Konformitätsbericht

Zielreifegrad: Reifegrad 5: optimiert

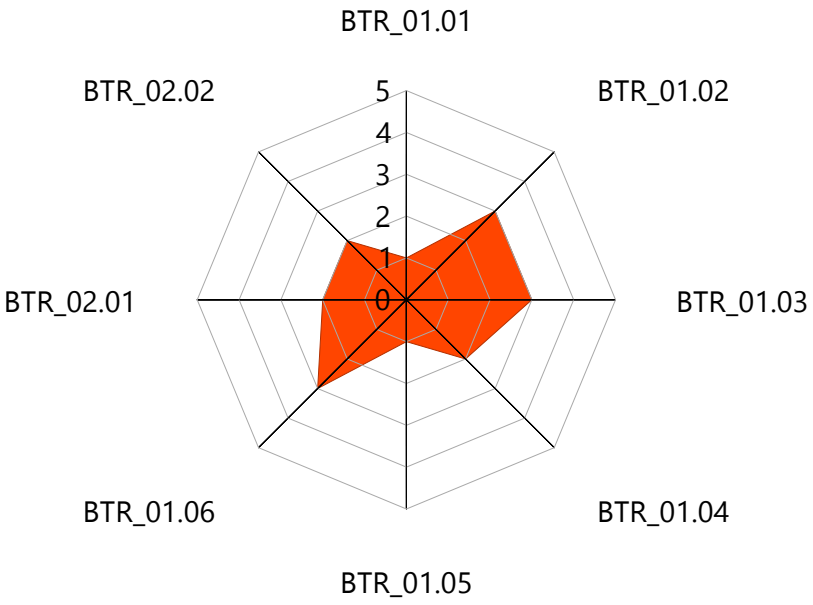
Inhaltsverzeichis

1. 1. Reaudit Betroffenenrechte

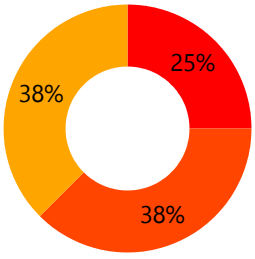
OrgEH:	Team Secure AG (TeSA)
Audit:	Internes Überwachungsaudit zur Umsetzung der DSGVO (INT_ÜA_DS_Jahr03)
Hauptprüfer:	Peter Innereiter
Interviewpartner:	Tom Leisch
Beschreibung:	es soll festgestellt werden, inwieweit die Betroffenenrechte nach Inkrafttreten der DSGVO nun bereits DSGVO-konform erfüllt werden.

Prüfobjekt:

1. Reaudit Betroffenenrechte



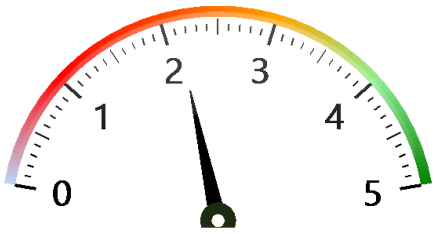
Prüfobjekt:	**1. Reaudit Betroffenenrechte (TeSA_BTR_02)**	22.01.2019 15:57
Verantwortlich(e):	Tom Leisch	
Wissensdatenbank:	DEMO: Assessment zur Umsetzung der Datenschutz-Grundverordnung, Version: 5	



Antworten:

- Reifegrad 1: initial (2/8)
- Reifegrad 2: gemanaged (3/8)
- Reifegrad 3: definiert (3/8)

Durchschnittlicher Reifegrad



Prüffrage(n):

BTR_01.00:	**Prozesse zur Erfüllung der Betroffenenrechte**	**Strukturfrage**
Frage:	Gibt es grundlegende Prozesse zur Erfüllung der Betroffenenrechte?	
Beschreibung:	Um die Rechte der Betroffenen fristgerecht erfüllen zu können, müssen Prozesse implementiert sein, die sicherstellen, dass Anfragen von Betroffenen umgehend entgegen genommen und rasch von den zuständigen Personen bearbeitet und abgeschlossen werden können. Folgende Aspekte sollten berücksichtigt werden: - gibt es eine Anlaufstelle für Betroffene, die Anfragen fristgerecht und ordnungsgemäß bearbeiten kann? - kann schnell festgestellt werden, ob personenbezogene Daten über die Person verarbeitet werden? - wird im Zweifel die Identität des Antragstellers überprüft? - wird die Zulässigkeit des Ansuchens festgestellt? - werden Anfragen und Beantwortung ordentlich dokumentiert?	
Antwort:	Reifegrad 2: gemanaged	
Begründung:	grundlegende Prozesse sind definiert und derzeit in Umsetzung/Erprobung	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

BTR_01.01:	**Verarbeitung personenbezogener Daten**	**Teilfrage**
Frage:	Kann festgestellt werden, ob und welche personenbezogenen Daten über eine betroffene Person verarbeitet werden	
Beschreibung:	Um die Betroffenenrechte gesetzeskonform erfüllen zu können, muss feststellbar sein: - ob über eine Person personenbezogene Daten verarbeitet werden - welche personenbezogenen Daten verarbeitet werden. Folgende Aspekte sollten positiv beantwortet werden können: - es ist eine Form des Datenmapping implementiert, damit schnell und sicher alle Orte identifiziert werden können, an denen sich personenbezogene Daten befinden. - alle Datenflüsse und Datentransfers zwischen Systemen sind nachvollziehbar dokumentiert.	
Antwort:	**Reifegrad 1: initial**	
Begründung:	derzeit noch kein standardisiertes Prozedere	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

BTR_01.02:	**zentrale Anlaufstelle für Betroffenenanfragen**	**Teilfrage**
Frage:	Gibt es eine zentrale Anlaufstelle, bei der Betroffene ihre Anfragen einbringen können?	
Beschreibung:	Um den Betroffenen eine einfache Ausübung der Betroffenenrechte zu ermöglichen, sollte eine zentrale Anlaufstelle geschaffen werden, an die Anfragen gerichtet werden können. Folgende Aspekte können positiv beantwortet werden: - es gibt eine (zentrale) Email-Adresse oder sonstige vergleichbare Kontaktmöglichkeit für Datenschutzfragen, von welcher Anfragen jederzeit bearbeitet werden (Zuständigkeiten bei Urlauben/Abwesenheiten sind geregelt) - Eine mündliche Auskunftserteilung wird ermöglicht, wenn es das Betroffenenklientel erfordert (insbesondere bei älteren bzw. mit elektronischen Medien nicht so vertrauten Personen).	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	zentrale Kontaktmöglichkeit wurde geschaffen	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

BTR_01.03:	**Identitätsnachweis**	**Teilfrage**
Frage:	Wird die Identität des Antragstellers überprüft?	
Beschreibung:	Folgende Aspekte sollten für die Bearbeiter von Betroffenenanfragen klar definiert sein: - unter welchen Umständen sollte ein Identitätsnachweis angefordert werden (zB bei telefonischen Anfragen, Anfragen von einer Fantasieemailadresse) - welche Art des Identitätsnachweises ist gefordert - wie ist mit dem Identitätsnachweis nach Feststellung der Identität zu verfahren	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	Prozess ist definiert	
Schutzziel(e):	Rechtskonformität	

BTR_01.04:	**Vorgehen bei exzessiven oder unbegründeten Anfragen**	**Teilfrage**
Frage:	Gibt es ein Vorgehen bei exzessiven bzw. offenkundig unbegründetenAnfragen eines Betroffenen?	
Beschreibung:	Folgende Aspekte werden dabei geregelt : - Definition, wann Anfragen als exzessiv oder unbegründet eingestuft werden - Begründung für Einstufung als exzessiv/unbegründet muss nachvollziehbar dokumentiert werden, da hierfür ein Nachweis erbracht werden können muss - Festlegung, ob in solchen Fällen ein Entgelt verlangt wird (Höhe des Entgelts unter Berücksichtigung des Verwaltungsaufwands definieren) oder das Tätigwerden verweigert wird.	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	grundsätzliches Vorgehen definiert	
Schutzziel(e):	Rechtskonformität	

BTR_01.05:	**Zulässigkeit des Betroffenenansuchens**	**Teilfrage**
Frage:	Wird geprüft, ob Ausnahmen nach nationalem Recht oder Unionsrecht bestehen, die der Erfüllung eines Betroffenenansuchens entgegen stehen?	
Beschreibung:	Folgende Aspekte werden bedacht: - relevante Rechtsvorschriften werden vorab identifiziert und zu dokumentiert - es wird geprüft, ob einem Betroffenenansuchen eine Beschränkung durch eine entsprechende Rechtsvorschrift entgegensteht - wenn der Eindruck besteht, dass eine rechtliche Beschränkung zutrifft, wird dies im Einzelfall gegebenenfalls juristisch abgeklärt	
Antwort:	**Reifegrad 1: initial**	
Begründung:	da brauchen wir noch rechtliche Beratung	
Schutzziel(e):	Rechtskonformität	

BTR_01.06:	**Dokumentation Betroffenenrechte**	**Teilfrage**
Frage:	Werden Anfrageeingang, Kommunikation und Beantwortung ordnungsgemäß dokumentiert?	
Beschreibung:	Um die ordnungsgemäße und fristgerechte Beantwortung von Betroffenenanfragen nachweisen zu können, - werden sowohl die Anfrage sowie die Kommunikation dazu und die finale Beantwortung dokumentiert und - als auch der zeitliche Ablauf sämtlicher Maßnahmen	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	Dokumentation wird gepflegt	
Schutzziel(e):	Rechtskonformität	

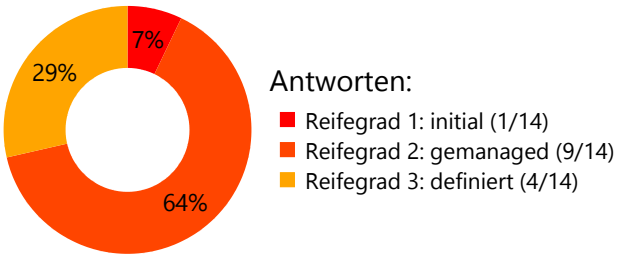
BTR_02.00:	**Prozesse zur Umsetzung eines Betroffenenansuchens**	**Strukturfrage**
Frage:	Sind Prozesse etabliert, um Betroffenenansuchen ausreichend umzusetzen?	
Beschreibung:	Es gibt Prozesse, die sicherstellen, dass - für jedes Betroffenerecht geeignete Maßnahmen gesetzt werden, um dieses DSGVO-konform umzusetzen - Betroffene ausreichend über die Umsetzung ihres Ansuchens informiert werden. Demnach existieren Prozesse zur Umsetzung des: - Rechts auf Auskunft - Rechts auf Berichtigung - Rechts auf Löschung - Rechts auf Einschränkung der Verarbeitung - Rechts auf Datenübertragbarkeit - Rechts auf Widerspruch	
Antwort:	Reifegrad 2: gemanaged	
Begründung:	großteils sind die Prozesse definiert	
Schutzziel(e):	Rechtskonformität ● ● ● ●	
BTR_02.01:	**Informationen an Betroffene iZm einem Betroffenenansuchen**	**Teilfrage**
Frage:	Ist sichergestellt, dass Betroffene alle für Sie relevanten Informationen iZm einem Betroffenenansuchen erhalten?	
Beschreibung:	Betroffene erhalten grundsätzlich Informationen über: - die Tatsache, ob ihrem Ansuchen entsprochen wurde - die Gründe für die Entscheidung - die Möglichkeit einer Beschwerde bei einer Aufsichtsbehörde - über die gesetzten Maßnahmen iZm ihrem Ansuchen	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	Vorlagen in Erarbeitung	
Schutzziel(e):	Rechtskonformität ● ● ● ●	
BTR_02.02:	**Maßnahmenplan zur Umsetzung von Betroffenenrechten**	**Teilfrage**
Frage:	Gibt es einen Maßnahmenplan zur Umsetzung für jedes Betroffenenrecht?	
Beschreibung:	Folgende Aspekte können positiv beantwortet werden: - Mitteilungspflicht an Empfänger personenbezogener Daten wird erfüllt - Auswirkungen auf die Weiterverarbeitung der personenbezogenen Daten im Falle eines Betroffenenansuchens werden geprüft - technische und organisatorische Maßnahmen zur Umsetzung eines Betroffenenansuchens werden in die Wege geleitet	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	Prozess erarbeitet	
Schutzziel(e):	Rechtskonformität ● ● ● ●	
BTR_03.00:	**Automatisierte Entscheidungen im Einzelfall**	**Strukturfrage**
Frage:	Führen Sie in Ihrem Unternehmen Verarbeitungstätigkeiten durch, bei denen im Einzelfall automatisierte Entscheidungen getroffen werden?	
Beschreibung:	Automatisierte Entscheidungen im Einzelfall - inkl. Profiling - sind grundsätzlich nicht erlaubt, wenn diese der betroffenen Person gegenüber rechtliche Wirkungen (zB Vertragskündigung) entfalten oder sie in ähnlicher Weise beeinträchtigen. Werden solche automatisierten Entscheidungsfindungen jedoch eingesetzt, sind gewisse Regeln zu beachten.	
Antwort:	Nein	

Schutzziel(e):	Rechtskonformität
BTR_03.01:	**Voraussetzungen zur Zulässigkeit automatisierter Einzelentscheidungen** **Teilfrage**
Frage:	Werden alle Voraussetzungen für die Zulässigkeit einer automatisiertes Einzelentscheidungen erfüllt?
Beschreibung:	Folgende Aspekte müssen positiv beantwortet werden können: - die betroffene Person hat ausdrücklich eingewilligt oder es liegt eine gesetzliche Grundlage vor oder die Entscheidung ist für die Erfüllung eines Vertrages mit dem Betroffenen erforderlich - die betroffene Person kann erwirken, dass eine natürliche Person seitens des Verantwortlichen in die Entscheidung involviert wird - die betroffene Person kann ihren eigenen Standpunkt darlegen und die Entscheidung anfechten - die Entscheidung erfolgt nicht auf Grundlage sensibler Daten - die betroffene Person wird rechtzeitig über die automatisierte Entscheidungsfindung, die involvierte Entscheidungslogik und die Tragweite und die angestrebten Auswirkungen informiert
Antwort:	Entbehrlich
Schutzziel(e):	Rechtskonformität

2. 1. Reaudit Datenschutzorganisation

OrgEH:	Team Secure AG (TeSA)
Audit:	Internes Überwachungsaudit zur Umsetzung der DSGVO (INT_ÜA_DS_Jahr03)
Hauptprüfer:	Peter Innereiter
Interviewpartner:	Tom Leisch
Beschreibung:	es soll festgestellt werden, inwieweit die Organisation die grundsätzlichen Anforderungen aus der DSGVO bereits umgesetzt hat

Prüfobjekt:	**1. Reaudit Datenschutzorganisation (TeSA_DSO_02)** 22.01.2019 16:12
Verantwortlich(e):	Tom Leisch
Wissensdatenbank:	DEMO: Assessment zur Umsetzung der Datenschutz-Grundverordnung, Version: 5



Prüffrage(n):

DSO_00.00:	**Committment der Geschäftsführung**
Frage:	Besteht Committment seitens der Geschäftsführung, die Umsetzung der DSGVO zu unterstützen?
Beschreibung:	Folgende Aspekte sollten positiv beantwortet werden können: - das Management ist sich der Anforderungen aus der DSGVO und der möglichen Folgen bei deren Nichterfüllung bewusst - das Management stellt die nötigen Ressourcen (Personal, Zeit, Budget) zur Umsetzung der DSGVO zur Verfügung - das Management unterstützt die nötigen Aktivitäten im Zuge der Umsetzung der DSGVO
Antwort:	**Reifegrad 3: definiert**
Begründung:	Managementunterstützung sichergestellt - laufende Betrachtung des Themas in regelmäßigen Meetings
Schutzziel(e):	Rechtskonformität
Zugeteiltes Risiko:	**mangelndes Bewusstsein bzgl. Datenschutz (DSO_001)**

DSO_01.00:	**Datenschutzkonzept**	**Strukturfrage**
Frage:	Haben Sie in Ihrem Unternehmen ein Datenschutzkonzept etabliert?	
Beschreibung:	Mit dieser Frage soll festgestellt werden, ob Datenschutz in Ihrem Unternehmen wahrgenommen und umgesetzt wird. Je nach Unternehmensgröße empfiehlt sich ein schlüssiges Datenschutzkonzept bis hin zu einem richtig gelebten Datenschutzmanagementsystem. Es sollten jedenfalls folgende Aspekte positiv beantwortet werden können: - eine Unternehmens-Datenschutzrichtlinie ist erstellt und kommuniziert - Verantwortlichkeiten in Bezug auf Datenschutzthemen sind definiert - Mitarbeiter sind in Bezug auf Datenschutz geschult - Vertraulichkeitsvereinbarungen mit allen relevanten Interessensgruppen werden abgeschlossen	
Antwort:	Reifegrad 2: gemanaged	
Begründung:	Richtlinie ist erstellt und Bewusstseinsbildung wird fokussiert	
Schutzziel(e):	Rechtskonformität	

DSO_01.01:	**Ressourcen und Verantwortlichkeiten**	**Teilfrage**
Frage:	Sind die benötigten Ressourcen verfügbar und die Verantwortlichkeiten definiert?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden: - personelle Ressourcen (intern oder extern) zur Erstellung und Umsetzung des Datenschutzkonzeptes sind vorhanden - die Verantwortlichkeiten zur Erstellung und Umsetzung des Datenschutzkonzeptes sind definiert	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	Verantwortlichkeiten definiert	
Schutzziel(e):	Rechtskonformität	

DSO_01.02:	**Datenschutz-Richtlinie**	**Teilfrage**
Frage:	Existiert eine Datenschutz-Richtlinie, die Vorgaben zu den wesentlichen Datenschutzgrundsätzen und interne Regeln zum Datenschutz enthält?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden. Die Richtlinie regelt: - rechtliche Rahmenbedinungen im Unternehmen - die wesentlichen Vorgaben zu den Datenschutzgrundsätzen (Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung und Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit) - grundsätzliche technische und organisatorische Maßnahmen zur Sicherstellung des Datenschutzes - generelle unternehmensinterne Regeln zum Datenschutz Die Richtlinie ist verschriftlicht und wird regelmäßig aktualisiert und kommuniziert werden.	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	erstellt und unterliegt Kontrolle	
Schutzziel(e):	Rechtskonformität	

DSO_01.03:	**Mitarbeiter-Awareness**	**Teilfrage**
Frage:	Werden Mitarbeiter regelmäßig auf Datenschutz-Themen geschult?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden: - die Datenschutzrichtlinie wird an die Mitarbeiter kommuniziert und die Inhalte im Zuge einer Basis-Schulung regelmäßig aufgefrischt - ggf. finden bereichsspezifische Schulungen zum Thema Datenschutz statt - Schulungen werden nachvollziehbar dokumentiert	
Antwort:	**Reifegrad 3: definiert**	
Begründung:	Schulung geplant und zT bereits durchgeführt	
Schutzziel(e):	Rechtskonformität	

DSO_01.04:	**Vertraulichkeitsvereinbarungen**	**Teilfrage**
Frage:	Werden standardmäßig Vertraulichkeitsvereinbarungen mit Vertretern aller relevanten Interessengruppen getroffen?	
Beschreibung:	Mitarbeiter, Lieferanten, Partner und andere Interessensgruppen, die mit personenbezogenen Daten in Berührung kommen sollten zur Vertraulichkeit verpflichtet werden. Folgende Aspekte sollten positiv beantwortet werden können: - es werden standardmäßig Vertraulichkeitsvereinbarungen abgeschlossen, wenn Personen im Zuge ihrer Tätigkeit, die in die Sphäre Ihres Unternehmens fällt, mit personenbezogenen Daten in Berührung kommen - Vertraulichkeitsvereinbarungen werden regelmäßig überprüft und ggf. angepasst	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	da müssen wir noch genauer hinschauen	
Schutzziel(e):	Rechtskonformität	

DSO_01.05:	**Datenübermittlungen in Drittländer**	**Teilfrage**
Frage:	Ist sichergestellt, dass bei Übermittlung personenbezogener Daten in Drittländer datenschutzrechtliche Anforderungen ausreichend erfüllt werden?	
Beschreibung:	Folgende Aspekte können positiv beantwortet werden: - es herrscht Bewusstsein darüber, wann personenbezogene Daten an Drittländer übermittelt werden - es gibt Prozesse, die bei der Übermittlung in Drittländer zur Anwendung kommen und - im Zuge derer Maßnahmen getroffen werden, die ein DSGVO-konformes Schutzniveau gewährleisten	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	Prozesse in Erarbeitung/Umsetzung	
Schutzziel(e):	Rechtskonformität	

DSO_02.00:	**Datenschutzgrundsätze**	**Strukturfrage**
Frage:	Ist sichergestellt, dass die Datenschutzgrundsätze eingehalten werden?	
Beschreibung:	Jede Verarbeitung personenbezogener Daten muss unter Einhaltung der Datenschutz-Grundsätze erfolgen. Deren Einhaltung muss sichergestellt und dokumentiert werden. Kann die Einhaltung und Dokumentation aller Datenschutzgrundsätze bejaht werden: - Rechtmäßigkeit, Transparenz - Zweckbindung - Datenminimierung - Richtigekeit - Speicherbegrenzung - Integrität und Vertraulichkeit	
Antwort:	Reifegrad 2: gemanaged	
Begründung:	erste Schritte gesetzt	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

DSO_02.01:	**Rechtmäßigkeit**	**Teilfrage**
Frage:	Wird überprüft ob personenbezogene Daten verarbeitet werden dürfen?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden: - Existiert eine Rechtsgrundlage für sämtliche Verarbeitungstätigkeiten (Gesetz, Vertrag, Einwilligung,...)? - Ist die Rechtsgrundlage für jede Verarbeitungstätigkeit dokumentiert?	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	wird gerade genauer betrachtet	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

DSO_02.02:	**Transparenz/Informationspflichten**	**Teilfrage**
Frage:	Wird den Informationspflichten ausreichend nachgekommen?	
Beschreibung:	Für betroffenen Personen muss nachvollziehbar sein, ob, zu welchem Zweck und wie personenbezogene Daten über sie verarbeitet werden. Können dazu folgende Aspekte positiv beantwortet werden: - Datenschutzerklärungen für alle relevanten Interessensgruppen liegen auf - die Datenschutzerklärungen decken alle relevanten Verarbeitungstätigkeiten ab - die Datenschutzerklärungen enthalten alle geforderten Informationen - die Datenschutzerklärungen werden aktuell gehalten - betroffenen Personen ist es leicht möglich, auf für sie relevante Datenschutzerklärungen zuzugreifen - insbesondere die Datenschutzerklärung auf der Unternehmenshomepage listet alle dort durchgeführten Verarbeitungen und ist leicht auffindbar	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	erste Schritte gesetzt - Datenschutzerklärung auf Homepage eingebunden und aktualisiert	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

DSO_02.03:	**Zweckbindung**	**Teilfrage**
Frage:	Wird für jede Verarbeitungstätigkeit definiert, zu welchem konkreten Zweck sie erfolgt?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden: - für jede Verarbeitungstätigkeit kann für betroffene Personen nachvollziehbar angegeben werden, wofür die personenbezogenen Daten verwendet werden - die Zwecke sind legitim und stehen im Einklang mit anderen rechtlichen Verpflichtungen (wie zB aus dem Arbeits- oder Vertragsrecht)	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	wird derzeit definiert/überprüft	
Schutzziel(e):	Rechtskonformität ● ● ● ●	

DSO_02.04:	**Datenminimierung**	**Teilfrage**
Frage:	Wird sichergestellt, dass nur die für den Zweck erforderlichen Daten erhoben und in weiterer Folge verarbeitet werden?	
Beschreibung:	Können dazu folgende Aspekte positiv beantwortet werden: - es werden nur die zur Erfüllung des Zwecks erforderlichen Daten verarbeitet - der Zweck kann nicht mit weniger oder gar keinen personenbezogenen Daten erfüllt werden	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	für neue Prozesse definiert, bestehende Verarbeitungen werden dahingehend geprüft	
Schutzziel(e):	Rechtskonformität	

DSO_02.05:	**Richtigkeit**	**Teilfrage**
Frage:	Wird sichergestellt, dass personenbezogene Daten auf dem aktuellen Stand sind, wenn dies für die Verarbeitung essentiell ist?	
Beschreibung:	Es gibt einen Prozess der sicherstellt, dass personenbezogene Daten auf dem aktuellen Stand und sachlich richtig sind, wenn dies für den Zweck der Verarbeitung erforderlich ist.	
Antwort:	**Reifegrad 1: initial**	
Begründung:	noch nicht definiert	
Schutzziel(e):	Rechtskonformität	

DSO_02.06:	**Speicherbegrenzung**	**Teilfrage**
Frage:	Wird sichergestellt, dass personenbezogene Daten nur solange gespeichert werden, wie es für die Zwecke der Verarbeitung erforderlich ist?	
Beschreibung:	Können folgende Aspekte positiv beantwortet werden: - personenbezogene Daten werden nur solange gespeichert, wie es für die Zwecke der Verarbeitung notwendig ist - sobald die Identifizierung der betroffenen Person nicht mehr erforderlich ist, werden die Daten anonymisiert bzw. zumindest pseudonymisiert - gesetzliche Aufbewahrungspflichten werden berücksichtigt	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	derzeit manuell - noch sehr fehleranfällig und nicht durchdefiniert	
Schutzziel(e):	Rechtskonformität	

DSO_02.07:	**Sicherheit der Verarbeitung**	**Teilfrage**
Frage:	Werden personenbezogene Daten in einer Weise verarbeitet, sodass ihre Integrität, Vertraulichkeit und Verfügbarkeit sichergestellt sind?	
Beschreibung:	Es werden Maßnahmen zum Schutz personenbezogener Daten hinsichtlich Vertraulichkeit, Integrität und Verfügbarkeit umgesetzt.	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	grundsätzliches Sicherheitskonzept besteht - Abgleich mit DSGVO Anforderungen noch ausständig	
Schutzziel(e):	Rechtskonformität	

DSO_02.08:	**Rechenschaftspflicht**	**Teilfrage**
Frage:	Kann die Einhaltung der Datenschutzgrundsätze nachgewiesen werden?	
Beschreibung:	Folgender Aspekt muss dazu bejaht werden können: Maßnahmen und Prozesse iZm Datenschutz werden nachweislich dokumentiert.	
Antwort:	**Reifegrad 2: gemanaged**	
Begründung:	Dokumentation ist vorgeschrieben, muss noch etabliert werden	
Schutzziel(e):	Rechtskonformität	