Mandantenfähigkeit: Datenabgrenzung

Vorbemerkung

Im folgenden wird die Datenabgrenzung verschiedener Mandanten sowohl mit, als auch ohne habbl-bezogene Geschäftsbeziehungen niedergeschrieben. Dafür wird die habbl-interne technische Umsetzung zusammengefasst. Dies wird unter Anderem unter Berücksichtigung des Leitfades „Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur: Orientierungshilfe und Mandantenfähigkeit“ (Version 1.0 vom 11.10.2012) realisiert. Hieraus sind für das nachfolgende Dokument die Definitionen **„Mandant“** und **„Mandant entrennung“** aus dem Abschnitt **Begriffsdefinition** zu entnehmen. Das nachfolgende Dokument ist lose an den Aufbau des oben genannten Leitfadens angelehnt.

Umsetzung des Datenschutzes hinsichtlich der Mandantentrennung

Technische Umsetzung der Mandantentrennung

Der Datenerhebung und Datenverarbeitung durch die EIKONA, im Rahmen des Softwareprodukts habbl, ist vertraglich (oder über die Nutzungsbestimmungen) durch die Mandanten zugestimmt, unerheblich ob die Datenerhebung durch das habblPORTAL oder die habblAPP geschieht. Hierbei werden jene Informationen erhoben, deren Art und Verwendungszweck ausdrücklich zugestimmt worden ist.

Dies wird durch das hierarchische Rollensystem von habbl realisiert, durch welches einzelne Produktfunktionalitäten an- bzw. abgeschaltet werden können. Diese Konfigurationsmöglichkeiten steuern einerseits, welche Art von Daten erhoben werden und andererseits auch deren Verwendungszweck. Dank der Vererbungsarchitektur dieses Rollensystems können nur mandantenspezifisch freigeschaltete Rechte und Funktionalitäten an einzelne untergeordnete Nutzerkonten weitergereicht bzw. vererbt werden (z. B. von einem Mandantenkonto für ein gesamtes habbl-Unternehmen an untergeordnete mitarbeiterspezifische Nutzerkonten). Dies stellt unter anderem sicher, dass zu keinem Zeitpunkt einem untergeordneten Nutzerkonto unberechtigterweise Zugang zu Daten gewährt wird, deren Zugang vom Mandanten explizit ausgeschlossen ist.

Um zunächst jedem Mandanten auch nur den Zugriff auf die eigenen Daten zu gewähren, ist jedem einzelnen von EIKONA durch habbl erhobenen, verwalteten oder gespeicherten Datensatz eine eindeutige Mandantenkennung und ein Zeitstempel zugewiesen. Unerheblich davon, ob Daten abgerufen oder weiterverarbeitet werden sollen, wird bei jeder einzelnen Abfrage eines Datensatzes diese Benutzerkennung mit den vorliegenden nutzerkontenspezifischen Login-Daten und den damit eindeutig verbundenen mandantenspezifischen Kennungsdaten abgeglichen und die anfrageeigene Berechtigung durch das Rollensystem geprüft. Liegt eine solche erforderliche Berechtigung nicht vor, so wird der Zugang zu den angeforderten Daten verwehrt und gegebenenfalls die Datenverarbeitung abgebrochen.

Ein systeminterner Datenaustausch zwischen verschiedenen Mandanten wird durch Verknüpfungen realisiert, diese kann jeder Mandant selbst einsehen und pflegen. Einer solchen Verknüpfung müssen alle Parteien ausdrücklich zustimmen, diese Zustimmung kann jederzeit widerrufen werden. Jeder einzelnen Verknüpfung sind Informationen wie Geschäftsbeziehung, Verknüpfungsstatus und Befugnisse zum Datenaustausch (ähnlich des Rollensystems) zugeordnet. Eine solche Verknüpfung ist eine zwingende Voraussetzung dafür, dass einem Mandanten die Daten eines anderen Mandanten bereitgestellt oder angezeigt werden können.

Unternehmensweite Datenschutzmaßnahmen

Unternehmensweit wurde ein Datenschutzbeauftragter bestellt, zusätzlich werden die Mitarbeiter in regelmäßigen Abständen über die aktuellen Datenschutzbestimmungen in eigenen Workshops dokumentationspflichtgerecht unterrichtet. Darüber hinaus wird bei der Entwicklung von habbl großer Wert auf eine im Vorfeld zu tätigende Risikoanalyse gelegt, egal ob vor der Planung und Implementierung einer Umstrukturierung und einer daraus resultierenden Änderung des laufenden Systems oder der Planung und Umsetzung neuer Features und Funktionalitäten. Den Grundsätzen zu Privacy by Default und Privacy by Design (gem. Art 25 DSGVO) wird in jedem Entwicklungsschritt, im Zusammenhang mit dem habblPORTAL und der habblAPP, Rechnung getragen.

Anlage

„Technische und organisatorische Anforderungen an die Trennung von automatisierten Verfahren bei der Benutzung einer gemeinsamen IT-Infrastruktur: Orientierungshilfe und Mandantenfähigkeit" (Version 1.0 vom 11.10.2012)

Quelle: https://www.lda.bayern.de/media/oh_mandantenfaehigkeit.pdf