GEMEINDE
BIRSFELDEN

ICT-Verordnung

Gültig ab 1. Januar 2024

Inhalt

A. ALLGEMEINE BESTIMMUNGEN

§ 1 Geltungsbereich

Diese Verordnung gilt für alle internen und externen Nutzenden (Mitarbeitende, Behördenmitglieder, Externe) der IT-Infrastruktur, der Informations- und Kommunikationstechnologien sowie Plattformen der Gemeinde Birsfelden.

§ 2 Gegenstand und Zweck

Gegenstand dieser Verordnung ist der sichere, rechtmässige und verantwortungsvolle Umgang mit Informationen und Daten sowie deren Schutz vor einem Verlust oder Missbrauch. Dies gilt unabhängig davon, ob Informationen und Daten auf den von der Gemeinde zur Verfügung gestellten Informations- und Kommunikationstechnologien oder auf den privaten Geräten der Mitarbeitenden, der Behördenmitglieder und Externen bearbeitet werden.

§ 3 Grundlagen

1 Diese Verordnung bezieht sich auf folgende rechtliche Grundlagen:

a) Gemeindegesetz (GG, SGS 180)
b) Gesetz über die Information und den Datenschutz (IDG, SGS 162)
c) Verordnung über die Information und den Datenschutz (IDV, SGS 162.11)
d) Weiter sind datenschutzrechtliche Bestimmungen in den verschiedenen Spezialgesetzen und -verordnungen (insbesondere im Personalrecht) zu beachten.

2 Im Anhang 1 zu dieser Verordnung sind grundlegende Begriffe und deren Definition aufgeführt. Sie sind ein wichtiger Bestandteil dieser Verordnung.

§ 4 Schützenswerte Informationen und Daten

1 Für den Umgang mit Informationen und Daten gelten die folgenden Schutzziele: Vertraulichkeit, Integrität, Authentizität und Nachvollziehbarkeit (Definition der Begriffe siehe Anhang 1 zu dieser Verordnung).

2 Informationen und Daten werden aufgrund ihrer Vertraulichkeit wie folgt klassifiziert: Streng vertraulich, vertraulich, intern und nicht klassifiziert (Definition der Begriffe siehe Anhang 1 zu dieser Verordnung).

3 Gemäss den rechtlichen Vorgaben werden Informationen, die als vertraulich oder streng vertraulich klassifiziert sind, als schützenswert eingestuft. Sie stellen das zentrale Element dieser Verordnung dar.

B. VERANTWORTUNG

§ 5 Gesamtverantwortung

Der Gemeinderat trägt die Verantwortung für den Umgang mit den Informationen, die Birsfelden als öffentliches Organ zur Erfüllung seiner gesetzlichen Aufgaben bearbeitet. (§ 6 Abs. 1 IDG). Er ist verantwortlich für die Kommunikation und Durchsetzung dieser Richtlinie und bleibt abschliessend auch verantwortlich für die durch externe Partner bearbeiteten Informationen (§ 7 Abs. 2 IDG).

§ 6 Verantwortung Informationssicherheit (ISV)

1 Die Stabsstelle Informatik ist die für die Informationssicherheit verantwortliche Stelle (ISV). Sie ist in dieser Funktion direkt dem Gemeinderat unterstellt.

2 Sie ist für die Umsetzung dieser Verordnung verantwortlich und damit befugt, den Mitarbeitenden Weisungen bezüglich Informationssicherheit zu erteilen.

§ 7 Verantwortung Mitarbeitende

1 Die Mitarbeitenden setzen die ihnen zur Verfügung gestellten ICT-Mittel recht- und zweckmässig ein und gehen mit den Informationen, insbesondere mit Personendaten und besonders schützenswerten Personendaten, mit der erforderlichen Vorsicht und unter Einhaltung der gesetzlichen Rahmenbedingungen um.

2 Die Mitarbeitenden stellen im Rahmen ihrer Möglichkeiten sicher, dass keine Unbefugten Zugriff / Zugang zu der Infrastruktur, den Informations- und Kommunikationsmitteln sowie den Daten der Gemeinde Birsfelden erhalten.

3 Der Verlust von Schlüsseln oder sonstigen Zugangsmitteln ist umgehend der Abteilung Bau, Verkehr & Umwelt (BVU) zu melden.

4 Besteht der Verdacht, dass Zugangsberechtigungen unberechtigt durch Drittpersonen genutzt werden, ist der IT-Partner, die ISV und die Geschäftsleitung umgehend zu informieren.

5 Der Arbeitsplatz in der Verwaltung sowie der externe Arbeitsplatz (Home Office) sind beim Verlassen so zu hinterlassen, dass keine vertraulichen oder schutzbedürftigen Unterlagen und Daten offen zugänglich sind (z. B. Sperren oder Herunterfahren des Systems, Abschliessen des Raumes, Verschliessen von Dokumenten und Datenträgern usw.).

6 Die Mitarbeitenden unterstützen den Schutz der Informationen mit einem entsprechenden Verhalten am Arbeitsplatz. Sie melden alle sicherheitsrelevanten Ereignisse (Probleme, Vorfälle, Mängel usw.) sowie Schäden und Verlust von Daten, Hardware und Software unmittelbar dem zuständigen externen IT-Partner und anschliessend der ISV.

7 Könnte der Vorfall zu einem Interessenkonflikt mit dem externen IT-Partner führen oder ist die Supportstelle nicht erreichbar, muss die Geschäftsleitung und der direkte Vorgesetzte unmittelbar informiert werden.

§ 8 Verantwortung der Supportstelle des IT-Partners

Der Support des externen IT-Partners ist Ansprechstelle für Fragen und für sicherheitsrelevante Vorkommnisse. Er rapportiert an den ISV, ergreift die notwendigen Massnahmen zur Behebung oder Minimierung des Schadens bei Vorfällen und koordiniert die Kommunikation an die Mitarbeitenden zusammen mit dem ISV. Die Supportstelle ist zu vereinbarten Zeiten erreichbar unter der Telefonnummer gemäss Supportkonzept.

C. BENÜTZUNG DER IT-INFRASTRUKTUR UND DER ICT-MITTEL

§ 9 Zugriffsschutz

1 Die Mitarbeitenden dürfen nur auf ihre persönlich zugeteilten Benutzerkonti mit den entsprechenden Zugriffsberechtigungen oder die ihnen zugeteilten funktionellen Konten zugreifen. Zugangsdaten dürfen nicht an andere weitergegeben werden.

2 Der Zugriff auf schützenswerte Informationen, die nicht zur Aufgabenerfüllung benötigt werden, ist soweit als möglich technisch zu verhindern und für die Mitarbeitenden verboten. Wird festgestellt, dass man Zugriff auf unautorisierte oder nicht notwendige Daten hat, ist dies der ISV zu melden.

3 Austretende haben unterschriftlich zu bestätigen, dass alle schützenswerten Informationen (insbesondere Personendaten), die ihnen zugänglich waren und die ausserhalb der Verwaltung bearbeitet oder gespeichert wurden, unwiderruflich gelöscht oder zurückgegeben wurden.

§ 10 Mobile Access – Fernzugriff

Ein Fernzugriff von ausserhalb ist nur über die vom IT-Partner definierten Übermittlungswege zulässig. Die festgelegten Sicherheitsmassnahmen müssen dabei eingehalten werden. Das Gerät darf während der Benützung des Fernzugriffes nicht durch Dritte verwendet werden.

§ 11 Passwörter

1 Passwörter sind persönlich und entsprechend vertraulich zu behandeln. Sie dürfen nicht aufgeschrieben, unverschlüsselt auf Systemen gespeichert oder anderen Personen bekannt gegeben werden. Die Passwörter müssen den Vorgaben der ISV entsprechen.

2 Passwörter sind sofort zu ändern, wenn ein Verdacht besteht, dass sie Dritten zur Kenntnis gelangt sind. Der Verdacht ist unmittelbar dem IT-Partner zu melden.

§ 12 Datensicherung sowie Entsorgung und Reparatur von Informationsträgern

Schützenswerte Informationen und Daten müssen ausschliesslich auf der dafür vorgesehenen Infrastruktur gespeichert werden. Defekte oder nicht mehr benötigte Datenträger und Geräte, die Informationen der Gemeinde enthalten oder einmal enthielten, sind der ISV zur Reparatur oder Vernichtung abzugeben.

§ 13 Virenschutz

Die Mitarbeitenden dürfen die Sicherheitssoftware (Virenschutz, Firewall, Verschlüsselung usw.) nicht ausschalten, blockieren oder umkonfigurieren. Nachrichten über verschiedene Kanäle (wie E-Mails, Anrufe, Chat usw.) mit zweifelhaftem Absender, verdächtigem Betreff oder unüblichem Inhalt sind äusserst kritisch zu beurteilen. Deren Beilagen oder Links dürfen keinesfalls geöffnet werden. Jeder Verdacht auf Virenbefall muss sofort dem Support des IT-Partner und der ISV gemeldet werden.

§ 14 Hardware und Systemeinstellungen

1 Die Nutzenden dürfen keine Software und keine Hardware-Erweiterungen, insbesondere keine Kommunikationseinrichtungen und externe Massenspeicher wie Harddisks etc. ohne Genehmigung der IT-Leitung installieren bzw. anschliessen. Externe Speichermedien für Datenübertragungen (bspw. Fotos, Präsentationen) sind erlaubt. Sollte ein externes Speichermedium benötigt werden, ist dieses bei der ISV zu beziehen. Die Daten auf dem Übertragungsmedium müssen nach dem Transfer gelöscht werden.

2 Die Nutzenden von mobilen Geräten sind für den sicheren Transport und die sichere Aufbewahrung verantwortlich (zum Beispiel zu Hause, im Auto und im ÖV).

3 Sie schützen die Geräte mit der erforderlichen Vorsicht vor Diebstahl, Verlust und Beschädigung. Mobile Arbeitsgeräte müssen mit einem Boot-Passwort, PIN oder biometrisch geschützt werden. Bei Nichtbenützung sind sie zeitnah zu sperren.

4 Bei der Nutzung eines Gerätes in der Öffentlichkeit und im privaten Umfeld ist auf angemessene Diskretion zu achten. Vertrauliche Dokumente sind ausser dem vor neugierigen Blicken zu schützen und sensible geschäftliche Telefongespräche mit dem Handy sind ausserhalb der Hörweite von Unbeteiligten zu führen.

5 Der Verlust eines geschäftlichen Gerätes mit Zugang zur Infrastruktur ist unverzüglich dem IT-Partner zu melden.

6 Änderungen an der Systemeinstellung (Installation, Deinstallation, Änderung der Konfiguration usw.) dürfen nur vom IT-Partner vorgenommen werden.

§ 15 E-Mail

1 E-Mails mit der Absenderadresse der Gemeinde (@birsfelden.ch) werden für die Erfüllung dienstlicher Aufgaben nach den Grundsätzen der Datensicherheit und des Datenschutzes eingesetzt und dürfen nicht für den privaten Gebrauch verwendet werden.

2 Bei der Nutzung von E-Mails für die Gemeindeverwaltung repräsentieren die Mitarbeitenden nicht nur sich selbst, sondern auch offiziell die Gemeinde. Daher ist bei dem Versand von Mails darauf zu achten, dass keine kompromittierenden, rufschädigenden Inhalte und Aussagen kommuniziert werden.

3 Der Versand von E-Mails an Externe mit schützenswertem Inhalt erfolgt verschlüsselt über die bereitgestellte E-Mail-Plattform.

4 Das automatische Weiterleiten von geschäftlichen E-Mails an eine private Mailadresse und das Freigeben der persönlichen Mailbox an eine Drittperson ausserhalb der Verwaltung sind nicht erlaubt.

§ 16 Internet

1 Bei der Benützung des Internets sind Warnhinweise des Browsers oder des Virenschutzes über Malware (Viren und andere Schadprogramme) stets zu beachten und unverzüglich dem Support des IT-Partners zu melden. Die installierten Sicherheitsvorkehrungen (Proxy-Einstellungen, Virenschutzprogramme etc.) dürfen nicht umgangen oder deaktiviert werden.

2 Die Mitarbeitenden dürfen nicht zwei Verbindungen ins Internet gleichzeitig aktiviert haben (z. B. Gemeindenetzwerk und Hotspot).

§ 17 Soziale Netzwerke

Die private Nutzung von sozialen Netzen bzw. die Pflege des darin befindlichen persönlichen Profils über die ICT-Mittel der Gemeinde wird ausserhalb der Arbeitszeit toleriert.

§ 18 Richtlinie betreffend Künstliche Intelligenz (KI)

1 Die Eingabe und Nutzung von vertraulichen Informationen und Daten sind bei der Anwendung generativer KI-Systeme oder öffentlicher Software (bspw. Browser, Suchmaschinen, Übersetzungstools) nicht erlaubt.

2 Die Zuverlässigkeit, Qualität und Objektivität des Outputs müssen stets hinterfragt werden.

3 Generell ist bei von KI generiertem Output Vorsicht geboten. Der Output stellt unter Umständen eine Urheberrechtsverletzung dar (Bspw. Textbausteine, Bilder oder Begriffe).

§ 19 Verwendung der eigenen ICT-Mittel

1 Die geschäftliche Nutzung von privaten Geräten („bring your own device“) ist unter Einhaltung folgender Bedingungen gestattet:

a) Keine Speicherung von geschäftlichen Daten auf dem Gerät (Ausnahme: Outlook, Mail)
b) Verschlüsselte Festplatte
c) Betriebssystem auf aktuellem Stand mit den aktuellen Sicherheitsupdates
d) Sichereres Benutzerpasswort gemäss interner Weisung
e) Sicherstellung, dass andere Personen keinen Zugriff haben (LebenspartnerIn, Kinder usw.)

2 Im Falle des Verlustes eines privaten Geräts mit Zugang zu Daten der Gemeindeverwaltung ist sicherzustellen, dass die Zugangsdaten / Passwörter für den Mitarbeitendenaccount und die Systeme geändert werden. Bei Unklarheiten ist der IT-Partner zur Unterstützung zu kontaktieren.

§ 20 Drucker

Ausdrucke mit vertraulichen Informationen sind umgehend aus dem Drucker zu entfernen. Ausdrucke im privaten Umfeld sind angemessen zu schützen und bei Nichtgebrauch sicher zu vernichten.

§ 21 Home Office

Bei der Arbeit im Home-Office sind die Bestimmungen der Verordnung "Arbeiten im Home-Office" ergänzend anzuwenden.

D. ÜBERWACHUNG UND SANKTIONEN

§ 22 Überwachung und Sanktionen

1 Zur Überwachung des richtigen Funktionierens, der Sicherheit, der Integrität und der Verfügbarkeit der Informatik werden Systeme eingesetzt, die Protokolle, Auswertungen und Warnmeldungen erzeugt, welche z. T. auch Rückschlüsse auf Personen zulassen können. Es werden keine personenbezogenen Nutzungsprofile erstellt.

2 Internetzugriffe werden aufgezeichnet und ein halbes Jahr gespeichert. Eine personenbezogene Auswertung der Internetverwendung ist bei begründetem Verdacht nur nach vorgängiger Information des Nutzenden möglich. Ausgenommen sind rechtswidrige, bzw. strafbare Handlungen.

3 Zuwiderhandlungen gegen die vorliegende Verordnung können gemäss den Anstellungsbedingungen von einer Verwarnung bis zur Auflösung des Arbeitsverhältnisses sanktioniert werden.

E. AUSNAHMEN

§ 23 Ausnahmen

1 Die ISV ist für die Entscheidung über Ausnahmen von dieser Verordnung zuständig. Anträge für solche Ausnahmen sind schriftlich vorzulegen und müssen mit einer angemessenen Begründung versehen sein.

2 Eine Übersicht der beantragten, gewährten und abgelehnten Ausnahmen ist (inklusive Begründung) der Geschäftsleitung jeweils Ende Semester vorzulegen.

F. INKRAFTTRETEN

§ 24 Inkrafttreten

Die ICT-Verordnung vom 19. Dezember 2023 tritt am 1. Januar 2024 in Kraft.

Birsfelden, 19. Dezember 2023, GRB Nr. 2023-638

GEMEINDERAT BIRSFELDEN

Ch. Hiltmann
Gemeindepräsident

M. Schürmann
Leiter Gemeindeverwaltung

Anhang 1

Schutzziele (§ 4 Abs. 1)

Vertraulichkeit:	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen und nur durch Berechtigte bearbeitet werden.
Integrität:	Informationen müssen richtig und vollständig sein.
Authentizität:	Informationsbearbeitungen müssen einer Person zugerechnet werden können.
Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein.

Klassifizierung der Vertraulichkeit (§ 4 Abs. 2)

Streng vertraulich

Streng vertrauliche Personendaten stellen, wenn sie nicht ausreichend vor unbefugter Verarbeitung geschützt sind, ein erhebliches Risiko für die betroffenen Personen dar.

Bei Informationen ohne Personenbezug betreffen die Risiken das öffentliche Organ. Ebenfalls streng vertraulich werden in der Regel die Informationen klassifiziert, für welche andere spezielle gesetzliche Geheimhaltungspflichten bestehen wie z.B. das Sozialversicherungsgeheimnis, das Sozialhilfegeheimnis, das Steuergeheimnis, die Daten zur Opferhilfe oder das Stimmgeheimnis.

Vertraulich

Vertrauliche Informationen sind von Gesetzes wegen oder aufgrund von geschäftlichen oder strategischen Anforderungen vor unrechtmässiger oder missbräuchlicher Datenbearbeitung zu schützen. Bei der unrechtmässigen Bearbeitung von vertraulichen Personendaten besteht die Gefahr von erheblichen negativen Folgen für die betroffene Person.

Intern

Als „intern“ werden Informationen klassifiziert, die weder als „streng vertraulich“ noch als „vertraulich“ klassifiziert werden müssen, deren Inhalt jedoch aufgrund schutzwürdiger Interessen nicht für die Veröffentlichung bestimmt oder geeignet ist.

Nicht klassifiziert

Als „nicht klassifiziert“ gelten Informationen, die weder intern, noch vertraulich, noch streng vertraulich klassifiziert sind. Es handelt sich demnach um öffentliche Informationen wie sie zum Beispiel auf der Website, in der Presse oder in Broschüren publiziert werden.