"Vertragliche Sicherheitsrichtlinien für externe IT-Dienstleistungen und Systemnutzung"

1 Geltungsbereich

Die Unternehmen der GASAG-Gruppe beauftragen externe Unternehmen (folgend Dienstleister) zur Erbringung von IT-basierten Dienstleistungen. Die dafür erforderliche Nutzung von IT-Systemen der GASAG-Gruppe sowie der Zugriff auf Daten der GASAG-Gruppe unterliegt u.a. den hier dargestellten Anforderungen zur Gewährleistung der Informationssicherheit.

Diese sind als Mindestvoraussetzung für die Leistungserbringung zu verstehen. Soweit diese Mindestanforderungen durch den Dienstleister nicht erfüllt werden können, ist eine Zusammenarbeit mit Unternehmen der GASAG-Gruppe ausgeschlossen.

2 Persönliche Verantwortung

Der Dienstleister ist selbst für seine eigene Informationsverarbeitung verantwortlich, die den hier festgelegten Regelungen zu folgen hat. Potenzielle Verstöße gegen die Festlegungen der vorliegenden Richtlinie können das Verhängen einer Pönale oder gesetzliche Schadenersatzforderungen nach sich ziehen.

Der Dienstleister gewährleistet, dass nur autorisiertes Personal Zugang zu den Systemen und Daten des Auftraggebers hat. Der Zugang ist auf das notwendige Minimum zu beschränken und regelmäßig zu überprüfen.

Der Dienstleister muss sicherstellen, dass seine Mitarbeiter regelmäßige IT-Sicherheitsunterweisungen und -schulungen erhalten, um ein Bewusstsein für die Bedeutung der Informationssicherheit zu entwickeln.

Die Berechtigung zur Nutzung der IT-Systeme der GASAG-Gruppe ist personengebunden und nicht übertragbar:

- Die Voraussetzungen der entsprechenden Berechtigung zur Nutzung der IT-Systeme, sowie urheberrechtliche, patentrechtliche Bestimmungen sowie Lizenzvereinbarungen über Software und einschlägige gesetzliche Bestimmungen sind einzuhalten.
- Der Dienstleister hat jederzeit sicher zu stellen, dass seine Handlungen nicht die Verfügbarkeit, die Integrität oder die Vertraulichkeit der IT-Systeme beeinträchtigen.

3 Datenschutz

Der Dienstleister verpflichtet sich, alle anvertrauten Daten gemäß der DSGVO und anderen relevanten Datenschutzbestimmungen zu behandeln.

Die Übertragung von Daten der GASAG-Gruppe an Dritte ist nicht zulässig. Ausnahmen erfordern eine gesonderte Genehmigung. Sämtlicher E-Mail-Verkehr zwischen der GASAG-Gruppe und dem Auftragnehmer ist vertraulich zu behandeln.

Das Speichern von Daten der GASAG-Gruppe auf mobilen Datenträgern (z.B. USB-Sticks) ist unzulässig. Ausnahmen erfordern eine gesonderte Genehmigung.

Daten aller Art, die im Rahmen der Leistungserbringung für die GASAG-Gruppe generiert werden, befinden sich im Eigentum der GASAG-Gruppe.

Nach Abschluss der Arbeiten sind Daten aller Art an die GASAG-Gruppe zurückzugeben, wobei keine Kopien, Auszüge oder sonstige vollständige oder teilweise Reproduktionen einbehalten werden dürfen.

4 Nutzung von IT-Systemen

Der Dienstleister hat sicherzustellen, dass ausschließlich mit der Auftragsbearbeitung betraute und sachkundige Personen Zugang zu den Systemen und Daten der GASAG-Gruppe erhalten. Der Dienstleister ist für die Handlungen oder Unterlassungen seiner Nachauftragnehmer auf die gleiche Weise wie für seine eigenen Handlungen oder Unterlassungen verantwortlich.

- Die erteilten Zugriffsberechtigungen und/oder die Verwendung personenbezogener und anderer betrieblicher Daten dienen ausschließlich der Erfüllung des Vertragsgegenstandes.
- Sicherheitsrelevante Konfigurationen sind generell nicht zu ändern oder außer Kraft zu setzen.
- Jeder Nutzer ist mitverantwortlich dafür, bei seiner täglichen Arbeit für die Sicherheit der IT-Systeme zu sorgen.

Systemupdates und Patches für Systeme im Verantwortungsbereich des Dienstleisters sind durch diesen regelmäßig und zeitnah durchzuführen, um bekannte Sicherheitslücken zu schließen. Durch den Dienstleister festgestellte oder vermutete Sicherheitslücken im Verantwortungsbereich der GASAG-Gruppe, sind durch den Dienstleister zu melden.

4.1 Multifaktorauthentifizierung (MFA)

Der Dienstleister muss ein Multifaktorauthentifizierungssystem oder vergleichbar sichere Lösungen für den Zugriff auf alle Systeme und Anwendungen, die mit den Daten und Netzwerken des Auftraggebers interagieren, implementieren und aufrechterhalten. Diese Maßnahme dient dazu, die Identität der Benutzer zu verifizieren und die Sicherheit der Zugangsdaten zu verstärken. Diese (MFA-)Systeme sollen regelmäßig aktualisiert und überprüft werden, um ihre Wirksamkeit sicherzustellen.

4.2 Zugriffsschutz

Im Verantwortungsbereich des Dienstleisters betriebene Systeme sind dem anerkannten Stand der Technik nach gegen den Zugriff durch Unbefugte zu schützen.

- Informationssysteme sind zu sperren, wenn diese nicht genutzt werden.
- Vorgegebene Initial-Passwörter sind durch ein komplexes Passwort zu ersetzen.
- Passwörter sind streng vertraulich zu behandeln und niemandem mitzuteilen.

5 Sicherheitsschulungen

Der Dienstleister verpflichtet sich, seine Mitarbeiter regelmäßig in Bezug auf Informationssicherheitspraktiken zu schulen, um das Bewusstsein und die Kompetenz im Umgang mit sensiblen Daten zu erhöhen.

6 Hard- und Software

Es ist vom Dienstleister sicherzustellen, dass alle eingesetzten Hard- und Softwareprodukte auf dem aktuellen Stand der Technik sind und regelmäßig auf Sicherheitsrisiken überprüft werden.

Die Anbindung von GASAG-Systemen an fremde IT-Systeme oder -Dienste ist ohne ausdrückliche Genehmigung der GASAG-Gruppe nicht zulässig.

Die Installation von Software auf Systemen der GASAG-Gruppe darf nur im mit dem Ziel der Dienstleistungserbringung erfolgen. Durch die Installation von Software entstehende Risiken sind durch den Dienstleister zu vermeiden bzw. dem Ansprechpartner der GASAG-Gruppe zu melden.

7 Regelungen zur E-Mail-Nutzung

Zur Erleichterung der auftragsbezogenen Kommunikation können bei Bedarf auch E-Mail Accounts innerhalb der GASAG-Gruppe eingerichtet werden.

- Die Nutzung des internen E-Mail-Dienstes ist ausschließlich im Zusammenhang mit dem Auftrag gestattet. Die private Nutzung ist nicht gestattet.
- Die Versendung von E-Mail an externe Empfänger außerhalb der GASAG-Gruppe ist nicht zulässig. Ausnahmen sind durch den Ansprechpartner der GASAG-Gruppe ausdrücklich zu genehmigen.
- Die automatische Weiterleitung von E-Mails an externe Postfächer ist nicht zulässig.

Alle E-Mails, die sensible oder vertrauliche Informationen enthalten, müssen verschlüsselt werden.

8 Umgang mit Störungen und Problemen

Der Dienstleister muss sicherstellen, dass ein Incident-Response-Plan existiert und regelmäßig aktualisiert wird.

Bei Auftreten von Problemen im IT-Bereich wendet sich der Dienstleister umgehend an den Ansprechpartner der GASAG-Gruppe.

Sicherheitsrelevante Ereignisse sind generell zu melden.

Benachrichtigen Sie Ihren Ansprechpartner der GASAG-Gruppe beispielsweise bei:

- vermutetem Datenverlust
- Verlust des Passworts
- Verlust von Hardware
- Erkennung eines Virus auf Hardware des Dienstleisters
- Bemerken verdächtiger Aktivitäten.

9 Kontrolle von IT-Systemen

Die GASAG-Gruppe ist berechtigt, Handlungen im Rahmen von IT-Systemen, die an das GASAG-Datennetz angebunden sind, sowie an Benutzerkonten zurückzuverfolgen und detailliert zu protokollieren.

10 Nutzungsbedingungen für den Fernzugriff

Jeglicher Fernzugriff auf Ressourcen der GASAG-Gruppe muss über sichere Kanäle wie VPN mit starker Verschlüsselung erfolgen. Die Nutzung von Fernzugriffen ist nur zur Erbringung der Dienstleistung zulässig. Die im Fernzugriff verfügbaren Daten sind vertraulich zu behandeln. Der Fernzugriff wird personenbezogen gewährt und ist nicht übertragbar.

Sämtliche Aktivitäten auf per Fernzugriff verfügbar gemachten Systemen können durch die GASAG-Gruppe protokolliert und ausgewertet werden. Die per Fernzugriff verfügbar gemachten Ressourcen sind sorgsam und schonend zu behandeln.

11 Zentrale Ansprechpartner

Als Dienstleister der GASAG-Gruppe benennt dieser mit Aufnahme der Tätigkeit eine Kontaktstelle für alle Belange der Informationssicherheit. Die vollständigen Kontaktdaten sind an das Postfach informationssicherheit@gasag.de zu senden.

12 Sicherheitsüberprüfung

Die GASAG-Gruppe ist berechtigt, in Bezug auf die vom Dienstleister erbrachten Leistungen, technische Überprüfungen aller Sicherheitsaspekte durchzuführen. Der Dienstleister verpflichtet sich zur Mitwirkung.

13 Verfügbarkeit

Die GASAG-Gruppe kann Zugänge ohne Nennung von Gründen und ohne in Kenntnissetzung des Dienstleisters aussetzen, sofern die Sicherheit der GASAG-Gruppe gefährdet ist.

14 Beginn/Beendigung

Zugriffe werden durch die GASAG-Gruppe bereitgestellt, sobald alle Voraussetzungen erfüllt sind. Die erteilten Zugriffe enden spätestens bei Auslaufen des Vertrages. Bei Beendigung der Vertragsverhältnisse gibt der Dienstleister innerhalb von 10 Werktagen alle Geräte zurück, die ggf. zur Ermöglichung des Fernzugriffs von der GASAG-Gruppe bereitgestellt wurden.

15 Haftung

Die GASAG-Gruppe übernimmt keine Verantwortung für Verluste, Schäden oder Kosten, die dem Dienstleister direkt oder indirekt durch die Nutzung oder Nicht-Verfügbarkeit des Fernzugriffs entstehen. Bei Verstößen gegen rechtliche Bestimmungen ist der Dienstleister für alle direkten und indirekten Verluste, Schäden und Kosten, die der GASAG-Gruppe entstehen, haftbar. Eine solche Haftung schließt jedoch weder andere Ansprüche aus noch stellt sie eine Außerkraftsetzung der GASAG-Gruppe per Gesetz oder anderweitig zustehender Rechte und Rechtsmittel dar.

Im Falle eines Sicherheitsvorfalls, der auf Fahrlässigkeit oder Nichtbefolgung der hier festgelegten Sicherheitsstandards zurückzuführen ist, haftet der Dienstleister für alle entstehenden direkten und indirekten Schäden.

16 Weitere Bestimmungen

Die vollständige oder teilweise Ungültigkeit von Punkten dieser Vertragsanlage beeinträchtigt nicht die Gültigkeit der anderen Punkte. Änderungen dieses Dokumentes sowie ergänzende Bestimmungen, einschließlich der in diesem Punkt festgelegten Anforderung, bedürfen der Schriftform; wobei Schriftform durch eine einfache beidseitige elektronische Signatur mittels DocuSign ersetzt werden kann.