

Vertrag über die Auftragsverarbeitung gemäß Artikel 28 DSGVO

Des Zweckverbandes Kommunale Informationsverarbeitung Sachsen „KISA“

Eilenburger Straße 1a

04317 Leipzig

-im Folgenden KISA, Auftragsverarbeiter oder Auftragnehmer-

und

dem Verantwortlichem / Auftraggeber-

-gemeinsam auch Vertragspartner-

Erstellt:	24.05.2018 15:47:00
Zuletzt geändert:	24.05.2018 16:25:00
Gültig ab:	25.05.2018
Gültigkeit Vorgängerversion:	--

Präambel

Seit dem 25. Mai 2018 ist die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung – **DSGVO**) unmittelbar geltendes Recht.

Die DSGVO verpflichtet Sie als Auftraggeber und Verantwortlichen für die Verarbeitung personenbezogener Daten in den Fällen einer Verarbeitung durch Dienstleister eine Vereinbarung zur Auftragsdatenverarbeitung abzuschließen, die den geänderten rechtlichen Anforderungen entspricht.

KISA stellt Verbandsmitgliedern und Kunden eine Vielzahl von Datenverarbeitungsverfahren und damit zusammenhängende Verarbeitungsleistungen zur Erledigung oder Vereinfachung von Verwaltungsaufgaben zur Verfügung. In den meisten Fällen unserer Beauftragung verarbeiten wir in diesem Zusammenhang personenbezogene Daten in Ihrem Auftrag. Die nachstehenden Regelungen konkretisieren die Pflichten der Vertragspartner zum Datenschutz in Fällen einer Auftragsverarbeitung personenbezogener Daten durch KISA.

Teil 1 – Anwendungsbereich, Zustandekommen, Änderungen

1. Sachlicher Anwendungsbereich

- 1.1. Zwischen KISA und dem Auftraggeber bestehen Verträge über die Erbringung von verschiedenen Leistungen zur Vereinfachung oder Erledigung von Verwaltungsaufgaben (Leistungsverträge).
- 1.2. Soweit KISA, Beschäftigte von KISA oder durch KISA beauftragte Dritte im Zusammenhang mit den genannten Leistungsverträgen personenbezogene Daten (Daten) des Auftraggebers verarbeiten, erfolgt dies wie in den Leistungsverträgen vereinbart ausschließlich auf Grundlage der nachstehenden Regelungen zur Auftragsverarbeitung.
- 1.3. Für Leistungsverträge, die bereits vor dem 25. Mai 2018 abgeschlossen wurden, treten die nachstehenden Regelungen zur Auftragsverarbeitung an die Stelle der in den Leistungsverträgen getroffenen Vereinbarungen zum Schutz personenbezogener Daten, die damit zugleich außer Kraft treten.

2. Zustandekommen

- 2.1. Diese Vereinbarung kommt mit Zugang der durch den Auftraggeber unterzeichneten Beitrittserklärung bei KISA rückwirkend zum 25. Mai 2018 zustande.
- 2.2. Eine Übermittlung der Beitrittserklärung als Scan per E-Mail ist ausreichend.

3. Änderungsvorbehalt, Widerspruchsregelung, Teilunwirksamkeit

- 3.1. KISA hat das Recht, die Regelungen dieser Vereinbarung zu ändern wenn dies zur Anpassung an den aktuellen Stand der Technik, an geänderte Betriebsabläufe, Änderungen einschlägiger Rechtsgrundlagen oder einschlägiger Rechtsprechung oder zur Umsetzung von Vorgaben ihrer Aufsichtsbehörden notwendig erscheint und der Auftraggeber durch die Änderung nicht wider Treu und Glauben benachteiligt wird.
- 3.2. Über die Änderungen informiert KISA den Auftraggeber in geeigneter Weise schriftlich oder in Textform. Die Änderungen werden Vertragsbestandteil, sofern der Auftraggeber ihrer Geltung nicht binnen einer Frist von vier Wochen nach Zugang der Änderungsmitteilung schriftlich oder in Textform widersprochen hat. Mit der Änderungsmitteilung weist KISA auf die Folgen eines fehlenden Widerspruchs hin.
- 3.3. Im Falle von Widersprüchen in den Vertragsdokumenten gelten die nachstehenden Regelungen dieser Vereinbarung im Zweifel vorrangig vor abweichenden allgemeinen Bestimmungen der Leistungsverträge.
- 3.4. Sollten einzelne Punkte dieser Vereinbarung unwirksam sein oder werden, so bleiben alle übrigen Bestimmungen davon unberührt. Im Falle unwirksamer Bestimmungen, Lücken, Unklarheiten oder bei Veränderungen der Grundlagen des Vertragswerks ist die Vereinbarung so auszulegen, wie es den wirtschaftlichen Interessen der Vertragspartner unter Berücksichtigung des Vertragszwecks am nächsten kommt. Der Vertrag ist - erforderlichenfalls unter Anpassung weiterer durch die Unwirksamkeit betroffener Bestimmungen - entsprechend zu ergänzen.

Teil 2 – Regelungen zur Auftragsverarbeitung

4. Gegenstand und Dauer der Verarbeitung und Konkretisierung des Auftrags

- 4.1. KISA verarbeitet personenbezogene Daten für den Verantwortlichen im Sinne von Art.4 Nr. 2 und Art. 28 DSGVO.
- 4.2. Die gemäß Art.28 Abs. 3 S. 1 DSGVO notwendigen Regelungen zu
 - 4.2.1. Gegenstand,
 - 4.2.2. Art und Umfang sowie
 - 4.2.3. Zweck der Verarbeitung personenbezogener Daten und
 - 4.2.4. Die Art der personenbezogenen Daten und
 - 4.2.5. Die Kategorien betroffener Personenergeben sich jeweils aus den Leistungsverträgen und deren Anlagen.
- 4.3. Diese Vereinbarung wird für die Laufzeit der referenzierten Leistungsverträge fest abgeschlossen. Sie endet, ohne dass es einer gesonderten Kündigung bedarf, mit dem Ende des letzten in Bezug genommenen Leistungsvertrages.

5. Ort der Verarbeitung

Die vereinbarte Datenverarbeitung findet ausschließlich in einem Mitgliedstaat der Europäischen Union oder in einem anderen Vertragsstaat des Abkommens über den Europäischen Wirtschaftsraum statt. Jede Verlagerung der Dienstleistung oder von Teilarbeiten in ein Drittland bedarf der vorherigen Zustimmung des Auftraggebers und darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DSGVO erfüllt sind (z.B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).

6. Rechte und Pflichten sowie Weisungsbefugnisse des Verantwortlichen

- 6.1. Für die Beurteilung der Zulässigkeit der Verarbeitung gemäß Art. 6 Abs. 1 DSGVO sowie für die Wahrung der Rechte der betroffenen Personen nach den Art. 12 bis 22 DSGVO ist allein der Auftraggeber verantwortlich. Gleichwohl ist KISA verpflichtet, alle solche Anfragen, sofern sie erkennbar ausschließlich an den Verantwortlichen gerichtet sind, unverzüglich an diesen weiterzuleiten.
- 6.2. Der Verantwortliche erteilt alle Aufträge, Teilaufträge und Weisungen in der Regel schriftlich oder in einem dokumentierten elektronischen Format. Mündliche Weisungen sind unverzüglich schriftlich oder in einem dokumentierten elektronischen Format zu bestätigen.
- 6.3. Änderungen des Verarbeitungsgegenstandes und Verfahrensänderungen sind gemeinsam zwischen Verantwortlichem und KISA abzustimmen und schriftlich oder in einem dokumentierten elektronischen Format festzulegen.
- 6.4. Der Verantwortliche informiert KISA unverzüglich, wenn er Fehler oder Unregelmäßigkeiten bei der Prüfung der Auftragsergebnisse feststellt.

- 6.5. Der Verantwortliche ist verpflichtet, alle im Rahmen des Vertragsverhältnisses erlangten Kenntnisse von Geschäftsgeheimnissen und Datensicherheitsmaßnahmen des Auftragsverarbeiters bzw. seiner Unterauftragnehmer vertraulich zu behandeln. Diese Verpflichtung bleibt auch nach Beendigung dieses Vertrages bestehen.

7. Weisungsberechtigte des Verantwortlichen und Weisungsempfänger des Auftraggebers

Weisungsberechtigte Personen des Verantwortlichen und Weisungsempfänger des Auftraggebers dokumentieren die Vertragspartner in den jeweiligen Leistungsverträgen. Ein Wechsel des berechtigten Personenkreises während der Vertragslaufzeit ist schriftlich zu dokumentieren, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO), sofern in den Leistungsverträgen keine strengeren Formvorschriften vereinbart wurden.

8. Pflichten des Auftragsverarbeiters

- 8.1. KISA und die bei ihr beschäftigten Personen verarbeiten personenbezogene Daten ausschließlich im Rahmen der hier und in den Leistungsverträgen getroffenen Vereinbarungen und nach Weisungen des Verantwortlichen, sofern KISA nicht zu einer anderen Verarbeitung durch das Recht der Union oder der Mitgliedstaaten, dem KISA unterliegt, hierzu verpflichtet ist (z. B. Ermittlungen von Strafverfolgungs- oder Staatsschutzbehörden); in einem solchen Fall teilt KISA dem Verantwortlichen diese rechtlichen Anforderungen vor der Verarbeitung mit, sofern das betreffende Recht eine solche Mitteilung nicht wegen eines wichtigen öffentlichen Interesses verbietet (Art. 28 Abs. 3 Satz 2 lit. a DSGVO).
- 8.2. Weisungen sind bzw. werden in den Leistungsverträgen festgelegt und können vom Auftraggeber danach in schriftlicher Form oder einem elektronischen Format durch einzelne Weisungen geändert, ergänzt oder ersetzt werden. Weisungen die im Leistungsvertrag nicht vorgesehen sind, werden wie ein Antrag auf Änderung des Leistungsinhalts behandelt. Daraus resultierender Mehraufwand für KISA ist im Zweifel gesondert gemäß jeweils aktueller Preisliste zu vergüten.
- 8.3. KISA informiert den Auftraggeber unverzüglich, wenn sie der Auffassung ist, dass eine Weisung gegen anwendbare Gesetze verstößt. KISA darf die Umsetzung der Weisung solange aussetzen, bis sie durch den Verantwortlichen nach Überprüfung bestätigt oder geändert wird.
- 8.4. KISA verwendet die zur Verarbeitung überlassenen personenbezogenen Daten für keine anderen, insbesondere nicht für eigene Zwecke. Kopien oder Duplikate der personenbezogenen Daten werden ohne Wissen des Verantwortlichen nicht erstellt.
- 8.5. KISA gewährleistet die vertragsgemäße Abwicklung aller vereinbarten Maßnahmen.
- 8.6. KISA verpflichtet zur Verarbeitung der personenbezogenen Daten eingesetzte oder befugte Mitarbeiter vor Aufnahme der Tätigkeit für die Zeit ihrer Tätigkeit wie auch nach Beendigung des Beschäftigungsverhältnisses in geeigneter Weise zur Verschwiegenheit und macht diese mit den für sie maßgebenden Bestimmungen des Datenschutzes vertraut (Art. 28 Abs. 3 Satz 2 lit. b und Art. 29 DSGVO). KISA wird die Einhaltung der datenschutzrechtlichen Vorschriften in ihrem Betrieb überwachen.
- 8.7. Die für den Verantwortlichen verarbeiteten Daten wird KISA von sonstigen Datenbeständen strikt trennen.

- 8.8. Bei der Erfüllung der Rechte der betroffenen Personen nach Art. 12 bis 22 DSGVO durch den Verantwortlichen, an der Erstellung der Verzeichnisse von Verarbeitungstätigkeiten sowie bei erforderlichen Datenschutz-Folgeabschätzungen des Verantwortlichen wird KISA im notwendigen Umfang mitwirken und den Verantwortlichen soweit möglich angemessen unterstützen (Art. 28 Abs. 3 Satz 2 lit e und f DSGVO). Er hat die dazu erforderlichen Angaben dem Verantwortlichen unverzüglich an die benannte Stelle weiterzuleiten.
- 8.9. KISA hat personenbezogene Daten aus dem Auftragsverhältnis zu berichtigen, zu löschen oder deren Verarbeitung einzuschränken, wenn der Verantwortliche dies mittels einer Weisung verlangt und berechtigte Interessen des Auftragsverarbeiters dem nicht entgegenstehen.
- 8.10. Unabhängig davon wird KISA personenbezogene Daten aus dem Auftragsverhältnis berichtigen, löschen oder deren Verarbeitung einschränken, wenn der Weisung des Verantwortlichen ein berechtigter Anspruch des Betroffenen aus Art. 16, 17 und 18 DSGVO zugrunde liegt.
- 8.11. Auskünfte über personenbezogene Daten aus dem Auftragsverhältnis an Dritte oder den Betroffenen darf der Auftragsverarbeiter nur nach vorheriger Weisung oder Zustimmung durch den Verantwortlichen erteilen.

9. Nachweis der Einhaltung datenschutzrechtlicher Pflichten und Kontrollrechte des Auftraggebers

- 9.1. Der Verantwortliche ist berechtigt, sich vor Beginn der Verarbeitung und sodann regelmäßig in angemessener Weise von der Einhaltung der bei KISA getroffenen technischen und organisatorischen Maßnahmen sowie der in diesem Vertrag festgelegten Verpflichtungen zu überzeugen.
- 9.2. KISA stellt dem Auftraggeber die erforderlichen Informationen zum Nachweis der Einhaltung ihrer vertraglichen und gesetzlichen Pflichten als Auftragsverarbeiter zur Verfügung.
- 9.3. Sofern der Auftraggeber Überprüfungen und Inspektionen durch eigene Beschäftigte oder von ihm beauftragte Prüfer für erforderlich hält, werden diese nach vorheriger Anmeldung unter Berücksichtigung einer angemessenen Ankündigungsfrist zu den üblichen Geschäftszeiten so durchgeführt, dass der Betriebsablauf bei KISA hierdurch nicht unzumutbar beeinträchtigt wird (Art. 28 Abs. 3 Satz 2 lit. h DSGVO). KISA ist berechtigt, die Inspektion von der Unterzeichnung einer Vertraulichkeitserklärung der Prüfer abhängig zu machen und die Inspektionen mehrerer Auftraggeber in einem Termin zusammenzufassen.

10. Beauftragung von Unterauftragnehmern

- 10.1. Der Auftraggeber ist damit einverstanden, dass KISA für die Verarbeitung personenbezogener Daten des Auftraggebers die in den jeweiligen Leistungsverträgen aufgeführten Unterauftragnehmer einsetzt.
- 10.2. Der Auftraggeber erteilt KISA die allgemeine Genehmigung, weitere Unterauftragnehmer einzusetzen oder eingesetzte Unterauftragnehmer auszuwechseln im Sinne des Art. 28 Abs. 2 DSGVO. KISA informiert den Auftraggeber vorab über jede beabsichtigte Beauftragung weiterer Unterauftragnehmer oder die Änderung bestehender Beauftragungen, wodurch der Verantwortliche die Möglichkeit erhält, gegen derartige Änderungen Einspruch zu erheben (§ 28 Abs. 2 Satz 2 DSGVO). Der Einspruch ist gegenüber KISA innerhalb einer Frist von zwei Wochen

gerechnet vom Tag nach Absendung der Information schriftlich oder in elektronischem Format unter Angabe von Gründen zu erklären.

- 10.3. Erhebt der Auftraggeber Einspruch gegen die angekündigte Maßnahme, hat KISA nach eigener Wahl das Recht, die Leistung ohne die beabsichtigte Änderung zu erbringen oder die von der Änderung betroffenen Leistungsverträge ganz oder teilweise binnen einer Frist von zwei Wochen nach Zugang des Einspruchs mit einer Frist von vier Wochen außerordentlich zu kündigen. Ein Anspruch des Auftraggebers auf Leistungserbringung ohne die beabsichtigte Änderung ist ausgeschlossen.
- 10.4. KISA wird die Unterauftragnehmer unter Berücksichtigung ihrer Eignung und der von ihnen getroffenen technischen und organisatorischen Maßnahmen im Sinne von Art. 32 DSGVO sorgfältig auswählen. Die relevanten Prüfunterlagen dazu sind dem Verantwortlichen auf Anfrage zur Verfügung zu stellen.
- 10.5. Eine Beauftragung von Subunternehmern in Drittstaaten darf nur erfolgen, wenn die besonderen Voraussetzungen der Art. 44 ff. DS-GVO erfüllt sind (z. B. Angemessenheitsbeschluss der Kommission, Standarddatenschutzklauseln, genehmigte Verhaltensregeln).
- 10.6. KISA stellt vertraglich sicher, dass die vereinbarten Regelungen zwischen Verantwortlichem und KISA auch gegenüber Unterauftragnehmern gelten. KISA stellt insbesondere sicher, dass der Unterauftragnehmer hinreichende Garantien bietet, dass geeignete technische und organisatorische Maßnahmen getroffen sind und so durchgeführt werden, dass die Verarbeitung entsprechend den Anforderungen des Datenschutzrechts und dieses Vertrags erfolgt. In dem Vertrag mit dem Subunternehmer sind die Angaben so konkret festzulegen, dass die Verantwortlichkeiten des KISA und des Unterauftragnehmern deutlich voneinander abgegrenzt werden. Werden mehrere Unterauftragnehmern eingesetzt, so gilt dies auch für die Verantwortlichkeiten zwischen diesen Unterauftragnehmern. Insbesondere muss der Verantwortliche berechtigt sein, im Bedarfsfall angemessene Überprüfungen und Inspektionen, auch vor Ort, bei Subunternehmern durchzuführen oder durch von ihm beauftragte Dritte durchführen zu lassen.
- 10.7. Den Vertrag mit dem Unterauftragnehmer muss schriftlich abgefasst werden, was auch in einem elektronischen Format erfolgen kann (Art. 28 Abs. 4 und Abs. 9 DSGVO).
- 10.8. KISA haftet gegenüber dem Verantwortlichen dafür, dass der Unterauftragnehmer den Datenschutzpflichten nachkommt, die ihm im Einklang mit dem vorliegenden Vertragsabschnitt vertraglich auferlegt wurden.

11. Mitteilungspflichten des Auftragsverarbeiters bei Störungen der Verarbeitung und bei Verletzung des Schutzes personenbezogener Daten

- 11.1. KISA teilt dem Verantwortlichen unverzüglich Störungen, Verstöße von KISA oder der bei ihr beschäftigten Personen sowie gegen datenschutzrechtliche Bestimmungen oder die im Auftrag getroffenen Festlegungen sowie den Verdacht auf Datenschutzverletzungen oder Unregelmäßigkeiten bei der Verarbeitung personenbezogener Daten mit. Dies gilt vor allem auch im Hinblick auf eventuelle Melde- und Benachrichtigungspflichten des Verantwortlichen nach Art. 33 und Art. 34 DSGVO.
- 11.2. KISA wird den Verantwortlichen unter Berücksichtigung der Art der Verarbeitung und der ihr zur Verfügung stehenden Informationen bei seinen Pflichten nach Art. 33 und 34 DSGVO

angemessen unterstützen (Art. 28 Abs. 3 Satz 2 lit. f DSGVO). Meldungen nach Art. 33 oder 34 DSGVO für den Verantwortlichen darf der Auftragsverarbeiter nur nach vorheriger Weisung durchführen.

12. Haftung

- 12.1. Für Verstöße gegen die Bestimmungen der DSGVO haften Vertragspartner geschädigten Personen im Außenverhältnis und einander im Innenverhältnis in dem in Art. 82 DSGVO geregelten Umfang.
- 12.2. Darüber hinaus bleiben die Regelungen der Leistungsverträge unberührt.

13. Pflichten nach Vertragsbeendigung

- 13.1. Nach Abschluss der vertraglichen Arbeiten oder vorher auf Anforderung des Auftraggebers wird KISA sämtliche in ihren Besitz sowie an Subunternehmen gelangte Daten, Unterlagen und erstellte Verarbeitungs- oder Nutzungsergebnisse, die im Zusammenhang mit dem Auftragsverhältnis stehen, dem Verantwortlichen aushändigen *oder* nach vorheriger Zustimmung des Auftraggebers datenschutzgerecht löschen bzw. vernichten/vernichten lassen. Das Protokoll der Löschung wird auf Verlangen herausgegeben.
- 13.2. Vereinbarungen zu den technischen und organisatorischen Maßnahmen sowie Kontroll- und Prüfungsunterlagen (auch zu Subunternehmen) sind von beiden Vertragspartnern für ihre Geltungsdauer und anschließend noch für drei volle Kalenderjahre aufzubewahren.

14. Vergütung, Zurückbehaltungsrecht

- 14.1. Die Pflicht von KISA, nach den vorstehenden Regelungen Weisungen des Auftraggebers Folge zu leisten oder ihn bei der Wahrnehmung seiner rechtlichen Pflichten zu unterstützen, lässt das Recht von KISA unberührt, für Leistungen, die nicht bereits vom Leistungsumfang der Leistungsverträge umfasst sind, ein angemessenes Entgelt zu verlangen. Dies gilt insbesondere für die Mitwirkung zur Gewährleistung der Betroffenenrechte und die Aufwände im Zusammenhang mit geforderten Inspektionen.
- 14.2. Über die voraussichtlichen Kosten zusätzlicher Leistungen wird KISA den Auftraggeber unverzüglich nach Kenntnisnahme der Anforderung informieren. Im Zweifel erfolgt die Abrechnung nach tatsächlichem Aufwand zu den in der jeweils aktuellen Preisliste festgeschriebenen Stundensätzen.

Teil 3 – Technisch-organisatorische Maßnahmen (ToM)

15. Maßnahmen zur Gewährleistung des Datenschutzes

- 15.1. KISA bietet hinreichende Garantien dafür, dass geeignete technische und organisatorische Maßnahmen (toM) so durchgeführt werden, dass die Verarbeitung im Einklang mit den Anforderungen der DSGVO erfolgt und den Schutz der Rechte der betroffenen Person gewährleistet. Unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere des Risikos für die Rechte und Freiheiten natürlicher Personen treffen der Verantwortliche und KISA geeignete technische und organisatorische Maßnahmen, um ein dem Risiko angemessenes Schutzniveau zu gewährleisten.
- 15.2. Die allgemeinen toM werden im Verzeichnis der Verarbeitungstätigkeiten gemäß Art.30 Abs. 2 DSGVO beschrieben.
- 15.3. KISA führt ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, das alle in Art. 30 Abs. 2 DSGVO aufgeführten Angaben enthält. KISA stellt dem Verantwortlichen auf Anforderung alle für den Auftraggeber relevanten Angaben aus diesem Verzeichnis zur Verfügung.
- 15.4. KISA unterstützt den Verantwortlichen bei der Erstellung und Pflege seiner Verzeichnisse der Verarbeitungstätigkeiten gemäß Artikel 30 Abs. 1 DSGVO.

Anlage – Beitrittserklärung

Kommunale Informationsverarbeitung Sachsen

Eilenburger Straße 1a

04317 Leipzig

oder

per E-Mail an: kundenmanagement@kisa.it

Wir,

Körperschaft:

vertreten durch:

Adresse:

erklären,

den **Vertrag über die Auftragsverarbeitung gemäß Artikel 28 DSGVO** des Zweckverbandes Kommunale Informationsverarbeitung Sachsen in der Fassung vom 24.05.2018 16:25:00 zur Kenntnis genommen zu haben und sind mit der Geltung der getroffenen Regelungen einverstanden.

Datum

Unterschrift