Die Bereitstellung und Weitergabe von Audi Daten an Partnerfirmen wurde in diesem Dokument nicht betrachtet.

Aus der Tabelle ergibt sich, dass **externes Hosting** eine public Cloud ist, an die die zusätzliche Anforderung einer dedizierter Hardware gestellt wird.
Eine ausgleichende Maßnahme für dedizierte Hardware ist die Verwendung einer Ablageverschlüsselung in Kombination mit einer Ende-zu-Ende Transportverschlüsselung

Die Speicherung oder Verarbeitung von personenbezogenen Daten durch cloud-basierte Anwendungen oder Infrastrukturkomponenten ist nur unter Einhaltung der EU-Datenschutzverordnung und den Datenschutzbestimmungen der jeweiligen Länder zulässig.

Diskussion der Cloud-Typen in Abhängigkeit des Schutzziels "Vertraulichkeit"

Cloud-Typ	Service Modell	Use-Case	Datenklassifikation	Anforderung
Public Cloud	**IaaS**	Datenablage	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich	Für Daten der Klassifikation **vertraulich** ist eine Transport- und Ablageverschlüsselung einzusetzen. Schlüsselhoheit liegt bei Audi. Starke Authentifizierung beim Zugriff auf die Daten
			intern	Für Daten der Klassifikation **intern** ist eine Transportverschlüsselung einzusetzen. Schlüsselhoheit liegt bei Audi. Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
			öffentlich	Keine zusätzliche Anforderungen
		Rechenleistung	geheim/ vertraulich	**Nicht** zulässig für Daten der Klassifikation **geheim / vertraulich**
			intern	Für Daten der Klassifikation intern bestehen folgende Anforderungen. - Transportverschlüsselung - Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
			öffentlich	Keine zusätzliche Anforderungen
	PaaS/SaaS	Datenablage	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich / intern	Für Daten der Klassifikation **intern** oder **vertraulich** ist eine Transport- und Ablageverschlüsselung einzusetzen. Schlüsselhoheit liegt bei Audi. Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
			öffentlich	keine Anforderungen
		Rechenleistung	geheim / vertraulich	**Nicht** zulässig für Daten der Klassifikation **geheim / vertraulich**
			intern	Eine Freigabe der IT-Sicherheit ist notwendig.
			öffentlich	Keine zusätzliche Anforderungen
Private Cloud	**IaaS/PaaS/SaaS**	Datenablage/ Rechenleistung	öffentlich/intern/vertraulich/geheim	Für alle Datenklassifikationen zulässig. IT Sicherheitsberatung (ITS-RISK) ist im Vorfeld durchzuführen.
Externes Hosting	**IaaS**	Datenablage	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich / intern	Zuässig für Daten der Klassifikation **vertraulich** unter Einhaltung der nachfolgenden Anforderungen: - Ablageverschlüsselung. - Transportverschlüsselung. - Die Schlüsselhoheit liegt bei Audi. - Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
			öffentlich	Keine zusätzliche Anforderungen
		Rechenleistung	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich / intern / öffentlich	Für Daten der Klassifikation intern bestehen folgende Anforderungen. - Transportverschlüsselung - Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
	PaaS/SaaS	Datenablage	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich / intern	Für Daten der Klassifikation **intern** oder **vertraulich** ist eine Transport- und Ablageverschlüsselung einzusetzen. Schlüsselhoheit liegt bei Audi. Starke Authentifizierung beim Zugriff auf die Daten (Einhaltung der Chain of Trust)
			öffentlich	Keine zusätzliche Anforderungen
		Rechenleistung	geheim / vertraulich	**Nicht** zulässig für Daten der Klassifikation **geheim / vertraulich**
			intern	Eine Freigabe der IT-Sicherheit ist notwendig.
			öffentlich	Keine zusätzliche Anforderungen
Externes Housing	**Co-Location**	Datenablage /Rechenleistung	geheim	**Nicht** zulässig für Daten der Klassifikation **geheim**
			vertraulich / intern / öffentlich	Zuässig für Daten der Klassifikation **intern** und **vertraulich** unter Einhaltung der nachfolgenden Auflagen: - Die Schlüsselhoheit darf ausschließlich bei der auftraggebenden Konzerngesellschaft liegen. - Die Hardware befindet sich im Eigentum der auftraggebenden Konzerngesellschaft. - Die Hardware befindet sich in einem abgeschlossenen, exklusiv für die auftraggebende Konzerngesellschaft bereitgestellten Raum (ggfs. auch Gitterkäfig), zu dem der Zutritt nur unter Anwesenheit eines Mitarbeiters dieser Konzerngesellschaft möglich ist (Ausnahme: Katastrophenfall). - Netzwerkseitige Zugriffe der auftraggebenden Konzerngesellschaft müssen über einen Zugang erfolgen, der der "Informationssicherheit Regelung Nr. 03.02.04 – Netzwerkzugänge" entspricht. - Die IT-Sicherheit behält sich das Recht zur Durchführung von On-Site Assessments zur Prüfung der oben genannten Anforderungen vor. - Insolvenzfall: Rückhohlung der Daten/ Hardware (Anforderung Rechtswesen?)

Hinweis: Eventuell auftretende Kosten sind durch den beauftragenden Fachbereich zu tragen.

Es wird unter anderem eine Abstimmung mit dem Rechtswesen, Datenschutz, Informationseigentümer und der (Sicherheits-)Architektur empfohlen.

Weitere Informationen
Link mit einer Definition der einzelnen Cloud-Typen (Quelle: BSI)
https://www.bsi.bund.de/DE/Themen/CloudComputing/Grundlagen/Grundlagen_node.html

Kriterium	Public Cloud	Private Cloud	Externes Hosting
Die Hardware wird ausschließlich für Audi bereitgestellt	Nein	Ja	Ja
Die Hardware ist innerhalb der Konzern-infrastruktur der Volkswagen AG verortet	Nein	Ja	Nein

	Ext. Housing	Servicemodelle Public Cloud /Private Cloud/ ext. Hosting		
	Co-Location	IaaS	PaaS	SaaS
Applikation				
Datenbanken				
Betriebssysteme				
Hardware				
Techn. Infrastruktur				

Bereitstellung durch Serviceprovider. (Bei Private Cloud durch Volkswagen IT, bei Public Cloud und externem Hosting durch externe Servicedienstleister.

Definition der Servicemodelle

1. Infrastructure as a Service (IaaS)

Bei IaaS werden IT-Ressourcen wie z. B. Rechenleistung, Datenspeicher oder Netze als Dienst angeboten. Ein Cloud-Kunde kauft diese virtualisierten und in hohem Maß standardisierten Services und baut darauf eigene Services zum internen oder externen Gebrauch auf. So kann ein Cloud-Kunde z. B. Rechenleistung, Arbeitsspeicher und Datenspeicher anmieten und darauf ein Betriebssystem mit Anwendungen seiner Wahl laufen lassen.

2. Platform as a Service (PaaS)

Ein PaaS-Provider stellt eine komplette Infrastruktur bereit und bietet dem Kunden auf der Plattform standardisierte Schnittstellen an, die von Diensten des Kunden genutzt werden. So kann die Plattform z. B. Mandantenfähigkeit, Skalierbarkeit, Zugriffskontrolle, Datenbankzugriffe, etc. als Service zur Verfügung stellen. Der Kunde hat keinen Zugriff auf die darunterliegenden Schichten (Betriebssystem, Hardware), er kann aber auf der Plattform eigene Anwendungen laufen lassen, für deren Entwicklung der CSP in der Regel eigene Werkzeuge anbietet.

3. Software as a Service (SaaS)

Sämtliche Angebote von Anwendungen, die den Kriterien des Cloud Computing entsprechen, fallen in diese Kategorie. Dem Angebotsspektrum sind hierbei keine Grenzen gesetzt. Als Beispiele seien Kontaktdatenmanagement, Finanzbuchhaltung, Textverarbeitung oder Kollaborationsanwendungen genannt.

Datenablage
Speicherung von Daten, die über den Bearbeitungszeitraum hinaus geschieht. (Nicht flüchtige Speicherung von Daten)

Rechenleistung
Verarbeitung von Daten und Informationen ohne Datenablage.