Anlage

Datenschutz TOMs GS DTM

adesso ISMS

Dok. Nr.:	AL_002
Version:	1.4
Status:	freigegeben
Datum:	10.12.2019
Einstufung:	intern
Bereich:	Datenschutz
Autor / Autoren:	Julius Hüttmann
Zielgruppe:	adesso Kunden
Geltungsbereich:	adesso SE
Dateiname:	AL-002_Datenschutz_TOMs_Dortmund
Dokumentvorlage:	Dokumentvorlage_530_Standarddokument

adesso SE
Adessoplatz 1
44269 Dortmund
Telefon +49 231 7000-7000
Telefax +49 231 7000-1000
info@adesso.de
www.adesso.de

Dokumenthistorie

Version	Datum	Autor/-en	Kommentare/ Status
1.0	15.12.2015	Julius Hüttmann	Freigegeben durch DSB
1.1	13.07.2016	Julius Hüttmann	Freigegeben durch DSB
1.2	07.06.2018	Nils Quermann	Freigegeben durch DSB
1.3	25.01.2019	Inessa Azizova	Freigegeben durch DSB
1.4	10.12.2019	Inessa Azizova	Freigegeben durch DSB

Review

Version	Datum	Durchgeführt von	Kommentar
1.0	28.04.2016	Julius Hüttmann	Version 1.1 erstellt
1.1	07.06.2018	Nils Quermann, Sascha Winekenstädde	Version 1.2 erstellt, Anpassung an die DS-GVO
1.2	25.01.2019	Inessa Azizova	Version 1.3 erstellt, kleine formale und inhaltliche Anpassungen
1.3	10.12.2019	Inessa Azizova	Version 1.4 erstellt, Rechtsform-wechsel
1.4	23.08.2022	Julius Hüttmann	Prüfung der Angaben auf Aktualität

Aktualität

Das Dokument wurde letztmalig am 23.08.2022 auf seine Richtigkeit und Aktualität überprüft.

Datenschutzbeauftragter der adesso SE

Julius Hüttmann
Adessoplatz 1
44269 Dortmund
T: +49 231 7000 2280
E: huettmann@adesso.de

Inhaltsverzeichnis

1 Technische und organisatorische Maßnahmen

Das oberste Ziel unserer Informationssicherheitsstrategie ist es, die Verfügbarkeit, Vertraulichkeit und Integrität von eigenen oder anvertrauten Informationen im jeweils erforderlichen Maß nachweislich zu schützen.

Alle hierfür relevanten Prozesse im Unternehmen sind definiert, sowie geregelt und nachvollziehbar umgesetzt. Die Umsetzung wird überwacht. Bei all dem ist berücksichtigt, dass alle Prozesse dem Spannungsverhältnis zwischen Sicherheit, Handlungsfähigkeit und Wirtschaftlichkeit ausgesetzt sind. Bei der Konzeption, Umsetzung und Überwachung von Prozessen haben wir daher stets darauf geachtet, dass, gemessen an den tatsächlich bestehenden Risiken, die Angemessenheit gewahrt bleibt.

Innerhalb der adesso gibt es eine Reihe von Grundsätzen sowie Ziele, die die Umsetzung der technischen und organisatorischen Maßnahmen betreffen. Außerdem gibt es generelle organisatorische Maßnahmen um bei der adesso den Datenschutz und die Informationssicherheit zu gewährleisten.

Grundsätze

Es gelten folgende Grundsätze:

- **Informationssicherheit ist eine Leitungsaufgabe und geht vom Management aus**. Aufbau, Aufrechterhaltung und Fortentwicklung von geeigneten Sicherheitsverfahren und -systemen wird durch den Vorstand aktiv unterstützt und ggf. durchgesetzt.
- Dem Management ist bewusst, dass sich ein angemessenes Sicherheitsniveau nur mit angemessenem Einsatz **personeller, zeitlicher und finanzieller Ressourcen** herstellen und aufrechterhalten lässt.
- Absolute Sicherheit ist nicht realisierbar. Viele Risiken lassen sich bei sachgemäßer Handhabung und Organisation aber minimieren oder beherrschen. **Gesetzliche, vertragliche und aufsichtsrechtliche Verpflichtungen sind immer zu erfüllen**. Sie definieren das Mindestniveau, welches im Unternehmen zu erreichen ist.
- Zur gesteuerten Erreichung unserer Ziele sind **definierte Prozesse** implementiert. Die Einhaltung der Prozesse und der Erfolg von Maßnahmen werden regelmäßig geprüft. Festgestellte Abweichungen werden behoben. Die **Wirksamkeit von Prozessen und Maßnahmen** ist auch unter sich verändernden Rahmenbedingungen sichergestellt. Notwendige Anpassungen werden zeitnah umgesetzt.
- Eine **angemessene Dokumentation** wird geführt. Zum einen sind gesetzliche und vertragliche Anforderungen zu erfüllen. Zum anderen dient die Dokumentation auch dem Nachweis unserer eigenen Bemühungen um Informationssicherheit und ist für Zertifizierungen notwendig.

- **Qualifiziertes Personal** ist einer der Schlüssel zu einer erfolgreichen Informationssicherheit. Es ist sichergestellt, dass alle Mitarbeiter die zur Erfüllung Ihrer Aufgaben sowohl die notwendigen Kenntnisse als auch die erforderliche Zuverlässigkeit besitzen. Es werden Fortbildungsmaßnahmen sowie eine ständige Sensibilisierung des eingesetzten Personals eingesetzt.
- **Informationssicherheit ist eine Gemeinschaftsaufgabe**, die von allen Mitarbeitern wahrgenommen werden muss. Dennoch ist unverzichtbar, dass **klare Verantwortlichkeiten und Befugnisse** zugewiesen sind. Für jeden Prozess ist festgelegt, wer die Umsetzungsverantwortung trägt, wer ggf. zu beteiligen oder zu informieren ist. Unverträglichkeiten zwischen Rollen sind zwingend zu vermeiden.
- Der Vorstand kann seiner Verantwortung dauerhaft nur nachkommen, wenn ein **angemessenes Berichtswesen** besteht. Das Management wird daher in angemessenen Abständen über Stand und Erfolg der Bemühungen zur Informationssicherheit informiert und bezieht diese Berichte in die Fortentwicklung der Unternehmensstrategie mit ein.

Ziele

Folgende Ziele dienen der Erfüllung der Anforderungen zur Verarbeitung personenbezogener Daten:

- Die gesamte Datenverarbeitung erfolgt **rechtmäßig, nach Treu und Glauben und transparent**. Das Unternehmen verarbeitet Daten nur innerhalb der gesetzlichen Grenzen und unter Beachtung bestehender Anforderungen. Dabei werden insbesondere die Interessen und Erwartungen betroffener Personen beachtet und ist diesen verständlich und nachvollziehbar dargestellt.
- Personenbezogene Daten werden nur für zulässige und eindeutig festgelegte Zwecke und unter Beachtung des Gebots der **Datenminimierung** verarbeitet. Die Verwendung von personenbezogenen Daten erfolgt nur soweit dies angemessen und erforderlich ist.
- Es werden angemessene Maßnahmen getroffen, um die **Richtigkeit** personenbezogener Daten zu gewährleisten. Sobald beim Umgang mit solchen Daten bekannt wird, dass diese nicht richtig oder nicht aktuell sind, werden diese Daten korrigiert oder gelöscht.
- Die **Speicherung personenbezogener Daten wird begrenzt**. Sie werden nur solange gespeichert wie es erforderlich oder gesetzlich geboten ist.

1.1 Generelle organisatorische Maßnahmen

- Bestellung eines Datenschutzbeauftragten (DSB)
- Bestellung eines Beauftragten für Informationssicherheit (CISO)
- Funktionstrennung zwischen Fachabteilungen und Technikabteilungen
- Zentrale Beschaffung von Hard- und Software
- Vorgaben in Richtlinien, Prozessbeschreibungen, Arbeitsanweisungen, Verfahrensbeschreibungen
- Die folgenden Richtlinien der adesso SE schaffen, neben weiteren Richtlinien, einen verbindlichen Rahmen zur Sicherstellung einer wirksamen Zutritts-, Zugangs- und Zugriffskontrolle:

Zutritt, Zugang, Zugriff	RL-007
Kryptographie	RL-008
Mobiler Arbeitsplatz	RL-009
Passwörter	RL-010
Mobile Endgeräte und Datenträger	RL-011
Entsorgung und Vernichtung	RL-012
Clean Desk, Clear Screen	RL-013

- Verpflichtung aller Mitarbeiter zum Datenschutz, zur Informationssicherheit und zur Geheimhaltung, sowie weiteren gesetzlichen Anforderungen (bspw. TKG, SGB, StGB)
  - > Es existieren interne Richtlinien/ Regelungen (z.B. zur Nutzung von E-Mail, Telefon und Internet)
- Regelmäßige Schulung aller Mitarbeiter
- Vorgaben für Verfahrensdokumentation
- Regelmäßige Überprüfung der Maßnahmen in internen Audits
- Allgemeines Notfallkonzept / Notfallhandbuch
- Backup- / Wiederherstellungskonzept

2 Einzelmaßnahmen

Im Folgenden werden die Ziele der technischen und organisatorischen Maßnahmen, in den Kategorien Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit sowie das Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung der Wirksamkeit der technischen und organisatorischen Maßnahmen zur Gewährleistung der Sicherheit der Verarbeitung erläutert.

Jeder dieser Kategorien sind jeweils mehrere Maßnahmen zugeordnet, die sicherstellen, dass das jeweilige Schutzziel erreicht wird.

Die Umsetzung der Maßnahmen ist am aktuellen Stand der Technik orientiert.

2.1 Vertraulichkeit

Ziel der Vertraulichkeit ist es, dass Unbefugte keine Kenntnis von (personenbezogenen) Daten erlangen. Die Erreichung dieses Zieles wird durch die nachfolgenden Maßnahmen sichergestellt.

2.1.1 Zutrittskontrolle

Ziel der Zutrittskontrolle ist es, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren:

Außensicherung:

- Alle Türen sind geschlossen und der Zutritt ist nur mit Zutrittsberechtigung bzw. in Begleitung eines Mitarbeiters der adesso möglich.
- Das Bürogebäude verfügt über alarmgesicherte Eingänge; Zugänge zu relevanten Gebäudeabschnitten sind alarmgesichert.
- Die Außenhaut des Gebäudes sowie die Eingänge sind videoüberwacht.
- Ein Wachdienst ist beauftragt und wird bei Auslösung der Alarmanlage benachrichtigt.

Schließanlage:

- Der Standort ist mit mechanischen / elektronischen Schließsystemen ausgestattet.
- Die Ausgabe neuer oder ersatzweiser Token / Karten / Schlüssel (im folgendem als Schlüssel bezeichnet) erfolgt grundsätzlich durch den Standortverantwortlichen. Die Erstellung / Beschaffung neuer Schlüssel und die Pflege der Zutrittsberechtigungen obliegen einem autorisierten Mitarbeiter (Standortverantwortlicher) an einem gesicherten Arbeitsplatz.
- Eine Überprüfung der Zutrittsberechtigung erfolgt regelmäßig, mindestens einmal jährlich, durch den Standortverantwortlichen, der Datenschutzbeauftragte überprüft dies stichprobenartig.
- Eine Überprüfung bei Räumen mit erhöhtem Schutzbedarf (Archive, Technikräume) wird zusätzlich einmal jährlich durch den DSB durchgeführt.
- Der Verlust eines Schlüssels wird sofort nach Kenntnisnahme bei dem Standortverantwortlichen angezeigt.
- Türen zu Sicherheitsbereichen verfügen über einen Knauf an der Außenseite, es sei denn, Vorschriften z.B. bzgl. Fluchtwegen, untersagen dies.
- Die Zutrittsberechtigungen werden enstprechend bestehender Richtlinien vergeben.

Technikraum:

- Technische Einrichtungen, die regelmäßig gewartet werden müssen (wie z.B. Telefonanlagen), sind in einem eigenen Technikraum installiert.
- Der Zutritt ist auf wenige interne Mitarbeiter begrenzt.

Inventur der Schlüssel:

Regelmäßige (mind. einmal jährlich) Inventur der ausgegebenen Schlüssel, Token und Zutrittsberechtigungen.

Besucherregelungen:

- Während den Geschäftszeiten haben Besucher nur nach Anmeldung und in Begleitung des besuchten Mitarbeiters Zugang zu den Büroräumen.
- Es wird ein elektronischer Nachweis zu Besuchern geführt.
- Der Besucher wird während des gesamten Aufenthaltes ständig durch den Besuchten oder seinen Vertreter begleitet, er erhält nur zu den Bereichen Zutritt, die für die Erledigung seiner Aufgaben notwendig sind (Ausnahme Empfangs- und Konferenzbereich).
- Unbekannte Personen ohne Begleitung werden von den Mitarbeitern der adesso angesprochen und ihr rechtmäßiger Aufenthalt überprüft. Dies gilt auch für Personen, die sich als Mitarbeiter ausgeben, aber nicht bekannt sind.
- Besucher und Externe in Funktionsausübung (wie z.B. Wartungstechniker, DS- und QM-Beauftragte) werden in den Technikraum begleitet.

2.1.2 Zugangskontrolle

Ziel der Zugangskontrolle ist es, zu verhindern, dass die Datenverarbeitungssysteme von Unbefugten genutzt werden können:

- Durch Zugangsregelungen, Benutzerkennungen, Passwörter und Zugriffsregelungen ist der Zugang auf Datenverarbeitungssysteme gesichert.
- Die Userpasswortlänge beträgt mindestens 10 Zeichen.
- Die Administratorpasswortlänge beträgt mindestens 12 Zeichen.
- Passwörter bestehen zwingend aus Großbuchstaben, Kleinbuchstaben, Ziffern oder Sonderzeichen, auszuschließen sind Trivialkennwörter, wie Benutzernamen, Wörtern in Wortlisten, fortlaufenden identische Zeichen.
- Dienstliche Passwörter dürfen nicht privat genutzt werden und umgekehrt.
- Passwörter sind streng vertraulich zu behandeln und nur von dem dazugehörigen User zu verwenden und werden bei Verdacht auf Kompromittierung unverzüglich geändert werden.
- Passwörter sind alle 365 Tage zu aktualisieren.
- Sichere Übermittlung des Initialpasswortes und direkte Änderung bei Erstanmeldung durch User.

- Arbeitsplatzrechner sind mit einem Bios Passwort ausgestattet.
- Automatische Bildschirmsperre nach 15 Minuten.
- Bildschirmschoner mit Kennworteingabe bei Reaktivierung.
- Es werden nur in Abstimmung mit dem Auftraggeber gesicherte Übertragungswege wie VPN-Verbindungen verwendet.
- Regelmäßige technische Prüfungen der im Netzwerk angeschlossenen Geräte auf Schwachstellen und Sicherheitslücken.

2.1.3 Zugriffskontrolle

Ziel der Zugriffskontrolle ist es, zu gewährleisten, dass die zur Benutzung eines Datenverarbeitungs-systems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegende Daten zugreifen können:

- Jeder Mitarbeiter achtet darauf, dass alle Dokumente und Datenträger, die schutzbedürftige Daten, wie sonstige personenbezogene oder personenbeziehbare Daten, Poststücke oder Bearbeitungslisten, enthalten, vor unberechtigtem Zugriff geschützt sind, d.h. das diese während der Arbeitszeit nicht frei einsehbar sind und nach Verlassen seines Arbeitsplatzes zugriffssicher verstaut werden (abschließbarer Schrank, etc.).
- Zugriffsberechtigungen werden aufgrund benutzerbezogener Rollen bzw. Konten erteilt.
- Durch Rollenkonzepte und Benutzerkennungen, Passwörter und Zugriffsregelungen ist der Zugriff auf entsprechende Datenbereiche gesichert.
- Zugriff auf Daten des Videosystems sind nur für berechtigte und eingetragene Nutzer des Dienstleister auf Anforderung der adesso aus möglich. Jeder Zugriff wird dafür protokolliert.
- Zugriff auf Daten des Videosystems und Zugangssystem der adesso sind nur für berechtigte und eingetragene Nutzer auf Anforderung des DSB möglich.
- Echtzeitprotokollierung der sicherheitsrelevanten Ereignisse.
- Anwendung des Vier-Augen-Prinzips beim Zugriff auf hochsensible Systeme (z.B. ERP Produktivsysteme).
- Schützenswerte Daten werden in verschlüsselter Form gespeichert.
- Es existieren Regelungen zum Umgang mit Massenspeichern (USB-Peripherie)
- Fotografieren ist generell verboten, Ausnahmen müssen vom DSB genehmigt werden.
- Die adesso ist mit einem Firewall System ausgestattet. Hierbei wird eine Filterung aufgrund von IP Adressen und Ports durchgeführt.
- Vertrauliche Dokumente werden in einer Datenschutztonne gesammelt und von einem Dienstleister datenschutzgerecht entsorgt. Die Entsorgung des Tonneninhaltes wird durch den Dienstleister bestätigt. Die Entsorgung erfolgt nach DIN 66399.

2.1.4 Trennungskontrolle

Ziel der Trennungskontrolle ist es, zu gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten grundsätzlich auch getrennt verarbeitet werden können. Eine Zusammenführung dieser Daten ist unzulässig, soweit dies nicht für die Erfüllung einer gesetzlichen Aufgabe erforderlich ist:

- Es bestehen nur Verarbeitungen für Kunden, mit denen vertragliche Regelungen über die Verarbeitung existieren.
- Die temporäre und dauerhafte Speicherung der Verarbeitungsdateien erfolgt mindestens in einer logischen Trennung zur weiteren Datenverarbeitung.
- Eine dauerhafte Datenhaltung am Standort erfolgt nur nach vertraglicher Regelung mit dem Auftraggeber.
- personenbezogene Daten sind in allen Stufen (Rohdaten, Produktionsdaten, Backup-Daten) physisch von anderen personenbezogenen Daten getrennt.

2.1.5 Pseudonymisierung

Ziel der Pseudonymisierung ist es, dass die Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, wobei diese zusätzlichen Informationen gesondert aufbewahrt werden und entsprechenden technischen und organisatorischen Maßnahmen unterliegen.

- Im Auftragskontext der zugrundeliegenden AV anfallende Daten mit Personenbezug werden nach Vereinbarung mit dem Kunden pseudonymisiert.

2.2 Integrität

Ziel der Integrität ist es, dass (personenbezogenen) Daten im Nachhinein nicht unbemerkt manipuliert oder gelöscht werden können. Die Erreichung dieses Zieles wird durch die nachfolgenden Maßnahmen sichergestellt.

2.2.1 Weitergabekontrolle

Maßnahmen um zu gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträgern nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können (Weitergabekontrolle):

- Daten werden mit anerkannten Verschlüsselungslogarithmen (AES-256) nach Abstimmung mit der beauftragenden Stelle verschlüsselt.

- E-Mail-Versand findet nach Abstimmung in verschlüsselter Form statt. Hierbei kommen wahlweise verschlüsselte ZIP-Files (AES-256) oder PGP bzw. S/MIME zum Einsatz.
- Datenträger werden durch einen Dienstleister datenschutzgerecht entsorgt.
- Sicherheitsverfahren werden regelmäßig kontrolliert.
- Alle Datenübertragungen werden protokolliert.
- Der Zugriff auf Druckdaten wird auf ein Minimum begrenzt. Zusätzlich werden nicht ausgeführte Druckaufträge zeitgesteuert gelöscht.

2.2.2 Eingabekontrolle

Maßnahmen um zu gewährleisten, dass nachträglich überprüft und erstgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind (Eingabekontrolle):

- Alle Dateizugriffe werden auf Benutzerebene protokolliert.
- Sicherheitsrelevanter Belange werden im Vier-Augen-Prinzip administriert.
- Bei Bedarf wird der Log-Level und die Aufbewahrungsfristen mit dem Kunden individuelle vereinbart.

2.3 Verfügbarkeit und Belastbarkeit

Ziel von Verfügbarkeit und Belastbarkeit ist es, sicherzustellen das die personenbezogenen Daten allzeit Verfügbar sind bzw. sich im Falle einer Störung die Daten schnell wieder zur Verfügung stehen.

2.3.1 Verfügbarkeitskontrolle

Ziel der Verfügbarkeitskontrolle ist es, zu gewährleisten, dass personenbezogene Datengegen vor einer zufälligen Zerstörung oder Verlust geschützt sind:

- Der Schutz vor Schadsoftware wird auf verschiedenen Ebenen (Client, Server, Gateway, etc.) umgesetzt, dabei werden Produkte von unterschiedlichen Herstellern eingesetzt.
- Ein Notfallkonzept zum Schutz vor elementaren Gefährdungen wie zum Beispiel Umwelteinflüsse oder höhere Gewalt wird umgesetzt. Die Wirksamkeit des Notfallkonzepts wird regelmäßig überprüft.
- Kritische IT-Infrastruktur, Server und Dienste sind redundant und / oder hochverfügbar ausgelegt.
- In IT-Räumen werden die Temperatur und die Luftfeuchtigkeit überwacht.
- Die das RZ betreffenden Maßnahmen sind den TOMs für das Rechenzentrum der adesso SE zu entnehmen.

2.3.2 Rasche Wiederherstellbarkeit

Ziel der raschen Wiederherstellbarkeit ist es, dass im Falle einer Störung sämtliche Daten ohne Beeinträchtigung des Betriebs wiederhergestellt werden:

- Es existiert ein mehrstufiges Backupkonzept; alle Server werden mindestens werktäglich gesichert, kritische Systeme täglich.
- Die Wiederherstellung wird regelmäßig getestet.

2.4 Überprüfung, Bewertung und Evaluierung

Ziel der Verfahren zur regelmäßigen Überprüfung, Bewertung und Evaluierung ist es, den Nachweis erbringen zu können, dass die umgesetzten Maßnahmen den Anforderungen der DS-GVO gerecht werden.

2.4.1 Datenschutz-Management

Ziel eines Datenschutz-Managements ist die Dokumentierungs- und Nachweispflicht im Hinblick auf die Rechenschaftspflicht (Accountability) der DS-GVO.

- Es finden regelmässige interne Audits statt.
- Das ISM-Team bespricht regelmäßig aktuelle Themen.
- Die Geschäftsstelle wurde nach ISO/IEC 27001 zertifiziert.

2.4.2 Incident-Response-Management

Ziel des Incident-Response-Management ist es, einen schriftliche Anweisungen zu haben, wie mit einem Datenschutzvorfall umgegangen werden soll und wie ein solcher frühzeitig entdeckt werden kann.

Es existiert ein Meldeweg und Verhaltensregeln für relevante Gruppen sowie ein Meldeformular für Datenschutzvorfälle, um geeignet auf Datenschutzvorfälle reagieren zu können. Die gemeldeten Vorfälle werden durch ein Ticketsystem durch das ISM-Team bearbeitet.

2.4.3 Datenschutzfreundliche Voreinstellungen

Ziel von Datenschutzfreindlichen Voreinstellungen ist es, dass bereits die Werkeinstellungen das größtmögliche Maß an Datenschutz für die betroffene Person bieten.

Es werden die Prinzipien „privacy by design“ und „privacy by default“ beachtet. Daher wird

- die Entwicklung von Software durch Vorgaben zur Umsetzung des Datenschutzes und der Datensicherheit geregelt
- und Webseiten mit datenschutzfreundlichen Voreinstellungen betrieben.

2.4.4 Auftragskontrolle

Ziel der Auftragskontrolle ist es, zu gewährleisten, dass Sozialdaten, die im Auftrag erhoben, verarbeitet oder genutzt werden, nur entsprechend den Weisungen des Auftraggebers erhoben, verarbeitet oder genutzt werden können:

- Zusätzliche Vereinbarungen mit Auftraggebern werden in Datenschutzvereinbarungen, in Datenfreigabeerklärungen sowie ggf. in Verfahrensbeschreibungen getroffen.
- Lieferanten werden durch den DSB einer Datenschutzprüfung unterzogen.
- Administration von hochsensiblen Systemen erfolgt im Vier-Augen-Prinzip.
- Bei Bedarf wird der Log-Level und die Aufbewahrungsfristen mit dem Kunden individuell vereinbart.

Die Auftragskontrolle schließt die Maßnahmen mit ein, die bei der Vergabe eines Unterauftrages durchgeführt werden.