSS-Feeds aus dem Internet für Nutzer einbinden. Das Abrufen der Informationen erfolgt durch das News-Modul. Die IP-Adresse des Nutzers ist für den Dienst nicht einsehbar.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Angelegte Beiträge werden mit der Löschung des Nutzers nicht gelöscht, lediglich die Zuordnung zum Nutzer wird entfernt.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Erfasste Inhalte können vom Modul „Infobildschirm“ und in der Startmaske angezeigt werden.
Eine Zwischenspeicherung findet nicht statt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer eingestellt werden.

Inhalte könnten für alle Benutzer sichtbar werden, wenn die Einschränkung auf Gruppen nicht genutzt wird.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Inhalte sind – gesteuert durch Gruppenangabe – nur für die entsprechenden Benutzer sichtbar.Der Ersteller hat jederzeit die Möglichkeit Beiträge zu ändern oder zu löschen.

OAuth- und Open-ID-Connect-Server

Welche personenbezogenen Daten werden verarbeitet?

Die Art der verarbeiteten Daten hängt von den konfigurierten Endpunkten und Scopes ab. Ohne Konfiguration eines Scopes erfolgt lediglich eine einfache Authentifizierung unter Nutzung einer pseudonymisierten ID.

Je nach verwendetem Scope können außerdem folgende Datenfelder übertragen werden:

* Vor- und Nachname
* E-Mail-Adresse
* eindeutige ID
* Gruppenmitgliedschaften
* Rollen

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Aus den Gruppenmitgliedschaften sind ggf. Hinweise auf die Weltanschauung abzuleiten.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Da i.d.R. eine Anbindung an Drittanbietersoftware erfolgt ist eine anderweitige pauschale Aussage hierzu nicht möglich.

Wird der Endpunkt nicht als vertrauenswürdig konfiguriert, müssen Benutzer der Übertragung der Daten explizit zustimmen.

Wer muss Zugriff auf diese Daten haben?

Berechtigte Administratoren haben auf die Daten zur Systempflege Zugriff. Außerdem werden die durch den Administrator konfigurierten Datenfelder an externe Anwendungen übergeben. Diese befinden sich außerhalb unseres Einflussbereiches.

Sind alle Felder wirklich notwendig?

-

Werden Daten an Dritte weitergegeben und warum?

Bei dem Modul handelt es sich um eine generische Schnittstelle. Eine Weitergabe an Dritte ist damit prinzipbedingt nötig. Die korrekte Konfiguration obliegt den Administratoren. Eine Verwendung ausschließlich zu internen Zwecken ist möglich.

Gibt es Löschfristen (automatisch oder empfohlen)?

-

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Die Daten werden ggf. von Drittanbieter-Anwendungen genutzt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Wird nicht die reine pseudonyme Authentifizierung verwendet, sind Rückschlüsse auf die Nutzer und damit z.B. auch Profilbildung beim Einsatz von Tracking-Cookies durch Drittanbieter möglich.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Es besteht kein zusätzliches Risiko.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Office

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Teste, Dokumente und Tabellen) und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nicht durch das Modul. Für den Inhalt der erstellten Dateien kann von IServ keine Verantwortung übernommen werden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Daten werden in selbsterstellten Daten zur Organisation der Dateien erfasst.

Wer muss Zugriff auf diese Daten haben?

Ausschließlich der Ersteller hat Zugriff auf die in dem Modul generierten Dateien, sofern die Speicherung in den eigenen Dateien vorgenommen wurde.

Wird die Speicherung in einen Gruppenordner vorgenommen, erhalten die Benutzer mit Gruppenzugehörigkeit ebenso Zugriff.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Mit jedem Weitergeben (z.B. per Mail) werden die Daten an andere übermittelt. Dies findet aber im pädagogischen Rahmen statt.

Gibt es Löschfristen (automatisch oder empfohlen)?

Bei der Löschung der Daten muss zwischen den Dateien selbst und den im Modul anfallenden Daten unterschieden werden.

Die Dateien selbst bleiben erhalten und werden durch das Modul nur aktualisiert. Die Löschung dieser Dateien liegt im Modul Dateien.

Das Modul selbst muss zum Bearbeiten der Dateien temporäre Kopien anlegen. Diese werden nach dem Bearbeiten automatisch wieder entfernt.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Für Dateien mit Gruppenzugriff besteht die Möglichkeit, das Arbeitsverhalten eines Nutzers zu analysieren.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer verwendet werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Online-Medien

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.

Des Weiteren werden Suchbegriffe zweckgebunden, nach Eingabe durch den Benutzer, an die hinterlegten Anbieter übermittelt. Dabei ist dem Anbieter keine Zuordnung zum Nutzer möglich.

Es gelten zusätzlich die Datenschutzvereinbarungen der Drittanbieter „Antares“ und „Merlin“.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Neben der Information zur Einwilligung in die Nutzung von IServ gibt dieses Dokument Transparenz.

Wer muss Zugriff auf diese Daten haben?

-

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein, da die Abfragen und das Herunterladen der Daten über den IServ Portalserver gesteuert wird.

Gibt es Löschfristen (automatisch oder empfohlen)?

Keine.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Suchanfragen können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer verarbeitet werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).
Die Verwendung des Moduls kann durch ein Recht gesteuert werden.

Pläne

Das Modul Pläne dient der Bereitstellung unterschiedlicher Pläne in Form von Dateien an die Nutzer.

Welche personenbezogenen Daten werden verarbeitet?

Das Modul verarbeitet grundsätzlich keine personenbezogenen Daten.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Es werden keine Daten verarbeitet.

Wer muss Zugriff auf diese Daten haben?

-

Sind alle Felder wirklich notwendig?

-

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

-

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

-

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

-

Welche technischen Maßnahmen schützen diese Daten?

-

Schnellumfragen

Das Modul ermöglicht es, „schnelle“ Umfrage zu erstellen. Diese bestehen immer aus einer Frage. Die Abfrage kann entweder anonym oder nicht-anonym durchgeführt werden. Die Nutzer werden über den Abfragetyp informiert.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten, benutzergenerierte Inhalte (Dateien) und IP-Adressen verarbeitet.

Die Teilnehmer einer Schnellumfrage werden anhand der vom Ersteller angegebenen Gruppen ermittelt.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Grundsätzlich verarbeitet das Modul keine sensiblen Daten. Ausnahme bilden hier die vom Nutzer erstellten Fragen, die sensible Daten abfragen könnten. Dies ist besonders bei nicht-anonymen Umfragen zu beachten und unterliegt den pädagogischen Regeln..

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Einwilligungs- und Informationspflichten müssen individuell durch die Kunden (Schulen) eingeholt bzw. erfüllt werden. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/.

Wer muss Zugriff auf diese Daten haben?

Lediglich der Ersteller der Schnellumfrage hat Zugriff auf die Daten.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Ist die Option „Anonym“ deaktiviert, können Rückschlüsse auf die von den Teilnehmern gewählten Optionen erfolgen.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Auswertung von Präferenzen bei nicht-anonymen Schnellumfragen. Dies ist aber auch unter anderem Ziel des Moduls.

Welche technischen Maßnahmen schützen diese Daten?

- Mit der Option „Anonym“ kann angegeben werden, ob die Ergebnisse auf die Teilnehmer zurückzuführen sind oder nicht. Dies betrifft lediglich die Auswertung der Daten und wird nur dem Ersteller der Schnellumfrage angezeigt. Sollte diese Option aktiviert werden, die Schnellumfrage also anonym sein, wird lediglich die Anzahl der Personen angezeigt, die für eine spezielle Antwort gestimmt haben. Ist diese Option deaktiviert, werden für jede Antwort zusätzlich noch die Personen aufgelistet, die für diese gestimmt haben.

Grundsätzlich hat nur der Ersteller der Schnellumfrage Einsicht in die erhobenen Daten.

Schülerkarriere

Welche personenbezogenen Daten werden verarbeitet?

Das Modul Schülerkarriere bindet Bilder von Servern der Schülerkarriere GmbH ein, die nicht durch IServ verantwortbar sind. Durch Abgleich der Daten ist es für Schülerkarriere möglich, festzustellen, welche Anzeigen besucht wurden.

Durch die Verwendung des Moduls wird der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen im Rahmen des Zugriffslogs verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Beim Wechsel zu der Seite ist ein IServ-Hinweis geplant, der auf den Wechsel des Anbieters hinweist. Schülerkarriere.de hat seine eigenen Datenschutzhinweise.

Wer muss Zugriff auf diese Daten haben?

Auf Logdateien besteht nur Zugriff durch berechtigte Administratoren.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nicht durch IServ.

Gibt es Löschfristen (automatisch oder empfohlen)?

Logdateien werden 7 Tage zur Nachverfolgung von Aktionen vorgehalten. Die Fristen können sich durch entsprechende Backups auf maximal 6 Monate verlängern.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Zu vom Benutzer über Filterkriterien gefundene Ergebnisse werden dem Benutzer auf der Startseite angezeigt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Es könnten Interessen des Nutzers ausgewertet werden. Dies ist allerdings unwahrscheinlich, weil nur der User selbst und verpflichtete Administratoren darauf zugreifen können.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer verwendet werden.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich hat nur der Benutzer selbst Zugriff auf die von ihm angegebenen Daten im Modul.

Softwareverteilung

Das Modul Softwareverteilung ist für die automatische Installation von Betriebssystemen (Windows und Linux) und Programmen (nur Windows) auf Computern zuständig. Dabei werden keine personenbezogenen Daten von Nutzer verarbeitet.

Die Verarbeitung von Daten durch die installierten Programme ist durch den jeweiligen Kunden zu prüfen und liegt außerhalb des Wirkungsbereichs der IServ GmbH.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.
Durch den ausschließlich administrativen Zugriff beschränken sich die Daten auf diese Benutzergruppe.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

./.

Wer muss Zugriff auf diese Daten haben?

Der Zugriff auf die Softwareverteilung kann ausschließlich erfolgen, wenn durch die Administration das entsprechende Recht dem Benutzer zugewiesen wurde.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Keine.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keine.

Welche technischen Maßnahmen schützen diese Daten?

Der Zugriff auf die Softwareverteilung kann ausschließlich nur dann erfolgen, wenn durch die Administration das entsprechende Recht dem Benutzer zugewiesen wurde.

Softwarepakete von Drittanbietern unterliegen gesonderten Datenschutzbestimmungen. Administratoren sind dazu angehalten, sicherzustellen, dass die Datenschutzrichtlinien der jeweiligen Produkte, denen der eigenen Organisation entsprechen, bevor diese eingesetzt werden.

Speicherplatzanzeige

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Gruppenmitgliedschaften, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Entfällt, da die Nutzer bereits informiert sind.

Wer muss Zugriff auf diese Daten haben?

Der Zugriff auf die Speicherplatzanzeige ist ausschließlich auf den jeweiligen Nutzer beschränkt. Dieser bekommen eine statische Auswertung des Speicherplatzverbrauchs.

Bei Überschreitung des von den Administratoren festgelegten Limits steht den Administratoren eine Liste mit Nutzern zur Verfügung, die dieses Limit überschreiten. Die Administratoren sehen dabei nur den Namen und den Gesamtwert des Speicherverbrauchs des Nutzers. Eine Aufschlüsselung steht nicht zur Verfügung.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im Modul anfallenden Daten werden spätestens zusammen mit dem jeweiligen Benutzer gelöscht. Sie ändern sich mit jeder Speicher- oder Löschaktion.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Der Administrierende Benutzer ist in der Lage die Speicherplatzbelegung anderer Benutzer einzusehen und auszuwerten, sofern diese das festgelegte Limit überschreiten.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keines. Außer gelegentlich ein Gespräch mit einem Admin.

Welche technischen Maßnahmen schützen diese Daten?

Grundsätzlich hat lediglich die Administration Zugriff auf das Modul.
Das Modul gibt nur Verbräuche derer Benutzer an, die über ein festgelegtes Limit liegen.
Eine inhaltliche Analyse ist nicht machbar.

Störungsmeldung

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet. Des Weiteren werden die durch die Erstellung der Störungsmeldung vom Benutzer erfassten Inhalte und Dateien verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Der Nutzer informiert hier über eine Störung, es werden nur die zur Protokollierung wichtigen Daten verarbeitet.

Wer muss Zugriff auf diese Daten haben?

Nur Benutzer mit entsprechendem Recht haben Zugriff auf das Modul und die dort hinterlegten Daten.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Bei Löschung des Nutzers werden die Zuordnung des erstellten Störungsmeldungen entfernt. Die Meldung selbst bleibt erhalten.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Das Erfassen einer Störungsmeldung löst den Versand einer internen E-Mail aus. Außerdem löst das Versenden Benachrichtigungen aus, die dann im Kern-Modul weiter verarbeitet werden. Die Benachrichtigungen werden nur dem empfangenden Benutzer zugestellt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Betreiber mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer verwendet werden.

Welche technischen Maßnahmen schützen diese Daten?

Das Erstellen einer Störungsmeldung ist ein zu vergebendes Recht.Grundsätzlich hat der Ersteller einer Störungsmeldung nur Zugriff auf die eigenen Störungsmeldungen.
Diese könnten jederzeit bearbeitet und etwaig hochgeladene Dateien gelöscht werden.

Nur Benutzer mit entsprechender Berechtigung können alle Störungsmeldungen einsehen und verwalten.

Stunden- und Vertretungsplan

In das Modul Stunden- und Vertretungsplan können die Stundenplandaten aus verschiedenen Planungsprogrammen importiert werden. Diese Daten werden aufbereitet und dem Nutzer der aktuelle Plan auf Basis der Klassenzugehörigkeit/Lehrerzuordnung angezeigt.

Welche personenbezogenen Daten werden verarbeitet?

In den Stundenplandaten können Lehrernamen enthalten sein, die angezeigt werden.
Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Nicht notwendig

Wer muss Zugriff auf diese Daten haben?

Die Nutzer haben Zugriff auf Ihren Stunden- und Vertretungsplan. Die Zuordnung erfolgt auf Basis der Info des Nutzers und der Klasseninformationen in den Stundenplandaten.

Benutzer mit erweiterten Rechten können Zugriff auf mehrere Stundenpläne bekommen.

Sind alle Felder wirklich notwendig?

Ja, die importierten Daten sind alle notwendig, um einen nutzbaren Stunden- und Vertretungsplan anzeigen zu können.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die Daten werden mit jedem Import komplett neu geschrieben. Eine Erweiterung bestehender Daten findet nicht statt. Daher sind die Löschfristen in diesem Fall an die Planungsprogramme und deren Exporte gebunden.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Auf der Startseite wird den Nutzern ein Auszug aus dem tagesaktuellen Stundenplan dargestellt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Theoretisch könnte durch Beobachtung des Stunden- und Vertretungsplan eine Auswertung zu der Abwesenheit von Lehrkräften erstellt werden.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Welche technischen Maßnahmen schützen diese Daten?

Die Anzeige von Lehrernamen kann abgeschaltet werden.

System-/Netzwerkmonitor

Welche personenbezogenen Daten werden verarbeitet?

In diesem Modul werden ausschließlich technische Eigenschaften über den Betriebsablauf des Servers erfasst.

Durch den Zugriff auf das Modul werden der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

./.

Wer muss Zugriff auf diese Daten haben?

Administratoren im von den Benutzern abgetrennten Verwaltungsbereich haben Zugriff auf die erfassten Daten.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Keine.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Die Komponente Netzwerkmonitor überträgt die gesammelten Daten an einen zentralen Server der IServ GmbH zur automatischen Auswertung. Diese Daten enthalten niemals personenbezogene Daten und dienen der Sicherstellung des reibungslosen Betriebs.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keine.

Welche technischen Maßnahmen schützen diese Daten?

Der Zugriff auf die Daten kann ausschließlich durch die Administration über einen von den Benutzern abgetrennten Verwaltungsbereich erfolgen.

Texte

Welche personenbezogenen Daten werden verarbeitet?

Neben der ID wird auch der Name und die Gruppenzugehörigkeit des Nutzers verarbeitet. Weitere Daten werden nicht durch IServ verwendet.
Um eine Freigabe zu erstellen, werden dem Benutzer Gruppen und andere Nutzer vorgeschlagen. Die vorgeschlagenen Einträge sind auf die eigenen Gruppen und deren Mitglieder beschränkt. Die Freigabe an andere Personen, deren Name vollständig bekannt ist, ist ebenfalls möglich.

Benutzer mit dem Recht "Teile Texte an alle Gruppen" sind von der Begrenzung der Vorschläge ausgenommen und bekommen alle Benutzer und Gruppen vorgeschlagen.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Lediglich in den Textinhalten könnten sich sensible Daten befinden.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Schulen müssen für die Nutzung von IServ Einwilligungen der Nutzer besitzen. Wir stellen passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung.
Dieses Dokument kann den Betroffenen zur Verfügung gestellt werden

Wer muss Zugriff auf diese Daten haben?

Zugriff auf die benutzergenerierten Inhalte haben jeweils die Eigentümer der Texte und die Nutzer, denen der Text freigegeben wurde.
Das Texte-Modul führt ein Änderungsprotokoll über sämtliche Texteingaben. Diese Änderungsprotokoll steht allen Nutzer mit Zugang zum Text zur Verfügung.
Auf die weiteren Logdateien besteht nur Zugriff durch berechtigte Administratoren oder IServ.

Sind alle Felder wirklich notwendig?

Ja.es ist auf das absolute Minimum an Feldern reduziert, Textinhalte obliegen der Verantwortung der User / der Schule.

Werden Daten an Dritte weitergegeben und warum?

Eine automatische Weitergabe an Dritte findet nicht statt. Die Daten werden nur durch Freigaben der Benutzer selbst weitergegeben. Ob eine Freigabe notwendig ist, entscheidet der User.
Dies verhält sich auch so bei Texten die nach Zusammenarbeit als Ergebnis gespeichert werden.

Ausnahmefall sind hier Benutzer mit dem Recht "Alle Texte verwalten". Diese Benutzer sind in der Lage die Berechtigungseinstellung eines Texte-Dokuments zu ändern, auf das sie mindestens Lesezugriff haben. Auf Texte, die nicht an diese Benutzer freigegeben sind, erhalten sie keinen Zugriff. Diese Personen müssen auf datenschutzkonformes Verhalten verpflichtet sein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Texte ohne Freigaben werden automatisch mit der Löschung des Nutzers entfernt.
Bei Texten, die anderen Nutzern freigegeben sind, bleibt der Text und auch die Zuordnung bei den Änderungen bestehen, solange der Text existiert. Sind alle verwaltenden Personen nicht mehr im System vorhanden, werden die verbleibenden Nutzer zu Managern befördert, die dann löschen können.

Das Änderungsprotokoll innerhalb eines Textes wird nicht automatisch gelöscht und kann nur mit dem Löschen des Textes entfernt werden.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Nutzer, denen ein Text freigegeben wurde, werden über die Freigabe per Benachrichtigung informiert. In der Benachrichtung wird der Ersteller und der Titel des Textes zusammen mit einer Verknüpfung genannt.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch das Änderungsprotokoll ist es möglich nachzuvollziehen, wann welcher Nutzer Änderungen vorgenommen hat. Daraus lässt sich ein Blick in das Arbeitsverhalten des Nutzers gewinnen.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Benutzergenerierte Inhalte können grundsätzlich vertrauliche und/oder persönliche Daten enthalten. Es ist durch den Verantwortlichen mithilfe von Dienstanweisungen sicherzustellen, dass besonders schützenswerte Daten und Daten, die nicht im pädagogischen Netz verarbeitet werden dürfen, nicht durch Benutzer hoch- / heruntergeladen und für andere Zwecke verwendet werden.

Das Änderungsprotokoll erfasst sämtliche Änderungen im Texte-Dokument. Daraus lassen auch Informationen einsehen, die dort eventuell versehentlich eingestellt wurden. Eine Modifikation des Änderungsprotokoll ist nicht möglich.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).
Den Zugriff auf die jeweiligen Inhalte der Texte steuern die Nutzer durch konfigurierbare Freigaben selbst. Ausnahmefall sind hier Benutzer mit dem Recht "Alle Texte verwalten". Diese Benutzer sind in der Lage die Berechtigungseinstellung eines Texte-Dokuments zu ändern, auf das sie mindestens Lesezugriff haben. Auf Texte, die nicht an diese Benutzer freigegeben sind, erhalten sie keinen Zugriff.

Webfilter

Der Webfilter jede aus dem lokalen Netzwerk der Schule aufgerufene Internetadresse und vergleicht diese mit hinterlegten Listen, um den Zugriff zu erlauben oder sperren.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, ausgeführte Aktionen, Zugriffszeiten und IP-Adressen verarbeitet.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die Nutzer sind über die Verarbeitung dieser Daten bereits informiert.

Wer muss Zugriff auf diese Daten haben?

Der Zugriff auf die Log-Daten ist ausschließlich auf die Administration beschränkt.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Die im System anfallenden Logdateien werden automatisch nach 7 Tagen entfernt. Im Backup sind diese Daten maximal 6 Monate verfügbar.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Keine.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Keine.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keine.

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Nutzer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung). Grundsätzlich hat nur die Administration Zugriff auf die Log-Daten.

Videokonferenz

Das Modul Videokonferenz besteht aus zwei Komponenten. Die erste Komponente ist das Modul auf dem lokalen Server. Ausgehend von diesem Modul werden die Nutzer auf Server der IServ GmbH weitergeleitet, über die die eigentlichen Videokonferenzen stattfinden.

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul auf dem Server werden die interne ID, der Name, die IP-Adresse und die Browserkennung verarbeitet.

Bei der Interaktion mit den Videokonferenzen (Raum anlegen, Konferenzbeitritt) werden Klarnamen der Teilnehmer, IP-Adressen, Browserkennungen, Berechtigungen, Videokonferenz-Raum-Einstellungen wie beispielsweise der Raumname und die Adresse

sowie eine eindeutige Identifikationsnummer Ihrer IServ-Instanz an Server der IServ GmbH übermittelt.

Bei der Verwendung des Moduls fallen ggf. Meta-Daten, wie Zeitpunkt des Beitritts oder das Verlassen einer Konferenz an. Diese Daten werden auf den Servern der IServ GmbH protokolliert und denen nur der Auswertung im Fehlerfall. Sie werden nach 7 Tagen automatisch entfernt.

Während einer Videokonferenz haben die Teilnehmer die Möglichkeit, Audio- und Videostream Ihres Geräts zu teilen, an Chat-Unterhaltungen teilzunehmen, Präsentationen hochzuladen etc. Diese benutzergenerierten Inhalte werden lediglich zur Durchführung der Konferenz benötigt und werden temporär gespeichert. Eine Aufzeichnung von Audio- und Videostreams findet nicht statt.

Welche sensiblen Daten werden lt. Art 9 DSGVO verarbeitet?

Durch IServ werden hier nur die Videodaten durchgeleitet, nichts gespeichert. Natürlich fallen aber während einer Konferenz / im Unterricht sensible Daten an (Meinungen, Bild- und Tondaten, rassische Merkmale).

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Einwilligungs- und Informationspflichten müssen individuell durch die Kunden (Schulen) eingeholt werden. IServ stellt passende Vorlagen unter https://iserv.de/downloads/privacy/ zur Verfügung. Datenschutzhinweise finden Kunden zusätzlich unter https://iserv.de/doc/privacy/process-description/#videokonferenzen.

Wer muss Zugriff auf diese Daten haben?

Die Teilnehmer einer Videokonferenz benötigen und erhalten Zugriff auf

- die Klarnamen der anderen Teilnehmer
- die Audio- und Videostreams der anderen Teilnehmer, sofern diese von den jeweiligen Teilnehmern freigegeben wurden
- während der Videokonferenz von den Teilnehmern erstellte Daten, wie Chatverläufe und Notizen

Alle weiteren Informationen, wie Serverprotokolle, sind nur den Administratoren der Serverinfrastruktur der IServ GmbH zugänglich oder müssen von der Schule bei IServ angefordert werden (AV)

Sind alle Felder wirklich notwendig?

IServ übermittelt und verarbeitet für die grundlegende Teilnehmer neben dem Klarnamen auch die IP-Adresse, Berechtigungen und Browserkennung. Diese sind für die Nutzung des Moduls notwendig.

Weitere Informationen, wie die Freigabe von Audio- und Videostreams, geteilte Notizen oder die Nutzung der Bildschirmfreigabe, obliegen den Teilnehmern und werden nicht von IServ verarbeitet.

Werden Daten an Dritte weitergegeben und warum?

Eine Weitergabe der Daten an Dritte findet nicht statt.

Gibt es Löschfristen (automatisch oder empfohlen)?

Zugriffe auf die Weboberfläche von IServ werden für maximal 7 Tage (zzgl. Backups) protokolliert.
Interaktionen mit Videokonferenzen werden für maximal 7 Tage (zzgl. Backups) protokolliert.

Die bei einer Videokonferenz entstandenen Daten, wie Präsentationen oder Chat-Unterhaltungen, werden frühestens zum Ende der Videokonferenz spätestens aber nach 7 Tagen gelöscht. Eine Sicherung dieser Daten findet nicht statt.

Die Löschung der Daten erfolgt automatisch.

Welche der Daten aus diesem Modul werden in anderen Modulen verwendet?

Es werden keine erfassten Daten in anderen Modulen verwendet.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Es sind keine Auswertungen / Pofilbildungen möglich (lediglich das Umfragemodul könnte so gesehen werden)

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Während eine Funktion zur Aufzeichnung von Videokonferenzen im Modul nicht vorhanden ist, besteht trotzdem das Risiko der Aufnahme durch Teilnehmer über Drittprogramme. Dies lässt sich nur über Nutzerordnungen unterbinden. Hier bieten sich für Ton oder Videodaten viele Risikomöglichkeiten (Veröffentlichung, Manipulation der Bilder, des Tons….)

Welche technischen Maßnahmen schützen diese Daten?

Die Daten der Teilnehmer werden grundsätzlich verschlüsselt übertragen (Transportverschlüsselung).

Der Zugriff auf die Protokolle auf den jeweiligen steht nur wenigen Personen der IServ GmbH nur auf Weisung der Schule zur Verfügung. Die Protokolle dürfen lediglich für die Fehleranalyse im Auftrag des Verantwortlichen genutzt werden.

Der Zugriff auf die Protokolle der Videokonferenz-Server der IServ GmbH steht nur ausgewählten Personen der IServ GmbH zur Verfügung. Die Protokolle werden nur genutzt, um die Stabilität des Systems zu gewährleisten und Fehler zu beheben.

In beiden Fällen ist, neben der Zugriffsbeschränkung pro Person, bei der Authentifizierung ein zweiter Faktor notwendig, bevor der Zugriff auf die Server gestattet wird. Sämtliche Zugriffe werden protokolliert und können den ausführenden Personen zugeordnet werden.

Weitere Informationen sind in der IServ Dokumentation unter
https://iserv.de/doc/privacy/process-description/#videokonferenzen zu finden.

WLAN

Welche personenbezogenen Daten werden verarbeitet?

In dem Modul werden der Benutzername, interne Benutzer IDs, Zugriffszeiten und IP-Adressen verarbeitet.
Die Verarbeitung erfolgt im Rahmen der Funktionalität sowie Logging.
Geräte, die automatisch in der Geräteverwaltung registriert werden, enthalten den Benutzernamen im Gerätenamen und haben einen Besitzer gesetzt.

Werden sensible Daten lt. Art 9 DSGVO verarbeitet?

Nein.

Wie wurden / werden die Nutzer über die Verarbeitungen informiert?

Die benutzer

Wer muss Zugriff auf diese Daten haben?

Die Daten sind nur direkt im System zugänglich. Ein Zugriff über die Weboberfläche ist nicht möglich.

Sind alle Felder wirklich notwendig?

Ja.

Werden Daten an Dritte weitergegeben und warum?

Nein.

Gibt es Löschfristen (automatisch oder empfohlen)?

Automatisch registrierte Geräte werden mit dem Löschen des Nutzers automatisch aus dem System entfernt. Außerdem kann eine automatische Löschung von Geräten nach einem bestimmten Zeitraum eingestellt werden.

Die Logfiles werden automatisch nach 7 Tagen aus dem System entfernt und stehen maximal 6 Monate im Backup zur Verfügung.

Welche dieser hier erfassten Daten werden auch in anderen Modulen verwendet?

Durch die übermittelte IP-Adresse werden die Einträge der Geräteverwaltung aktualisiert. Darunter auch, der Zeitpunkt, an denen das Gerät zuletzt online war.

Welche Möglichkeit zur Auswertung oder Profilbildung ergibt sich daraus?

Durch die Anmeldungen können Rückschlüsse auf die zeitliche Verwendung von Geräten erfolgen.

Welches Risiko für den Nutzer kann sich aus den Daten in diesem Modul ergeben?

Keines.

Welche technischen Maßnahmen schützen diese Daten?

Auf die verarbeiteten Daten haben ausschließlich Benutzer mit administrativen Rechen Zugriff.

Eingebundene Seiten von Drittanbietern

Es ist möglich, in IServ Internetseiten als Link einzubinden oder per Schnittstelle aufzurufen. Sobald man diese Seiten betritt, werden die personenbezogenen Daten durch eben diese Drittanbieter verarbeitet.
IServ weist vor dem Wechsel darauf hin.
Im Falle von Single Sign On werden die IServ-Anmeldedaten auch für andere Programme verwendet. Hier sind Administratoren in der Lage, die jeweiligen Seiten als vertrauenswürdig einzustufen, es erscheint dann nur der o.g. Hinweis.