Informationssicherheitsrichtlinie

der GISA GmbH

für Vertragspartner

Stand: 27.05.2025

Um Risiken für die Informationssicherheit und die Geschäftsprozesse von GISA und seiner Vertragspartner zu minimieren, ist die Einhaltung von Regeln und Vorgaben beim Umgang mit der IT-Infrastruktur und den zu verarbeitenden Daten und Informationen unabdingbar.

Vorliegende Informationssicherheitsrichtlinie enthält verpflichtende Regelungen für Vertragspartner von GISA, das Personal des Vertragspartners und für alle weiteren ggf. von ihm beauftragten Personen/Institutionen, welche Zugriff auf die IT-Infrastruktur sowie Daten und Informationen von GISA erhalten. Wenn nicht anders vermerkt, umfasst „IT-Infrastruktur von GISA“ (z. B. Netzwerke, IT-Systeme, Anwendungen, sonstige IT-Komponenten) auch die IT-Infrastruktur, deren Betrieb GISA im Auftrag Dritter verantwortet.

Sollten vom Vertragspartner weitere Dienstleister zur Vertragserfüllung gegenüber GISA gebunden werden oder sich beim Vertragspartner wesentliche Änderungen an der anzuschließenden IT-Infrastruktur ergeben, so ist dies dem IT-Sicherheitsbeauftragten der GISA GmbH unmittelbar mitzuteilen.

Der Vertragspartner stellt sicher, dass sein Personal und von ihm beauftragte Personen/Institutionen, welche auf IT-Infrastrukturen und/oder Daten von GISA zugreifen sollen, vor Beginn derartiger Aktivitäten über die jeweils aktuell vorliegende Informationssicherheitsrichtlinie von GISA informiert sind und verantwortet die Einhaltung der darin enthaltenen Regelungen.

Durch den IT-Sicherheitsbeauftragten der GISA oder von ihm Beauftragte kann eine Prüfung der relevanten Infrastruktur und/oder der bestehenden Kommunikationsverbindungen des Vertragspartners erfolgen. Der Vertragspartner wird die für die Überprüfung notwendige Einsichtnahme in Dokumente, in Prozessabläufe, in den IT-Betrieb usw. gestatten, die Durchführung der Prüfung sachgerecht unterstützen und insbesondere den Zutritt zu allen relevanten Betriebsstätten gewährleisten.

Durch GISA kommunizierte Änderungen – resultierend aus vorliegender Sicherheitsrichtlinie von GISA – sind vom Vertragspartner im vorgegebenen Zeitraum vollständig umzusetzen. Eine Überprüfung der umzusetzenden Maßnahmen kann durch GISA oder ihre Beauftragten entsprechend o. g. Regelung erfolgen.

Eine gewünschte bzw. erforderliche Anbindung an das GISA-Netzwerk kann erst nach positivem Bescheid der für Informationssicherheit zuständigen GISA-Gremien auf Basis der vom Vertragspartner eingereichten Unterlagen und ggf. weiterer Prüfungen erfolgen.

Der Vertragspartner stellt sicher, dass sein Personal und alle weiteren ggf. von ihm beauftragten Personen/Institutionen auf die Einhaltung der Bestimmungen der EU-DSGVO sowie des BDSG, TKG und UWG in ihren jeweils aktuellen Fassungen verpflichtet sind.

Zur Vertragserfüllung werden dem beauftragten Personal des Vertragspartners durch GISA bedarfsweise IT-Infrastruktur und Zugangs- bzw. Zugriffsberechtigungen bereitgestellt. Die zu erteilenden Berechtigungen müssen durch entsprechende Identifikations- und Authentifikations-mechanismen einen eindeutigen Rückschluss auf eine Person zulassen. Die jeweiligen Personen erhalten dazu personifizierte Accounts mit dedizierten Berechtigungen. In Ausnahmefällen kann durch die GISA eine Zugangsberechtigung einer kleinen geschlossenen Benutzergruppe erteilt werden.

Folgende Sicherheitsvorgaben sind für den Vertragspartner, sein Personal und alle weiteren ggf. von ihm beauftragten Personen/Institutionen verpflichtend:

1. Vor Beginn der Tätigkeit im Umfeld der IT-Infrastruktur von GISA hat eine Einweisung durch einen GISA-Beauftragten zu erfolgen – zu den konkreten Rahmenbedingungen des Einsatzes und ggf. zu spezifischen Sicherheitsvorgaben.

2. Dem vom Vertragspartner beauftragten Personal sind die einschlägigen Grundregeln zur Gewährleistung von Informationssicherheit bekannt. Das Personal wird mindestens jährlich im eigenen Unternehmen zur Einhaltung solcher Regeln belehrt.

3. Zugang und Zugriffe auf die IT-Infrastruktur von GISA (Netzwerk, Computersysteme, Anwendungen und sonstige IT-Komponenten) erfolgen ausschließlich mittels von GISA bereitgestellter bzw. mit GISA abgestimmter Verfahren und Systeme.

4. Von GISA bereitgestellte bzw. betreute/administrierte IT-Infrastruktur ist ausschließlich zur Erbringung der beauftragten (mit GISA vereinbarten) Leistungen zu nutzen.

5. Rechner sind beim Verlassen des Arbeitsplatzes vor unberechtigten Zugriffen zu schützen (zumindest zu sperren).

6. Bei mobilen Rechnern und Smartphones zur dienstlichen Nutzung ist besondere Vorsicht geboten. Mobile Geräte sind bei Nichtnutzung sicher aufzubewahren.

7. IT-Systeme und Daten sind durch persönliche, geheime und sichere (komplexe, hinreichend lange) Kennwörter zu schützen.

8. Mit erteilten Zugriffsberechtigungen ist verantwortungsbewusst umzugehen, insbesondere wenn administrative Rechte erteilt wurden. Die gewährten Berechtigungen sind ausschließlich zur Erfüllung der jeweils vereinbarten Arbeitsaufgaben zu nutzen.

9. Beim Zugriff auf besonders sensible Systeme bzw. Daten ist ggf. das 4-Augen-Prinzip vorgeschrieben. Der jeweils zuständige GISA-Verantwortliche ist dazu aussagefähig.

10. Versuche, sich unberechtigt Zugriff auf Daten und Informationen zu verschaffen, sind zu unterlassen.

11. Bei jeglicher Nutzung von Hardware, Software(-Lizenzen), Daten und Informationen (Texte, Bilder, Filme, ...) sind die gesetzlich geschützten Urheberrechte zu beachten (vgl. UrhG u. a.).

12. Das Umgehen oder Außerkraftsetzen von Sicherheitsbeschränkungen, Sicherheitseinrichtungen, Zugangs- und Zutrittskontrollsystemen o. ä. ist nicht gestattet.

13. Der Anschluss von IT-Geräten, welche nicht von GISA betreut bzw. administriert werden, an die von GISA betreute bzw. administrierte IT-Infrastruktur (Geräte, Datennetze usw.) ist nicht gestattet.

14. Für Endgeräte des Vertragspartners kann zum Einsatz in GISA-Lokationen ein spezielles WLAN für den Zugang ins Internet zur Verfügung gestellt werden.

15. Informationen von GISA oder seiner Partner sind vor unbefugter Einsichtnahme zu schützen. Datenträger (auch Ausdrucke o. ä.) mit schützenswerten Daten sind unter Verschluss zu halten. Für mobile elektronische Datenträger sind sichere Verschlüsselungsverfahren zu nutzen.

16. Die eigenmächtige Installation von Software auf Geräten, welche von GISA betreut bzw. administriert werden, ist nicht gestattet. Mit den zuständigen GISA-Verantwortlichen abgestimmte Installationen im Rahmen vereinbarter Arbeitsaufgaben bei Gewährleistung (bzw. zur Herstellung) der Informations- und Betriebssicherheit sind zulässig.

17. Eigenmächtige Veränderungen der Konfiguration der von GISA betreuten IT-Infrastruktur sind nicht gestattet, insbesondere nicht die Veränderung sicherheitsrelevanter Komponenten. Ausnahmen sind Anpassungen der persönlichen Arbeitsumgebung im von Betriebssystem- oder Anwendungssoftware vorgesehenen Rahmen. Mit den zuständigen GISA-Verantwortlichen abgestimmte Konfigurationsänderungen im Rahmen vereinbarter Arbeitsaufgaben bei Gewährleistung (bzw. zur Herstellung) der Informations- und Betriebssicherheit sind zulässig.

18. Alle im Rahmen des Einsatzes vorgenommenen Änderungen an der von GISA betreuten bzw. administrierten IT-Infrastruktur sind so zu protokollieren, dass sie vom zuständigen IT-Personal der GISA jederzeit nachvollzogen werden können.

19. Zugriffe auf das Internet sowie der Fernzugriff auf von GISA betreute bzw. administrierte Datennetze sind nur über die von GISA bereitgestellten bzw. freigegebenen Verfahren, Zugriffswege und Zugriffssoftware erlaubt. Die Nutzung dieser Zugriffsmöglichkeiten hat sich auf das für die Erfüllung der Arbeitsaufgaben notwendige Maß zu beschränken.

20. Soziale Netze bzw. Medien (Social Networks, Social Media), Public Clouds und andere „fremde“ Systeme außerhalb von GISA oder seiner Partner sind nicht zur Ablage oder für Transfers von dienstlichen Informationen (Informationen von bzw. über GISA und Partner) zu nutzen – es sei denn, es gehört im Einzelfall ausdrücklich zur vereinbarten Arbeitsaufgabe.

21. Alle Handlungen, wodurch die von GISA betreuten bzw. administrierten Datennetze für den Zugriff aus anderen Netzen „geöffnet“ werden könnten, sind zu unterlassen.

22. Datenträger sind vor ihrer Nutzung auf Malware zu prüfen.

23. Nicht mehr benötigte Akten sind sicher und datenschutzgerecht zu entsorgen. In allen GISA-Lokationen existieren dafür verschlossene Sicherheitsbehälter. Für elektronische Datenträger stehen besondere Sicherheitsbehälter bereit.

24. Bei Versand oder Übertragung schutzbedürftiger Informationen über öffentliche Netze sind sichere Kanäle (wie sog. Tunnel), aktuelle Verschlüsselungsverfahren, digitale Signaturen usw. anzuwenden.

25. Daten (incl. der Arbeitsergebnisse) sind vor Verlust zu schützen. Sie sind auf dafür vorgesehenen gesicherten Systemen zu speichern. Im Zweifelsfall (z. B. bei Test-Systemen) ist sich zu vergewissern, dass anfallende Daten tatsächlich mittels Backups „bedarfsgerecht“ gesichert werden.

26. Erkannte Mängel oder Schwachstellen mit möglichen nachteiligen Folgen für die Informationssicherheit von GISA oder seiner Partner sind umgehend dem IT-Sicherheitsbeauftragten von GISA zu melden.

27. Arbeitsergebnisse sind in der mit dem Auftraggeber bzw. mit den zuständigen GISA-Verantwortlichen vereinbarten Form zu dokumentieren.

28. Nach Erbringung der vereinbarten Leistungen sind alle Arbeitsergebnisse, Zwischenergebnisse, Protokolle, Dokumentationen und sonstigen generierten Daten dem Auftraggeber bzw. den zuständigen GISA-Verantwortlichen auszuhändigen. Eine Weitergabe jeglicher Daten an Dritte ist nicht gestattet.

29. Nicht mehr benötigte Daten (z. B. Sicherheitskopien) sind sicher zu löschen.

30. Zeitweilig überlassene IT-Infrastruktur von GISA (Endgeräte und sonstige Hard- und Software) sowie Ausweise und Authentisierungskomponenten sind nach Einsatzende an die jeweiligen GISA-Verantwortlichen zurückzugeben.

31. Hinweis zur Aufbewahrungspflicht: Zugriffe werden ggf. protokolliert; die Logs werden für die gesetzlich vorgeschriebene/zulässige Zeit aufbewahrt.

32. Bei Fragen zur Informationssicherheit geben Mitarbeiter des *Security Analytics & Response Teams* von GISA sowie der IT-Sicherheitsbeauftragte gern Auskunft.

33. Über Ergänzungen oder Ausnahmen bzgl. o. g. Regeln und Vorgaben entscheidet der IT-Sicherheitsbeauftragte von GISA.