

AGB-IT-BR – 06/2020

Besondere Bestimmungen zu Vertraulichkeit, Datenschutz und IT-Sicherheit im BR

Nachfolgende besondere Bestimmungen gelten ergänzend zu den AGB-BR für alle juristischen und natürlichen Personen einschließlich deren Erfüllungsgehilfen (nachfolgend: Auftragnehmer - AN -), die der BR (nachfolgend: Auftraggeber - AG -) im Rahmen einer vertraglichen Vereinbarung mit der Erbringung von Leistungen betraut. Der AN wird eigene Arbeitnehmer und sonstige Erfüllungsgehilfen in geeigneter Weise zur Einhaltung dieser Bestimmungen verpflichten und dies dem AG auf Verlangen nachweisen. Er haftet für alle Schäden in vollem Umfang, die dem AG durch Verletzung dieser Bestimmungen entstehen. Der AG kann geeignete Maßnahmen treffen, um die Einhaltung dieser Bestimmungen zu überwachen.

I. Vertraulichkeit

- Der AN wird die einschlägigen EU-rechtlichen, bundes- und landesrechtlichen Bestimmungen über den Datenschutz beachten. Er wird, soweit nicht vertraglich anderes verabredet ist,
 - die aus dem Bereich des AG erlangten Informationen über Geschäftsvorgänge vertraulich behandeln, nicht an Dritte weitergeben oder sonst verwerten und verwenden.
 - Aufzeichnungen von Informationen über Geschäftsvorgänge des AG unterlassen.
 - die erbrachten Leistungen und sonstigen Arbeitsergebnisse weder ganz noch teilweise in einer nicht oder nur unwesentlich veränderten Form weitergeben.
 - alle Kenntnisse darüber, dass und in welcher Weise die Leistungen und sonstigen Arbeitsergebnisse durch den AG genutzt werden, vertraulich behandeln.
- Die Pflicht zur Vertraulichkeit dauert auch nach Beendigung der Zusammenarbeit an.
- Der AN wird auf Verlangen des AG alle an ihn oder seine Erfüllungsgehilfen ausgehändigten Arbeitsunterlagen und Datenträger sowie sämtliche davon angefertigten Kopien zurückgeben bzw. nachweisbar vernichten.

II. IT-Sicherheit

Zur Gewährleistung der informationstechnischen Sicherheit in den Datennetzen des AG sind, soweit vertraglich nichts anderes vereinbart ist, vom AN die nachfolgenden Regelungen einzuhalten.

1. Allgemeine Pflichten

- Hard- und Software, Daten und Dienste des BR, sind nur für die mit dem BR vereinbarten Tätigkeiten zu nutzen. Die Nutzung für andere, z.B. private, Zwecke ist ausgeschlossen.
- Es sind ausschließlich die vom BR freigegebenen Kommunikationswege und Systeme zu nutzen. Diese sind ggf. vor Vertragsabschluss auf Eignung zu prüfen.
- Die Zugriffssicherungen, Passwörter und äquivalenten vertraulichen Daten und Lösungen sind geheim zu halten und nicht an Dritte weiterzugeben.
- Es sind alle Versuche zu unterlassen, über den Vertragsgegenstand hinausgehende Informationen über das Netzwerk sowie die Informationstechnik und die verwalteten Daten zu erhalten.
- Schwachstellen und IT-Sicherheitsvorfälle sind unverzüglich den zuständigen Stellen im BR anzuzeigen. Dies sind der/die Datenschutzbeauftragte und der/die IT- Sicherheitsbeauftragte oder dessen Vertreter, sowie die vertraglich benannten Ansprechpartner des AG.
- Der AN ist verpflichtet, die datenschutzrechtlichen Grundsätze nach Art. 5 DS-GVO zu beachten und ihre Einhaltung nachzuweisen. Insbesondere trifft er angemessene technische und organisatorische Maßnahmen auf dem Stand der Technik, um die Integrität, Verfügbarkeit und Vertraulichkeit von Informationen und personenbezogenen Daten sicherzustellen.

Der AN garantiert, dass die von ihm genutzten Systeme sowie alle Kommunikationsschnittstellen zum/vom BR, sicherheitstechnisch dem aktuellen Stand der Technik entsprechen und nach diesem betrieben werden. Insbesondere sichert der AN zu, den Zugang zum BR-Netzwerk und den Informationssystemen nur über Systeme herzustellen, die

- keine Schaden stiftende Software enthalten und diesbezüglich geprüft sind.
- einen aktuellen Sicherheitspatch-Stand entsprechend den Informationen der Anbieter der auf den Systemen verwendeten Softwareprodukte besitzen.

Weiterhin verpflichtet sich der AN dazu,

- einen aktiven und aktuellen Schutz vor Schadsoftware (Maleware, Viren etc.) verwenden.
- den Betrieb von AN-eigenen Geräten am BR-Netzwerk vorab dem AG rechtzeitig anzuzeigen und von der/dem IT-Sicherheitsbeauftragten eine Betriebsgenehmigung einzuholen.

Der/die Datenschutzbeauftragte und/oder der/die IT-Sicherheitsbeauftragte des BR und ggf. andere Beauftragte des AG sind berechtigt, zu den üblichen Geschäftszeiten unangemeldet den AN aufzusuchen, um sich über die Einhaltung der in diesem Vertrag festgelegten Verarbeitungsregelungen zu informieren und zu prüfen, ob den Belangen des Datenschutzes und/oder der IT-Sicherheit in ausreichendem Maße Rechnung getragen wird.

Vorsätzlich oder grob fahrlässig verursachte Verstöße gegen die Nutzungsbestimmungen und die Bestimmungen über den Datenschutz und die Datensicherheit können den sofortigen Entzug aller Berechtigungen, die Kündigung des Auftrages aus wichtigem Grund und eine Strafanzeige zur Folge haben.

Soweit dem AG durch derartige Verstöße Schäden verursacht werden, stehen ihm insoweit auch die gesetzlichen Schadensersatzansprüche zu.

2. Besondere Pflichten bei Zugriffen auf das Datennetz des BR über externe Kommunikationsmittel

Ist zur Leistungserbringung der Einsatz externer Kommunikationsmittel (Hard- und Softwarelösungen zur Verbindungsaufnahme, wie z. B. Modems, ISDN-Adapter, ISDN-Router, DSL-Anschlüsse o. ä.) im Datennetz des BR vereinbart, so gelten nachfolgende Vorgaben:

- Eine Verbindung über externe Kommunikationsmittel darf nur zur Erfüllung einer vertraglichen Vereinbarung hergestellt werden.
- Zur Herstellung von Verbindungen dürfen innerhalb des BR nur Kommunikationswege und -mittel eingesetzt werden, die vor der Auftragsvergabe vom AG geprüft und genehmigt worden sind.
- Externe Kommunikationswege und -mittel müssen Daten verschlüsselt übertragen und die eindeutige Autorisierung der Absenderadresse, in der Regel des externen Telekommunikationssystems, mit sich führen.
- Die Systemkonfiguration auf der AG-Seite erfolgt ausschließlich durch Administratoren des AG.
- Externe Zugriffe auf Systeme im BR-Netzwerk finden in der Regel WEB-basiert und verschlüsselt statt. Die Authentisierung am Zugangsportal erfolgt mittels vom AG bereitgestellter RSA - Secure Token. Der Systemadministrator des AG weist dem AN über diese Benutzeranmeldung definierte Zugriffsrechte zu. Passwörter dürfen durch den AN nicht abgespeichert oder weitergegeben werden.

3. Besondere Pflichten bei Einräumung administrativer Rechte

Sofern zur Leistungserbringung die Einräumung von Administratoren-, Superuser- oder Root-Rechten notwendig sind, wird der AN zudem sicherstellen, dass

- diese Zugriffe zeitlich auf ein Minimum begrenzt und ausschließlich im Rahmen und zum Zwecke der Leistungserbringung eingesetzt werden.
- nutzerbezogene Informationen (z.B. Protokolldaten) nur für betriebliche Zwecke im Rahmen der Leistungserbringung verwendet werden.
- Änderungen an BR-Systemen nur nach Rücksprache mit den verantwortlichen Stellen beim BR vorgenommen werden.

- Nutzerbezogene Protokolldaten** der IT-Systeme dürfen **ausschließlich** an den/die Datenschutzbeauftragte/n sowie den/die IT-Sicherheitsbeauftragte/n des BR und nur auf deren schriftliche Anforderung herausgegeben werden. Für den Fall, dass der AN im Rahmen einer **Auftragsdatenverarbeitung** personenbezogene Daten des BR verarbeitet, unterwirft er sich der Kontrolle des/der Datenschutzbeauftragten des BR