Informationssicherheit

Übergreifende Richtlinien und Prozesse

Regelung Nr. 03.01.09

Ausnahmeprozess

Klassifikation: Intern – KSU 2.1

Geltungsbereich: Die Regelungen gelten für die AUDI BRUSSELS

Version 1.1

Inhalt

I. Zweck

Der Zweck dieser Regelung ist die Definition grundlegender Prinzipien für den Umgang mit Abweichung vom Informationssicherheitsregelwerk im Rahmen eines Ausnahmeprozesses. Dieser Prozess wird bei der AUDI BRUSSELS als Risikoübernahmeprozess umgesetzt.

Dieses Dokument deckt sowohl Ausnahmen vom Informationssicherheitsregelwerk des Konzerns, als auch Ausnahmen von gesellschaftsspezifischen Regelwerken ab.

Im Sinne dieser Regelung bezeichnet der Begriff Informationssicherheit die IT-Sicherheit als Bestandteil der ganzheitlichen Informationssicherheit.

1. Ausnahmeprozess

1.1. Ziel

In diesem Kapitel wird der Prozess zur Beantragung, Prüfung und Genehmigung von Ausnahmen beschrieben.

1.2. Abgrenzung

Das Informationssicherheitsregelwerk des Konzerns ist für alle internen und externen Mitarbeiter des Konzerns umzusetzen und zu beachten. Das Informationssicherheitsregelwerk der Gesellschaften besteht aus dem Informationssicherheitsregelwerk des Konzerns (oder Teilen hiervon) und möglichen gesellschaftsspezifischen Rahmenwerken. Wenn die Einhaltung von Vorgaben in gerechtfertigten Fällen nicht möglich ist, z.B. aus technischen oder organisatorischen Gründen, muss von der zuständigen Stelle eine Ausnahme beantragt werden[1]. Bei Genehmigung der Ausnahme, ist die Abweichung, die das Sicherheitsniveau senkt, von den Vorgaben des Informationssicherheitsregelwerks temporär erlaubt.

1.3. Definitionen

1.3.1 Anforderungen

Eine „Anforderung“ ist in diesem Dokument wie folgt definiert:

- Eine Anforderung aus den Informationssicherheitshandlungsleitlinien des Konzerns oder aus Regelungen (konzernweite Anforderung) oder einer Anforderung aus zusätzlichen gesellschaftsspezifischen Leitlinien oder Regelungen, die beachtet werden müssen.
- Eine Einstellung aus einem der Dokumente zu den systembezogenen Regelungen[2].

1.3.2 Ausnahmen

Eine Ausnahme ist eine zeitlich begrenzte und genehmigte Abweichung von Informationssicherheitsanforderungen, die das Sicherheitsniveau senken.

[1] Weitere Informationen finden Sie in Kapitel 1.4

[2] Siehe Anhang A.1.4

Ausnahmen werden, abhängig von deren Auswirkung, in globale und lokale Ausnahmen unterteilt:

- Globale Ausnahme: Wenn eine Ausnahme für eine Abweichung von einer konzernweiten Anforderung genehmigt wird, die negative Auswirkung auf das Sicherheitsniveau anderer Konzerngesellschaften oder des gesamten Konzerns hat, wird diese Ausnahme als globale Ausnahme bezeichnet.
- Lokale Ausnahme: Eine Abweichung von einer konzernweiten oder gesellschaftsspezifischen Anforderung, die nur eingeschränkte Auswirkung z. B. auf eine einzelne Konzerngesellschaft hat, wird diese Ausnahme als lokale Ausnahme bezeichnet.

1.4. Grundlegende Anforderungen

- Wenn eine konzern- oder gesellschaftsspezifische Anforderung nicht eingehalten werden kann, muss eine Ausnahme entsprechend des definierten Prozesses beantragt werden[3].
- Eine Ausnahme ist nicht notwendig, wenn eine Abweichung das Sicherheitsniveau erhöht (z. B. kürzere Timeouts, komplexere Passwörter, …). Diese sind zu dokumentieren (z.B. im Betriebshandbuch).
- Ausnahmeanträge müssen dokumentiert werden und eine ausführliche Begründung enthalten.
- Risiken, die durch die beantragte Ausnahme verursacht werden können, müssen bewertet werden.
- Die Einstufung des Risikos in ein globales oder lokales Risiko muss dokumentiert werden[4].
- Ausnahmen dürfen nur für eine begrenzte Zeit genehmigt werden.
- Ausnahmen sind nicht mehr gültig, wenn die zugrundeliegenden Parameter sich geändert haben (z. B. Änderung der Klassifizierung der Anwendung).
- Jede Gesellschaft muss einen lokalen Prozess[5] für den Umgang mit Ausnahmen definieren. Dieser Prozess muss mindestens festlegen:

- Wer eine Ausnahme beantragen darf
- Die zuständige Stelle für die Beantragung einer Ausnahme
- Welche Informationen der Ausnahmeantrag beinhalten muss[6]
- Eine Beschreibung, wie die IT-Sicherheitsspezialisten der Gesellschaft eingebunden sind
- Einen Prozess zur Bewertung der durch die Ausnahme verursachten Risiken[7]. Im Prozess muss die Verantwortung der Fachbereiche definiert werden.

[3] Siehe Kapitel 1.5

[4] Siehe Kapitel 1.3.2

[5] Siehe Anhang B.1.2

[6] Siehe Anhang B.1.3

[7] Siehe Anhang A.1.3

- Einen Prozess zur Dokumentation der Ausnahmen incl. Festlegung des Speicherorts
- Wer die Ausnahmen genehmigt oder ablehnt (4-Augen-Prinzip ist verpflichtend)
- Einen Prozess zur Definition, wann eine Ausnahme an die zentrale Stelle zur Behandlung von Ausnahmen zu eskalieren ist[8].

1.4.1 Stellen zur Bearbeitung von Ausnahmen

1.4.1.1 Zentrale Stelle zur Behandlung von Ausnahmen

- Eine zentrale Stelle zur Behandlung von Ausnahmen[9] muss definiert werden.
- Die zentrale Stelle zur Behandlung von Ausnahmen muss die beantragten Ausnahmen auf Abweichungen von Anforderungen, die negative Auswirkungen auf das Sicherheitsniveau des gesamten Konzerns haben können (globale Ausnahme[10]), bearbeiten.
- Die zentrale Stelle zur Behandlung von Ausnahmen muss andere Konzerngesellschaften über genehmigte Ausnahmen informieren, die negative Auswirkungen auf das Sicherheitsniveau dieser Gesellschaften haben können.

1.4.1.2 Lokale Stelle zur Behandlung von Ausnahmen

- Jede Konzerngesellschaft muss eine lokale Stelle zur Behandlung von Ausnahmen definieren[11].
- Es wird empfohlen, dass die lokale Stelle zur Behandlung von Ausnahmen durch Mitarbeiter der IT-Sicherheit besetzt wird. Die Mitglieder der lokalen Stelle zur Behandlung von Ausnahmen benötigen tiefgreifende Kenntnisse über die IT-Infrastruktur der Gesellschaft, um eine wirksame Prüfung möglicher Auswirkungen durch nicht beachtete spezifische Anforderungen durchführen zu können.
- Die lokalen Stelle zur Behandlung von Ausnahmen muss sowohl Abweichungen von gesellschaftsspezifischen als auch von konzernweiten Anforderungen prüfen, wenn die Abweichungen nur die Konzerngesellschaft selbst betreffen (lokale Ausnahme[12]).
- Wenn eine beantragte Ausnahme negative Auswirkungen auf das Sicherheitsniveau anderer Konzerngesellschaften hat oder haben kann, muss die lokale Stelle zur Behandlung von Ausnahmen den Ausnahmeantrag an die zentrale Stelle zur Behandlung von Ausnahmen weiterleiten.
- Die lokale Stelle zur Behandlung von Ausnahmen muss verantwortliche Ansprechpartner für die zentrale Stelle zur Behandlung von Ausnahmen benennen.

---

[8] Siehe Kapitel 1.4.1.2

[9] Siehe Anhang B.1.1

[10] Siehe Kapitel 1.3.2

[11] Wenn nötig kann eine Konzerngesellschaft mehrere lokale Stellen zur Behandlung von Ausnahmen definieren. Auch eine Übernahme des Ausnahmeprozesses durch eine andere (übergeordnete) Konzerngesellschaft ist möglich.

[12] Siehe Kapitel 1.3.2

1.5. Prozess für Beantragung und Gewährung von Ausnahmen

Abbildung 1 gibt einen Überblick über den Ausnahmeprozess. Die unterschiedlichen Schritte sind in den Kapiteln 1.5.1 bis 1.5.3.3 beschrieben.

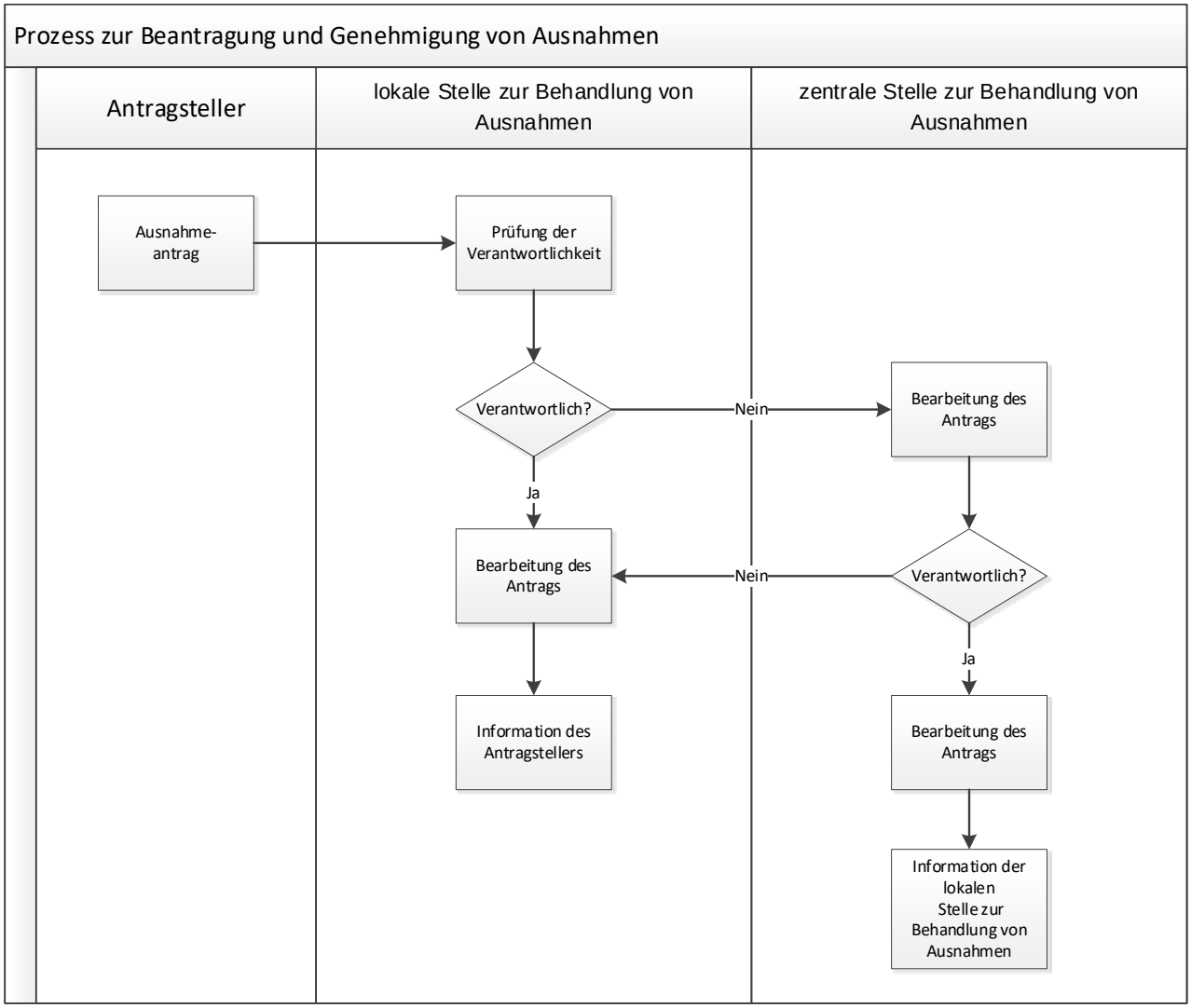

Abbildung 1: Ausnahmeprozess

1.5.1 Beantragung von Ausnahmen

Jede Ausnahme muss zuerst bei der lokalen Stelle zur Behandlung von Ausnahmen beantragt werden[13].

1.5.2 Aktivitäten der lokalen Stelle zur Behandlung von Ausnahmen

1.5.2.1 Prüfung der Verantwortlichkeit

Die lokale Stelle zur Behandlung von Ausnahmen muss prüfen, ob die beantragte Ausnahme das Sicherheitsniveau anderer Konzerngesellschaften oder das des gesamten Konzerns

[13] Für weiterführende Informationen siehe Kapitel 1.4.1.2

senkt. In diesem Fall prüft die lokale Stelle zur Behandlung von Ausnahmen, ob alle notwendigen Informationen in Ausnahmeantrag enthalten sind und sendet diesen an die zentrale Stelle zur Behandlung von Ausnahmen[14] Hierfür sollte das Standard-Antragsformular[15] genutzt werden.

Wenn der Ausnahmeantrag nur die Gesellschaft selbst betrifft, bearbeitet die lokale Stelle zur Behandlung von Ausnahmen den Antrag.

1.5.2.2 Bearbeitung des Antrags

Die lokale Stelle zur Behandlung von Ausnahmen muss jedes Risiko prüfen, das durch die Abweichung von den relevanten Informationssicherheitsvorgaben verursacht wird und die Ausnahmeanträge entsprechend des definierten lokalen Ausnahmeprozesses bearbeiten[16].

Die Ergebnisse der Risikoanalyse müssen bei der Entscheidung über Genehmigung oder Ablehnung der Ausnahme berücksichtigt werden.

Die folgenden Entscheidungen sind möglich:

- Genehmigung für einen begrenzten Zeitraum. Die Länge des Zeitraums muss das Ergebnis der Risikoanalyse berücksichtigen und darf drei Jahre nicht überschreiten.
- Genehmigung für einen begrenzten Zeitraum mit zusätzlichen Maßnahmen. Die Länge des Zeitraums muss das Ergebnis der Risikoanalyse berücksichtigen und darf drei Jahre nicht überschreiten.
- Ablehnung
- Weiterleitung an die zentrale Stelle zur Behandlung von Ausnahmen

1.5.2.3 Information des Antragstellers über die Entscheidung

Der Antragsteller muss über die Entscheidung und seine damit verbundenen Pflichten informiert werden[17].

1.5.3 Aktivitäten der zentralen Stelle zur Behandlung von Ausnahmen

1.5.3.1 Prüfung der Verantwortlichkeit

Wenn eine lokale Stelle zur Behandlung von Ausnahmen einen Ausnahmeantrag an die zentrale Stelle zur Behandlung von Ausnahmen stellt, muss diese prüfen, ob die Ausnahme andere Konzerngesellschaften oder den gesamten Konzern betrifft. In diesem Fall bearbeitet[18] die zentrale Stelle zur Behandlung von Ausnahmen den Antrag selbst. Anderenfalls sendet die zentrale Stelle zur Behandlung von Ausnahmen den Antrag zur weiteren Bearbeitung zurück an die lokale Stelle zur Behandlung von Ausnahmen.

[14] Siehe Kapitel 1.4.1.1

[15] Siehe Anhang A.3.2

[16] Siehe Kapitel 1.4

[17] Siehe Kapitel 1.5.4

[18] Siehe Kapitel 1.5.3.2

1.5.3.2 Bearbeitung des Antrags

Die zentrale Stelle zur Behandlung von Ausnahmen muss jedes Risiko prüfen, das durch die Abweichung von den relevanten Informationssicherheitsvorgaben verursacht wird.

Die Ergebnisse der Risikoanalyse müssen bei der Entscheidung über Genehmigung oder Ablehnung der Ausnahme berücksichtigt werden.

Die folgenden Entscheidungen sind möglich:

- Genehmigung für einen begrenzten Zeitraum. Die Länge des Zeitraums muss das Ergebnis der Risikoanalyse berücksichtigen und darf drei Jahre nicht überschreiten.
- Genehmigung für einen begrenzten Zeitraum mit zusätzlichen Maßnahmen. Die Länge des Zeitraums muss das Ergebnis der Risikoanalyse berücksichtigen und darf drei Jahre nicht überschreiten.
- Ablehnung

1.5.3.3 Information des Antragstellers über die Entscheidung

Die zentrale Stelle zur Behandlung von Ausnahmen erstellt einen Ausnahmebericht, Der Ausnahmebericht enthält die folgenden Informationen:

- Stelle, die den Ausnahmebericht erstellt hat
- Details zum Antragsteller
  - Nachname, Vorname
  - Gesellschaft und Organisationseinheit
- Vorgangsnummer aus dem Ausnahmeprozess
- Beschreibung des Antrags
- Spezifizierung der Vorgaben auf die sich die Ausnahme bezieht
- Entscheidung über die Genehmigung
  - Genehmigung für einen begrenzten Zeitraum
  - Genehmigung für einen begrenzten Zeitraum mit zusätzlichen Maßnahmen
  - Ablehnung
- Spezifizierung der Maßnahmen (wenn erforderlich) und Verantwortlichkeit für deren Umsetzung inklusive zeitlicher Vorgaben
- Begründung
- Unterschrift der zentralen Stelle zur Behandlung von Ausnahmen (handschriftlich oder elektronisch)

Der Ausnahmebericht ist der lokalen Stelle zur Behandlung von Ausnahmen, die den Antrag übermittelt hat zu übersenden.

1.5.4 Pflichten des Antragstellers

Zur Nachverfolgung sind der Ausnahmeantrag und der zugehörige Ausnahmebericht vom Antragsteller zu speichern[19] (z. B. zusammen mit der Systemdokumentation). Es muss sichergestellt sein, dass die Dokumentation der Ausnahme bei Änderungen von Rollen oder Verantwortlichkeiten dem entsprechenden Nachfolger übergeben werden.

Der Antragsteller muss sicherstellen, dass die Abweichung vom Informationssicherheitsregelwerk beseitigt ist, bevor die Befristung der Ausnahme abgelaufen ist. Nachdem der festgelegte Zeitraum abgelaufen ist, ist die Ausnahme nicht mehr gültig.

Sollte die Abweichung vom Informationssicherheitsregelwerk nach Ablauf der Gültigkeit der Ausnahme noch nicht beseitigt sein, muss der Antrag erneut gestellt und durch die zuständige Stelle zur Behandlung von Ausnahmen erneut geprüft werden.

Ist die Genehmigung der Ausnahme mit zusätzlichen Maßnahmen verbunden, muss der Antragsteller sicherstellen, dass alle für die Genehmigung verbindlichen Maßnahmen in der vorgegebenen Zeit umgesetzt werden.

Der Antragsteller muss detailliert beschreiben, welche Punkte der einzelnen Richtlinien bzw. Regelungen nicht eingehalten werden können.

[19] Die Konzernvorgaben zur Archivierung (KSU) müssen berücksichtigt werden.

II. Verantwortlichkeiten

II.I Kapitel 1: Ausnahmeprozess

Diese Regelung ist von allen Bereichen, die für die Umsetzung und Beachtung von Vorgaben des Informationssicherheitsregelwerks verantwortlich sind einzuhalten.

Abweichungen von dieser Regelung, die das Sicherheitsniveau senken, sind nur in Abstimmung mit der IT-Sicherheit und grundsätzlich nur zeitlich begrenzt zulässig.

Anhang

A. Allgemeines

A.1 Mitgeltende Dokumente

A.1.1 Nicht Referenziert

A.1.2 Informationssicherheitshandlungsleitlinien für Mitarbeiterinnen und Mitarbeiter

A.1.3 Informationssicherheit Regelung Nr. 03.01.15 Risikomanagement in der Informationssicherheit

A.1.4 Informationssicherheit Regelung Nr. 03.01.01 Anti Malware & Systemschutz

A.1.5 PS_UP4_FP.05-Information-Security-Risk-Management

A.2 Referenzen zu Standards

Die folgende Tabelle zeigt die Referenzen zu den Standards ISO/IEC 27001:2013, ISO/IEC 27001:2005 und VDA.

Thema	Kapitel	ISO 27001:2013	ISO 27001:2005	VDA
Das Informationssicherheits-Managementsystem sollte beinhalten: b) dokumentierte Informationen der Organisation, die für die Effektivität des Informationssicherheits-Managementsystems wichtig sind,	alle	7.5.1	4.3.1	-

A.3 Anlagen

A.3.1 Anlage 1 Feedbackformular

Das Feedbackformular für Änderungsvorschläge zu Regelungen kann von der MyNet-Webseite Gesellschaften → Audi Brussels → Organisation → Finanz (B/F) → IT (B/FP) → IT-Sicherheit → Regelwerk heruntergeladen werden.

Das Feedback-Formular ist folgendermaßen auszufüllen:

Die Spalten 2 bis 6 müssen für jede vorgeschlagene Änderung ausgefüllt werden. Änderungen, für die nicht alle Spalten 2 bis 6 ausgefüllt sind, werden automatisch ohne weitere Prüfung abgelehnt.

Spalte 3: Folgende Kommentararten sind möglich: a=allgemein, f=fachlich, r=redaktionell

Spalte 4: Bitte bisherigen Text, Tabelle oder Bild einfügen

Spalte 5: Bitte vollständig umformulierten Text, geänderte Tabelle oder geändertes Bild einfügen

Spalte 6: Bitte begründen Sie die gewünschte Änderung möglichst ausführlich.

Bitte senden Sie das ausgefüllte Formular an: it-security.audibx@audi.de

A.3.2 Anlage 2 Antrag zur Risikoübernahme bei Abweichungen vom Informationssicherheits-Regelwerk

Gemäß dem Risikoübernahmeprozess ist das Risikoübernahmeformular zu verwenden.

Dieses kann von der MyNet-Webseite Geschäftsbereiche → Beschaffung und IT → Organisation → IT → IT-Sicherheit heruntergeladen werden.

A.4 Abkürzungen und Definitionen

In diesem Abschnitt werden ausschließlich Begriffe und Abkürzungen aus dem Informationssicherheitsbereich definiert. Begriffe und Abkürzungen aus anderen Bereichen werden durch die dafür verantwortlichen Stellen definiert.

Abkürzung/Begriff	Erklärung
4-Augen-Prinzip	Für eine Einrichtung von z.B. Zugangs-/Zugriffsberechtigungen ist die Genehmigung mehrerer Personen notwendig, um einen möglichen Missbrauch durch einzelne Personen zu verhindern.
Risikoanalyse	Prozessschritt des Risikomanagements, zur Identifikation und Bewertung der identifizierten Gefahren hinsichtlich ihrer Eintrittswahrscheinlichkeiten und möglichen Auswirkungen. (ISO 31000:2009)

A.5 Gültigkeit

Diese Regelung ist mit der Veröffentlichung sofort gültig.

Bereits bestehende Ausnahmeregelungen sind spätestens bei der nächsten Änderung (z.B. Verlängerung, Änderung der Auflagen) an diese Regelung anzupassen

Nächster Überprüfungstermin: 01.10.2023

Für die Meldung von Änderungswünschen verwenden Sie bitte das vorgegebene Formular[20].

A.6 Dokumentenhistorie

Version	Name	Org.-Einheit	Datum	Bemerkung
1.0	Andreas Walter	B/FP	07.08.2019	Veröffentlicht
1.1	Andreas Walter	B/FP	01.10.2020	Anpassung A.1.5 und B.1.2

[20] Siehe Anhang A.3.1 Anlage 1 Feedbackformular

B. Spezifische Ausprägungen

B.1 Kapitel 1: Ausnahmeprozess

B.1.1 Verantwortlich für Informationssicherheitsregelungen: IT-Sicherheit Verantwortlich für Informationssicherheitshandlungsleitlinien: Datenschutz/Datensicherheit, Office des DPO

B.1.2 Prozess zur Risikoübernahme bei Abweichungen vom Informationssicherheitsregelwerk

PS_UP4_FP.05-Information-Security-Risk-Management

B.1.3 Folgende Informationen sollten vom Antragsteller im Ausnahmeantragsformular abgefragt werden:

- Details zu Antragsteller
  - Name und Vorname
  - Telefonnummer
  - E-Mail Adresse
  - Organisationseinheit
  - Kostenstellenverantwortlicher
- Art des Antrags
  - Neuer Antrag
  - Antrag für einen bestehenden Prozess (inkl. der betroffenen Prozessnummer)
- Beschreibung der Ausnahme und, wenn nötig, die Liste der betroffenen Systeme
- Angabe der Vorgabe/Regelung, auf die sich der Ausnahmeantrag bezieht
- Details zu den betroffenen Daten oder Informationen
  - Klassifizierung[21]
  - Beschreibung
  - Information, ob personenbezogene Daten verarbeitet werden
- Informationen über bestehende Vereinbarungen mit anderen Organisationseinheiten (wenn zutreffend)

[21] Siehe Anhang A.1.2