Sicherheitskonzept

Datensicherheit bei der AEB SE

Technische und organisatorische Maßnahmen / Controls

30.04.2019

www.aeb.com

Inhalt

1 Grundsätzliches zum Dokument

Dieses Dokument führt alle Sicherheits-Kontrollsysteme der Services der AEB SE auf.

Die Maßnahmen können sowohl technischer als auch organisatorischer Natur sein. Sie sind auf dem **Stand der Technik** und schließen auch den Faktor Mensch mit ein.

AEB ist berechtigt, die erforderlichen Maßnahmen anzupassen, sofern das bisher erreichte Sicherheitsniveau nicht unterschritten wird. Die hier dargestellten Maßnahmen sind - wenn nicht anders vereinbart - übergreifend im Sinne für alle Kunden gleich ausgelegt.

Dieses Dokument ist mit Angabe des Datums (Stand) versioniert.

1.1 Verwendungszweck Datenschutz

Nach geltenden Gesetzen (z.B. die EU-Datenschutz-Grundverordnung mit Art. 32 DS-GVO) sind geeignete **technische und organisatorische Maßnahmen** zu wählen, die dem erforderlichen Schutzbedarf der (personenbezogenen) Daten entsprechend den gesetzlichen Anforderungen genügen. Erforderlich sind Maßnahmen nur, soweit ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.

1.2 Verwendungszweck Security / Informationssicherheit

Dieses Dokument stellt den Stand der AEB-Sicherheitsmaßnahmen und -prinzipien dar. Diese werden als Minimal-Anforderungen Bestandteil eines Vertrags (Aufgrund AGB oder SLA) der AEB.

1.3 Verwendungszweck SOX Compliance

Aufgrund der Anforderungen an Service Provider, die vor allem im Abschnitt 404 des Sarbanes-Oxley Acts (SOX) formuliert sind, sollen ausgelagerte Compliance-relevante Aufgaben eines Unternehmens, das dem SOX unterliegt, auch geprüft werden.

Um diese Überprüfung zu vereinfachen, gibt es die Möglichkeit, einen Bericht über die ausgelagerten Services erstellen zu lassen. In diesem Report beschreibt der Service Provider selbst sein internes Kontrollsystem (Datenschutz, Datensicherheit, Zugriffssicherheit, Datenintegrität…). Dieses Kontrollsystem muss angemessen ausgestaltet sein, um die angegebenen Ziele zu erreichen. Und es muss vollständig implementiert sein. Die Relevanz kann von einem externen Prüfer bescheinigt werden.

Weitere Hinweise dazu:

- **SSAE16** (Statement on Standards for Attestation Engagements No. 16) mit Bezug zu Standard **ISAE 3402** (International Standard on Assurance Engagements No. 3402)
- In Deutschland gibt es auch den Prüfungsstandard **PS 951** des IDW (Institut der Wirtschaftsprüfer in Deutschland e.V.), der sich auf den Standard ISAE 3402 bezieht.
- Frühere Grundlage: SAS 70 (Report Type 2)

2 Beschreibung der generellen Kontrolle

2.1 Applikationsablaufkontrolle

» Sorge zu tragen, dass Applikationen richtig implementiert sind und die richtige Datenverarbeitung durch die Applikationen erfolgt.

- Sowohl die Services als auch die zugehörigen Techniken und Prozesse werden von der Koordinierenden Stelle (KoSt) ATLAS bei der Oberfinanzdirektion Karlsruhe geprüft und nur bei vollständiger Abbildung der Anforderungen zertifiziert.
- Prüf- und Zertifizierungsprotokolle liegen auch der KoSt ATLAS vor.

2.2 Allg. organisatorische Kontrolle (Managementsysteme)

2.2.1 Datenschutz

Der betriebliche Datenschutzbeauftragte prüft und kontrolliert die Einhaltung der relevanten gesetzlichen Vorschriften. Der Datenschutzbeauftragte hält ein Datenschutzkonzept verfügbar. Einige der nachfolgend geschilderten Kontrollen sind verpflichtend gemäß Art. 32 DS-GVO (technische und organisatorische Maßnahmen zur Sicherheit der Verarbeitung).

Eine begrenzte Auswahl aus den IT-Teams vergibt Zugangsberechtigungen mit 4-Augen-Prinzip. Die Berechtigungen werden regelmäßig Ereignis- und Zeit-gesteuert kontrolliert; insbesondere mit Blick auf den Betrieb des Rechenzentrums. Die obige Auswahl kann Einspruch erheben und ihr Veto einlegen.

2.2.2 Sicherheitskontrolle, Risikomanagement

Der Betrieb des ISMS (Information Security Management System in Verbindung mit dem Zertifikat zur ISO 27001) stellt das IT-Security Management als kontinuierlichen Prozess-orientierten PDCA-Kreislauf sicher. Dieser Prozess basierend auf assets (Informationen, Werten) schließt Schutzbedarfsermittlung und detaillierte Risiko-Betrachtungen (Risikobewertung und -behandlung) ein.

Die wichtigsten und relevanten Sicherheitskriterien sind

- Verfügbarkeit
- Vertraulichkeit
- Integrität

Das ISMS enthält Kontrollen der Check-Phase u.a. in Form von internen und externen Audits sowie regelmäßige Managementbewertungen. Eine weitere Ebene ist die Sicherstellung eines hohen Sicherheitsbewußtseins (security awareness) mit Hilfe diverser Maßnahmen zur Aus- und Weiterbildung der Beschäftigten.

Für eine umfassende Darstellung verweisen wir auf unsere Informationssicherheitsleitlinie (als Teil der Leitlinie Integriertes Managementsystem) in https://service.aeb.de/open/leitlinien-und-zertifikate/.

2.3 Technische und organisatorische Maßnahmen

Die nachfolgende Zuordnung der Maßnahmen orientiert sich bis auf weiteres noch an der bis 25.05.2018 gültigen Fassung des (alten) BDSG.

Aus der ab 25.05.2018 anwendbaren EU-Datenschutz-Grundverordnung (kurz: DS-GVO) lassen sich auch Zuordnungen ableiten etwa nach den Sicherheitskriterien Verfügbarkeit, Vertraulichkeit, Integrität (und Belastbarkeit). Zumindest für eine gewisse Übergangszeit erleichtern Verweise in den nachfolgenden Abschnitten entsprechende Zuordnungsmöglichkeiten.

2.3.1 Eingabekontrolle

» Sorge zu tragen, dass nachträglich geprüft und festgestellt werden kann, ob und von wem Daten, insbesondere personenbezogene Daten, in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- Alle Produkte, die personenbezogene Stammdaten verarbeiten, protokollieren sämtliche Eingaben, Änderungen, Löschungen. Diese Protokollierung stellt sicher, dass nachträglich festgestellt werden kann, ob und wenn von wem personenbezogene Stammdaten eingegeben, verändert oder entfernt worden sind.
- Personalisierte Benutzerkonten auch in den Fachanwendungen.
- Trennung von System- und Anwendungsprotokollen, dadurch ist eine Manipulation der Anwendungsprotokolle auf Systemebene ausgeschlossen.
- Zuordnung DS-GVO: Integrität

2.3.2 Auftragskontrolle

» Sorge zu tragen, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- Regelung der Weisungen im Hauptleistungs- und Auftragsverarbeitungsvertrag
- Benutzer- und Rechteverwaltung auf Anwendungsebene durch den Auftraggeber.
- Übermittlung/Erfassung der Daten durch den Auftraggeber. Er entscheidet, wann welche Daten übermittelt werden.
- Zugriff auf diese Daten haben nur Rollen mit entsprechender Zugriffsbefugnis
- Automatisierte Verarbeitung der Daten durch zertifizierte Software (z.B. Verfahren ATLAS, Compliance etc.). Dadurch wird sichergestellt, dass die Daten gem. beauftragten Verfahren verarbeitet werden.
- Einsatz von Standardverträgen gemäß gesetzlichen Vorgaben für Verhältnisse mit Kunden und Dienstleistern.
- Einbindung von Subunternehmen mit entsprechenden Verträgen zu Vertraulichkeit, Auftragsverarbeitung, Systemzugang.
- Zuordnung DS-GVO: Verfügbarkeit, Vertraulichkeit

2.3.3 Trennungskontrolle

» Sorge zu tragen, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- Trennung von:

  - Mitarbeiterdaten
  - Kundenkontaktdaten
  - Kundentestdaten (Projektarbeit, Kundenentwicklungen)
  - Fernwartungszugangsdaten
  - Kundendaten im AEB-Rechenzentrum
- Systemebene:

  Kundendaten im Rechenzentrum werden von Daten der AEB (u.a. auch zu CRM-System) streng getrennt und in verschiedenen Systemen (Datenbanken...) verwaltet.
- Unterschiedliche Anwendungen:

  Für Kundendaten und Mitarbeiterdaten werden unterschiedliche Anwendungen eingesetzt.
- Berechtigungen innerhalb der Anwendung:

  Kundenkontaktdaten sind streng von Fernwartungszugangsdaten getrennt.
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit

2.3.4 Zutrittskontrolle

» Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen die Daten, insbesondere personenbezogene Daten, verarbeitet und genutzt werden, verwehren.

- Mehrstufige technische Schließsysteme, teilweise mit Ausrüstung zur Alarmierung.
- Sicherung des Gebäudes und Identitätskontrolle aller Anwesenden außerhalb der Geschäftszeiten durch einen Wachdienst.
- Regelung zur Zutrittsberechtigung für Nicht-Angestellte
- Zentrale Aufbewahrung zur Vergabe von elektronischen Codeschlüsseln (Tokens), Protokollierung der Aus- und Rückgabe.
- Server und Infrastrukturen (z.B. Fernwartungsrouter) sind durch Zutrittskontrolle (Codeschlösser, Codeschlüssel) zum Serverraum geschützt.
- Video-Überwachung zentraler Bereiche und systemkritischer Komponenten
- Fernwartungssysteme sind gesichert durch:
  - Zugriff auf Fernwartungsdaten nur für Berechtigte.
  - Systeme für Fernwartungszugänge zu Kunden stehen in einer abgeschotteten Netzwerkumgebung.
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit

2.3.5 Zugangskontrolle

» Zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- Arbeitsplatzrechner sind gesichert durch:
  - Anmeldung nur durch zentral gesteuertes Identity Management.
  - Verpflichtung der Mitarbeiter zur Sperrung des Arbeitsplatzrechners.
  - Automatische Sperrung der Arbeitsplatzrechner nach höchstens 15 Minuten.

  - Eine Entsperrung ist nur mit dem persönlichen Zugangscode möglich
- Zentrale Kennwortrichtline
  - für Administrationszugänge (regelmäßiger Zwang zur Änderung der Kennwörter, Mindestanforderung an Kennwortlänge und Komplexität, 2-Faktor-Authentifizierung).
  - für Mitarbeiterzugänge (Mindestanforderung an Kennwortlänge und Komplexität, 2-Faktor-Authentifizierung).
  - für Kundenzugänge (regelmäßiger Zwang zur Änderung der Kennwörter, Mindestanforderung an Kennwortlänge und Komplexität).
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

2.3.6 Zugriffskontrolle

» Sorge zu tragen, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass Daten, insbesondere personenbezogene Daten, bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- Zentrale Berechtigungsverwaltung, getrennt für System- und Anwendungszugang.
- Anwender können Berechtigungen nicht selbständig ändern.
- Anwender können nicht ohne Freigabe durch Verantwortlichen eine Änderung beantragen; hierzu ist ein Freigabeprozess etabliert.
- Grundsätzlich keine externen Zugänge außer VPN- bzw. SSH gesicherte Verbindungen.
- Daten werden verschlüsselt gespeichert (z.B. in Datenbanken)
- Sicherheitsprüfungen / Penetrationstests der externen Zugänge durch darauf spezialisierte Firmen.
- Regelung bei Aufgaben- oder Rollenwechsel innerhalb Unternehmen.
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

2.3.7 Weitergabekontrolle

» Sorge zu tragen, dass Daten, insbesondere personenbezogene Daten, bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung Daten, insbesondere personenbezogene Daten, durch Einrichtungen zur Datenübertragung vorgesehen ist.

- Der unternehmensweite Security Guide verbietet grundsätzlich den Versand von unverschlüsselten Daten.
- Alle Download-/Upload-Verbindungen via Internet sind gesichert durch entweder SSL/TLS, SSH oder VPN.
- Alle Niederlassungen bzw. mobilen Systeme verwenden ausschließlich VPN oder SSH gesicherte Verbindungen, die der Hoheit der AEB unterliegen.
- Es findet keine lokale Speicherung personenbezogener Daten statt, alle Daten werden zentral in den Systemen der AEB gehalten.
- Externe Verbindungen sind nur über freigegebene Anwendungen möglich.
- Externe Verbindungen sind nur über freigegebene Services möglich.

- Alle DFÜ-Verbindungen werden protokolliert soweit technisch machbar.
- Regelung zur Entsorgung von Abfällen mit vertraulichen Inhalten im Einklang mit relevanten DIN-Vorschriften (zu Schutzklasse und Sicherheitsstufen)
- Zuordnung DS-GVO: Vertraulichkeit, Verfügbarkeit, Integrität

2.3.8 Verfügbarkeitskontrolle

» Sorge zu tragen, dass Daten, insbesondere personenbezogene Daten, gegen zufällige Zerstörung oder Verlust geschützt sind.

- Daten werden verschlüsselt gespeichert (z.B. in Datenbanken)
- Redundante Systeme
  - Datenbank: Cluster (bei Bedarf)
  - Fileserver: Cluster
  - SAN/Storage: redundante Komponenten
- Unterbrechungsfreie Stromversorgung (USV) incl. Netzersatzanlage (NEA)
- Brandmelde- und Brandlöschanlagen
- Bandsicherung
  - Regelmäßige Bandsicherung
  - Auslagerung der Daten in gesonderten Brandabschnitt/gesondertes Gebäude
  - Zuzüglich untertags regelmäßiger Sicherung der Nutzdaten auf Basis Datenbank-Tools
- Früherkennung von systemkritischen Zuständen durch Monitoring und Alerting
- Führen eines Notfallkonzepts (Business Continuity Management) zur Notfall-Prävention und -Bewältigung
- Regelmäßige Tests u.a. der Datensicherung/Back-up-Systeme
- Zuordnung DS-GVO: Verfügbarkeit, Belastbarkeit

2.3.9 Maßnahmen zu Pseudonymisierung und Verschlüsselung

» Sorge zu tragen, dass eine Rückbeziehbarkeit von Daten auf (natürliche) Personen zumindest eingeschränkt ist

- Maßnahmen zu Privacy-by-design und Privacy-by-default; incl. entsprechenden Schulungsmaßnahmen im Produktebereich; mit Geboten zur Datenvermeidung und Datensparsamkeit
- Alle Download-/Upload-Verbindungen via Internet sind gesichert durch entweder SSL/TLS, SSH oder VPN
- Standard-Prozess zur Festplattenverschlüsselung der Clients der Mitarbeiter
- Möglichkeit zum remote wiping für mobile Geräte; Betrieb eines Mobile Device Managements (MDM)
- Eine Pseudonymisierung der Daten ist derzeit nicht vorgesehen. Begründung: Die personenbezogenen Daten sind geschäftlicher, nicht privater Natur. In der Interessensabwägung überwiegen die geschäftlichen Interessen. Diese bestehen u.a. auch in der Sicherstellung einer Revisionssicherheit.

2.3.10 Maßnahmen zur Wiederherstellbarkeit und Zuverlässigkeit

» Gewährleistung, dass eingesetzte Systeme im Störungsfall wiederhergestellt werden können sowie Gewährleistung, dass alle Funktionen des Systems zur Verfügung stehen und auftretende Fehlfunktionen gemeldet werden

- Betrieb eines etablierten Incident Managements, mit entsprechenden Rollen zur Abarbeitung
- Früherkennung von systemkritischen Zuständen durch Monitoring, automatischer Behebung von Fehlzuständen und Benachrichtigung durch Alerting
- Vorhalten eines Prozesses zum Emergency Management samt regelmäßiger Übungen dazu
- Vorhalten von Backup-Systemen

2.3.11 Maßnahmen zur Sicherstellung der Belastbarkeit

» Sorge zu tragen, dass eine ausreichende Widerstandsfähigkeit oder Robustheit auf Dauer vorliegt

- Betrieb ISMS -> prozessorientiert wird regelmäßig auf Schwachstellen und Bedrohungen geschaut; damit untermauern wir eine Nachhaltigkeit
- Führung einer Übersicht von Verarbeitungstätigkeiten mit integrierter Datenschutz-Folgenabschätzung und Einschätzung der Angemessenheit der technischen und organisatorischen Maßnahmen
- Integration Privacy-by-design im Produktmanagement -> Triggerung zur Vorabkontrolle durch Verfahrensverantwortlichen im Verbund mit dem DSB, auch zur Datenschutz-Folgenabschätzung (Pflege Verfahren samt Checks, Abstimmung, Analyse und Bewertung)
- Konkrete Prüfungen durch Penetrationstests.
- Einsatz von Next Generation Firewalls
- Aber auch Monitoring. Gutes Monitoring sorgt auch zu Früherkennung und somit zumindest Schadensbegrenzung, wenn nicht sogar noch Abwehr von Schädigungen durch Malware.
- Vorhalten von Puffern (Ressourcen) zum Abfangen außergewöhnlicher Last-Spitzen

2.3.12 Maßnahmen zur regelmäßigen Überprüfung der Wirksamkeit

» Zur Gewährleistung der Sicherheit der Verarbeitung

- Durchführung von internen und externen Audits zu ISO 27001, Auftragsverarbeitung
- Regelmäßige Überprüfung der technischen und organisatorischen Maßnahmen mit den verantwortlichen Rollen, auch hinsichtlich des Stands der Technik
- Einbeziehung möglicher Referenzen (z.B. zu SDM-Standard-Datenschutzmodell)
- Konkrete regelmäßige Prüfungen durch Penetrationstests; mit Auswertung und Weiterverfolgung anhand der Befunde
- Managementbewertungen als regelmäßige Routine mit Geschäftsleitung und Datenschutzbeauftragtem

2.3.13 Maßnahmen zur Berücksichtigung von (möglichen) Risiken

» Sorge zu tragen, dass eine Risikoabwägung in die Verarbeitung oder Auswahl geeigneter technischer und organisatorischer Maßnahmen einfließt

- Betrieb eines ISMS mit zugehörigen Prozessen, Rollen und Werkzeugen

- Durchführung eines Verfahrens zur Datenschutz-Folgenabschätzung mit Integration in die Verfahren/Verarbeitungstätigkeiten und möglicher Einbeziehung der zuständigen Aufsichtsbehörde
- Berücksichtigung der einschlägigen Technischen Richtlinien und Empfehlungen des Bundesamtes für Sicherheit in der Informationstechnik (BSI), soweit als Auftragsverarbeiter von Bedeutung

2.3.14 Maßnahmen zur Nichtverkettung

» Sorge zu tragen, dass Daten nur für den Zweck verarbeitet werden, zu dem sie erhoben wurden (Zweckbindungsgrundsatz).

- Einsatz eines Rollenkonzepts zur Einschränkung von Verarbeitungs-, Nutzungs- und Übermittlungsrechten
- programmtechnische Unterlassung bzw. Schließung von Schnittstellen in Verfahren und Verfahrenskomponenten
- regelnde Maßgaben zum Verbot von Backdoors sowie qualitätssichernde Revisionen zur Compliance bei der Softwareentwicklung
- Funktionstrennung gemäß Rollenkonzept
- Trennung mittels Rollenkonzepten mit abgestuften Zugriffsrechten auf der Basis eines Identitätsmanagements und eines sicheren Authentisierungsverfahrens
- geregelte Zweckänderungsverfahren (unter Berücksichtigung von Rechtsgrundlage, Erforderlichkeit, Vereinbarkeit)
- Durchführung regelmäßiger Schulungen zur Awareness.

2.3.15 Maßnahmen zur Transparenz

» Sorge zu tragen, dass Informations- und Auskunftspflichten Rechnung getragen werden.

- Führen eines Verzeichnisses von Verarbeitungstätigkeiten gemäß Art. 30 DS-GVO (sowohl als Verantwortlicher als auch als Auftragsverarbeiter)
- Datenschutzerklärung als Teil des Web-Auftritts der AEB
- Unterstützung zu Informationspflichten zu Art. 30 DS-GVO, dargestellt im Datenschutz-Portal der AEB
- Integration datenschutzrechtlicher Prüfungen in den Freigabeprozess von Produkten oder Applications
- Vermittlung der Auskunftsrechte von Betroffenen an die Belegschaft
- Dokumentation der Verträge mit den internen Mitarbeitern, Verträge mit externen Dienstleistern und Dritten, von denen Daten erhoben bzw. an die Daten übermittelt werden.

2.3.16 Maßnahmen zur Intervenierbarkeit

» Sorge zu tragen, dass Betroffene ihre Rechte zur Intervention ausüben können

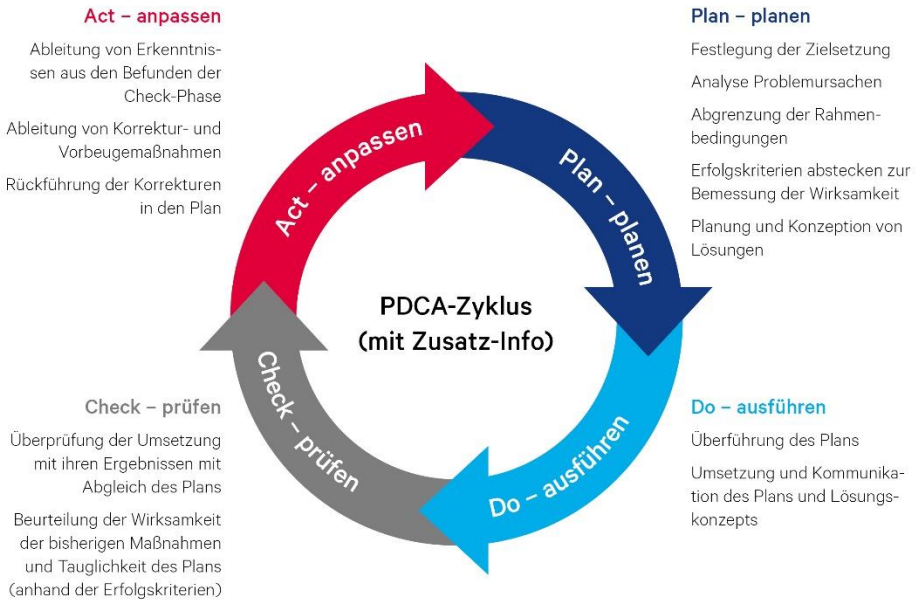
- dokumentierte Bearbeitung von Störungen, Problembearbeitungen und Änderungen am Verfahren sowie an den Schutzmaßnahmen der IT-Sicherheit und des Datenschutzes
- wo möglich Deaktivierungsmöglichkeit einzelner Funktionalitäten ohne Mitleidenschaft für das Gesamtsystem
- Nachverfolgbarkeit der Aktivitäten des Verantwortlichen zur Gewährung der Betroffenenrechte

- Einrichtung eines Verfahrens für das Zusammenspiel zwischen Verantwortlichem und Auftragsverarbeiter für den Umgang mit Vorgängen Betroffener
- operative Möglichkeit zur Zusammenstellung, konsistenten Berichtigung, Sperrung und Löschung aller zu einer Person gespeicherten Daten.

3 Beschreibung der Applikationskontrolle

3.1 Qualitätssicherung

Qualität steht in allen Bereichen der AEB im Vordergrund. Ihr wird eine besondere Stellung eingeräumt. Aufgaben- und Prozessverantwortliche definieren, optimieren und prüfen die Prozesse der Applikationsentwicklung, aber auch der Wartung und des Services anhand des PDCA-Kreislaufs.



Im Bereich der Applikationen werden dabei nicht nur Funktions- sondern auch Usability-Tests durchgeführt. Jede Neuerung wird dabei mehrfach geprüft und abgenommen.

Aktualität fachlicher Anforderungen wird ständig verfolgt und umgesetzt. Im engen Kundenkontakt wird Wartung und Service bewertet und optimiert. Die Arbeitsweise ist Service- und Prozess-orientiert.

3.2 Qualitätssicherung durch definierte Prozesse

Alle Schritte der Neuentwicklung sowie die Wartung der Applikationen durchlaufen definierte und kommunizierte Prozesse (Prinzip der Transparenz). Alle Applikationsentwicklungs- und Wartungsaufgaben werden als Projekte mit definiertem Projektablauf (manifestiert in Muster-Projekten) und einem beschriebenen Prozess realisiert. Darin integriert ist ein umfassendes Rollenkonzept mit diversen Stufen der Freigaben unter Nutzung des 4-Augen-Prinzips. Zur Sicherstellung der Compliance sind außerdem Sicherheits-Checks vorgesehen.

3.3 Qualitätssicherung durch externe Prüfer

Applikationen werden - wo erforderlich - auch durch externe Prüfer geprüft und zertifiziert.

Dies geschieht u.a. in Anlehnung an IDW-Prüfungsstandards und Stellungnahmen wie IDW PS 330 („Abschlussprüfung bei Einsatz von Informationstechnologie“) oder IDW RS FAIT 1 („Grundsätze ordnungsgemäßer Buchführung bei Einsatz von Informationstechnologie“).

AEB SE . Hauptsitz . Sigmaringer Straße 109 . 70567 Stuttgart . Deutschland . +49 711 72842 0 . www.aeb.com . info.de@aeb.com . Registergericht: Amtsgericht Stuttgart . HRB 767 414 . Geschäftsführende Direktoren: Matthias Kieß, Markus Meißner . Vorsitzende des Verwaltungsrats: Maria Meißner

Standorte

Düsseldorf . Hamburg . Lübeck . Mainz . Malmö . München . New York . Paris . Prag . Rotterdam . Salzburg . Singapur . Soest . Stuttgart . Warwick . Zürich