Schleswig-Holstein
Der Ministerpräsident
Staatskanzlei

§ 59 Vereinbarung ITSM-SH

Vereinbarung mit den Spitzenorganisationen der Gewerkschaften nach § 59 des Gesetzes über die Mitbestimmung der Personalräte (Mitbestimmungsgesetz Schleswig-Holstein – MBG Schl.-H.) vom 11. Dezember 1990 (GVOBl. Schl.-H. S. 577), zuletzt geändert durch Art. 16 Landesverordnung zur Anpassung von Rechtsvorschriften an geänderte Zuständigkeiten der obersten Landesbehörden und geänderte Ressortbezeichnungen vom 16.01.2019 (GVOBl. Schl.-H. S. 30)

Zwischen

dem Land Schleswig-Holstein vertreten durch die Staatskanzlei - Zentrales IT-Management (Land) – einerseits

und

dem Deutschen Gewerkschaftsbund - Bezirk Nord und dem dbb beamtenbund und tarifunion - Landesbund Schleswig-Holstein (Spitzenorganisationen) – andererseits

über das IT-Verfahren IT-Service-Management-System (ITSM-SH).

Redaktioneller Hinweis

Im Dokument wurden möglichst geschlechtsneutrale Begriffe verwendet. In Fällen, in denen männliche oder weibliche Begriffe aus sprachlichen Gründen gewählt werden mussten, sind selbstverständlich alle Geschlechter angesprochen.

§ 1 Gegenstand

Gegenstand dieser Vereinbarung ist der Einsatz des IT-Verfahrens **ITSM-SH** in den Behörden und Dienststellen in der schleswig-holsteinischen Landesverwaltung. Der Gegenstand wird insbesondere in **Anlage 1** dieser Vereinbarung näher beschrieben.

§ 2 Geltungsbereich

Diese Vereinbarung gilt in den Behörden und Dienststellen für die Beschäftigten der unmittelbaren Landesverwaltung im Sinne des § 3 Abs. 1 in Verbindung mit § 2 Abs. 1 Mitbestimmungsgesetz des Landes Schleswig-Holstein (MBG).

Diese Vereinbarung findet keine Anwendung, sofern die Regelungen des IT-Gesetzes für die Justiz des Landes Schleswig-Holstein (ITJG) bzw. die auf dieser Grundlage getroffenen Bestimmungen und Regelungen dem entgegenstehen.

Sie gilt entsprechend für die Landtagsverwaltung und den Landesrechnungshof, wenn deren Präsidentinnen oder Präsidenten ihr Einvernehmen nach § 59 Absatz 4 des Mitbestimmungsgesetzes Schleswig-Holstein erklärt haben.

§ 3 Verfahrensumfang

In dem ITSM-SH sind mehrere IT-Dienstleistungen (IT-Services) insbesondere zu bestehenden IT-Verfahren hinterlegt, die mithilfe von standardisierten IT-Prozessen zu betreuen sind. Das Software-Produkt für das ITSM-SH ist assyst (Näheres siehe **Anlage 1**).

Ziel ist es, die Qualität, Wirtschaftlichkeit und Ordnungsmäßigkeit der IT-Services zu verbessern und die Zufriedenheit der Anwendenden mit Hilfe des IT-Verfahrens ITSM-SH zu erhöhen.

Betroffen sind zum einen die Endanwendenden der durch das ITSM-SH unterstützten IT-Verfahren, insbesondere wenn die Endanwendenden Anliegen zu diesen IT-Verfahren melden, zum anderen die Anwendenden und Verantwortlichen des ITSM-SH selbst.

Die Schnittstellen des ITSM-SH, die eine Übertragung personenbezogener Daten von Beschäftigten beinhalten, sind in **Anlage 3** dieser Vereinbarung mit den betreffenden Daten und dem jeweiligen Zweck der Übertragung aufgeführt.

Für jedes Ressort wird im ITSM-SH ein eigener, geschützter Zugriffsbereich (Mandant) erstellt, in dem die ressortspezifischen IT-Services der IT-Verfahren abgebildet und bearbeitet werden.

Daneben besteht ein ressortübergreifender Mandant, über den ressortübergreifende IT-Services und IT-Verfahren für die anderen Mandanten zur Verfügung gestellt werden.

Sofern für IT-Verfahren besondere Auflagen oder Anforderungen an den Datenschutz und die Informationssicherheit gelten, werden darüber hinaus gesonderte Mandanten für diese eingerichtet.

§ 4 Zuständigkeiten

Gemäß der Landesverordnung über die zentrale Stelle (ZStVO) ist die für das Zentrale IT-Management zuständige oberste Landesbehörde zentrale Stelle für das ITSM-SH. Die ZStVO regelt auch den Umfang der Zuständigkeit der zentralen Stelle des ITSM-SH. Die Aufgaben der zentralen Stelle werden im Zentralen IT-Management SH durch die IT-Verantwortung (ITV) ITSM-SH wahrgenommen.

Die zentrale Stelle beauftragt Dataport als Auftragsverarbeiter gemäß Art. 28 EU DSGVO mit dem ITSM-SH.

Beteiligte Stellen sind gemäß der Landesverordnung die Landesbehörden, die das ITSM-SH nutzen.

§ 5 Rechte und Rollen, Dokumentation

Der Zugriff auf ITSM-SH erfolgt auf Basis eines Rahmen-Berechtigungskonzeptes, das von der zentralen Stelle verantwortet wird (siehe **Anlage 2**). Beteiligte Stellen prägen das Rahmen-Berechtigungskonzept für ihren Bereich spezifisch aus. Diese Ausprägung stimmen sie mit den für ihren Bereich zuständigen Vertretungen von Personalinteressen (Personalvertretungen, Gleichstellungsbeauftragte, Schwerbehindertenvertretungen) ab. Sie machen der zentralen Stelle ihr individuelles Konzept zugänglich.

Die Vergabe, Änderung und Löschung von Zugriffsberechtigungen sind durch die beteiligten Stellen gesondert zu dokumentieren. Die Dokumentation ist der zentralen Stelle zugänglich zu machen.

§ 6 Verarbeitung von Daten mit ITSM-SH

Das ITSM-SH und die damit einhergehende Verarbeitung von Daten dienen der Unterstützung der schrittweisen, arbeitsteiligen Bearbeitung und Dokumentation von IT-fachlichen Aufgaben mithilfe von standardisierten IT-Prozessen durch ITSM-SH und Dataport. Dies ist notwendigerweise mit einer personenbezogenen Erfassung der Service-Anfragen verbunden. Die personenbezogenen Daten werden entweder direkt im ITSM-SH gepflegt oder automatisiert über die Schnittstellen übernommen und schreibgeschützt im ITSM-SH angezeigt (siehe **Anlage 3**).

Die mit dem Einsatz des ITSM-SH verbundene Verarbeitung von Daten dient zugleich der Wahrnehmung von Aufsichts- und Steuerungsbefugnissen der zentralen Stelle und der beteiligten Stellen.

Daten von Beschäftigten, die bei Einsatz des ITSM-SH verarbeitet werden, dürfen nicht zu Zwecken der personenbezogenen Verhaltens- oder Leistungskontrolle ausgewertet werden.

§ 7 Berichte

Im IT-Verfahren ITSM-SH werden Standard-Berichte in dem in Anlage 4 dargestellten Umfang bereitgestellt (siehe **Anlage 4**). Diese Berichte sind durch die Verwendung einer „Ereignis-Referenz“ an Stelle von User-Kennungen pseudonymisiert.

Soweit über die Standard-Berichte hinaus Berichte erforderlich sind, fordert eine beteiligte Stelle oder mehrere beteiligte Stellen gemeinsam diese bei der zentralen Stelle des ITSM-SH an. Werden in diesen Berichten personenbezogene Daten verarbeitet, die über den mit den Spitzenorganisationen abgestimmten Umfang gemäß Anlage 4 hinausgehen, sind diese mit den Spitzenorganisationen abzustimmen.

Alle Berichte sind nur im Rahmen der Zweckbindung von ITSM-SH zulässig. Personenbezogene Daten von Beschäftigten dürfen in den Berichten nur dann genutzt werden, wenn dies für die Umsetzung der Servicezwecke erforderlich ist.

§ 8 Ergonomie und Barrierefreiheit

Da die Nutzung des ITSM-SH mit einer veränderten Arbeitsweise verbunden sein kann, kann dies im Einzelfall Anlass einer Gefährdungsanalyse nach § 5 Abs. 1 Arbeitsschutzgesetz an den betroffenen Arbeitsplätzen sein.

Die technische Ausstattung an betroffenen Arbeitsplätzen ist bedarfsabhängig zu prüfen. Dabei finden die einschlägigen gesetzlichen Bestimmungen Anwendung; gesicherte arbeitswissenschaftliche Erkenntnisse werden berücksichtigt.

Die geltenden Normen zur Gebrauchstauglichkeit werden beachtet.

Die barrierefreie Nutzbarkeit des IT-Verfahrens ITSM-SH wurde durch Konformität des Software-Produktes assyst mit den zum Zeitpunkt der Beauftragung geltenden gesetzlichen Anforderungen weitestgehend umgesetzt. Durch die Weiterentwicklung des Software-Produktes assyst sollen auch gesetzliche Anforderungen erfüllt werden, die sich seit Beauftragung geändert haben oder zukünftig ändern werden. Darüber hinaus wird die barrierefreie Nutzbarkeit durch individuelle Anpassungen am Arbeitsplatz erhöht.

Erfahrungswerte aus der Nutzung des ITSM-SH, insbesondere im Hinblick auf ergonomische Gesichtspunkte, fließen bei Optimierungen mit ein. Dies gilt auch für

übergreifend zu entscheidende Optimierungen im Rahmen der Zusammenarbeit mit der für das ITSM-SH zuständigen zentralen Stelle.

§ 9 Schulung

Die Verwaltung stellt individuell bedarfsgerechte und adressatengerechte Schulungsmaßnahmen zur Verfügung, um alle Anwendenden des ITSM-SH zu einer selbständigen und sicheren Erledigung ihrer Aufgaben mit Hilfe des IT-Verfahrens zu befähigen.

§ 10 Änderungen am IT-Verfahren

Vom Land beabsichtigte Änderungen des IT-Verfahrens ITSM-SH, die den in den Anlagen dokumentierten Zustand betreffen, bedürfen der Zustimmung der Spitzenorganisationen. Die Zustimmung gilt als erteilt, wenn nicht innerhalb von vier Wochen nach Mitteilung durch die Spitzenorganisation widersprochen wird. Die Anlagen sind danach entsprechend anzupassen.

§ 11 Schlussbestimmungen

Diese Vereinbarung tritt am Tage ihrer Unterzeichnung in Kraft.

Sie wird im Amtsblatt und im Transparenzportal Schleswig-Holstein veröffentlicht.

Diese Vereinbarung wird außerdem im Extranet der Öffentlichen Verwaltung Schleswig-Holstein (SHIP) bereitgestellt. Dies gilt auch für geänderte Fassungen gemäß § 10.

Diese Vereinbarung kann einvernehmlich geändert werden.

Diese Vereinbarung kann von beiden Seiten mit einer Frist von sechs Monaten zum Jahresende gekündigt werden.

Anlage 1 - Produktübersicht ITSM-SH

Anlage 2 - Rollen und Rechte im ITSM-SH

Anlage 3 - Personenbezogene Daten und Schnittstellen

Anlage 4 - Berichte

_____

Ort, Datum

Für die
Staatskanzlei
- Zentrales IT-Management –

_____

StK CdS Dirk Schrödter

_____

Ort, Datum

Für den
Deutschen Gewerkschaftsbund
- Bezirk Nord –

_____

Olaf Schwede

_____

Ort, Datum

Für den
dbb beamtenbund und tarifunion
- Landesbund Schleswig-Holstein -

_____

Kai Tellkamp

Schleswig-Holstein
Der Ministerpräsident
Staatskanzlei

Produktübersicht ITSM-SH

Anlage 1

Zur Vereinbarung nach § 59 MBG SH

über das IT-Verfahren IT-Service-Management-System (ITSM-SH)

Redaktioneller Hinweis

Im Dokument wurden möglichst geschlechtsneutrale Begriffe verwendet. In Fällen, in denen männliche oder weibliche Begriffe aus sprachlichen Gründen gewählt werden mussten, sind selbstverständlich alle Geschlechter angesprochen.

Inhaltsverzeichnis

1 ITSM-SH Übersicht

Das Software-Produkt, das zur Realisierung eines professionellen IT-Service-Management (ITSM) im Rahmen des Verfahrens ITSM-SH in der Landesverwaltung Schleswig-Holstein Anwendung findet, ist assyst von der Firma IFS.

Das ITSM-SH gliedert sich grundlegend in folgende Funktionsbereiche:

1. **Servicekatalog**: Definition und Bereitstellung der verschiedenen IT-Services
2. **Service-Desk Software**: Erfassung, Bearbeitung und Dokumentation der IT-fachlichen Aufgaben mithilfe der standardisierten IT-Prozesse durch die Anwendenden des ITSM-SH.
3. **Self-Service Portal**: Übersichtliche und funktions-reduzierte Oberfläche für die Anwendenden der unterstützen IT-Verfahren (Einsatz ggf. geplant) sowie eingeschränkten Erfassung, Bearbeitung und Dokumentation von IT-fachlichen Aufgaben durch die Anwendenden des ITSM-SH selbst
4. **Berichtswesen**: (Automatisierte) Bereitstellung von Berichten zu den IT-Services
5. **Konfigurations-Datenbank (CMDB)**: Bereitstellung von Anwendenden-, Organisations- und Lokationsstammdaten sowie PC-Stammdaten und Softwareinformationen, die zuvor über die Schnittstellen eingelesen wurden (vgl. **Anlage 2**)

2 ITSM-SH Prozessübersicht

Folgende standardisierte Prozesse sind im ITSM-SH im Einsatz (E) beziehungsweise für den Einsatz geplant (P):

1. **Störungs-Management (Incident-Management)** (E): Das Störungs-Management stellt die schnellstmögliche Wiederherstellung des normalen IT-Betriebes und die Minimierung der Auswirkungen auf die IT-Funktionsfähigkeit der Landesverwaltung Schleswig-Holstein sicher.
2. **Problem-Management** (P): Prozess, der die Ursachenanalyse zur Bestimmung und Behebung der Ursachen von Störungen sowie proaktive Maßnahmen zur Ermittlung und Vermeidung künftiger IT-Probleme/Störungen beinhaltet.
3. **Änderungs-Management (Change-Management)** (E): Der Prozess Änderungs-Management stellt standardisierte Verfahren für eine strukturierte Vorbereitung und Steuerung von Änderungen an der IT-Infrastruktur und den IT-Verfahren zur Verfügung.
4. **Anforderungs-Management (Demand-Management)** (E): Der Prozess Anforderungs-Management stellt standardisierte Verfahren für eine strukturierte Vorbereitung und Steuerung von IT-Anforderungen zur Verfügung.
5. **Konfigurations-Management (Configuration-Management)** (P): Der Prozess Konfigurations-Management stellt allen anderen beteiligten Prozessen Informationen über die aktuelle IT-Infrastruktur zur Verfügung.

6. **Versionsmanagement-Management** (Release-Management) (P): Prozess mit dem Zweck, den Aufbau, Test und die Entwicklung von Releases (z. B. bei Hardware, Software) zu planen und zu steuern, sowie neue IT-Funktionen gemäß den Geschäftsanforderungen bereitzustellen und gleichzeitig die Integrität bestehender IT-Services zu schützen.
7. **Vertrags-/Vereinbarungs-Management (Service Level Management) und IT-Dienstleister-Management (Supplier Management)** (P): Der Prozess Vertrags-/Vereinbarungs-Management ist für das Verhandeln von erreichbaren Vereinbarungen (Service Level) sowie die Überprüfung deren Einhaltung verantwortlich. Der Prozess IT-Dienstleister-Management stellt sicher, dass alle Verträge mit Lieferanten die geschäftsseitigen Notwendigkeiten unterstützen und dass alle IT-Dienstleister ihre vertraglichen Pflichten erfüllen.
8. **Zugriffs-Management (Access-Management)** (P): Das Zugriffs-Management ist der Prozess, der es autorisierten Anwendenden erlaubt, auf einen IT-Service zuzugreifen und den unautorisierten Zugriff verhindert.
9. **Kontinuierliche Service Verbesserung (Continual Service Improvement)** (P): Die kontinuierliche Service-Verbesserung setzt Methoden des Qualitätsmanagements ein, um aus Erfolgen und Misserfolgen der Vergangenheit zu lernen.

SH Schleswig-Holstein
Der Ministerpräsident
Staatskanzlei

Organisatorisches Rollen- und Rechtekonzept

Anlage 2

Zur Vereinbarung nach § 59 MBG SH

über das IT-Verfahren IT-Service-Management-System (ITSM-SH)

Inhaltsverzeichnis

Abbildungen und Tabellen

Redaktioneller Hinweis

Im Dokument wurden möglichst geschlechtsneutrale Begriffe verwendet. In Fällen, in denen männliche oder weibliche Begriffe aus sprachlichen Gründen gewählt werden mussten, sind selbstverständlich alle Geschlechter angesprochen.

1 Dokumenteninformation

1.1 Ausgangslage

Die Landesverwaltung Schleswig-Holstein hat in einem Vergabeverfahren unter Einbeziehung der Anforderungen insbesondere des Justizministeriums das IT-Service-Management-Tool (ITSM-Tool) ITSM-SH der Firma IFS ausgewählt, welches in den teilnehmenden Behörden der unmittelbaren Landesverwaltung zum Einsatz kommen soll und somit landeseinheitliche Standardprozesse zum Management von IT-Services implementiert werden sollen.

Die Implementierung muss zu einem ordnungsgemäßen Betrieb des ITSM-SH-Tools führen. Die Verantwortung für den ordnungsgemäßen Betrieb des IT-Verfahrens ITSM-SH liegt bei der zentralen Stelle im zentralen IT-Management (ZIT SH). Die grundsätzliche Struktur (Applikationsdesign) des ITSM-SH-Tools (z.B. Mandantenstruktur, Schnittstellenanforderungen, übergreifendes Reporting, usw.) wird vom ZIT SH vorgegeben.

Das vorliegende Konzept beschreibt, wie die Rollen- und Rechtevergabe aus organisatorischer Sicht abläuft.

1.2 Geltungsbereich

Dieses Dokument gilt für die Landesverwaltung Schleswig-Holstein.

1.3 Ziel

Es handelt sich bei diesem Konzept um ein ergänzendes Rollen- und Rechtekonzept, das die vom Hersteller gelieferte technische Rollen- und Rechtekonzeption um verwaltungsorganisatorisch relevante Aspekte ergänzt.

2 Rollen und Rechte im ITSM-SH-Tool

Im „ITSM-SH“-Tool werden Mitarbeiterinnen und Mitarbeiter zu „Berechtigungsgruppen“ zugeordnet und erhalten durch diese Zuordnung die entsprechenden Zugriffrechte auf die Formulare und Daten, die zur Erfüllung ihrer Aufgaben benötigt werden. Das ITSM-SH-Tool und die damit einhergehende Verarbeitung von personenbezogenen Daten dienen der Unterstützung der schrittweisen, arbeitsteiligen Bearbeitung und Dokumentation von IT-fachlichen Aufgaben mithilfe von standardisierten IT-Prozessen.

Die personenbezogenen Daten werden gemäß Art. 5 Abs. 1 DSGVO rein zweckgebunden verarbeitet. Die erforderlichen personenbezogenen Daten sind Grundlage für die Nutzung des IT-Verfahrens und ermöglichen folgende verfahrensrelevante Notwendigkeiten:

a) Zuordnung eines Tickets zu der Person, die dieses aufgegeben hat
b) Zuordnung des Anwendenden zu dessen Hardware
c) Kontaktaufnahme über E-Mail
d) Gemeinsame Bearbeitung der IT-fachlichen Aufgaben mit Dataport

Eine Übersicht der personenbezogenen Daten findet sich in der ergänzenden Unterlage „Übersicht personenbezogener Daten und Schnittstellen“ wieder.

Zusätzlich zu den Berechtigungsgruppen erfolgt innerhalb des Tools eine Mandanten-Trennung. Die Funktion der Mandanten-Trennung erlaubt es, Informationen im ITSM-SH-Tool, seien es Infrastrukturdatensätze[1] oder Ereignisse[2], Mandanten zuzuordnen und somit den Zugriff auf diese Informationen nur bestimmten Personenkreisen zu erlauben. Eine Übersicht der aktuellen Mandanten, welche das Tool nutzen, findet sich in Anlage 4 „Standard-Berichte im ITSM-SH“.

Nachfolgend befindet sich eine Auflistung der implementierten Berechtigungsgruppen mit einer kurzen Erläuterung. Eine detailliertere Beschreibung über Zugriffe auf bestimmte Funktionalitäten befindet sich im technischem Rollen- und Rechtekonzept.

[1] Es handelt sich hierbei um sog. Konfigurationselemente(CI), die Gesamtheit aller an den Geschäftsprozessen beteiligten Betriebsmittel, wie bspw. Services, Gebäude, Organisation usw.,
[2] Ereignisse sind alle Aktivitäten, die im Tool vorgenommen werden können, bspw. die Erstellung eines Tickets, die Bearbeitung von Aufgaben

Berechtigungsgruppe	Beschreibung
Service Operations	Diese Berechtigungsgruppe ist die Standard-Berechtigungsgruppe für die ITSM-SH-Tool Nutzerinnen und Nutzer des Landes Schleswig-Holstein. Mitglieder dieser Berechtigungsgruppe haben lesenden Zugriff auf alle Infrastrukturdaten[1] (gem. ihrer Mandanten-Zuordnung). Es ist ihnen nicht gestattet Infrastrukturdaten anzulegen, zu ändern oder zu löschen. Eigene Ereignis- und Objektabfragen, Spaltenprofile sowie Ereignisverknüpfungen dürfen erstellt, geändert und gelöscht werden. Prozessual in der Ereignisbearbeitung ist Mitgliedern dieser Gruppe das Erstellen und Sichten von Ereignissen sowie das Ausführen von Aktionen auf Ereignissen nur innerhalb der eigenen SVA (Serviceabteilung / Supportgruppe) gestattet.
Service Operations Justiz	Diese Berechtigungsgruppe ist die Standard-Berechtigungsgruppe für die ITSM-SH-Tool Nutzerinnen und Nutzer des Mandanten „Justiz“ des Landes Schleswig-Holstein. Diese Berechtigungsgruppe ist analog zur der Berechtigungsgruppe „Service Operations“ angelegt. Prozessual in der Ereignisbearbeitung ist Mitgliedern dieser Gruppe, abweichend zur Berechtigungsgruppe Service Operations, das Sichten von Ereignissen aller SVAs (Serviceabteilungen / Supportgruppen) des Mandanten Justiz gestattet.
assystNET Benutzer	Diese Berechtigungsgruppe ist für alle assystNET-Benutzerinnen und Benutzer implementiert. assystNET ist eine Plattform des ITSM-SH-Tools, das sog. „Self-Service-Portal“ für die Kontaktbenutzer (Endbenutzerinnen/Endbenutzer). Mit assystNET wird dem Benutzenden ein alternativer Web-Zugang zum System mit eingeschränkten Funktionalitäten zur Verfügung gestellt (Self-Service-Portal). Der Benutzende kann Ereignisse für sich und für andere Benutzende (Betroffene) auf einer reduzierten Oberfläche aufnehmen und deren Bearbeitungsstatus abfragen.

Berechtigungsgruppe	Beschreibung
Mandanten Administrator	Diese Berechtigungsgruppe ist für Administratorinnen und Administratoren der einzelnen Mandanten eingerichtet. Mitglieder dieser Berechtigungsgruppe nehmen Aufgaben der Administration innerhalb ihres Mandanten wahr. Hierzu gehört zum Beispiel das Recht, Gebäude, Service Abteilungen, Abfrage Profile usw. anzuzeigen, anzulegen und zu verändern. Weiterhin erhalten Mitglieder dieser Berechtigungsgruppe Zugriff auf administrative Funktionen, wie zum Beispiel den Service-Designer, mit dem Service-Angebote hinzugefügt oder verändert werden können. Mandantenadministratorinnen und -administratoren erhalten keine Rechte auf die Konfiguration, Einstellungen, Protokolle oder Berechtigungen des Tools.
Administrative Gruppe	Diese Berechtigungsgruppe ist für die Administratorinnen und Administratoren des ITSM-SH-Tools. Diese Mitarbeiterinnen und Mitarbeiter haben vollumfänglichen Zugriff auf das System und die angebundenen Schnittstellen. Dieser Berechtigungsgruppe werden keine Mitarbeiter der Mandanten zugeordnet. Die Hoheit der Administration liegt bei Dataport.
INTEGRATIONSPLATFORM_ GROUP | etmusers	Diese Berechtigungsgruppe dient lediglich der Zugriffsteuerung zur Schnittstellenapplikation. Benutzerinnen und Benutzer, die dieser Gruppe zugeordnet sind, können sich an dieser Oberfläche anmelden und dann hierrüber die Schnittstellen überwachen, einrichten und administrieren. Es sind dieser Gruppe keine weiteren administrativen oder prozessualen Rechte zugeordnet. Dieser Berechtigungsgruppe werden ausschließlich Mitarbeiterinnen und Mitarbeiter von Dataport zugeordnet.

Tabelle 1: Übersicht Berechtigungsgruppen

Durch die beschriebene Implementierung der Rechte im ITSM-SH-Tool wird sichergestellt, dass Mitarbeiterinnen und Mitarbeiter nur Zugriff auf die für ihre Arbeit notwendigen Daten erhalten und keine Daten und Informationen einsehen können, die für ihren Bereich nicht relevant sind.

Zudem spiegeln die definierten Berechtigungen im ITSM-SH-Tool keine Führungsfunktion innerhalb der Mandanten wieder. Es gibt somit keine dedizierte Rolle die an eine Führungsfunktion gekoppelt ist.

3 Prozess zur Rechte- und Rollenvergabe

In diesem Abschnitt wird die Rollen- und Rechtevergabe von Service-Mitarbeiterinnen und -Mitarbeitern im ITSM-SH-Tool beschrieben.

Soll eine neue Service-Mitarbeiterin oder ein neuer Service-Mitarbeiter Rechte im ITSM-SH-Tool bekommen, so kann der/die IT-Koordinierende eines Mandanten (beteiligte Stelle[3]) selbst die Anlage eines neuen Benutzers im Tool anfordern. Dafür erstellt er/sie ein Ticket (Service-Anfrage) im ITSM-SH-Tool und definiert dabei, welche Rechte und Rollen die Person erhalten soll. Die Anfrage zur Einrichtung der Rechtevergabe ist im zweiten Schritt durch die/den IT-Koordinierende/nauf Richtigkeit zu überprüfen und entsprechend freizugeben.

Anschließend landet die Service-Anfrage bei der IT-Verantwortung der zentralen Stelle[4]. Diese prüft die Ordnungsmäßigkeit und aktuelle Lizenzauslastung und gibt anschließend die Anforderung frei. Nach dieser Freigabe wird die Anfrage an die Administrierenden bei Dataport weitergeleitet, sodass die Rechtevergabe im System eingerichtet wird. Ist die Rechtevergabe umgesetzt prüft abschließend die IT-Verantwortung der zentralen Stelle sowie die/der IT-Koordinierende/r der beteiligten Stelle, ob die Anforderung ordnungsgemäß umgesetzt wurde.

Nach der Neuanlage einer Service-Mitarbeiterin/ eines Servicemitarbeiters hat die beteiligte Stelle jederzeit die Möglichkeit, die bestehenden Rechte und Rollen im ITSM-SH-Tool zu ändern bzw. zu deaktivieren. Diese Änderungen/Deaktivierungen erfolgen gemäß der Vorgehensweise inkl. der Freigabeinstanzen wie bei der Anlage einer neuen Service-Mitarbeiterin/ eines neuen Service-Mitarbeiters.

[3] Beteiligte Stellen sind diejenigen Landesbehörden im Sinne des Landesverwaltungsgesetzes, die die von der zentralen Stelle verantworteten automatisierten Verfahren jeweils nutzen (hier: ITSM-SH).
[4] Zentrale Stelle nach § 7 Absatz 4 des Landesdatenschutzgesetzes für ITSM-SH die für das zentrale IT-Management zuständige oberste Landesbehörde.

Schleswig-Holstein
Der Ministerpräsident
Staatskanzlei

Personenbezogene Daten und Schnittstellen

Anlage 3

Zur Vereinbarung nach § 59 MBG SH

über das IT-Verfahren IT-Service-Management-System (ITSM-SH)

Inhaltsverzeichnis

Redaktioneller Hinweis

Im Dokument wurden möglichst geschlechtsneutrale Begriffe verwendet. In Fällen, in denen männliche oder weibliche Begriffe aus sprachlichen Gründen gewählt werden mussten, sind selbstverständlich alle Geschlechter angesprochen.

1 Personenbezogene Daten von Endanwendenden und Service-Mitarbeitenden im ITSM-SH

Folgende Daten werden im ITSM-SH von Endanwendenden und Service-Mitarbeitenden für eine Verknüpfung der Benutzer und der IT-Objekte mit den jeweiligen Organisationseinheiten und Räumlichkeiten genutzt und sind insofern personenbezogene Daten:

Daten zur Person	**Beispiel / Erläuterung (Stand per 01.07.2020)**	**Ggf. Eingang über Schnittstelle**
Aktiv	Nur Benutzer, die im AD als aktiv („enabled“) gekennzeichnet sind, werden nach ITSM-SH importiert. Dieses Datum wird beim Import verarbeitet jedoch nicht importiert.	Active Directory (lesend)
Anmeldename	Max.Mustermann	Active Directory (lesend)
Anzeige-Name	Mustermann, Max (Finanzministerium)	Active Directory (lesend)
Vorname	Max	Active Directory (lesend)
Nachname	Mustermann	Active Directory (lesend)
E-Mail-Adresse	Max.Mustermann@fimi.landsh.de	Active Directory (lesend)
Büro-Telefon	+49 431 988-1234	Active Directory (lesend)
Faxnummer	+49-431-988-6-161234	Active Directory (lesend)
Mobiles-Telefon (dienstlich)	+49 171 1234-123456	Active Directory (lesend)
Bereich	Haushalt und Beteiligungen	Active Directory (lesend)
Abteilung	Kassen- und Rechnungswesen	Active Directory (lesend)

Daten zur Person	Beispiel / Erläuterung (Stand per 01.07.2020)	Ggf. Eingang über Schnittstelle
Gebäude (Benutzer-Gebäude-Zuordnung)	Düsternbrooker Weg 64, 24105 Kiel	Active Directory (lesend)
Raum (Raum-Gebäude-Zuordnung)	112	Active Directory (lesend)
Gruppen-mitgliedschaften	Nur Benutzer, die im AD vordefinierten Gruppen zugewiesen werden, werden importiert. Die Gruppenmitgliedschaften werden demnach beim Import verarbeitet jedoch nicht importiert.	Active Directory (lesend)
Benutzer-Kennung	Max.Mustermann Entspricht dem Anmeldenamen	Ham.s.t.er (lesend)
Identifikations-nummer Inventarnummer der IT-Objekte	308366 Stellt die Verbindung zwischen Endanwendenen und IT-Objekten her.	Ham.s.t.er (lesend)
IP-Adresse der IT-Objekte		Ham.s.t.er (lesend)
MAC-Adresse der IT-Objekte		Ham.s.t.er (lesend)
Seriennummer der IT-Objekte		Ham.s.t.er (lesend)
Gebäude der IT-Objekte	Düsternbrooker Weg 64, 24105 Kiel	Ham.s.t.er (lesend)
Raum der IT-Objekte	112	Ham.s.t.er (lesend)
E-Mail-Adresse	Beim Versand von E-Mails wird die E-Mail-Adresse des Empfängers übergeben Beim Empfang einer E-Mail wird die E-	Exchange

Daten zur Person	Beispiel / Erläuterung (Stand per 01.07.2020)	Ggf. Eingang über Schnittstelle
	Mail-Adresse des Versendenden übergeben.	
Anmeldename	Für die gemeinsame Bearbeitung der IT-fachlichen Aufgaben mit Dataport wird der Anmeldename des Endanwendenden mit dem ITSM-System von Dataport ausgetauscht.	ITSM-System von Dataport

Daten zur Organisation	Beispiel / Erläuterung	Ggf. Eingang über Schnittstelle
Ressort	Ressort VI	Import der Daten mittels Excel-Liste
Oberste Landesbehörden	Finanzministerium	Import der Daten mittels Excel-Liste
zugeordnetes Amt	Amt für Informationstechnik (AIT)	Import der Daten mittels Excel-Liste
Landesober-behörde	Dienstleistungszentrum Personal des Landes Schleswig-Holsteins	Import der Daten mittels Excel-Liste
Untere Landesbehörde	Finanzamt Plön	Import der Daten mittels Excel-Liste
Abteilung	Abteilung VI 2 - Haushalt und Beteiligungen	Import der Daten mittels Excel-Liste
Referat	VI 24 Kassen- und Rechnungswesen	Import der Daten mittels Excel-Liste
Dezernat	AIT IT 3	Import der Daten mittels Excel-

		Liste
Sachgebiet	AIT IT 31	Import der Daten mittels Excel-Liste

Daten zur Lokation	**Beispiel / Erläuterung**	**Ggf. Eingang über Schnittstelle**
Land	Deutschland	Import der Daten mittels Excel-Liste
Bundesland	Schleswig-Holstein	Import der Daten mittels Excel-Liste
Ortschaft	Kiel	Import der Daten mittels Excel-Liste

Die Organisations- und Lokationsdaten dienen als Stammdaten im ITSM-SH der Strukturierung und bilden die Grundlage. Über die hergestellten Beziehungen können die Standorte der Anwendenden und die der IT-Objekte identifiziert werden.

Die im ITSM-SH genutzten personenbezogenen Daten werden entweder direkt im ITSM-SH-Tool gepflegt oder über die in der Tabelle genannten Schnittstellen automatisiert importiert. Die importierten personenbezogenen Daten werden schreibgeschützt im ITSM-SH-Tool angezeigt.

Die personenbezogenen Daten werden rein zweckgebunden verarbeitet. Die erforderlichen personenbezogenen Daten sind Grundlage für die Nutzung des IT-Verfahrens und ermöglichen folgende verfahrensrelevante Notwendigkeiten:

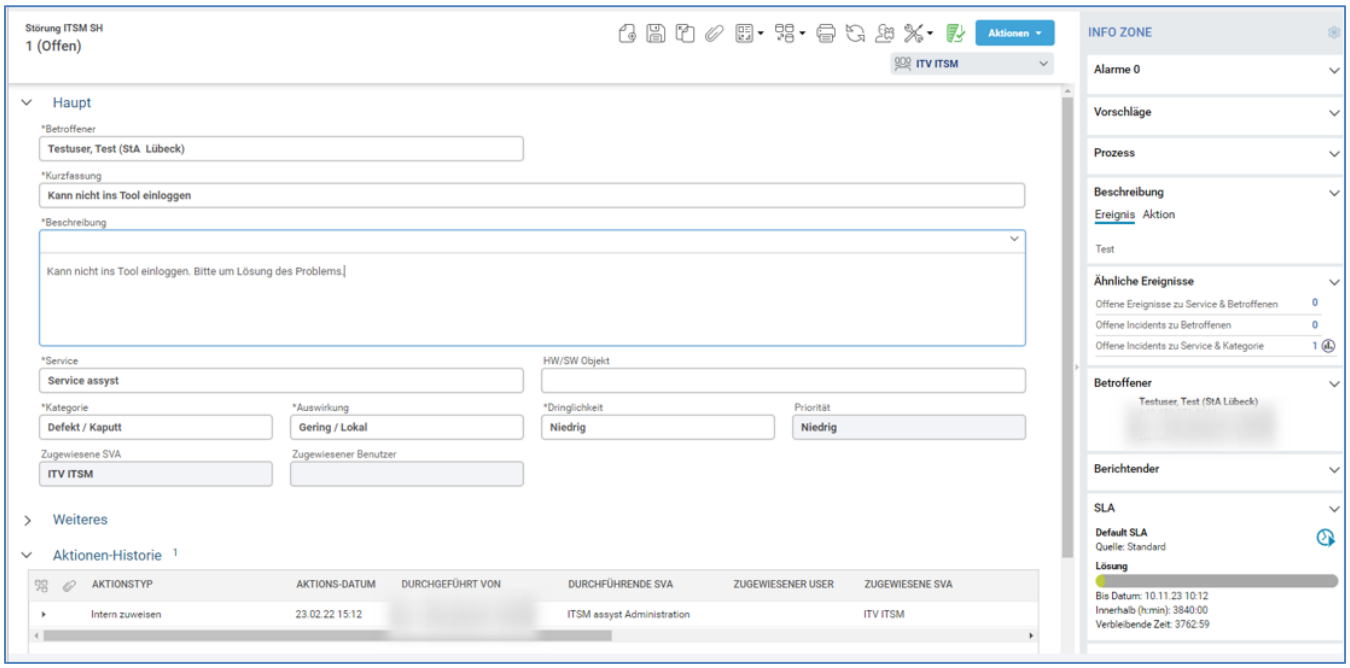
a) Ermöglichung einer Zuordnung eines Tickets zu der Person, die dieses aufgegeben hat (AD)
b) Herstellen einer Verbindung des Anwendenden zu dessen Hardware (Ham.s.t.er)
c) Kontaktaufnahme über E-Mail (Exchange)
d) Ermöglichung einer gemeinsamen Bearbeitung der IT-fachlichen Aufgaben mit Dataport (ITSM-System von Dataport)

Die beteiligten Stellen sind verantwortlich für die Pflege der eigenen Organisations-struktur im ITSM-SH-Tool bis auf Referats-, Dezernats- bzw. Sachgebiets-Ebene.

Die beteiligten Stellen sind verantwortlich für die Pflege der Lokationsstruktur (siehe unten) im ITSM-SH-Tool für die selbst genutzten Liegenschaften.

Wie und durch welche Rollen die Stammdatenpflege im ITSM-SH-Tool erfolgt, ist in der entsprechenden Pflegeanleitung beschrieben. Die organisatorische Vergabe der jeweiligen Rollen obliegt der zentralen Stelle und den beteiligten Stellen jeweils für ihren Bereich.

Neben den Anwenderstammdaten aus Active Directory und Ham.s.t.er sind die im System genutzten „Tickets“ zur Meldung und Weiterverfolgung von Incidents, Changes, Problems etc. in Gänze personenbezogen. Sie beinhalten die folgenden Daten:



2 Weitere Personenbezogene Daten von Service-Mitarbeitenden

Für die Service-Mitarbeitenden werden darüber hinaus weitere personenbezogene Daten erfasst, welche sich aus der Bearbeitung der Aufgaben im Tool ergeben.

Darunter fallen die ausgeführten Aktionen der Service-Mitarbeitenden, welche in der Ticket-Historie festgehalten werden. Dabei werden folgende Informationen erfasst:

Daten	**Beispiel / Erläuterung**
Aktionstyp	siehe nachfolgende Tabelle
Aktions-Datum	31.01.22 9:45
Durchgeführt von	Mustermann, Max Service-Mitarbeitende, welche/r die Aktion durchgeführt hat

Zugewiesener User	Musterfrau, Marta Service-Mitarbeitende, welche/r hauptsächlich das Ticket bearbeitet

Nachfolgend befindet sich die Auflistung der Aktionen.

Aktionsbezeichnung	**Kurze Erläuterung**
Abgelehnt	Service-Mitarbeiterin/Service-Mitarbeiter lehnt das Ticket mit entsprechender Begründung ab.
Dokumentation	Service-Mitarbeiterin/Service-Mitarbeiter dokumentiert die Bearbeitungsschritte innerhalb eines Tickets.
E-Mail Kommunikation	Service-Mitarbeiterin/Service-Mitarbeiter führt diese Aktion aus, um eine E-Mail aus dem ITSM-SH-Tool z.B. an die betroffenen Person zu senden.
Verknüpfe Change	Service-Mitarbeiterin/Service-Mitarbeiter erstellt aus einem existierenden Incident-Ticket ein Change-Ticket.
Zurückgewiesen	Service-Mitarbeiterin/Service-Mitarbeiter weist das zugewiesene Ticket zurück an den vorherigen Ticketbearbeiter.
Erinnerung	Service-Mitarbeiterin/Service-Mitarbeiter stellt eine Erinnerung ein, um später dann die Ticketbearbeitung fortzusetzen.
Interne Zuweisen	Service-Mitarbeiterin/Service-Mitarbeiter weist das Ticket an eine andere Abteilung zu.
Gelöst	Service-Mitarbeiterin/Service-Mitarbeiter hat die Bearbeitung des Tickets erfolgreich abgeschlossen und setzt das Ticket auf „gelöst“.
Schließen	Service-Mitarbeiterin/Service-Mitarbeiter schließt das Ticket nach der erfolgreichen Bearbeitung.
Zuweisung zu Lieferant	Service-Mitarbeiterin/Service-Mitarbeiter beauftragt die Bearbeitung durch einen externen Lieferanten.

3 Schnittstellen im Überblick

Hier eine Kurzbeschreibung der Schnittstellen, die eine Übertragung personenbezogener Daten von Beschäftigten beinhalten:

1. **Windows Active Directory (AD)**: Lesende Schnittstelle zur automatisierten Anmeldung der Betroffenen am ITSM-SH, zur Auswertung der im AD festgelegten Berechtigungen und zur Anzeige der Funktionsträgerdaten der Betroffenen im ITSM-SH
2. **Inventarisierungssystem Ham.s.t.er**: Lesende Schnittstelle zum Abruf von PC-Stammdaten und Softwareinformationen (IT-Objekte)
3. **Exchange**: Bidirektionale Schnittstelle zum Senden und Empfangen von (standardisierten) E-Mails
4. **ITSM-System von Dataport**: Bidirektionale Schnittstelle zur gemeinsamen Bearbeitung der IT-fachlichen Aufgaben im Rahmen von ausgewählten IT-Prozessen

Schnittstellen, die eine Übertragung personenbezogener Daten von Beschäftigten beinhalten, zu folgenden Systemen sind u.a. geplant:

1. **Outlook**: Schnittstelle zum Übertragen der Aufgaben und Terminen aus dem ITSM-SH in die Outlook-Kalender der Service-Mitarbeiter
2. **Microsoft System Center Configuration Manager (SCCM)**: Lesende Schnittstelle zum Abruf von Hard- und Softwareinformationen der Windows Rechner, um die Umsetzung in den IT-Prozessen (bspw. Software Installation, RAM Erweiterung) überprüfen zu können.
3. **Inventarisierungssystem Ham.s.t.er**: Schreibende Schnittstelle zum Austausch von PC-Stammdaten und Softwareinformationen

Schleswig-Holstein
Der Ministerpräsident
Staatskanzlei

Standard-Berichte im ITSM-SH

Anlage 4

Zur Vereinbarung nach § 59 MBG SH

über das IT-Verfahren IT-Service-Management-System (ITSM-SH)

Inhaltsverzeichnis

Abbildungs- und Tabellenverzeichnis

Redaktioneller Hinweis

Im Dokument wurden möglichst geschlechtsneutrale Begriffe verwendet. In Fällen, in denen männliche oder weibliche Begriffe aus sprachlichen Gründen gewählt werden mussten, sind selbstverständlich alle Geschlechter angesprochen.

1 Einleitung

Die nachfolgende Auflistung stellt die Standard-Berichte des ITSM-SH dar. Die Berechtigungen zur Einsicht dieser Berichte müssen aktiv durch Dataport vergeben werden. Die Berichte enthalten ausschließlich pseudonymisierte Daten und können nur von Dataport erstellt werden.

2 Übersicht der Berichte

Bericht Titel	Beschreibung
<Prozess>-04 Offene Tickets / Täglich / <Mandant/Servicetyp>	Alle Tickets des Prozesses eines Mandanten/Servicetyps, die zu einem definierten Zeitpunkt den Status „offen“ besitzen.
<Prozess>-05 Ticketvolumen der letzten 30 Tage / <Mandant/Servicetyp>	Alle Tickets des Prozesses eines Mandanten/Servicetyps, die in den letzten 30 Tagen aufgenommen wurden, dargestellt im Zeitverlauf.
<Prozess>-05 Ticketvolumen der letzten 7 Tage / <Mandant/Servicetyp>	Alle Tickets des Prozesses eines Mandanten/Servicetyps, die in den letzten 7 Tagen aufgenommen wurden, dargestellt im Zeitverlauf.
<Prozess>-06 Offene Tickets nach Priorität und Kategorie / <Mandant/Servicetyp>	Alle Tickets des Prozesses eines Mandanten/Servicetyps, welche den Status „offen“ besitzen, geordnet nach Priorität und Kategorie.
<Prozess>-07 Bearbeitungsdauer Tickets / <Mandant/Servicetyp>	Die Durchschnittszeit aller gelösten Tickets des Prozesses, geordnet nach Priorität. Die Zeit wird gemessen von der Aufnahme bis zur Lösung eines Tickets.

Tabelle 1: Liste der Berichte im ITSM-SH

Die sich im Einsatz befindlichen beziehungsweise geplanten standardisierte Prozesse sind unter der Anlage 1 beschrieben. Nachfolgend werden die Mandanten und Servicetypen weiter spezifiziert.

<Mandant/Servicetyp> Bezeichnung	Beschreibung
Mandant: DigiZeit	Digitale Zeitwirtschaft
Mandant: ITSM-SH	IT-Service Management Schleswig Holstein
Mandant: Justiz	Ministerium für Justiz, Europa und Verbraucherschutz SH
Mandant: Ziaf	Zahlstellen- und Integriertes Verwaltungs- und Kontrollsystem AgrarFörderung
Servicetyp: Standard-AP-HW	Standard-Arbeitsplatz-Hardware

Servicetyp: Standard-AP-PW	Standard-Arbeitsplatz-Passwort
Servicetyp: Standard-AP-SW	Standard-Arbeitsplatz-Software

Tabelle 2: Beispielhafte Liste der Mandanten-/Servicebezeichnungen

Zudem werden folgende Prioritäten und Kategorien in den Berichten abgebildet.

<table>
<tr><td>Prioritäten</td><td>Die Priorität (niedrig, mittel, hoch, kritisch) ergibt sich aus der Auswirkung und Dringlichkeit. Dies wird in der folgenden Prioritätenmatrix verdeutlicht:
<table>
<tr><th colspan="2" rowspan="2">Priorität</th><th colspan="4">Auswirkung</th></tr>
<tr><th>Großflächig / Verbreitet</th><th>Erheblich / Groß</th><th>Moderat / Begrenzt</th><th>Gering/Lokal</th></tr>
<tr><th rowspan="4">Dringlichkeit</th><th>Kritisch</th><td>Kritisch</td><td>Kritisch</td><td>Hoch</td><td>Hoch</td></tr>
<tr><th>Hoch</th><td>Kritisch</td><td>Hoch</td><td>Hoch</td><td>Mittel</td></tr>
<tr><th>Mittel</th><td>Hoch</td><td>Hoch</td><td>Mittel</td><td>Niedrig</td></tr>
<tr><th>Niedrig</th><td>Hoch</td><td>Mittel</td><td>Niedrig</td><td>Niedrig</td></tr>
</table></td></tr>
<tr><td>Kategorie</td><td>Beispielhaft: Defekt / Kaputt, Fehlfunktion, Known Error (insgesamt über 50 Kategorien)</td></tr>
</table>

Tabelle 3: Prioritäten und Kategorien

3 Beispielhafte Darstellung

Das ITSM-SH-Tool bietet zwei unterschiedliche Darstellungen innerhalb eines Berichtes. Eine grafische Darstellung sowie eine tabellarische Darstellung der Ereignisse (=Tickets).

Die **Abbildung 1** zeigt beispielhaft die **grafische Darstellung** der Ereignisse. Diese werden in Abhängigkeit der Datengruppierung in Form von Kreis- oder Balkendiagrammen dargestellt.

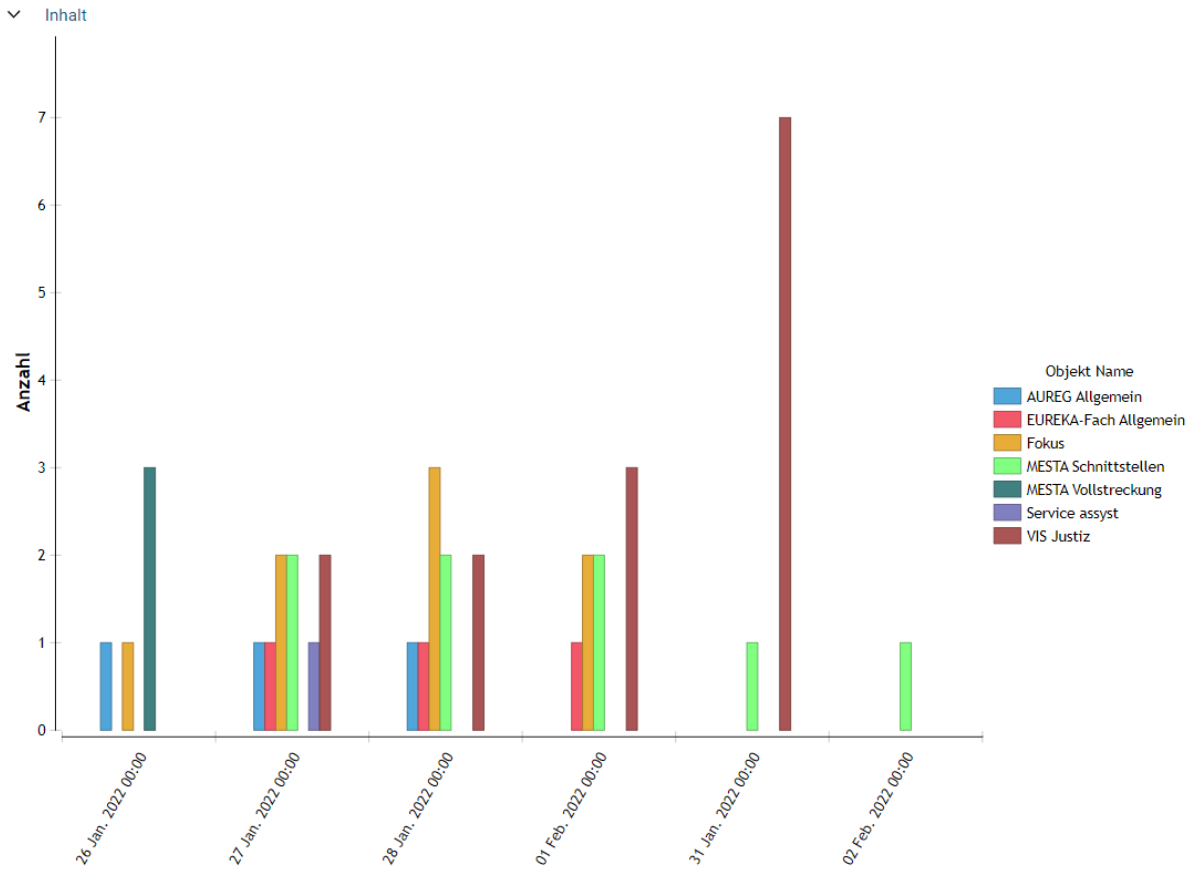


Abbildung 1: Grafische Darstellung der Ereignisse

Die **Abbildung 2** zeigt beispielhaft die **tabellarische Darstellung** der Ereignisse. Hierbei werden die Ereignisse eines entsprechenden Zeitraums zur Auswertung herangezogenen und mit ihrer Ereignis-Referenz, dem Protokollierungsdatum, der Priorität, der Kategorie, der zugewiesenen Service-Abteilung (SVA) sowie einer Kurzbeschreibung in Form der Ereignis-Übersicht aufgeführt.

Ereignis-Referenz		Protokollierungs-Datum	Priorität Name	Kategorie Name	Zugewiesene SVA Name	Ereignis-Übersicht
Defekt / Kaputt	Anzahl: 90					
Hoch	Anzahl: 19					
21522		01.07.2021, 10:22	Hoch	Defekt / Kaputt	VPS eAkte	Ausfall VIS-Justiz
28586		15.10.2021, 07:42	Hoch	Defekt / Kaputt	VPS Aureg	Kommanditisten können nicht importiert werden
30645		04.11.2021, 08:54	Hoch	Defekt / Kaputt	VPS VIS Justiz	OCR-Erkennung fehlgeschlagen
33946		28.12.2021, 14:43	Hoch	Defekt /	VPS assyst	Unzuverlässige Übertragung von Tickets über die F

Abbildung 2: Tabellarische Darstellung

Die Ereignis-Referenz in Form einer Ticket-Nummer stellt ein pseudonymisiertes Datum dar. Nachfolgend wird begründet, warum eine tabellarische Darstellung insbesondere mit der Ereignis-Referenz notwendig ist.

Das Ziel der Einführung des ITSM-SH-Tools ist u.a. die IT-Services zu verbessern und die Zufriedenheit der Anwendenden zu erhöhen. Um dieser Anforderung nachzukommen, ist es einerseits notwendig **quantitative Analysen** durchzuführen, um bspw. Veränderungen der Ticketanzahl über gewisse Zeiträume beobachten zu können (Abb. 1). Andererseits ist es für die Wahrnehmung der Aufgaben von Service-Mitarbeitenden notwendig, ebenfalls **qualitative Analysen** durchführen zu können (Abb. 2). Zu den Aufgaben der Service-Mitarbeitenden, welche zur Zielerreichung beitragen, gehört es, u.a. Prozessverbesserungen anzustreben sowie Fehlereingrenzung und -einschätzung zu betreiben. Ohne die detaillierte Auflistung der Ereignisse können die Aufgaben nicht ordnungsgemäß durchgeführt werden. Beispielsweise kann die Ursache von vielen niedrig priorisierten Tickets ein größeres Problem an der Infrastruktur sein. Solch ein Problem kann der/die Service-Mitarbeitende dann jedoch nur erkennen, wenn auf einen Blick alle relevanten Informationen dargestellt werden. Zudem ist es hierfür auch notwendig die Ticketnummer einzusehen, da damit analysiert werden kann, wie mit den verschiedenen Störungen bisher umgegangen wurde und, ob die Lösung des einen Tickets auch bei der Lösung eines anderen helfen kann.

Dasselbe gilt für die Analysen von Änderungen. Hierbei können bspw. mithilfe der detaillierten Darstellung der Ereignisse Konflikte zwischen angeforderten Änderungen erkannt werden. Zudem dient es dazu vorausschauend zu agieren, da ggf. frühzeitig Bestände aufgestockt und finanzielle Mittel eingeplant werden müssen. Um identifizieren zu können, dass beantragte Änderungen zu einem Konflikt führen könnten, oder Änderungen auf dieselben Mittel abzielen, ist es notwendig, weitere Informationen in den zugehörigen Tickets nachlesen zu können.

Somit ist sowohl die grafische Darstellung hilfreich für einen schnellen groben Überblick, als auch die tabellarische Darstellung notwendig für tiefergehende Analysen im Umgang mit Fehlern und Änderungen.