kommunit
IT-Zweckverband Schleswig-Holstein

# Satzung
# zum kommunit Datenschutz

Aufgrund des § 5 Abs. 6 des Gesetzes über kommunale Zusammenarbeit (GkZ) in der Fassung vom 28.02.2003, zuletzt geändert durch Ges.v.21.06.2016, GVOBl. S. 528 i.V.m. § 4 der Gemeindeordnung für Schleswig-Holstein (Gemeindeordnung- GO) in der Fassung vom 28.02.2003, zuletzt geändert durch Ges. v. 04.01.2018, GVOBl. S.6, wird nach Beschluss der Verbandsversammlung vom 10. Februar 2020 folgende Satzung zum kommunit Datenschutz erlassen:

## § 1 Gegenstand

(1) Zwischen den einzelnen Verbandsmitgliedern und kommunit besteht eine gemeinsame Verantwortung im Sinne des Art. 26 i.V.m. Art. 4 Nr. 7 DSGVO. Diese Satzung regelt die datenschutzrechtlichen Aufgaben, Rechte und Pflichten des Verbandsmitgliedes und kommunit bei der Zusammenarbeit hinsichtlich der Verarbeitung von personenbezogenen Daten (Daten). Dies umfasst insbesondere die Konkretisierung, wer die Rechte der betroffenen Personen wahrnimmt, wer die Sicherheit der Datenverarbeitung gewährleistet und wer welchen Informationspflichten gemäß den Artikeln 13 und 14 DSGVO nachkommt.

(2) Im Bewusstsein der gemeinsamen Verantwortung und dem Ziel eines einheitlich hohen Datenschutzniveaus im IT-Zweckverband kommunit erfolgt eine darüberhinausgehende und in dieser Satzung geregelte datenschutzrechtlich enge Zusammenarbeit und die Etablierung eines gemeinsamen und übergreifenden Datenschutzmanagements. Ziel ist eine enge und zentralisierte Zusammenarbeit unter ein einheitliches Datenschutzkonzept.

## § 2 Zweck, Mittel und Umfang der gemeinsamen Datenverarbeitung

(1) Der Gegenstand, der Zweck, die Mittel sowie der Umfang der Datenverarbeitung ergeben sich aus der Verbandssatzung und den jeweiligen öffentlich-rechtlichen Verträgen sowie aus der Erfüllung der Aufgaben der Verbandsmitglieder und des IT-Zweckverbandes kommunit kraft öffentlichen Rechts.

(2) Die Verantwortung für die Ordnungsmäßigkeit der IT-Infrastruktur ist nach § 4 der Verbandssatzung auf kommunit übergegangen. Die Verantwortung für die Datenverarbeitung im Rahmen der Erfüllung ihrer Aufgaben (inhaltliche Datenverarbeitung) verbleibt beim jeweiligen Verbandsmitglied. Die Aufteilung der Verantwortlichkeiten und Einhaltung gesetzlicher Vorgaben folgt dem Aufgabenbereich. Ist die Datenverarbeitung dem satzungsgemäß übertragenen IT-Bereich zuzuordnen, liegt die Verantwortung bei kommunit. Im Übrigen liegt die Verantwortung bei den jeweiligen Verbandsmitgliedern.

(3) Eine Zuordnung von Verantwortlichkeiten ist in der Anlage 1 vorgenommen worden, die Bestandteil der Satzung ist.

(4) kommunit verarbeitet Daten der Beschäftigten der Verbandsmitglieder im Rahmen der Aufgabenwahrnehmung (z.B. Service Desk, Vor-Ort Service, IT-Support). Hierbei handelt es sich um den Namen und die dienstlichen Kontaktdaten der Beschäftigten und Informationen, die im Rahmen der Aufgabenwahrnehmung anfallen (u.a. Büronummer, Grund der Unterstützung (Ticket), Angaben zur IT-Ausstattung). Zudem besteht die Möglichkeit des Zugriffs auf Daten in den Verfahren der Verbandsmitglieder:

   a. Servicedesk: Es besteht die Notwendigkeit, dass im Zuge von Supportanfragen ein Zugriff seitens des Servicedesk auf die Daten des Verfahrens erfolgen kann, wenn zum Beispiel ein Zugriff über die Fernwartung auf den Desktop des Bearbeitenden stattfindet.

   b. Administratoren der Anwendungen: Es besteht die Notwendigkeit, dass im Zuge von Wartungs- und Supporttätigkeiten ein Zugriff seitens der Administratoren auf Inhalte der Datenbestände des jeweiligen Verfahrens erfolgen kann.

   c. In Zuge von Wiederherstellungen und anlassbezogen Löschungen in Datenbanken ist ein Zugriff auf die Daten in den bei kommunit hinterlegten Backups erforderlich.

(5) Die einzelnen Arten der personenbezogenen Daten, sowie die Kategorien der betroffenen Personen werden in dem jeweiligen Verzeichnis von Verarbeitungstätigkeiten entsprechend Art. 30 DSGVO dokumentiert.

(6) Es wird von den Parteien dafür Sorge getragen, dass innerhalb der gemeinsamen Verantwortung nur personenbezogene Daten erhoben werden, die für die rechtmäßige Aufgabenwahrnehmung zwingend erforderlich sind und für die die Zwecke und Mittel der Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben sind. Im Übrigen beachten die Vertragsparteien den Grundsatz der Datenminimierung im Sinne von Art. 5 Abs. 1 c DSGVO.

(7) Die Rechte der betroffenen Personen werden gewährleistet. Anlaufstelle für die betroffenen Personen ist das jeweilige Verbandsmitglied, bei welcher die inhaltliche Datenverarbeitung stattfindet. Wendet sich die betroffene Person an kommunit, besteht aber keine direkte Beziehung zu kommunit, erhält sie unverzüglich die Kontaktdaten des zuständigen Verbandsmitgliedes und wird an jenes verwiesen. Die Regelung des Art. 26 Abs. 3 DSGVO bleibt davon unberührt.

(8) Die Informationspflichten nach Art. 13 und 14 DSGVO sowie Ersuche entsprechend Kapitel III DSGVO nimmt das jeweilige Verbandsmitglied, bei welchem die inhaltliche Datenverarbeitung stattfindet, wahr.

(9) Bei der Gewährleistung der Rechte der betroffenen Personen unterstützt kommunit das jeweilige Verbandsmitglied. Dies gilt insbesondere bei der Einhaltung möglicher Fristen. kommunit wird das Verbandsmitglied im Rahmen seiner Informationspflicht gegenüber der betroffenen Person unterstützen und ihm in diesem Zusammenhang sämtliche relevanten Informationen zur Verfügung stellen.

## § 3 Datenschutzorganisation

(1) Zur Umsetzung der gemeinsamen Verantwortung und zur Gewährleistung eines einheitlich hohen Datenschutzstandards und der Datensicherheit innerhalb des IT-Zweckverbandes und ihrer Verbandsmitglieder wird eine enge Zusammenarbeit und der Aufbau einer zentralen Datenschutzorganisation implementiert. Die zentrale Datenschutzorganisation wird in einem Datenschutzkonzept umgesetzt.

a. Ausgehend von der gemeinsamen Verantwortung, soll das zentrale Datenschutzkonzept verbandsweit einen angemessenen Rahmen vorgeben. Aufbauend auf dem Konzept können die Verbandsmitglieder unter Beachtung der lokal rechtlichen Gegebenheiten in die jeweilige Struktur Konzeptbestandteile anpassen und bei sich einführen.

b. Ein verbandsweites zentrales Datenschutzmanagementsystem soll gewährleisten, dass die Aufbau- und Ablauforganisation hinsichtlich des Datenschutzes klar geregelt ist, dass der Datenschutz in alle relevanten Geschäftsprozesse integriert wird, Verantwortlichkeiten geregelt sind und die verlässliche Implementierung von Prozessen und Verfahren gewährleistet wird.

c. Soweit dies Gewährleistung eines einheitlich hohen Datenschutzstandards und der Datensicherheit im unmittelbaren Bezug zur gemeinsamen Verarbeitung dient, kann das Konzept unter Umständen auch Einfluss auf Bereiche und Aufgaben haben, die nicht an den IT-Zweckverband übertragen wurden.

(2) Die Zusammenarbeit und Abstimmung zu allen wichtigen verbandsweiten Fragen des Datenschutzes, die Einfluss auf der gemeinsamen Verantwortung und den damit betroffenen personenbezogenen Daten haben, erfolgt über einen zentralen Datenschutzbeauftragten bei kommunit.

(3) Die Verbandsmitglieder bestellen einen Datenschutzbeauftragten. Die Datenschutzbeauftragten und der zentrale Datenschutzbeauftragte werden eng zusammenarbeiten.

## § 4 Verfahrensbeauftragte

(1) Die Parteien bestellen für eigene Verarbeitungstätigkeiten, die personenbezogenen Daten betreffen, jeweils einen Verfahrensbeauftragter. Die Bestellung hat grundsätzlich vor der Einführung einer Verarbeitung zu erfolgen.

(2) Bei gleichen Verfahren können die Verfahrensbeauftragten eng zusammenarbeiten.

(3) Die Bestellung des Verfahrensbeauftragten bei den Verbandsmitgliedern ist kommunit zur Kenntnis zu geben.

## § 5 Verarbeitungsverzeichnis

(1) Die jeweiligen Verzeichnisse der Verarbeitungstätigkeiten gemäß Art. 30 DSGVO werden jeweils von den Parteien erstellt und stets aktualisiert.

(2) Die Verbandsmitglieder und kommunit werden sich bei der Dokumentation der Verarbeitungstätigkeiten unterstützen und streben eine zentrale und einheitliche Dokumentation an. Sie werden insbesondere bei ähnlichen Verfahren den gegenseitigen Austausch suchen.

## § 6 Datensicherheit

(1) Die innerbetriebliche Organisation wird im eigenen Verantwortungsbereich so gestaltet, dass sie den besonderen Anforderungen des Datenschutzes gerecht wird. Es werden technische und organisatorische Maßnahmen zur angemessenen Sicherung der Daten hinsichtlich Vertraulichkeit, Verfügbarkeit und Integrität, sowie Maßnahmen zur Gewährleistung der Datenminimierung, Nichtverkettung, Transparenz und Intervenierbarkeit im jeweiligen Verantwortungsbereich getroffen, die den Anforderungen der entsprechenden datenschutzrechtlichen Bestimmungen entsprechen.

(2) Zum Schutz der IT-Systeme und zur Gewährleistung eines einheitlich hohen Datenschutzstandards innerhalb der IT-Komponente ist der IT-Zweckverband berechtigt, verbandsweite Vorgaben zu erstellen.

(3) Die verbandsweiten Vorgaben, die unter Beteiligung der Verbandsmitglieder beschlossen werden, werden umgesetzt. Es handelt sich hierbei um zwingende Mindeststandards, welche nach oben korrigiert werden können. Ausnahmen von der Einhaltung, aufgrund z.B. lokaler Gegebenheiten oder rechtlicher Hinderungsgründe, sind dem IT-Zweckverband mitzuteilen und mit diesem abzustimmen.

## § 7 Datenschutzfolgeabschätzung

Datenschutzfolgeabschätzung wird durch die für die inhaltliche Datenverarbeitung verantwortliche Partei durchgeführt, soweit dies durch das Gesetz erforderlich ist. Eine gegenseitige Unterstützung findet statt.

## § 8 Datenschutzverstoß

Bei Datenschutzverstößen erfolgt eine enge Zusammenarbeit. Es erfolgt unter den jeweils betroffenen Parteien eine unverzügliche und vollständige Information, wenn Fehler oder Unregelmäßigkeiten bzgl. datenschutzrechtlicher Bestimmungen festgestellt worden sind.

## § 9 Datentransfer und Auftragsverarbeitung

(1) Soweit Dienstleister Daten der Parteien verarbeiten sollen, erfolgt eine vorherige Prüfung der Dienstleister nach Datenschutz- und Datensicherheitsaspekten.

(2) Ein Datentransfer außerhalb der EU/EWG oder in einem Drittland erfolgt nur, soweit das Verbandsmitglied vorab informiert und dessen Zustimmung eingeholt wurde.

(3) Grundsätzlich schließen die Parteien eigene Auftragsverarbeitungsverträge ab. Soweit Tätigkeiten einen Bezug zur Aufgabenwahrnehmung von kommunit haben, schließt kommunit die Auftragsverarbeitungsverträge mit den Dienstleistern ab.

## § 10 Aufsichtsbehörde

Gegenüber der Aufsichtsbehörde erfolgt eine Zusammenarbeit und gegenseitige Unterstützung durch die jeweils betroffenen Parteien.

## § 11 Wahrung der Vertraulichkeit und sonstiger Geheimnisse

Die Wahrung der Vertraulichkeit und sonstiger Geheimnisse erfolgt nach den gesetzlichen Vorgaben. Es werden geeignete Maßnahmen zur Sicherstellung getroffen.

## § 12 Beendigung und Ausscheiden

(1) Scheidet ein Verbandsmitglied aus dem IT-Zweckverband aus, so gehen mit Ausscheiden alle datenschutzrechtlichen Pflichten und Rechte wieder auf das Verbandsmitglied über.

(2) kommunit wird dem ausscheidenden Verbandsmitglied entsprechend § 22 Abs. 3 der Verbandssatzung die betreffenden Datenbestände zur Verfügung stellen.

(3) Soweit kommunit die Auftragsverarbeitungsverträge für das Verbandsmitglied geschlossen hat und das Verbandsmitglied Vertragspartner geworden ist, ist das ausscheidende Verbandsmitglied verpflichtet, Auftragnehmer oder Auftraggeber über das Ausscheiden und damit einhergehende etwaige Änderungen im Vertragsverhältnis zu informieren. kommunit wird dem ausscheidenden Verbandsmitglied hierzu eine Liste der relevanten geschlossenen Auftragsverarbeitungsverträge zur Verfügung stellen. Ist kommunit Vertragspartner geworden, werden in Abstimmung mit dem Verbandmitglied die geschlossenen Verträge gekündigt oder - soweit möglich - eine Übernahme der Verträge durch das Verbandsmitglied ermöglicht.

(4) Soweit einzelne Datenverarbeitungen nach Ausscheiden inklusive der Übergangszeit, bei kommunit verbleiben, ist das ausscheidende Verbandsmitglied für die ordnungsgemäße Verarbeitung und die Erfüllung aller datenschutzrechtlichen Anforderungen verantwortlich; entsprechende Vereinbarungen sind zu treffen.

## § 13 Mitgeltendes Dokument

Anlage 1 - Aufteilung der Verantwortungsbereiche im IT-Zweckverband

## § 14 Inkrafttreten

Die Satzung tritt am Tage nach ihrer Bekanntmachung in Kraft.

Quickborn, 10.02.2020

Ort, Datum

Verbandsvorsteher

**Anlage - Aufteilung der Verantwortungsbereiche im IT-Zweckverband**

Die Verbandsmitglieder und der IT-Zweckverband gewährleisten gemeinsam die reibungslose und sichere elektronische Verarbeitung personenbezogener Daten in den Verarbeitungsprozessen der Verbandsmitglieder. Hierbei sind die Aufgaben zwischen den gemeinsam Verantwortlichen voneinander getrennt. Personenbezogene Daten werden durch die Parteien jeweils nach den Prinzipien Least Privilege (Zuweisung von Nutzerrechten im geringstmöglichen Umfang) und Need-to-know (Kenntnis von Daten nur, wenn nötig) verarbeitet. Während die Verbandsmitglieder die jeweils zuständige inhaltliche Datenverarbeitung (Rechtmäßigkeit der Verarbeitung, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit) gewährleisten, trägt der IT-Zweckverband für die satzungsgemäß übertragenen IT-Aufgaben Sorge.

Die unterschiedlichen Aufgaben der Parteien, bei denen personenbezogene Daten verarbeitet werden, werden verbindlich in der nachfolgenden Liste beschrieben. Die Liste dient zudem als Auslegungshilfe bei Unklarheiten hinsichtlich der Aufgabenübertragung.

### *Verantwortung bei kommunit*

Rechenzentrum und Datenverarbeitungsräumen (Verteilerräume, Datensicherungsräume etc.)

- Gewährleistung des Rechenzentrumbetriebes
- Gewährleistung der Sicherheit (Vertraulichkeit, Verfügbarkeit und Integrität) des Rechenzentrums mit technischen und organisatorischen Maßnahmen
- Ausfallsicherung aller Systeme bei kommunit und den Verbandsmitgliedern im Rechenzentrum
- Physikalische Datenspeicherung
- Zugang zu zentralen Komponenten und Verteilern (Verschluss, Raumsicherung)
- Risikoanalyse im Zuständigkeitsbereich
- Dokumentation und Festlegung möglicher technischer und organisatorischer Maßnahmen

Hard- und Software

- Umfassende und ausschließliche Beschaffung der Hardware, Software und anderen Betriebsmitteln.
- Definition der Standard- Hardware
- Festlegung der technischen und organisatorischen Anforderungen der Hardware und Software im Zuständigkeitsbereich in Bezug auf Sicherheit unter Berücksichtigung der mitgeteilten Schutzziele.
- Ausschließliche Installation und Betrieb von Software (Installation, Update, Schnittstellen)
- Gewährleistung der Sicherheit der eingesetzten Hardware
- Gewährleistung Stand der Technik
- Sichere Entsorgung der Hardware
- Gewährung von Zugriffen nach Weisung des Mitglieds für Verfahrensverantwortliche
- Dokumentation und Festlegung möglicher technischer und organisatorischer Maßnahmen im IT-Bereich
- Beurteilung von Apps bezüglich der MDM (Mobil Device Management) Umgebung

IT-Netz

- Sicherheit des IT-Netzes
- Virenschutz und Angriffsabwehr in zentralen, mobilen und dezentralen Systemen und Erstellung entsprechender Regelungen für kommunit und Mitglieder
- Sicherheit der Verbindungen (Leitungen und WLAN etc.)
- Sicherheit der Übermittlung von Daten an Dritten im Auftrage des Mitgliedes
- Regelung und Sicherung des Zugangs Dritter auf Systeme des Zweckverbandes auf Systemebene
- Dokumentation und Festlegung möglicher technischer und organisatorischer Maßnahmen im IT-Bereich

Daten

- Sicherung der Datenbestände (Backup)

- Sicherheit der Übermittlung von Daten an Dritten im Auftrage des Mitgliedes
- Technische Programmfreigabe und Durchführung von Testverfahren bei zentralen und Systemanwendungen
- Gewährleistung der Vertraulichkeit, Integrität, Verfügbarkeit der Daten unter Berücksichtigung der mitgeteilten Schutzziele
- Definition der Schutzstufen (Zur Einstufung der Schutzziele)
- Dokumentation und Festlegung möglicher technischer und organisatorischer Maßnahmen im IT-Bereich

### *Verantwortung bei dem Verbandsmitglied*

- Gewährleistung der inhaltlichen Datenverarbeitung (insbesondere Rechtmäßigkeit der Verarbeitung, Transparenz, Zweckbindung, Datenminimierung, Richtigkeit, Integrität, Nichtverkettung und Intervenierbarkeit)
- Gewährleistung der Schutzmaßnahmen außerhalb des Verantwortungsbereiches von kommunit (z.B. Physische Sicherheit in den eigenen Räumlichkeiten, Verschlossene Schränke etc.)
- Löschen von Daten
- Einholen notwendiger Einwilligungen
- Prüfung und Freigabe automatisierter Einzelentscheidung
- Entscheidung und Betrieb von Videoüberwachungsanlagen in öffentlichen Räumen
- Programmfreigabe und Durchführung von Testverfahren bei Fachanwendungen
- Einstufung der Schutzziele
- Dokumentation und Risikobewertung
- Regelung und Sicherung des Zugangs Dritter über Wartungszugänge etc. bei Fachanwendungen.
- Organisation im Zuständigkeitsbereich (Anweisungen, Regeln, Einhaltung dieser)
- Regelung von Zugriffen im Zuständigkeitsbereich (Fachanwendungen und Nutzer)
- Anweisung von kommunit bzgl. des Zuganges von Verfahrensverantwortlichen (Admin Fachanwendungen)