EMBRACH
GEMEINDERAT

Reglement zur Informationssicherheit und den Datenschutz (RID)

Genehmigt GRB 119/15.06.2026
Inkraftsetzung: 01.07.2026

Gemeinde Embrach | Gemeinderat | Dorfstrasse 9 | 8424 Embrach
Telefon 044 866 36 19 | gemeinde@embrach.ch | www.embrach.ch

Inhaltsverzeichnis

I. Allgemeine Bestimmungen

Art. 1. Rechtsgrundlage

Die Grundlage dieses Reglements bildet § 7 des Gesetzes über die Information und den Datenschutz (IDG, LS 170.4) sowie die weiteren anwendbaren gesetzlichen Bestimmungen.

Art. 2. Geltungsbereich

[1] Dieses Reglement sowie die damit zusammenhängenden Dokumente gelten für sämtliche Mitarbeitenden der Gemeinde Embrach, für Behörden- und Kommissionsmitglieder sowie für Mitarbeitende der Primarschule, die im Netzwerk der Gemeinde Embrach registriert sind[1].

[2] Vertragspartnerinnen und Vertragspartner, die im Auftrag der Gemeinde Embrach Daten bearbeiten, werden vertraglich zur Einhaltung der in diesem Reglement festgelegten Anforderungen verpflichtet.

Art. 3. Ziel des Reglements

Dieses Reglement bezweckt:

a. die Sicherstellung eines angemessenen Schutzniveaus für Informationen und Informationssysteme der Gemeinde Embrach

b. die Festlegung von Grundsätzen, Zuständigkeiten und Verantwortlichkeiten im Bereich der Informations- und Kommunikationstechnologie sowie der Informationssicherheit

c. die Unterstützung einer rechtskonformen, effizienten und sicheren Aufgabenerfüllung der Gemeinde Embrach

d. die Sensibilisierung der Mitarbeitenden für den sorgfältigen und verantwortungsvollen Umgang mit Informationen und Informations- und Kommunikationstechnologie (IKT)-Systemen

Art. 4. Ausnahmen

[1] Der Gemeinderat entscheidet über Ausnahmen von diesem Reglement. Die Geschäftsführung entscheidet über Ausnahmen von den von ihr erlassenen internen Weisungen und Richtlinien.

[2] Gesuche um Ausnahmen sind unter Angabe einer Begründung per E-Mail einzureichen und aus Gründen der Nachvollziehbarkeit zu dokumentieren.

[3] Für jede Ausnahme sind der Zeitpunkt, die Dauer sowie die antragstellende und die verantwortliche Person festzulegen.

[4] Bestehende Ausnahmen sind periodisch zu überprüfen.

[1] Schulverwaltung, Schulleitung, Schulpsychologie

II. Organisation und Verantwortlichkeit

Art. 5. Gemeinderat

Der Gemeinderat trägt die Gesamtverantwortung für die Informationssicherheit und den Datenschutz der Gemeinde. Er genehmigt die für die Informationssicherheit erforderlichen Massnahmen sowie die dafür notwendigen Mittel im Rahmen des Budgets.

Art. 6. Geschäftsführung

[1] Die Geschäftsführung trägt im Rahmen der operativen Gesamtverantwortung die Verantwortung für die Informations- und Kommunikationstechnologie und bildet die Verantwortliche Stelle für den Datenschutz

[2] Sie stellt die Umsetzung der Beschlüsse des Gemeinderates im Bereich der Informationssicherheit sicher.

[3] Sie erlässt insbesondere folgende internen Weisungen:

a. interne Weisung zur Informationssicherheit und zum Datenschutz

b. interne Weisung für den technischen Betrieb von Informationssystemen sowie zur Massnahmenplanung und -umsetzung

[4] In ihrer Funktion als verantwortliche Stelle für den Datenschutz ist die Geschäftsführung insbesondere verpflichtet:

a. als Ansprechstelle für alle Personen gemäss Art. 2 dieses Reglements in Belangen des Datenschutzes zu fungieren

b. den Austausch mit der kantonalen Datenschutzbeauftragten (DSB) bei datenschutzrechtlichen Fragestellungen sicherzustellen

c. die Einhaltung der gesetzlichen Meldepflichten bei Datenschutzvorfällen sicherzustellen

d. als Ansprechstelle für betroffene Personen, insbesondere bei Auskunfts- und Löschbegehren, zu handeln

e. Sensibilisierungs- und Schulungsmassnahmen zum Thema Datenschutz zu planen, zu koordinieren und umzusetzen

Art. 7. Abteilungsleitende (AL)

[1] Die Abteilungsleitenden bilden die Schnittstelle zwischen der Geschäftsführung und den Mitarbeitenden und verfügen in ihrem jeweiligen Fachbereich über spezialisiertes Wissen, insbesondere in datenschutzrelevanten Belangen.

[2] Sie nehmen in ihrem Zuständigkeitsbereich insbesondere folgende Aufgaben wahr:

a. Funktion als Ansprechperson für die Mitarbeitenden in Fragen des Datenschutzes

b. Wahrnehmung der Schnittstellenfunktion zur Geschäftsführung

c. Sicherstellung der Vermittlung des spezialisierten Wissens zu datenschutzrelevanten Vorschriften an die Mitarbeitenden

d. Information des Teams über allfällige Datenschutzvorfälle sowie über erforderliche Vorsichtsmassnahmen

e. Klassifizierung der in der jeweiligen Abteilung bearbeiteten Daten nach Vertraulichkeit, Integrität und Verfügbarkeit

f. Kontrolle der Einhaltung der geltenden Datenschutzbestimmungen

g. Mitarbeit bei der Erstellung und Pflege von Notfallplänen für längere Ausfälle

Art. 8. Bereichsleitung ICT

Die Bereichsleitung ICT ist die verantwortliche Stelle für die Informationssicherheit (ISV).

[1] Sie ist für die Umsetzung der Informationssicherheitsziele sowie für die Überwachung der Einhaltung des angestrebten Sicherheitsniveaus verantwortlich.

[2] Sie erstellt die erforderliche Betriebs- und Systemdokumentation und führt diese laufend nach.

[3] Für die Erfüllung ihrer bzw. seiner Aufgaben werden der ISV angemessene zeitliche und finanzielle Ressourcen zur Verfügung gestellt. Die Geschäftsführung, die Abteilungsleitenden, die Power-User sowie alle Mitarbeiterinnen und Mitarbeiter haben die ISV bei der Wahrnehmung ihrer Aufgaben zu unterstützen.

[4] Sie ist in sämtliche Projekte mit sicherheitsrelevanten Auswirkungen frühzeitig einzubeziehen, damit die sicherheitsrelevanten Aspekte angemessen berücksichtigt werden können.

[5] In sicherheitsrelevanten Fragestellungen ist die ISV weisungsberechtigt. Sie ist zentrale Anlaufstelle für Fragen der Informationssicherheit sowie für Hinweise auf Schwachstellen und verfügt über die hierfür erforderlichen fachlichen Kenntnisse und Fähigkeiten.

[6] Die ISV nimmt insbesondere folgende Aufgaben wahr:

a. Betreuung der IKT-Umgebung der Gemeinde sowie Funktion als Schnittstelle zu externen Betreibern

b. Führen und Nachführen des IKT-Inventars c. Verwaltung der Domainnamen der Gemeinde, insbesondere die fristgerechte Verlängerung der Registrierungen

c. Verwaltung der digitalen Zertifikate, soweit vorhanden, einschliesslich der Überwachung der Gültigkeitsdauer

d. Anpassen, Überprüfen und Weiterentwickeln der Sicherheitsvorgaben

e. Kontrolle des Fortschritts der Umsetzung der in ihrem bzw. seinem Verantwortungsbereich liegenden Informationssicherheitsmassnahmen

f. Periodische Information der Geschäftsführung über den Stand der Informationssicherheit

g. Erteilung verbindlicher Anordnungen zur Abwehr unmittelbar drohender Gefahren im Zusammenhang mit Informationssicherheitsvorfällen

h. Austausch mit internen und externen Stellen über Informationssicherheitsvorfälle unter Wahrung der Informationsklassifizierung und der Vertraulichkeit

i. Beratung der Geschäftsführung sowie der Mitarbeitenden in Fragen der Informationssicherheit

j. Umsetzung, Pflege und Weiterentwicklung des übergreifenden Rollen- und Berechtigungskonzepts

k. Planung, Koordination und Umsetzung von Sensibilisierungs- und Schulungsmassnahmen im Bereich der Informationssicherheit

Art. 9. Anwendungsverantwortliche Stelle (Power – User)

[1] Für alle Daten und Anwendungen wird im Dokument «Organisation ICT / Prozesslandkarte» durch die Geschäftsleitung eine verantwortliche Person (Power-User) bestimmt.

[2] Die Power-User sind in ihren Zuständigkeitsbereichen insbesondere verantwortlich für:

a. die Vergabe und Verwaltung von Berechtigungen

b. die Sicherstellung, dass der Zugriff auf Informationssysteme zur Nutzung, Administration, Wartung und zu weiteren Zwecken ausschliesslich durch berechtigte Personen erfolgt

c. den sicheren Betrieb der verantworteten Anwendungen, insbesondere hinsichtlich der Vertraulichkeit und Integrität der Datensammlungen sowie der Verfügbarkeit der Anwendungen und Daten

d. die Funktion als Informations- und Anlaufstelle für die in ihrem bzw. seinem Verantwortungsbereich liegenden Anwendungen und Datensammlungen

e. die ordnungsgemässe Bearbeitung einschliesslich Bekanntgabe und Weitergabe, Aufbewahrung, Archivierung oder Vernichtung der in ihrem bzw. seinem Verantwortungsbereich liegenden Daten

f. die Schulung der betroffenen Mitarbeitenden

g. die Funktion als erste Ansprechperson bei Störungen sowie bei Anfragen der Mitarbeitenden

Art. 10. Mitarbeitende

[1] Die Mitarbeitenden nehmen ihre Verantwortung durch korrektes, sorgfältiges Handeln sowie im Kontakt mit betroffenen Personen wahr und tragen damit zur Sicherstellung des Datenschutzes und der Informationssicherheit bei.

[2] Sie sind insbesondere verpflichtet:

a. an Sensibilisierungs- und Schulungsaktivitäten teilzunehmen und das erforderliche Verständnis sicherzustellen

b. die einschlägigen gesetzlichen Bestimmungen, vertraglichen Regelungen sowie internen Weisungen einzuhalten und sich bei Unsicherheiten selbständig zu informieren

c. die Sicherheitsmassnahmen durch eine sicherheitsbewusste Arbeitsweise aktiv zu unterstützen

d. ein angemessenes Risikobewusstsein aufrechtzuerhalten und bei Unsicherheiten Rückfragen zu stellen

e. Informationssicherheitsvorfälle sowie Hinweise auf Schwachstellen unverzüglich der für die Informationssicherheit verantwortlichen Person, der anwendungs- oder datenverantwortlichen Stelle oder der Abteilungsleiterin bzw. dem Abteilungsleiter zu melden

III. Informationssicherheit

Art. 11. Schutzbedarfsanalyse

[1] Für alle Informationen und Informationssysteme ist eine Schutzbedarfsanalyse durchzuführen.

[2] Die Schutzbedarfsanalyse hat systematisch zu erfolgen und dient der Ermittlung des Sicherheitsbedarfs, der Identifikation und Bewertung potenzieller Risiken sowie der Festlegung angemessener Sicherheitsmassnahmen.

[3] Auf Grundlage der Schutzbedarfsanalyse ist ein angemessenes Sicherheitsniveau sicherzustellen und die Informationssicherheit kontinuierlich zu verbessern.

Art. 11.1. Durchführung der Schutzbedarfsanalyse

[1] Kategorisierung der Informationen
Informationen sind nach ihrer Bedeutung für die Gemeinde sowie nach dem potenziellen Schaden bei Verlust, Manipulation oder unbefugtem Zugriff zu klassifizieren. Die Klassifizierung hat mindestens in die Schutzbedarfskategorien „normal“, „hoch“ oder „sehr hoch“ zu erfolgen.

[2] Bewertung der Schutzbedarfsfaktoren
Die Schutzbedarfsanalyse hat die Ziele der Informationssicherheit gemäss Art. 12 zu berücksichtigen. Die Schutzbedarfsfaktoren Vertraulichkeit, Integrität und Verfügbarkeit sind getrennt zu beurteilen, da sie unterschiedliche Sicherheitsanforderungen nach sich ziehen.

[3] Festlegung von Sicherheitsmassnahmen
Gestützt auf die Ergebnisse der Schutzbedarfsanalyse sind geeignete technische, organisatorische und personelle Sicherheitsmassnahmen festzulegen und umzusetzen, um den festgestellten Schutzbedarf angemessen abzudecken.

Art. 12. Ziele der Informationssicherheit

[1] Integrität	Informationen müssen richtig und vollständig sein.
[2] Nachvollziehbarkeit	Veränderungen von Informationen müssen erkennbar und nachvollziehbar sein
[3] Verantwortung	Die politischen Behörden und die Mitarbeitenden der Gemeinde sind sich ihrer Verantwortung beim Umgang mit Informationen, IKT-Systemen und Anwendungen bewusst. Sie unterstützen die Informationssicherheitsziele.
[4] Verfügbarkeit	Informationen müssen bei Bedarf vorhanden sein. Die Ausfallzeiten dürfen keine wesentlichen Auswirkungen auf den Verwaltungsbetrieb haben.
[5] Vertraulichkeit	Informationen dürfen nicht unrechtmässig zur Kenntnis gelangen.
[6] Zurechenbarkeit	Informationsbearbeitungen müssen einer Person zugerechnet werden können.

Art. 13. Massnahmen zu den Zielen der Informationssicherheit
[1] Die Auswahl und Ausgestaltung der technischen, organisatorischen und personellen Massnahmen hat sich an den Anforderungen der Norm ISO/IEC 27001 zu orientieren.

[2] Die Geschäftsführung hat dem Gemeinderat jährlich einen Bericht über den Stand der Umsetzung der Massnahmen zur Informationssicherheit zu unterbreiten.

IV. Controlling, Überprüfung und Weiterentwicklung

Art. 14. Controlling
Die Geschäftsführung wird beauftragt, ein systematisches und periodisches Risikomanagement einzuführen und sicherzustellen, dass sicherheitsrelevante Entscheidungen nachvollziehbar, verhältnismässig und unter Berücksichtigung der aktuellen Bedrohungslage getroffen werden.

Art. 15. Protokollierung
Aktivitäten der Benutzerinnen und Benutzer auf den IKT-Systemen der [Gemeinde/Stadt] können zur Gewährleistung der Nachvollziehbarkeit sowie zur Überwachung der Funktionstüchtigkeit, der Sicherheit, der Integrität und der Verfügbarkeit aufgezeichnet werden.

Eine personenbezogene Auswertung erfolgt nur nach vorgängiger Information der betroffenen Benutzerin oder des betroffenen Benutzers.

Art. 16. Periodische Überarbeitung dieses Reglements

Der Gemeinderat legt mit der periodischen Überarbeitung dieses Reglements die verbindlichen Leitplanken für eine sichere und gesetzeskonforme Informationsverarbeitung fest. Das Reglement ist mindestens alle drei Jahre zu überprüfen.

V. Schlussbestimmungen

Art. 17. Inkraftsetzung

Dieses Reglement tritt per 1. Juli 2026 in Kraft

Anhang 1
Informationssicherheitsmassnahmen

Anforderung	Beschreibung
Zuständig: **Verantwortliche Stelle für die Informations- und Kommunikationstechnologie (VIKT)**	
Archivierung / Löschung	Alle Daten werden gemäss den regulatorischen Vorgaben archiviert. Falls eine Aufbewahrung nicht mehr erforderlich ist, werden diese sicher gelöscht.
Organisation	Die relevanten Funktionen der Organisation sind festgelegt und im Organisations- und Verwaltungsreglement (OVR) dokumentiert. Für alle Funktionen ist die Stellvertretung geregelt. Durch ausreichende Dokumentation und Instruktion wird sichergestellt, dass die Stellvertretenden ihre Aufgabe erfüllen können.
Risikomanagement	Die Gemeinde erkennt, bewertet und steuert Risiken für ihre Informationen und Systeme systematisch.
Verschlüsselung	Die Datenübertragung von Informationen, die aufgrund ihres Missbrauchspotenzials und der damit zusammenhängenden Risiken einen erhöhten Schutz benötigen, beispielsweise besondere Personendaten, erfolgt verschlüsselt über öffentliche Netze.
Weisungen	Die Mitarbeiterinnen und Mitarbeiter werden geschult, die Gesetze sowie die vertraglichen Regelungen und internen Weisungen und Richtlinien umzusetzen. Sie unterstützen durch eine sicherheitsbewusste Arbeitsweise die Sicherheitsmassnahmen. Informationssicherheitsfragen und Hinweise auf Schwachstellen werden an die für die Informationssicherheit verantwortliche Person gerichtet.
Zuständig: **Verantwortliche Stelle für den Datenschutz (VSD)**	
Aktualisierungen (Updates)	Alle IKT-Systeme (Server, Clients und Netzwerkkomponenten) werden regelmässig aktualisiert und mit den aktuellen Sicherheitsupdates versorgt.
Berechtigungskonzept	Der Zugriff auf die Informationen ist durch ein Berechtigungskonzept geregelt. Die Zugriffsberechtigungen der Behördenmitglieder, der Mitarbeitenden sowie der Lernenden auf Systeme und Netzwerke sind für die Erfüllung der Aufgaben erforderlich und

	geeignet.
Datenschutz	Alle Daten werden gemäss den datenschutzrechtlichen Vorgaben bearbeitet. Es existieren Prozesse, um die Rechte der betroffenen Personen auf Auskunft, Berichtigung, Sperrung, Löschung sowie Einsicht sicherzustellen.
Zuständig: **Abteilungsleiter Finanzen, Steuern + ICT (Vorgesetzte Steller der ISV)**	
Datensicherung (Backup)	Die Datensicherung wird regelmässig durchgeführt. Die Sicherungsmedien werden an getrennten Orten aufbewahrt und sind physisch geschützt. Es wird gewährleistet, dass verlorene oder fehlerhafte Teile des Informationsbestands über eine ausreichende Dauer wiederhergestellt werden können.
IKT-Systeme	Die IKT-Systeme werden nach der Beschaffung sicher installiert (gemäss anerkannten Sicherheitsstandards) und betrieben, mittels eines Änderungsmanagements verwaltet und in einem geregelten Prozess ausser Betrieb genommen.
Mobile Geräte / Software	Der Einsatz von Arbeitsplatzrechnern und mobilen Geräten inklusive der Verwendung von privaten Geräten (Bring Your Own Device) sowie der Installation von Software auf Arbeitsplatzrechnern und Servern sind im Detail geregelt. Für Daten mit erhöhtem Risiko auf Missbrauch werden die entsprechenden technischen und organisatorischen Massnahmen ergriffen.
Nachvollziehbarkeit	Es ist sicherzustellen, dass sämtliche Veränderungen von Informationen eindeutig erkennbar, zeitlich zuordenbar und für berechtigte Stellen jederzeit nachvollziehbar dokumentiert sind.
Netzwerk / Firewall	Alle Netzwerkzugänge werden gesichert. Schutzmechanismen werden so konfiguriert und administriert, dass sie einen wirkungsvollen Schutz gewährleisten und Manipulationen verhindern. Die vom Kanton vorgegebene Network Security Policy der übergeordneten Netzwerke (Leunet) wird eingehalten.
Outsourcing	Bei der Auslagerung von Datenbearbeitungen werden der Datenschutz und die Informationssicherheit gewährleistet, indem schriftliche Verträge abgeschlossen und entsprechende Kontrollmassnahmen vereinbart

	werden.
Passwörter	Die Zugänge zu allen Systemen, Daten und Anwendungen sind durch mitarbeiterabhängige Passwörter gesichert. Es wird eine ausreichende Qualität der Passwörter sichergestellt.
Physische Sicherheit	Gebäude und Räume mit IKT- und Netzwerksystemen werden angemessen vor physischen Risiken geschützt (Brandschutzmassnahmen, Klimatisierung, etc.).
„Security by Design“ und „Privacy by Design“	Sicherheit und Datenschutz werden von Beginn an in Prozesse und Systeme integriert.
Sensibilisierung / Schulung	Die Mitarbeiterinnen und Mitarbeiter nehmen mindestens jährlich an einer internen Sicherheitsschulung der für die Informationssicherheitsverantwortlichen Stelle teil. Sie werden regelmässig über aktuelle Gefahren und zu treffende Massnahmen informiert.
Virenschutz / Internet	Virenschutzprogramme werden auf allen IKT-Systemen eingesetzt. Durch entsprechende Massnahmen wird sichergestellt, dass die Risiken der Internetnutzung möglichst gering bleiben.
Zutritt	Gebäude und Räume sowie IKT- und Netzwerksysteme werden durch ein ausreichendes Schliesssystem und weitere Massnahmen für die physische Sicherheit angemessen geschützt.