Allgemeine Geschäftsbedingungen der Volkswagen Group Retail Deutschland (VGRD GmbH) für InfoSec, Stand: 21.01.2026

1. Grundlagen

Anwendungsbereich dieser AGB sind sowohl die Lieferung von IT-Systemen (insb. jegliche Form von elektronischer Soft- und Hardware) als auch IT-Systeme von Lieferanten, die diese in der Zusammenarbeit mit dem Auftraggeber einsetzen. Neben diesen AGB für IT Systeme können weitere AGB des Auftraggebers zum Tragen kommen, sofern deren Anwendungsbereich gegeben ist.
Das IT-System entspricht zu jedem Zeitpunkt des Vertrages dem Stand der Technik und erfüllt alle rechtlichen Vorgaben. Die zur Vermeidung von Interessenkonflikten beim Informationssicherheitspersonal anerkannten Maßnahmen sind angemessen umzusetzen, z.B. personelle Trennung von Informationssicherheit und IT.
Rechte des Auftraggebers im Sinne dieser AGB berechtigen und schützen auch alle verbundenen Tochtergesellschaften der VGRD im Anwendungsbereich des Vertrages.

2. Sicherheit in der Informationstechnik

Konkret sind von Auftragnehmer folgende Maßnahmen zu ergreifen, um die Informationssicherheit adäquat zu sichern:

- In Projekten und aus Projekten resultierende Informationssicherheitsrisiken müssen systematisch identifiziert und behandelt werden.
- Schnittstellen der Anwendungen/Software sowie alle Informationen, die verarbeitet werden, müssen identifiziert, auf ihre Schutzbedürftigkeit hin bewertet, dokumentiert und getestet (Penetrationstest) werden.
- Angemessene, d.h. dem Schutzbedarf, und den regulatorischen Vorgaben entsprechende physische Sicherheitszonen (insbesondere für Server) und Maßnahmen (insb. Clean-Desk-Policy, Verschlüsselung / Sicherung von Endgeräten und Medien (u.a. Speichermedien), automatische Sperrung nach Inaktivitätszeiten, Drucken oder Nutzung sonstiger Geräte ohne Zugriffsbeschränkungen für Unberechtigte, Schutz vor unberechtigten Netzwerkzugriffen, Verzicht auf technische Benutzerkonten) sind zu definieren und entsprechend dem Stand der Technik einzusetzen.
- Notfallpläne sind vorzuhalten und jährlich zu testen.
- Netzwerke und Netzwerkdienste müssen angemessen überwacht werden. Es ist eine dem Stand der Technik entsprechend Segmentierung und TLS-Verschlüsselung und E-Mail Filterung sicherzustellen.
- Eine hinreichende Sicherheit, u.a. i.S. der Verarbeitung gem. Art. 32 DS-GVO, muss entsprechend dem Risiko der zu verarbeitenden Daten gewährleistet werden (z.B. durch Zertifizierung nach TISAX oder ISO 27001). Software-Schwachstellen müssen systematisch erkannt, unverzüglich beseitigt (Sicherheitsupdate) und an den Auftraggeber gemeldet werden. Dies gilt insbesondere für den Fall von IT-Sicherheitsvorfällen. In einem solchen Fall hat der Auftragnehmer den Auftraggeber bestmöglich zu unterstützen.
- Auf allen Geräten muss ein dem Stand der Technik entsprechender Viren - und Malwareschutz aktiviert sein und die Geräte müssen vor unbefugtem Zugriff geschützt werden. Aktuelle Geschehnisse sind durch zentrales Management analysieren.
- Der Zugang / Zugriff auf die Anwendung darf ausschließlich für geschulte Berechtigte gestattet sein und muss durch ein anerkanntes Authentisierungs-/und Authentifizierungsverfahren sichergestellt werden. Privilegierte Accounts (z.B. Admin) sind zu separieren.
- Passwörter, ihre Verwendung, Speicherung oder Änderungszyklen müssen dem jeweils aktuellen Stand der Technik entsprechen (z.B. Passwortempfehlungen des Bundesamtes für Sicherheit in der Informationstechnologie).
- Es ist eine dem aktuellen Stand der Technik entsprechende Verschlüsselung sämtlicher IT-Einrichtungen (inkl. WLAN) einzusetzen, die frei von bekannten Schwachstellen ist.
- Alle Schnittstellen müssen durch Authentifizierung geschützt werden.
- Die Anwendung/Software muss Eingabe-/Ausgabevalidierungsfunktionen bereitstellen und die Ausgabe detaillierter Systeminformationen an der Benutzeroberfläche verhindern.
- Schützenswerte Daten müssen insbesondere bei Übertragung über öffentliche Netze verschlüsselt übertragen werden mit Methoden, die dem Stand der Technik entsprechen.
- Der Auftragnehmer stellt dem Auftraggeber vor Beauftragung der Software eine Schwachstellenanalyse zur Verfügung und aktualisiert diese im Nutzungszeitraum regelmäßig. Eingaben in die Anwendung müssen geprüft werden, u.a. auf ausführbaren Code. Eine Software darf keine Ausgaben mit Bezug zum Systemaufbau, Produktnamen, Versionsnummern etc. an eine Benutzerschnittstelle vorsehen. Sofern für ein IT-System vor Vertragsschluss eine Schutzbedarfsanalyse vom Auftragnehmer an den zuständigen Fachbereich des Auftraggebers übermittelt wurde, gilt diese als vertraglicher Mindeststandard, insoweit sie strengere Anforderungen als diese IT AGB enthält.

3. Informationsklassifizierung

Elektronische Dokumente, Dokumente auf Papier oder Speichermedien müssen umfassend entsprechend ihrer Vertraulichkeit und inklusive Aufbewahrungsfrist gekennzeichnet werden. Daten des Auftraggebers oder Medien, die den Zugang zu diesen Daten ermöglichen (inkl. Benutzerinformationen), sind stets mindestens vertraulich zu behandeln, es sei denn dies wurde anderweitig vereinbart.
Es muss ein automatisiertes Berechtigungskonzept (z.B. Benutzerrollen, Rechte, Änderungen) umgesetzt werden, mit dem das „need-to-know" Prinzip sichergestellt wird, bzw. werden kann. Administrative / höherwertige Rechte und Rollen sind auf das notwendige Minimum zu beschränken. Die autorisierten Personen müssen vor Zugriff auf die Daten auf die jeweilige Vertraulichkeit verpflichtet werden. Es müssen Prozesse für Eintritt, Austritt und Wechsel von Mitarbeitern vorhanden sein, die eine aktuelle und zutreffend Berechtigung des Mitarbeiters gewährleisten.
Das Erstellen von Kopien von Informationen muss vom Informationsbesitzer genehmigt werden und das elektronische Kopieren von Informationen müssen vom Informationseigentümer genehmigt werden.

4. Entwicklung

Der Einsatz von Entwicklungswerkzeugen, Test- und Standardbenutzerkonten sind in Produktivsystemen untersagt. Jede (Weiter-)Entwicklung (z.B. update) einer Anwendung muss im Rahmen des Change-Managements vor Umsetzung vom Auftraggeber schriftlich freigegeben werden und den anerkannten technischen Standards und Codierungsnormen entsprechen. Verwendete Testsysteme mit Produktivdaten müssen den Anforderungen der Produktivumgebung für jede Anwendung mindestens entsprechen. Der Auftragnehmer hat dem Auftraggeber alle zur Prüfung erforderlichen Unterlagen zur Verfügung zu stellen.

5. Datensicherung

Für jede Anwendung/Software muss ein dokumentiertes Datensicherungskonzept erstellt und umgesetzt werden (Backup-Zeitplan/-Intervalle; Art und Speicherung des Backups; regelmäßige Restaurierungstests; Logfile-Dokumentation). Dies umfasst auch mobile Endgeräte,

Cloud Anwendungen, Druck- und Exportfunktionen sowie alle Accountänderungen und System Events (z.B. fehlgeschlagene Logins und administrative Änderungen).

6. Datenschutz

Datenschutzhinweise zur Erfüllung der datenschutzrechtlichen Informationspflichten müssen für alle Gesellschaften im Anwendungsbereich des Vertrags (d.h. konzernverbundene Gesellschaften der VGRD-Gruppe) eingebunden und einfach für den Betroffenen abrufbar sein.
Es gelten die Grundsätze der Datenminimierung und Datensparsamkeit (Privacy by Design/ Privacy by Default).
Der Auftragnehmer hat sicherzustellen, dass für jede Verarbeitung von personenbezogenen Daten im Zusammenhang mit den Vertragsverhältnis zum Auftraggeber ein Rechtsgrund existiert.
Rechtlich unzulässige Verarbeitungen personenbezogener Daten haben zu unterbleiben. Jede zulässige Verarbeitung muss vorab ins Verarbeitungsverzeichnis der VGRD aufgenommen werden. Dafür sind dem VGRD Datenschutz alle nach DS-GVO erforderlichen Angaben rechtzeitig vor Auftragserteilung dem Datenschutzbeauftragten mitzuteilen. Im Falle einer erforderlichen Datenschutzfolgeabschätzung (**DSFA**) hat der Auftragnehmer den Auftraggeber dabei zu unterstützen.
Die Anwendung/Software muss durch geeignete Technikgestaltung das Trennungsgebot der DS-GVO umsetzen und über eine Mandantentrennung verfügen.
Beim Rechtsgrund „Einwilligung" muss diese für 5 Jahre nach Beendigung der auf diesen Rechtsgrund gestützten Verarbeitung (bzw. nach erteiltem Widerruf) revisionssicher dokumentiert werden. Ggf. muss sichergestellt werden, dass bei Datenverarbeitungen Minderjähriger die Einwilligung ihrer Erziehungsberechtigten eingeholt wird. Eine Applikation / Software, die sich auf diesen Rechtsgrund stützt, muss entsprechende Funktionalitäten zur Verfügung stellen.
Die Anwendung/Software muss die Umsetzung der Betroffenenrechte gemäß DS-GVO sicherstellen (d.h. Auskunft/Löschen/Berichtigen/Einschränken der Verarbeitung/ Datenportabilität). Entsprechende Konzepte sind dem Auftraggeber vom Auftragnehmer vorzulegen. Auf Verlangen sind diese anzupassen, soweit dies zur Erfüllung gesetzlicher Vorgaben zweckmäßig ist.
Nach Entfall des Verarbeitungszweckes / Entfall der Rechtsgrundlage muss nach konkreter Vorgabe eine Löschung oder Rückgabe der Daten erfolgen. Daten, die für einen bestimmten Zweck erhoben worden sind, dürfen nicht für andere Zwecke verarbeitet werden (Prinzip der Nichtverkettung).
Die Verarbeitung der Daten erfolgt im Europäischen Wirtschaftsraum (EWR). Abweichungen hiervon bedürfen der Zustimmung des Auftraggebers und es sind die rechtlichen Vorgaben zum Drittstaatentransfer in ihrer jeweils gültigen Form anzuwenden.

7. Dritte

Outsourcing, d.h. der Einsatz Dritter ist nur nach schriftlicher Zustimmung des Auftraggebers zulässig. Die Zustimmung darf nicht unbillig verweigert werden. Bei der Auslagerung der Informationsverarbeitung muss die Einhaltung der in diesem Dokument enthaltenen Anforderungen durch den Outsourcing-Partner Teil des Outsourcing-Vertrags sein. Im Übrigen sind im Outsourcing Vertrag die Verfügbarkeit von Informationen sowie mögliche Szenarien zu regeln (d.h. Normalbetrieb, Notfälle, Krisen und Katastrophen). Sofern in die Software/Applikation Technologien Dritter eingebunden sind (z.B. Cookies), ist der Auftragnehmer verpflichtet, deren Rechtmäßigkeit nachzuweisen und den datenschutzkonformen Einsatz durch den Auftraggeber sicherzustellen (insb. Informationspflichten). Die Einhaltung der zu vereinbarenden Vorgaben ist risikoangemessen zu kontrollieren.

8. Info-Sec und Datenschutzorganisation

Der Auftragnehmer muss eine angemessene Datenschutz- und Informationssicherheitsorganisation mit nachweislich qualifiziertem Personal vorhalten und in relevante Prozesse und Projekte im Zusammenhang mit der Software/Applikation maßgeblich einbinden. Der Aufbau der Organisationen muss, u.a. tone-from-the-top, kommuniziert sein. Mitarbeiter und Externe sind regelmäßig zu Datenschutz- und Informationssicherheit zu schulen.
Abstimmungen und Absprachen zu Datenschutz (inkl. Datenschutzbeauftragter) oder Informationssicherheit werden nicht gesondert berechnet.

9. Dokumentation

Umzusetzende Maßnahmen für die IT-Sicherheit und Datenschutz sind zu dokumentieren und dem Auftraggeber auf Verlangen (ggf. durch ein Audit) nachzuweisen. Hierzu gehören insbesondere:

- Alle IT-Netzwerke, Netzwerkdienste und Geräte, die für die Informationsverarbeitung genutzt werden, müssen systematisch dokumentiert und wenigstens jährlich kontrolliert werden.
- Jegliche administrative Datenzugriffe, Berechtigungen, Rollen, Verfahren der Datenverarbeitung, Wiederherstellung von Sicherungen, Aufbewahrungsfristen für Protokolle sowie der Überführungsprozess von Produktivdaten in nicht-produktive Systeme. Es muss ein dokumentiertes Verfahren für die Gewährung und den Widerruf des Zugangs zu Netzen und Netzwerkdiensten sowie für Sicherheitsupdates eingerichtet werden.
- Die Anforderungen nach diesem Vertrag und die in diesen IT-AGB enthaltenen Vorgaben.
- Monitoring und Logging entsprechend dem Stand der Technik.

Die Dokumentation von Verschlüsselungsalgorithmen umfasst Prozesse zur Erstellung, Speicherung, Archivierung, Zugriff, Verteilung, Deaktivierung und Löschung von Schlüsseln.

10. Anwendbarkeit von Auftragsverarbeitungsvertrag (AVV) und Geheimhaltungsvereinbarung (GHV)

Weitergehende Regelungen in einem Auftragsverarbeitungsvertrag (AVV) oder einer Geheimhaltungsvereinbarung (GHV) haben Vorrang von diesen AGB, die einen Mindeststandard darstellen. Sofern der Auftragnehmer Datenverarbeiter im Sinne der DS-GVO ist, hat dieser vorab eine AVV gemäß dem Standard der VGRD abzuschließen. Im Übrigen ist eine entsprechende Geheimhaltungsvereinbarung (GHV) zu vereinbaren.

11. Rechte

Der Auftragnehmer stellt sicher, dass beim Einsatz eines IT-Systems keine Rechte Dritter an dem IT-System oder Teilen des Systems bestehen und dass der Auftraggeber das IT-System uneingeschränkt nutzen kann.

12. IT-Service Level

Sofern kein weitergehendes Servicelevel vereinbart ist, stellt der Lieferant eines IT-Systems mindestens die Verfügbarkeit seines Services an Werktagen, d.h. von Montag bis Samstag, von 07:00 bis 18:00 Uhr sicher.