

Anlage Informationssicherheit

Die Deutsche Gesellschaft für Internationale Zusammenarbeit (GIZ) GmbH betreibt ein Informationssicherheits-Managementsystem (ISMS) und plant eine Zertifizierung gemäß ISO/IEC 27001 sowie die Aufrechterhaltung dieses Zertifikats. Im Rahmen der Zertifizierung wird die aktuelle Version des genannten Standards umgesetzt.

Folgende Regelungen zur Informationssicherheit finden bei der Leistungserbringung Anwendung:

1 Umgang mit vertraulichen Informationen

Sämtliche auftragsbezogenen Daten und sonstigen Informationen wie beispielsweise übergebene Unterlagen und ausgetauschte Informationen, die der AN und ihren Mitarbeitenden bei der Vertragsdurchführung bekannt werden, sind während und über die Vertragslaufzeit hinaus vertraulich zu behandeln. Außerdem gilt der Grundsatz, dass sie nur Personen zugänglich gemacht und bekannt gegeben werden, die diese Informationen zur Erfüllung ihres Auftrages unbedingt benötigen (Need-to-know-Prinzip). Das gilt selbst dann, wenn diese Unterlagen oder Informationen nicht ausdrücklich als geheim oder vertraulich bezeichnet worden sind. Unterlagen und Arbeitsergebnisse aller Art, insbesondere Berichte, dürfen Dritten durch die AN nicht zugänglich gemacht werden, wenn die AG nicht vorher in Textform zugestimmt hat. Zu Dritten nach dieser Regelung zählt ebenfalls der Oberauftraggeber. Auch eine Verwendung dieser Daten und Informationen zu eigenen Zwecken der AN ist unzulässig.

2 Unterauftragnehmerregelung

Die AN darf Aufträge nur an fachkundige und leistungsfähige Anbietende, an deren Zuverlässigkeit keine Zweifel bestehen, nach wettbewerblichen Gesichtspunkten zu wirtschaftlichen Bedingungen vergeben. Die AN hat bei der Beschaffung auf Transparenz, Gleichbehandlung, Bieterernennung und Nachhaltigkeit zu achten. Soweit möglich sind mindestens drei Angebote einzuholen.

Ab Erreichen des jeweils gültigen EU-Schwellenwerts für Auftragsvergaben von Liefer- und Dienstleistungen sind das Gesetz gegen Wettbewerbsbeschränkungen (GWB) sowie die Vergabeverordnung (VgV) in ihrer jeweils aktuellen Fassung anzuwenden, wenn die AN die Beschaffung im Europäischen Wirtschaftsraum vornimmt. Bei Beschaffungen außerhalb des Europäischen Wirtschaftsraums sind diese Regelungen sinngemäß anzuwenden.

Im Falle der Untervergabe von Leistungen bleiben die Leistungspflichten der AN unberührt. Die Vergabe von Leistungen an Dritte durch die AN bedarf der vorherigen Zustimmung der AG in Textform, es sei denn, es handelt sich um Leistungen, die gemäß Vertrag von der AN zu beschaffen sind. Die AN verpflichtet die von ihr eingesetzten unterauftragnehmende Partei zur Einhaltung der Regelungen dieser Vertragsbedingungen.

3 Meldung von Sicherheitsvorfällen

Die AN informiert die AG (informationsecuritymanagement@giz.de) unverzüglich und in angemessener Form über Informationssicherheitsvorfälle, die (auch) Informationen der GIZ betreffen.

Ein Informationssicherheitsvorfall ist ein Ereignis, durch welches eine Beeinträchtigung der Informationssicherheit möglich oder bereits erfolgt ist, z.B. durch unberechtigte

Einsichtnahme/Weitergabe von Informationen (Verlust der Vertraulichkeit), Modifikation von Informationen (Verlust der Integrität) oder Löschen von Informationen/Behinderung des Zugriffs auf Informationen (Verlust der Verfügbarkeit).

4 Aufbewahrung von GIZ-bezogenen Unterlagen, Vertragsende

Auftragsbezogene Unterlagen und Arbeitsergebnisse, einschließlich der finanziellen Dokumentation, sind von der AN zehn Jahre nach Abnahme des Schlussberichts bzw. der Werkleistung aufzubewahren. Auf Verlangen der AG sind diese zu übergeben.

Sonstige von der AG erhaltene Unterlagen, Hilfsmittel, Materialien oder Gegenstände, die der AN bestimmungsgemäß nicht dauerhaft überlassen wurden, hat der AN mit Vertragsende unverzüglich und unaufgefordert zu übergeben. Dies gilt auch für alle Kopien.

In den obengenannten Fällen hat die Übergabe in einem vom Auftraggeber definierten Verfahren zu erfolgen. Die Auftraggeberin ist auch berechtigt, ganz oder teilweise die sichere Löschung (d.h. nicht rekonstruierbar) oder Vernichtung zu verlangen. Die Löschung und das angewandte Löschverfahren sind der Auftraggeberin auf Verlangen z.B. durch eine schriftliche Erklärung nachzuweisen. Eine zusätzliche Vergütung erfolgt nicht.

Gesetzliche Aufbewahrungspflichten und -fristen bleiben von dieser Regelung unberührt.

5 Qualifikation und Anforderung der eingesetzten Fachkräfte

Die AN ist verpflichtet, nur solche Fachkräfte einzusetzen, die vertrauenswürdig und den gestellten Aufgaben gewachsen sind, die notwendigen Fach- und Landeskennnisse besitzen, über die Sicherheitssituation im Einsatzland ausreichend informiert sowie auf diese vorbereitet sind. Der Auftragnehmer stellt sicher, dass die eingesetzten Fachkräfte über die vertraglichen Regelungen zur Informationssicherheit angemessen unterrichtet sind. Soweit die Teilnahme der AN und/oder ihrer Fachkräfte an speziellen Vorbereitungskursen vereinbart ist, ist die Vorbereitungszeit keine Einsatzzeit.

6 Zugriff auf Informationen

Der Auftragnehmer darf ausschließlich auf die im Rahmen der Leistungserbringung spezifizierten Informationen analog oder über technische Zugänge zugreifen.

Der Zugriff auf davon abweichende Bereiche und Informationen ist untersagt.

Die Auftraggeberin legt bei Bedarf fest, wie der Auftragnehmer mit Metadaten umzugehen hat (unter Berücksichtigung des Vertraulichkeitsprinzips; Need-to-Know).

7 Nutzung von Endgeräten

Bei der Nutzung von Endgeräten im Rahmen der Auftragsdurchführung stellt die AN sicher, dass der Ort der Nutzung angemessen sicher ist und dass unbefugte Dritte diese nicht benutzen können. Es muss weiterhin sichergestellt werden, dass unbefugte Dritte keine GIZ-bezogenen Informationen einsehen können (z.B. über Blickschutzfolien).