1. Diese IT-Nutzungsordnung gilt für alle Personen, die IT-Dienste oder IT-Geräte der Schule verwenden (User). Im Übrigen wird darauf verwiesen, dass auch die IKT-Nutzungsverordnung - IKT-NV, BGBl. II Nr. 281/2009 i.d.F. BGBl. II Nr. 107/2018 (siehe Anhang) gilt.
2. Das Herunterladen und Speichern von Programmen auf Geräten der Schule ist nicht gestattet, es sei denn, das IT-Management/IT-Kustodiat stimmt dem zu.
3. Ein Recht auf Zurückführung von privaten Daten bei Datenverlust sowie ausreichenden Speicherplatz zur Ablage privater Daten oder zur Sicherung dieser Daten besteht nicht. Der Dienstgeber haftet in keinem Fall für den Verlust von privaten Daten.
4. Es ist gem. § 5 IKT-Schulverordnung (siehe Anhang) untersagt, Kennwörter weiterzugeben. Sie sind so zu verwahren, dass ein Unbefugter vom Kennwort keine Kenntnis erlangen kann.
5. User dürfen IT-Geräte, bei denen sie angemeldet sind und der Bildschirm nicht gesperrt ist, nicht unbeaufsichtigt zurücklassen.
6. Die von der Schule oder dem Dienstgeber zur Verfügung gestellten Mailadressen dürfen nicht zur Registrierung bei externen Dienstleistern für private Zwecke verwendet werden. Externe Dienstleister sind insbesondere Versicherungen, Onlinehändler oder soziale Medien.
7. Bei einer Beschädigung eines schuleigenen IT-Gerätes ist die Schule zu informieren.
8. Die Verwendung von IT-Geräten und IT-Diensten der Schule ist ausschließlich unter den Bedingungen von § 12 IKT-Schulverordnung zulässig.

**IT-Nutzungsbedingungen**

**§ 12.** (1) Unter Berücksichtigung der Anforderungen des § 11 ist die Verwendung eines digitalen Endgerätes im Schulnetz als Arbeitsmittel im IKT-gestützten Unterricht, zum eigenständigen Lernen und für Zwecke der Schulverwaltung zulässig.

(2) Unzulässig ist

1. eine Verwendung für kommerzielle oder gewerbliche Zwecke,
2. eine übermäßige Auslastung des Schulnetzes für private Zwecke,
3. die Integration von kommerzieller Werbung (ausgenommen die Diskussion über die Vor- und Nachteile eines Produktes durch Benutzerinnen und Benutzer) in schüler- oder lehrerbezogene Webpräsenzen sowie Lernplattformen,
4. eine Verwendung mit dem Ziel der Realisierung von illegalen Handlungen sowie der Versuch, unberechtigten Zugang zu Systemen, Software, Diensten oder Informationen zu erlangen,
5. eine Verwendung zu Zwecken der Nachrichtenübermittlung, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet oder gegen Gesetze verstößt,
6. eine Verwendung, die eine Belästigung oder Verängstigung anderer Benutzerinnen oder Benutzer bewirkt,
7. jegliche Verwendung, die andere Benutzerinnen oder Benutzer behindert oder das gute Funktionieren der Services des Schulnetzes stört,
8. die unberechtigte Vervielfältigung und Verteilung von Software sowie jede Art der Verwendung, die im Widerspruch zum Urheberrechtsgesetz, BGBl. Nr. 111/1936, steht.

(3) Über die Zulässigkeit einer konkreten Verwendung hat im Zweifelsfall die Schulleitung zu entscheiden.

(4) Die Schulleitung kann weitere standortspezifische IT-Nutzungsbedingungen anordnen. Sie kann dabei das Schulforum bzw. den Schulgemeinschaftsausschuss beratend beiziehen.

9. Von der Schule bereitgestellte Accounts werden spätestens zwölf Monate nach dem Ausscheiden eines Users aus der Schulverwaltung gelöscht. Der User ist für die Sicherung seiner Daten selbst verantwortlich.
10. Besteht beim Verlust von privaten oder schulischen Datenträgern die Möglichkeit, dass sich darauf schulische Daten befanden, hat der User dies ehestmöglich der Schulleitung zu melden.
11. Bereitgestellte IT-Geräte im Eigentum der Schule sind vor Ausscheiden aus dem Schuldienst oder vor einer längeren Dienstunterbrechung, der Schule zurückzugeben. Personenbezogene Daten sind davor zu löschen.

**Anhang:**
IKT-Schulverordnung, BGBl. II/2021/382
IKT-Nutzungsverordnung – IFT-NV, BGBl. II Nr. 281/2009

# Gesamte Rechtsvorschrift für IKT-Schulverordnung, Fassung vom 19.03.2025

## Langtitel

Verordnung des Bundesministers für Bildung, Wissenschaft und Forschung über IKT-gestützten Unterricht und Datensicherheitsmaßnahmen im Schulwesen (IKT-Schulverordnung)
StF: BGBl. II Nr. 382/2021

## Präambel/Promulgationsklausel

Auf Grund

1. des § 4 Abs. 3 Z 1 des Bildungsdokumentationsgesetzes 2020 – BilDokG 2020, BGBl. I Nr. 20/2021,
2. des § 14a Abs. 3 und § 70a des Schulunterrichtsgesetzes – SchUG, BGBl. Nr. 472/1986, zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 170/2021, sowie
3. des § 6 des Bundesgesetzes zur Finanzierung der Digitalisierung des Schulunterrichts – SchDigiG, BGBl. I Nr. 9/2021,

wird verordnet:

**Inhaltsverzeichnis**


| Paragraph | Gegenstand |
|---|---|
| | **1. Abschnitt**<br>**Allgemeine Bestimmungen** |
| § 1. | Geltungsbereich |
| § 2. | Regelungszweck |
| § 3. | Personenbezogene Bezeichnungen |
| § 4. | Begriffsbestimmungen |
| | **2. Abschnitt**<br>**Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung bei schulischen Verarbeitungen** |
| § 5. | Authentifizierung |
| § 6. | Bildungsstammportale und Bildungsportalverbund |
| § 7. | Anforderungen an IT-Systeme und Dienste |
| § 8. | Hosting |
| § 9. | Organisatorische Datensicherheitsmaßnahmen |
| | **3. Abschnitt**<br>**Technische und organisatorische Maßnahmen bei digitalen Endgeräten** |
| § 10. | Endgeräteverwaltung für digitale Endgeräte |
| § 11. | Anwendungsbezogene Anforderungen an digitale Endgeräte |
| | **4. Abschnitt**<br>**Technische und organisatorische Maßnahmen beim IKT-gestützten Unterricht und für Lern- und Arbeitsplattformen** |
| § 12. | IT-Nutzungsbedingungen |
| § 13. | Funktionalitäten der Endgeräte im IKT-gestützten Unterricht |
| § 14. | Elektronische Kommunikation mit Erziehungsberechtigten |
| | **5. Abschnitt**<br>**Verantwortlichkeit bei schulischen Datenverarbeitungen** |
| § 15. | Abgrenzung der datenschutzrechtlichen Verantwortlichkeit bei Datenverarbeitungen am Schulstandort |

**6. Abschnitt**
**Schlussbestimmungen**

§ 16. Übergangsbestimmung
§ 17. Verweise auf Bundesgesetze
§ 18. Inkrafttreten

## Text

## 1. Abschnitt
## Allgemeine Bestimmungen

### Geltungsbereich

**§ 1.** Diese Verordnung gilt für Bildungseinrichtungen gemäß

1. § 2 Z 1 lit. a, c und e des Bildungsdokumentationsgesetzes 2020 – BilDokG 2020, BGBl. I Nr. 20/2021, mit der Maßgabe, dass
   a) hinsichtlich der Privatschulen ohne gesetzlich geregelte Schulartbezeichnung nur der 2. Abschnitt anzuwenden ist,
   b) die §§ 13 und 14 nur auf Bildungseinrichtungen im Geltungsbereich des Schulunterrichtsgesetzes – SchUG, BGBl. Nr. 472/1986, anzuwenden sind,
2. § 2 Z 1 lit. b und d BilDokG 2020, ausgenommen die §§ 5 bis 9, 12, 15 und 16.

### Regelungszweck

**§ 2.** Diese Verordnung verfolgt die Zwecke

1. der Konkretisierung technischer und organisatorischer Maßnahmen im Sinne der Art.32 der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 127 vom 23.05.2018 S. 2 (im Folgenden: DSGVO) zur Gewährleistung der Sicherheit bei Datenverarbeitungen im Bereich der Schulverwaltung, der Unterrichtsdokumentation und der elektronischen Kommunikation im Schulbereich (2. Abschnitt);
2. der Festlegung von Vorgaben gemäß § 14a des Schulunterrichtsgesetzes – SchUG über die erforderlichen technischen und organisatorischen Maßnahmen für IKT-gestützten Unterricht, digitale Lern- und Arbeitsformen sowie für den Einsatz digitaler Endgeräte im Rahmen der schulischen Verwendung, insbesondere auch hinsichtlich der Funktionalität für den Unterricht und der Sicherheit der Geräte (zB Mobile Device Management und Fernverwaltung) im Sinne des § 6 des Bundesgesetzes zur Finanzierung der Digitalisierung des Unterrichts – SchDigiG, BGBl. I Nr. 9/2021;
3. der Regelung der elektronischen Kommunikation mit Schülerinnen und Schülern sowie Erziehungsberechtigten (zB elektronisches Mitteilungsheft).

### Personenbezogene Bezeichnungen

**§ 3.** Soweit in dieser Verordnung auf natürliche Personen bezogene Bezeichnungen angeführt sind, beziehen sich diese auf alle Geschlechtsformen in gleicher Weise. Bei der Anwendung der Bezeichnung auf bestimmte natürliche Personen ist die jeweils geschlechtsspezifische Form zu verwenden.

### Begriffsbestimmungen

**§ 4.** Im Sinne dieser Verordnung sind zu verstehen:

1. unter dem Begriff „Schulverwaltung“: sämtliche Verarbeitungen personenbezogener Daten, die in datenschutzrechtlicher Verantwortung der Schulleitung am Schulstandort aufgrund schulgesetzlicher Regelungen vorzunehmen sind, soweit sie nicht in den Z 3 bis 6 geregelt sind; davon umfasst sind
   a) Verarbeitungen von Schülerinnen- und Schülerdaten in den Evidenzen gemäß § 5 BilDokG 2020; dazu gehören jedenfalls alle IT-Systeme und Dienste, soweit deren Benutzerinnen und Benutzer, insbesondere in der Rolle der Schulleitung oder Sokrates-Administration damit schulweit auf personenbezogene Daten von Schülerinnen und Schülern

zugreifen können, oder die überwiegend zur Verwaltung personenbezogener Daten nach Art. 9 Abs. 1 DSGVO eingesetzt werden,

b) Verarbeitungen von Schülerinnen- und Schülerdaten im Datenverbund der Schulen gemäß § 6 BilDokG 2020,

c) Verarbeitungen von Schülerinnen- und Schülerdaten zur Ausstellung von Zeugnissen,

d) Datenverarbeitungen in Bezug auf Stundenplanerstellung, Personalverwaltung, aktenmäßige Kommunikation zwischen Schule und Schulbehörde;

2. unter dem Begriff „Endgeräteverwaltung (Mobile Device Management)“: ein IT-System zur zentralisierten Verwaltung von digitalen Endgeräten gemäß Z 10; dieses IT-System dient der Erfüllung der in § 10 festgelegten Funktionalität;
3. unter dem Begriff „Unterrichtsdokumentation“: sämtliche Verarbeitungen von Schülerinnen- und Schülerdaten, die zu Zwecken der laufenden Dokumentation des Unterrichts und der Leistungsbeurteilung durch die Lehrperson vorgenommen werden sowie Datenverarbeitungen zur Durchführung von Kompetenzerhebungen;
4. unter dem Begriff „IT-Services für pädagogische Zwecke“: Maßnahmen zur Schaffung der technischen Rahmenbedingungen für IKT-gestützten Unterricht und elektronische Kommunikation, insbesondere die Zurverfügungstellung von Lernplattformen sowie die Einrichtung von Schülerinnen- und Schüler-Mail-Postfächern, Online-Office-Umgebungen, Onlinespeicherplatz und Webpräsenzen (zB für Projekte);
5. unter dem Begriff „Fernverwaltung“: der Zugriff von Lehrpersonen auf die Schülerinnen- und Schülergeräte während des IKT-gestützten Unterrichts;
6. unter dem Begriff „Authentifizierung“: die Überprüfung der Identität einer Benutzerin oder eines Benutzers im Zuge eines Anmeldevorgangs an einem IT-System und Dienst;
7. unter dem Begriff „Bildungsstammportal“: ein Portal, das der Benutzer- und Berechtigungsverwaltung zugriffsberechtigter Personen (Schülerinnen und Schüler, Lehrpersonen sowie Erziehungsberechtigte) für den Zugang zu IT-Systemen und Diensten gemäß Z 1 bis 4 dient;
8. unter dem Begriff „Bildungsportalverbund“: die Gesamtheit der Bildungsstammportale, deren Betreiber eine Vereinbarung zu gemeinsamen Rechten, Pflichten und Nutzungsbedingungen (Bildungsportalverbundvereinbarung) unterzeichnet haben;
9. unter dem Begriff „IT-Systeme und Dienste“: Systeme und Dienste gemäß Art. 32 DSGVO, über deren Einsatz durch die Stelle gemäß § 15 Z 2 entschieden wurde und die in Schulen zur Erfüllung der gesetzlichen Aufgaben bzw. im öffentlichen Interesse sowie zur Durchführung der Datenverarbeitungen nach Z 1 bis 7 eingesetzt werden;
10. unter dem Begriff „digitale Endgeräte“: Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegtbildern sowie Daten, die zur Datenverarbeitung und -kommunikation eingesetzt werden können, insbesondere Notebooks oder Tablets; diese können durch den Dienstgeber als Sachbehelf gemäß § 80 des Beamten-Dienstrechtsgesetzes 1979 – BDG 1979, BGBl. Nr. 333/1979, bzw. § 23 des Vertragsbedienstetengesetzes 1948 – VBG, BGBl. Nr. 86/1948, oder durch die Erziehungsberechtigten als Arbeitsmittel gemäß § 14a iVm § 61 SchUG bereitgestellt werden;
11. unter dem Begriff „Schulnetz“: die Gesamtheit aller Netzwerke, Komponenten und Server, die Software, Dienste und Daten bereitstellen, um am Schulstandort durch digitale Endgeräte (unabhängig vom wirtschaftlichen Eigentümer) genutzt zu werden.

## 2. Abschnitt

## Technische und organisatorische Maßnahmen zur Gewährleistung der Sicherheit der Datenverarbeitung bei schulischen Verarbeitungen

### Authentifizierung

**§ 5.** (1) Beim Login an IT-Systemen und Diensten, etwa durch Anmeldung im Schulnetz bzw. an einem Bildungsstammportal, ist eine Authentifizierung durch personenbezogene Benutzerkennung und Passwort erforderlich. Dabei sind die IT-Systeme und Dienste so zu konfigurieren, dass Passwörter ausreichend komplex zu gestalten sind. Weiters sind die Benutzerinnen und Benutzer zu belehren, dass Passwörter nicht weitergegeben werden dürfen.

(2) Bei IT-Systemen und Diensten für Datenverarbeitungen gemäß § 4 Z 1 und 2 ist zusätzlich eine Mehr-Faktor-Authentifizierung erforderlich (etwa mittels Technologien wie Handysignatur, TANs über dienstliche Mail-Adresse, biometrische Merkmale oder gleichwertige Maßnahmen).

**Bildungsstammportale und Bildungsportalverbund**

**§ 6.** (1) Zur Gewährleistung der IT-Sicherheit in Schulen, in der Schulverwaltung und zum Schutz der Rechte von Schülerinnen und Schülern, Lehrpersonen und Erziehungsberechtigten ist für die Anmeldung und Nutzung von IT-Systemen und Diensten im Schulwesen ein Identity- und Access-Management vorzusehen. Zu diesem Zweck ist für alle öffentlichen und privaten Schulen von der Bundesministerin oder vom Bundesminister für Bildung, Wissenschaft und Forschung als Verantwortliche bzw. als Verantwortlicher ein Bildungsstammportal zu betreiben, sofern deren Erhalter nicht von der Möglichkeit des Betriebs eines eigenen Bildungsstammportals gemäß Abs. 2 Gebrauch machen. Jenes umfasst als Access-Management das IT-System „Portal Digitale Schule (PoDS)“ und verwaltet die Zugriffsberechtigungen von Schülerinnen und Schülern, Lehr- und Verwaltungspersonal sowie von Erziehungsberechtigten auf schulbezogene IT-Systeme und Dienste. Die dafür benötigten Identitätsdaten dieser Personengruppen werden im IT-System „edu.IDAM“ für Schülerinnen und Schüler, im PoDS für Erziehungsberechtigte als Identitätsmanagement verwaltet und aus den lokalen Evidenzen nach § 5 BilDokG 2020 bzw. den Personalverwaltungssystemen gespeist.

(2) Eine Stelle nach § 15 Z 2 oder ein Schulerhalter kann als Verantwortlicher ein Bildungsstammportal für die Schülerinnen und Schüler, deren Erziehungsberechtigte sowie Lehr- und Verwaltungspersonal im eigenen Zuständigkeitsbereich betreiben. Solche Bildungsstammportale haben für die Aufnahme in den Bildungsportalverbund gemäß § 4 Z 8 die allgemeine Zugänglichkeit für Schülerinnen und Schüler, Lehr- und Verwaltungspersonal sowie Erziehungsberechtigte im jeweiligen Geltungsbereich eines Bildungsstammportals zu gewährleisten und für das Access-Management für bundesweite IT-Systeme und Dienste im Bildungsbereich und Synchronisation mit anderen bundesweiten Verzeichnisdiensten Schnittstellen zu den IT-Systemen PoDS und edu.IDAM vorzusehen und die dafür benötigten Daten gemäß Abs. 3 zur Verfügung zu stellen. Dafür haben die Betreiber eines Bildungsstammportals dem Bildungsportalverbund beizutreten und eine unterzeichnete Bildungsportalverbundvereinbarung bei der Bundesministerin oder beim Bundesminister für Bildung, Wissenschaft und Forschung als Depositär zu hinterlegen. Diese Vereinbarung hat der Festlegung gemeinsamer Rechte, Pflichten und Nutzungsbedingungen der Betreiber von Bildungsstammportalen zu dienen und einen einheitlichen Rahmen für den Zugriff auf verschiedene IT-Systeme und Dienste, wie sie insbesondere im PoDS beinhaltet sind, zu schaffen. Der Text der Bildungsportalverbundvereinbarung ist auf der Webseite des Bundesministeriums für Bildung, Wissenschaft und Forschung zu veröffentlichen.

(3) Für die Nutzung eines Bildungsstammportals gemäß Abs. 1 und 2 durch Schülerinnen und Schüler sowie deren Erziehungsberechtigte und durch Bedienstete des Bundes an Schulen und Landeslehrpersonen sind im Bildungsportalverbund zu verarbeiten und bereitzustellen:

1. folgende Daten der Schülerinnen und Schüler aus den Evidenzen der Schülerinnen und Schüler bzw. der Studierenden gemäß § 5 sowie Anlage 1 und 2 BilDokG 2020 in Verbindung mit § 14a SchUG sowie das bPK-BF aus dem Stammzahlenregister:
   a) Angaben zur besuchten Schule (Schulkennzahl, Schulbezeichnung, Anschrift),
   b) ein bildungseinrichtungsspezifisches Personenkennzeichen gemäß § 5 Abs. 1 Z 3 BilDokG2020,
   c) das bereichsspezifische Personenkennzeichen des Tätigkeitsbereichs „Bildung und Forschung“ (bPK-BF),
   d) die Namen (Vor- und Familiennamen, einschließlich allfälliger akademischer Grade),
   e) das Geburtsdatum,
   f) das Geschlecht,
   g) Angaben zur besuchten Klasse bzw. zum besuchten Jahrgang, Klassen- bzw. Jahrgangsvorstand oder Klassen- bzw. Jahrgangsvorständin sowie Zuordnung zum Stundenplan,
   h) der Schülerinnen- bzw. Schülerstatus (ordentlich oder außerordentlich),
   i) die Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse),
2. folgende Daten der Erziehungsberechtigten aus den Evidenzen der Schülerinnen und Schüler gemäß § 5 Abs. 1 Z 20 sowie Anlage 2 Z 9 BilDokG 2020 in Verbindung mit § 14a SchUG :
   a) die Schulkennzahl bzw. Schulkennzahlen der von den zugehörigen Schülerinnen und Schülern besuchten Schule bzw. Schulen,

b) das bPK-BF, dieses nach Erklärung der Einwilligung gem. Art 7 DSGVO der oder des Erziehungsberechtigten,
c) die Namen (Vor- und Familiennamen einschließlich allfälliger akademischer Grade),
d) das Geschlecht,
e) die Zuordnung zu den zugehörigen Schülerinnen und Schüler je Schulkennzahl,
f) die Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse),

3. folgende Daten der Bediensteten des Bundes an Schulen gemäß § 280 Abs. 1 Z 1 BDG und der Landeslehrpersonen gemäß § 119a des Landeslehrer-Dienstrechtsgesetzes – LDG, BGBl. Nr. 302/1984, in Verbindung mit § 280 Abs. 1 Z 7 BDG:
a) die Schulkennzahl bzw. Schulkennzahlen,
b) das bPK-BF,
c) die Namen (Vor- und Familiennamen einschließlich allfälliger akademischer Grade),
d) das Geschlecht,
e) die SAP-Personalnummer,
f) die Zuordnung zu Stundenplänen (Klasse bzw. Jahrgang),
g) die Kontaktdaten (Anschrift, Telefonnummer, E-Mail-Adresse).

(4) Schulleitungen oder Dienstgeber, die das Bildungsstammportal gemäß Abs. 1 nutzen, haben die Daten gemäß Abs. 3 über Schnittstellen aus den jeweiligen lokalen Evidenzen gemäß § 5 BilDokG 2020 sowie den Personalverwaltungssystemen, soweit sie nicht Bundesbedienstete betreffen, für Zwecke des Identitätsmanagements und der Synchronisation in den IT-Systemen PoDS und edu.IDAM zu übermitteln. Sie haben die Kosten zu tragen, die durch die Herstellung und den Betrieb der Schnittstelle zur Anbindung an das Bildungsstammportal des Bundes entstehen.

**Anforderungen an IT-Systeme und Dienste**

**§ 7.** (1) Zur Integration weiterer IT-Systeme und Dienste in das PoDS auf Vorschlag einer Bildungsdirektion oder eines privaten Schulerhalters ist durch den Diensteanbieter als Auftragsverarbeiter eine Auftragsverarbeitervereinbarung mit der Bundesministerin oder dem Bundesminister für Bildung, Wissenschaft und Forschung als Verantwortlicher für PoDS abzuschließen und zu dokumentieren, wie die technischen und organisatorischen Maßnahmen dieser Verordnung sowie die Schnittstellenspezifikation und Teilnahmebedingungen des PoDS eingehalten werden.

(2) IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 1 und 2 sind grundsätzlich webbasiert zur Verfügung zu stellen, soweit sie nicht ausschließlich auf dienstlichen Endgeräten im Schulnetz verwendet werden. Beim Design des IT-Systems oder Dienstes ist darauf zu achten, dass die für die Anwenderinnen und Anwender benötigte Funktionalität grundsätzlich ohne Speicherung personenbezogener Daten am Endgerät gewährleistet ist. Die Datensicherheit der IT-Systeme und Dienste kann insbesondere über einschlägige Zertifizierungen nachgewiesen werden. Im Zuge der ersten Inbetriebnahme ist ein dem Stand der Technik entsprechender und dem Risikopotential der Anwendung angemessener Penetrationstest sowie ein Third Party Review zur Bewertung der IT-Sicherheit durchzuführen.

**Hosting**

**§ 8.** (1) IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 1 für Schulen sind in Rechenzentren zu betreiben, die sich im EWR-Raum bzw. in Staaten, hinsichtlich derer ein Angemessenheitsbeschluss der Europäischen Kommission gemäß Art. 45 DSGVO besteht, befinden und geeignete und verhältnismäßige technische und organisatorische Sicherheitsvorkehrungen aufweisen. Diese haben den Stand der Technik zu berücksichtigen und dem Risiko, das mit vernünftigem Aufwand feststellbar ist, angemessen zu sein.

(2) IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 2 bis 4 können über die Regelung in Abs. 1 hinaus auch in sonstigen Rechenzentren geeigneter Clouddiensteanbieter gehostet werden. Beim Heranziehen solcher Clouddiensteanbieter sind jedenfalls die Bestimmungen des Europäischen Datenschutzausschusses zu genehmigten Verhaltensregeln nach Art. 40 DSGVO zu berücksichtigen. Es sind nur jene Clouddiensteanbieter heranzuziehen, die eine Vereinbarung mit dem BMBWF abgeschlossen haben. Diese hat sich nach den Rahmenbedingungen des Bundesministeriums für Bildung, Wissenschaft und Forschung für den Einsatz privater Clouddiensteanbieter im IKT-gestützten Unterricht zu richten.

(3) Zur Sicherstellung der IT-Sicherheit können IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 1 bis 5 auch für mehrere Schulen zentral gehostet werden, wobei durch eine

Berechtigungsverwaltung sicherzustellen ist, dass auf Schülerinnen- und Schülerdaten einer Schule nur durch die jeweilige Schulleitung zugegriffen werden darf.

**Organisatorische Datensicherheitsmaßnahmen**

**§ 9.** Die Schulleitung hat sicherzustellen, dass

1. Datenverarbeitungen gemäß § 4 Z 1 vor unbefugter Einsicht geschützt sind,
2. der Zutritt zu Räumen, in denen solche Datenverarbeitungen stattfinden, nur befugten Benutzerinnen und Benutzern möglich ist und bei etwaigem Parteienverkehr in diesen Räumen keine Einsichtnahme in die Daten erfolgen kann,
3. Datenverarbeitungen gemäß § 4 Z 1 bis 4 nur durch Bedienstete der eigenen Dienststelle nach Abwägung der Erforderlichkeit für die Erfüllung der schulrechtlich vorgesehenen Zwecke möglich sind, und nur diesen die dafür erforderlichen Zugangsberechtigungen eingeräumt werden,
4. Bedienstete der eigenen Dienststelle in regelmäßigen Abständen über die Bestimmungen der DSGVO und des Datenschutzgesetzes – DSG, BGBl. I Nr. 165/1999, belehrt werden, insbesondere hinsichtlich
   a) der Wahrung des Datengeheimnisses gemäß § 6 DSG,
   b) der datenschutzrechtlichen Zweckbindung, auf deren Grundlage personenbezogene Daten nur für die schulrechtlich vorgesehenen Zwecke verarbeitet werden, dürfen sowie
   c) des Inhalts dieser Verordnung.

## 3. Abschnitt
## Technische und organisatorische Maßnahmen bei digitalen Endgeräten

**Endgeräteverwaltung für digitale Endgeräte**

**§ 10.** Um die Funktionalität und Sicherheit aller digitalen Endgeräte mittels geeigneter technischer Maßnahmen, insbesondere durch Integration in eine Endgeräteverwaltung (Mobile Device Management), sicherzustellen, haben die von der Stelle gemäß § 15 Z 2 bzw. vom Dienstgeber eingesetzten Systeme zur Endgeräteverwaltung folgende technische und organisatorische Maßnahmen zu gewährleisten:

1. automatisiertes Einspielen von Sicherheits- und Betriebssystemupdates auf den digitalen Endgeräten,
2. aktueller Schutz vor Schadsoftware auf digitalen Endgeräten zum Schutz des Schulnetzes,
3. sicherer Betrieb im Schulnetz gemäß den für die jeweilige Benutzerin oder den jeweiligen Benutzer festgelegten Zugriffsrechten,
4. bei Verlust die Möglichkeit zur Fernlokalisierung, Fernsperre bzw. Fernlöschung der digitalen Endgeräte bei technischer Möglichkeit auf ausdrücklichen und dokumentierten Wunsch der Geräteinhaberin oder des Geräteinhabers, soweit das Endgerät erreichbar ist, und
5. Aktivierung der für die Endgeräteverwaltung erforderlichen Software-Komponenten auf den verwalteten digitalen Endgeräten.

**Anwendungsbezogene Anforderungen an digitale Endgeräte**

**§ 11.** (1) Die Verwendung digitaler Endgeräte ist zulässig

1. für Datenverarbeitungen gemäß § 4 Z 1 und 2, sofern die Endgeräte
   a) durch den Dienstgeber als Sachbehelf gemäß § 80 BDG 1979 bzw. § 23 VBG zur Verfügung gestellt werden,
   b) die vorgesehenen Methoden im Rahmen der Mehr-Faktor-Authentifizierung gemäß § 5 Abs. 2 unterstützen,
   c) mit einer Endgeräteverwaltung gemäß § 10 betrieben werden bzw. durch die Betreuung der Dienstgeräte im Rahmen der Schul-IT alle Anforderungen des § 10 Z 1 bis 4 gewährleistet sind und
   d) lokale Daten möglichst in verschlüsselter Form speichern und
2. für Datenverarbeitungen gemäß § 4 Z 3 und 4, sofern die im Schulnetz befindlichen Endgeräte mit einer Endgeräteverwaltung gemäß § 10 betrieben werden.

(2) Wenn an einem Schulstandort die Entscheidung für die einheitliche Verwendung digitaler Endgeräte insbesondere im Rahmen eines Digitalisierungskonzepts gemäß § 2 Abs. 2 SchDigiG getroffen wurde, so ist eine Beschreibung der Gerätetypen festzulegen und sind ausschließlich Endgeräte dieser Typen zu verwenden.

(3) Um die Speicherung personenbezogener Schülerinnen- und Schülerdaten am Endgerät zu vermeiden, sind IT-Systeme und Dienste für Datenverarbeitungen gemäß § 4 Z 1 und 2 grundsätzlich webbasiert zur Verfügung zu stellen. Stehen ausnahmsweise an Schulen keine webbasierten IT-Systeme und Dienste für die genannten Datenverarbeitungen zur Verfügung, so sind durch die jeweiligen Stellen gemäß § 15 Z 2 technische und organisatorische Maßnahmen, die eine gleichwertige IT-Sicherheit wie beim Einsatz webbasierter Lösungen gewährleisten, vorzusehen und diesbezügliche Regelungen, wie etwa Festplattenverschlüsselung, für die Verwendung festzulegen.

(4) Anstelle einer Einbindung in eine Endgeräteverwaltung gemäß § 10 können Zugriffe auf IT-Systeme und Dienste über ein schulseitig betriebene Remote Desktop Service erfolgen, sofern gewährleistet ist, dass alle Anforderungen dieser Verordnung hinsichtlich Authentifizierung, Hosting des Remote Desktop Service, organisatorischer Maßnahmen sowie eines sicheren Betriebs ohne direkte Datenhaltung am Endgerät durch die Funktionalität des Remote Desktop Services erfüllt werden.,

## 4. Abschnitt

## Technische und organisatorische Maßnahmen beim IKT-gestützten Unterricht und für Lern- und Arbeitsplattformen

### IT-Nutzungsbedingungen

**§ 12.** (1) Unter Berücksichtigung der Anforderungen des § 11 ist die Verwendung eines digitalen Endgerätes im Schulnetz als Arbeitsmittel im IKT-gestützten Unterricht, zum eigenständigen Lernen und für Zwecke der Schulverwaltung zulässig.

(2) Unzulässig ist

1. eine Verwendung für kommerzielle oder gewerbliche Zwecke,
2. eine übermäßige Auslastung des Schulnetzes für private Zwecke,
3. die Integration von kommerzieller Werbung (ausgenommen die Diskussion über die Vor- und Nachteile eines Produktes durch Benutzerinnen und Benutzer) in schüler- oder lehrerbezogene Webpräsenzen sowie Lernplattformen,
4. eine Verwendung mit dem Ziel der Realisierung von illegalen Handlungen sowie der Versuch, unberechtigten Zugang zu Systemen, Software, Diensten oder Informationen zu erlangen,
5. eine Verwendung zu Zwecken der Nachrichtenübermittlung, welche die öffentliche Ordnung und Sicherheit oder die Sittlichkeit gefährdet oder gegen Gesetze verstößt,
6. eine Verwendung, die eine Belästigung oder Verängstigung anderer Benutzerinnen oder Benutzer bewirkt,
7. jegliche Verwendung, die andere Benutzerinnen oder Benutzer behindert oder das gute Funktionieren der Services des Schulnetzes stört,
8. die unberechtigte Vervielfältigung und Verteilung von Software sowie jede Art der Verwendung, die im Widerspruch zum Urheberrechtsgesetz, BGBl. Nr. 111/1936, steht.

(3) Über die Zulässigkeit einer konkreten Verwendung hat im Zweifelsfall die Schulleitung zu entscheiden.

(4) Die Schulleitung kann weitere standortspezifische IT-Nutzungsbedingungen anordnen. Sie kann dabei das Schulforum bzw. den Schulgemeinschaftsausschuss beratend beiziehen.

### Funktionalitäten der Endgeräte im IKT-gestützten Unterricht

**§ 13.** (1) Die im IKT-gestützten Unterricht eingesetzten IT-Systeme und Dienste haben den Videoeinsatz und die Präsentationsmöglichkeiten zu unterstützen.

(2) Bei Aktivierung der Kameras sind die technischen Möglichkeiten der Schülerinnen und Schüler, der Schutz der familiären Privatsphäre in der Wohnung der Schülerinnen und Schüler sowie die besonderen Bedürfnisse von Schülerinnen und Schülern mit Behinderung nach Maßgabe der technischen Möglichkeiten zu berücksichtigen.

(3) Aufzeichnungen des Unterrichts durch Video- oder Audioaufnahmen oder Screenshots sind nur mit Einwilligung aller Betroffenen gemäß Art. 7 DSGVO in Verbindung mit § 4 Abs. 4 DSG zulässig.

### Elektronische Kommunikation mit Erziehungsberechtigten

**§ 14.** Sofern die Erziehungsberechtigten die Möglichkeit einer elektronischen Kommunikation mit der Schule nützen wollen, ist durch die zum Einsatz kommenden IT-Systeme und Dienste sicherzustellen, dass die elektronische Kommunikation mit den Erziehungsberechtigten der jeweiligen Schülerin bzw. des

jeweiligen Schülers erfolgt und die Kenntnisnahme der Nachricht durch die Erziehungsberechtigten für die Schule nachvollziehbar ist.

## 5. Abschnitt
## Verantwortlichkeit bei schulischen Datenverarbeitungen

### Abgrenzung der datenschutzrechtlichen Verantwortlichkeit bei Datenverarbeitungen am Schulstandort

**§ 15.** Verantwortlicher im Sinne des Art. 4 Z 7 DSGVO ist

1. hinsichtlich der Rechtmäßigkeit der Verarbeitung personenbezogener Daten und Einhaltung der Grundsätze des Art. 5 DSGVO durch die Bildungseinrichtung sowie hinsichtlich der Wahrung des Datenschutzes am Schulstandort gemäß § 4 Abs. 1 BilDokG 2020 die jeweilige Schulleitung und
2. hinsichtlich der Gewährleistung der Datensicherheit der nötigen IT-Systeme und Dienste für Datenverarbeitungen (zB einer Schulverwaltungssoftware und deren Hosting) jene Stelle, die als Maßnahme bezüglich der IT-Ausstattung an Schulen die Entscheidung darüber trifft.

## 6. Abschnitt
## Schlussbestimmungen

### Übergangsbestimmung

**§ 16.** Allen Schülerinnen und Schülern an Bundesschulen sowie deren Erziehungsberechtigten ist die Teilnahme am Bildungsstammportal gemäß § 6 Abs. 1 ab 30. September 2021 zu ermöglichen. Schnittstellen gemäß § 6 Abs. 2 und 4 sind bis spätestens 30. September 2022 durch die Stelle gemäß § 15 Z 2 einzurichten. § 10 und § 11 sind nach Maßgabe der technischen Voraussetzungen an den Schulstandorten bis spätestens 31. Jänner 2022 umzusetzen.

### Verweise auf Bundesgesetze

**§ 17.** Soweit in dieser Verordnung auf Bundesgesetze verwiesen wird, sind diese in der mit dem Inkrafttreten der jeweils letzten Novelle dieser Verordnung geltenden Fassung anzuwenden.

### Inkrafttreten

**§ 18.** Diese Verordnung tritt mit 1. September 2021 in Kraft.

# Gesamte Rechtsvorschrift für IKT-Nutzungsverordnung, Fassung vom 13.04.2026

## Langtitel

Verordnung der Bundesregierung über die private Nutzung der Informations- und Kommunikationstechnik-Infrastruktur des Bundes durch Bedienstete des Bundes (IKT-Nutzungsverordnung – IKT-NV)
StF: BGBl. II Nr. 281/2009

## Änderung

BGBl. II Nr. 107/2018

## Präambel/Promulgationsklausel

Auf Grund des § 79d des Beamten-Dienstrechtsgesetzes 1979, BGBl. Nr. 333, und des § 29n des Vertragsbedienstetengesetzes 1948, BGBl. Nr. 86, beide zuletzt geändert durch das Bundesgesetz BGBl. I Nr. 77/2009 wird verordnet:

## Text

### Begriffsbestimmungen

**§ 1.** Im Sinne dieser Verordnung bedeuten die folgenden Begriffe:

1. „IKT“ (Informations- und Kommunikationstechnologie oder -technik): alle Einrichtungen zur elektronischen oder nachrichtentechnischen Übermittlung, Speicherung und Verarbeitung von Sprache, Text, Stand- und Bewegbildern sowie Daten,
2. „IKT-Infrastruktur“: alle Geräte („Hardware“), die vom Dienstgeber zur Verfügung gestellt werden oder im Einvernehmen mit dem Dienstgeber für dienstliche Zwecke benutzt werden und der Informationsverarbeitung für Zwecke des Dienstgebers dienen, sowie die darauf befindlichen Programme und Daten („Software“),
3. „korrekte Funktionsfähigkeit“: Wahrung der Vertraulichkeit, der Integrität und Verfügbarkeit der IKT-Infrastruktur.

### Gegenstand

**§ 2.** Diese Verordnung regelt die private Nutzung der IKT-Infrastruktur durch Bedienstete des Bundes.

### Allgemeine Grundsätze für die private Nutzung der IKT-Infrastruktur

**§ 3.** Die Nutzung der für den Dienstbetrieb zur Verfügung stehenden IKT-Infrastruktur für private Zwecke ist im eingeschränkten Ausmaß zulässig. Sie darf jedoch nicht missbräuchlich erfolgen, dem Ansehen des öffentlichen Dienstes nicht schaden, der Aufrechterhaltung eines geordneten Dienstbetriebes nicht entgegenstehen und die Sicherheit und Leistungsfähigkeit der IKT-Infrastruktur nicht gefährden. Sie darf außerdem nur unter Beachtung sämtlicher weiterer ressort- oder arbeitsplatzspezifischer Nutzungsregelungen erfolgen. Insbesondere ist eine eigenmächtige Veränderung der zur Verfügung gestellten IKT-Infrastruktur (Hard- und Software) unzulässig. Die Bediensteten haben keinen Anspruch auf private Nutzung der vom Dienstgeber für den Dienstbetrieb zur Verfügung gestellten IKT-Infrastruktur.

### Internet

**§ 4.** (1) Die Bediensteten dürfen vom Dienstgeber bereitgestellte Internetdienste für private Zwecke nur dann verwenden, wenn

1. eine Beeinträchtigung des Ansehens des öffentlichen Dienstes,
2. ein mehr als bloß geringfügiger Zeitaufwand während der Dienstzeit,
3. eine Anscheinserweckung, dass die Nutzung im Namen, Interesse oder mit Wissen des Dienstgebers vorgenommen wird,

4. die Erzeugung negativer Rechtsfolgen beim Dienstgeber,
5. eine Verletzung von Geheimhaltungspflichten,
6. eine Verletzung eigener oder fremder Dienstpflichten,
7. eine Verursachung von mehr als bloß geringfügigen Kosten und
8. eine Störung des Dienstbetriebes

ausgeschlossen sind.

(2) Das Abschließen von privaten Geschäften unter Zuhilfenahme der vom Dienstgeber zur Verfügung gestellten technischen Einrichtungen ist nur insoweit zulässig, als dabei in eindeutiger Weise der private Charakter des Vorgangs ersichtlich ist.

(3) Die Bediensteten haben keinen Anspruch auf Nutzung von Internetdiensten, die vom Dienstgeber als für den Dienstbetrieb nicht erforderlich erachtet werden. Der Dienstgeber kann zur Wahrung der in § 3 angeführten Nutzungsgrundsätze die Privatnutzung von Internet-Diensten beschränken oder gänzlich untersagen. Er darf dabei insbesondere Web-Inhalte durch den Einsatz von Filtersoftware sperren.

(4) Jedenfalls untersagt ist

1. der Zugriff auf strafrechtlich verbotene oder sonstige gesetzwidrige Inhalte,
2. jegliche Benutzung der zur Verfügung gestellten Ressourcen im Rahmen eines strafrechtlich relevanten Tatbestandes,
3. der Zugriff auf Internetseiten mit pornografischem Inhalt,
4. der Zugriff auf Seiten, die eine Zahlungsverpflichtung des Dienstgebers verursachen sowie
5. das Herunterladen von bestimmten, besonders für deren Größe oder Anfälligkeit für Schadprogramme bekannten ausführenden Dateitypen.

(5) Bei einem irrtümlichen Zugriff auf Seiten, die unter Abs. 4 fallen, sind diese unverzüglich wieder zu verlassen.

### E-Mail

**§ 5.** (1) Die Bediensteten dürfen die vom Dienstgeber bereitgestellten E-Mail-Dienste für private Zwecke nur unter den für die Internetnutzung angeführten Bedingungen verwenden.

(2) Bedienstete dürfen in privaten E-Mails, die sie unter Verwendung ihrer dienstlichen E-Mail-Adresse versenden, keinen Hinweis auf ihre dienstliche Stellung oder ihre dienstliche Postadresse aufnehmen. Insbesondere das Hinzufügen der dienstlichen E-Mail-Signatur ist unzulässig.

(3) Der Dienstgeber darf private E-Mails in einem für die Abwehr von Schäden an der IKT-Infrastruktur oder zur Gewährleistung ihrer korrekten Funktionsfähigkeit notwendigen Ausmaß auf Schadsoftware und Spam scannen. Als Schadsoftware oder Spam identifizierte E-Mails werden je nach ressortspezifischer Strategie behandelt (Quarantäne, Löschung, etc.), wobei der oder die Bedienstete von mit Schadsoftware identifizierten E-Mails, soweit technisch möglich, unverzüglich in geeigneter Weise in Kenntnis zu setzen ist. Dies gilt in gleichem Maß für ein- und ausgehende E-Mails.

### Soziale Medien

**§ 5a.** (1) Die Bediensteten dürfen die Registrierungen und Profile des Dienstgebers in sozialen Medien nicht für private Zwecke verwenden, soweit nicht durch ressort- oder arbeitsplatzspezifische Nutzungsregelungen Abweichendes festgelegt ist.

(2) Bedienstete dürfen im Rahmen der Verwendung privater Registrierungen und Profile in sozialen Medien nicht den Anschein erwecken, dass die Nutzung im Namen, Interesse oder mit Wissen des Dienstgebers vorgenommen wird.

(3) Darüber hinaus gelten die §§ 3 bis 5 sinngemäß für die Verwendung von Registrierungen und Profilen in sozialen Medien.

### Weitere Dienste

**§ 6.** Beim Einsatz weiterer IKT-Infrastruktur-Dienste sind die §§ 3 bis 5a sinngemäß anzuwenden.

### Datenspeicherung und Datensicherung

**§ 7.** (1) Die Bediensteten haben die Bestimmungen der Verordnung (EU) 2016/679 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), ABl. Nr. L 119 vom 04.05.2016 S. 1, in der Fassung der Berichtigung ABl. Nr. L 314 vom 22.11.2016 S. 72, des Datenschutzgesetzes, BGBl. I Nr. 165/1999, und der weiteren datenschutzrechtlichen Vorgaben in der jeweils geltenden Fassung einzuhalten.

(2) Ein Recht auf Zurückführung von Daten bei Datenverlust sowie auf ausreichenden Speicherplatz zur Ablage privater Daten oder zur Sicherung dieser Daten besteht nicht. Der Dienstgeber haftet in keinem Fall für den Verlust von privaten Daten.

(3) Der Speicherplatz für private Daten ist von den dienstlichen Bereichen bestmöglich zu trennen und zu kennzeichnen.

**Schlussbestimmungen**

**§ 8.** (1) § 5a samt Überschrift, § 6, § 7 Abs. 1 und § 8 samt Überschrift in der Fassung der Verordnung BGBl. II Nr. 107/2018 treten mit 25. Mai 2018 in Kraft.