thebranch

SVIT SCHWEIZ

2023 als Datenjahr: Wie das neue Datenschutzgesetz zu neuen Datenstandards in der Immobilienwirtschaft beitragen kann.

10 Merksätze und ein paar Fragen zum zukünftigen Umgang mit Daten in der Immobilienwirtschaft.

Branch Talk in Kooperation mit dem SVIT Schweiz

Stefan Zanetti, Vorstand The Branch /
Gründer Allthings Technologies AG

thebranch

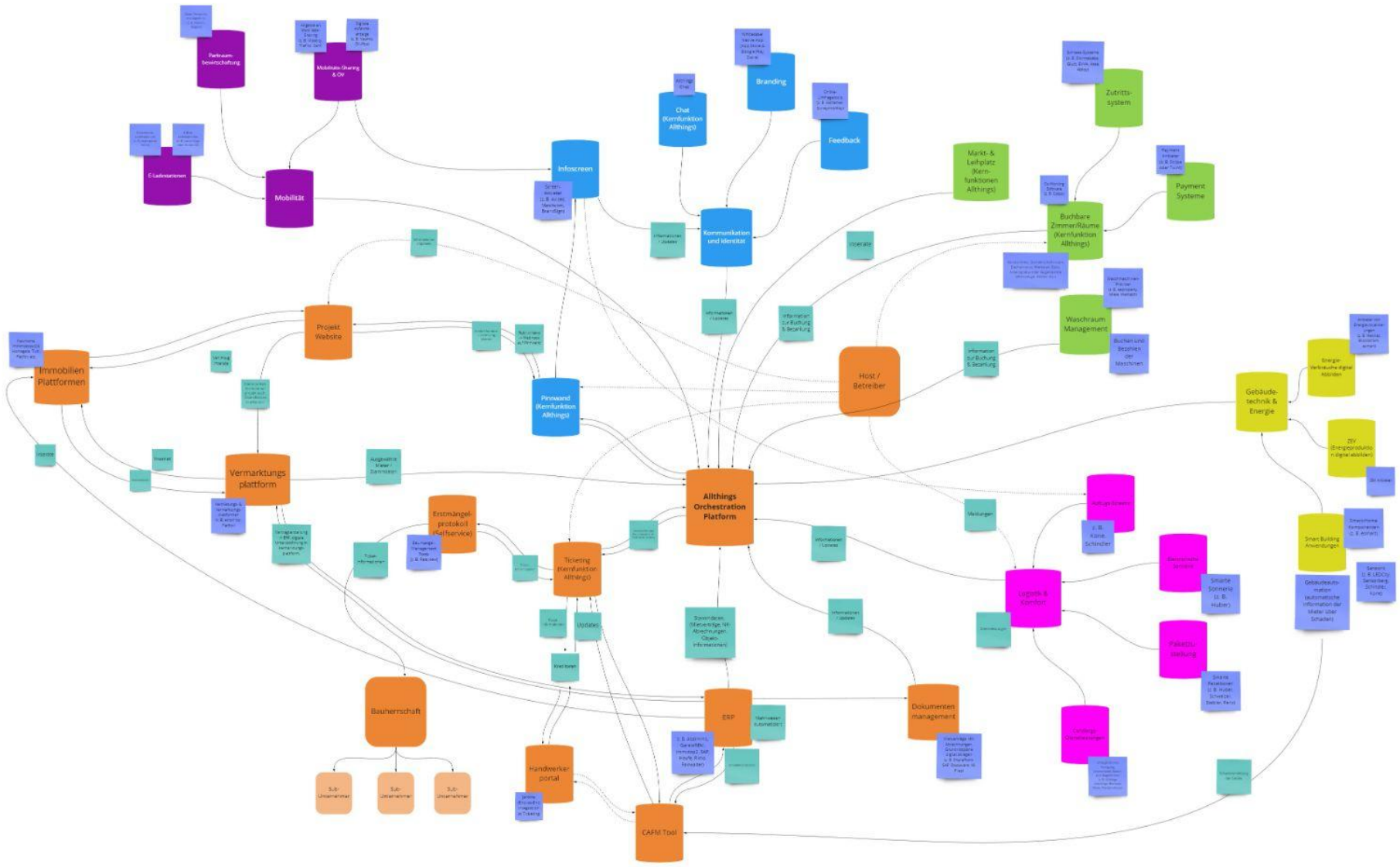
1. Immobilienwirtschaft: extrem fragmentiert

… im Vergleich zu bspw. Banken und Versicherungen

thebranch

2. Datenaustauschbedarf heute schon hoch

- und sehr viel höher in Zukunft.



Legende

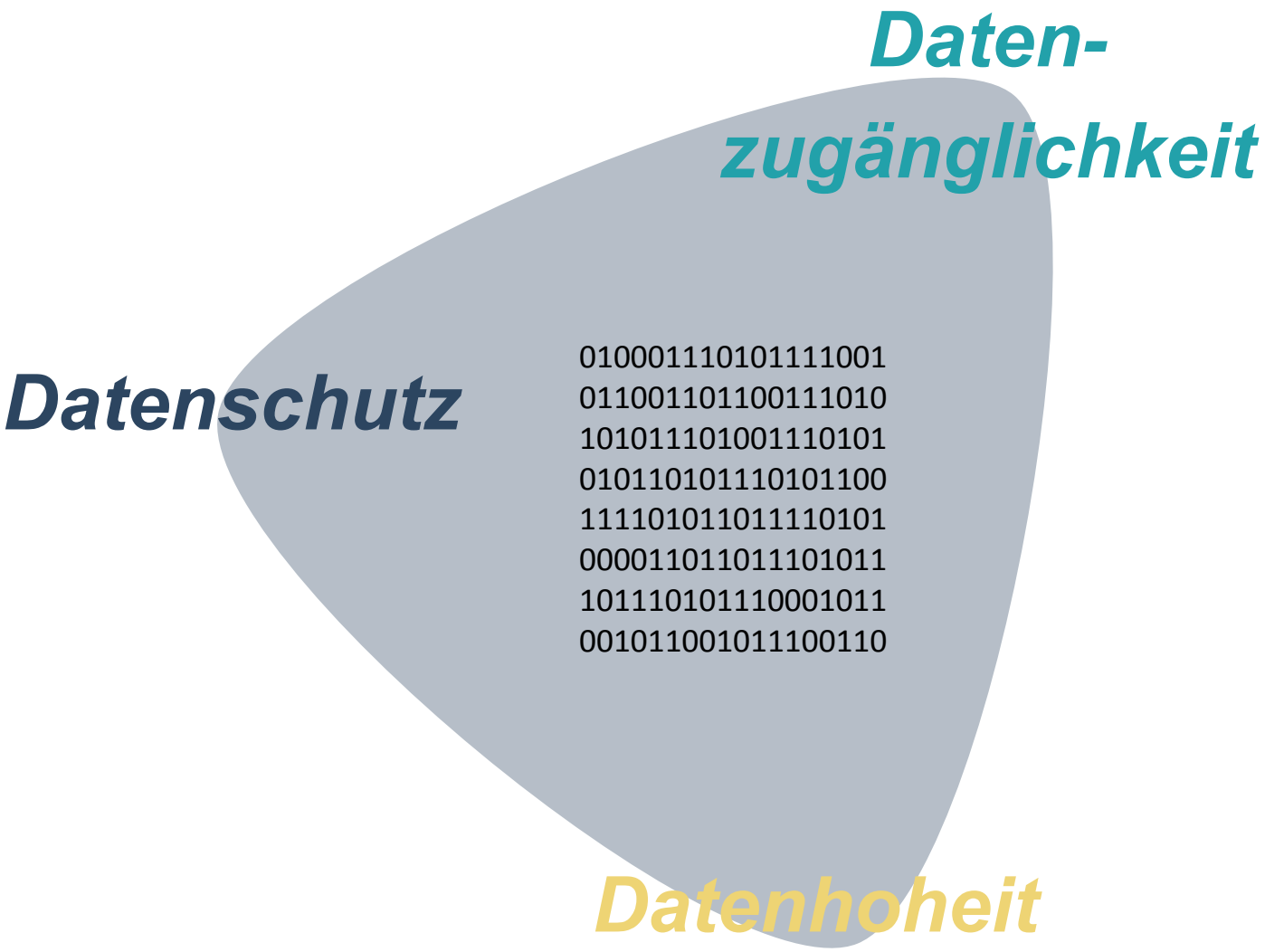
- Mobilität & Parkraum
- Kommunikation & Identität
- Gemeinsam genutzte Ressourcen & DL
- Gebäudetechnik & Energie
- Management & Administration
- Logistik & Komfort

- Schnittstellen
- Kommentare

thebranch

3. **Das magische Dreieck im Umgang mit Daten zwischen Unternehmen besteht aus: *Datenschutz*, *Datenhoheit* *und* *Datenzugänglichkeit.***

thebranch


Daten-
zugänglichkeit
Datenschutz
010001110101111001
011001101100111010
101011101001110101
010110101110101100
111101011011110101
000011011011101011
101110101110001011
001011001011100110
Datenhoheit

thebranch

4. **Andere Branchen zeigen, dass Standards / Quasi-Standards im Umgang mit Daten grössten Hebel haben auf:** ***Fundamentale Effizienzgewinne, höhere Transparenz, ESG-Zielerfüllung und bessere Nutzer-/Mitarbeitererlebnisse.***

FREE INSURANCE DATA
INITIATIVE

Use-Cases

Pension-API
Der FRIDA-Use-Case konzentriert sich auf die Bereitstellung von Daten zur Transparenz in der Altersvorsorge z.B. mithilfe eines Rentencockpits.

Health-Care API
Der FRIDA-Use-Case konzentriert sich auf Anwendungsfälle im Gesundheitsbereich z.B. Integriertes Vertrags- und Leistungsmanagement.

Car-Claims-API
Der FRIDA-Use-Case konzentriert sich auf den Austausch von Versicherungsdaten im Schadenfall z.B. via Wallet.

Cyber-API
Der FRIDA-Use-Case konzentriert sich auf Anwendungsfälle im Kontext von Cyber-Versicherungen z.B. die Standardisierung von Key-Risk-Indikators und den Datenaustausch zwischen Drittanbietern und Versicherern.

thebranch

5. Die Ecke Datenschutz:

Die SVIT Handlungsanleitung und das Branch DPA / ADB für die Immobilienwirtschaft

thebranch

SVIT SCHWEIZ

Branchenempfehlung zum revidierten Datenschutzgesetz – **Grundlagen**

Branchenempfehlung 12.22de, Version 1.0

1. Zielsetzung der Branchenempfehlung

Diese Branchenempfehlung gibt einen Überblick über die Massnahmen, die in Betrieben der Immobilienwirtschaft zur rechtskonformen Umsetzung des revidierten Datenschutzgesetzes (nachfolgend: DSG, es wird nur Bezug genommen auf die revidierte Gesetzesfassung) und der revidierten Datenschutzverordnung (DSV) zu treffen sind. Im Fokus stehen dabei die typischen Dienstleistungen der Immobilienwirtschaft gegenüber Privatpersonen.

Die Immobilienwirtschaft und angrenzende Branchen verarbeitet viele Daten. In der überragenden Mehrheit sind dies jedoch keine besonders schützenswerten Personendaten gemäss DSG. Ungeachtet dessen hat die Gesetzesrevision für die Immobilienwirtschaft ein Bedeutung von erheblicher Tragweite. Im Kern geht es darum, sich über den Datenanfall, den Umgang mit Daten, die Verantwortungszuordnung sowie die Sicherung und Archivierung von Daten in einem Unternehmen bewusst zu werden. Es gilt, entsprechende Prozesse zu definieren und das Thema auf Stufe Geschäftsleitung fest zu verankern. Bei kleineren und mittleren Unternehmen der Immobilienwirtschaft wird sich der Aufwand für eine gesetzeskonforme Umsetzung des DSG in überschaubarem Rahmen halten. Eine wichtige Hilfe sollen dabei die vorliegenden Empfehlungen und weitere Standardunterlagen von Branchenorganisationen sein, auf die im Weiteren verwiesen wird. Beratung durch externe Spezialisten (Datenschutzexperten, Rechtsanwälte, Informatiker) ist namentlich bei besonderen Geschäftsmodellen und Geschäftstätigkeiten angezeigt.

2. Rechtshinweis

Der SVIT Schweiz weist darauf hin, dass die nachfolgend aufgeführten Massnahmen in jedem Unternehmen und in jedem Einzelfall den tatsächlichen Gegebenheiten und Geschäftspraktiken anzupassen sind und lediglich

thebranch

ADB+

Revidiertes Datenschutzgesetze ab Sept. 2023: Standard der Immobilien-Wirtschaft für die Zusammenarbeit zwischen Unternehmen

ADB Auftrag zur Datenbearbeitung
DPA Data Processing Agreement

Anleitung

12. Dezember 2022 / Version 0.73

Das Wichtigste in Kürze

Das neue Datenschutzgesetz (nDSG) tritt am 1. September 2023 in Kraft. Ab dann gelten verschärfte Vorgaben für den Umgang mit Personendaten.

Vom neuen Gesetz ist auch die Zusammenarbeit zwischen Unternehmen der Immobilienbranche betroffen. Wenn Personendaten zur Bearbeitung ausgetauscht werden, besteht die Verpflichtung zum Abschluss eines Auftrags zur Datenbearbeitung (ADB). Für diese Fälle haben Branchenspezialisten den ADB+ Standard (Auftrag zur Datenbearbeitung) für die Immobilien-Wirtschaft entwickelt.

Der ADB+ Standard ist ein Mustervertrag, der die Datenbearbeitung zwischen zwei Unternehmen regelt. Er enthält zudem die notwendigen Beilagen zur richtigen Umsetzung der Vorgaben aus dem nDSG. Seine Anwendung spart Zeit und Kosten. Die Umsetzung umfasst drei wesentliche Punkte:

1. Immobilienunternehmen sehen auf 1Seite 5 dieser Anleitung, mit welchen Partnern sie ein ADB+ abschliessen sollten.
2. Die ADB+ Vorlage kann auf der Branch-Page (2Link) oder der SVIT-Page (3Link) kostenlos heruntergeladen werden.
3. Die ADB+ Vorlage ist für jede einzelne Vertragsbeziehung separat abzuschliessen und mit dem jeweiligen Vertragspartner zu unterzeichnen.

Was sollten Immobilienunternehmen ausserdem tun, um das nDSG angemessen umzusetzen?

- Einen Überblick gewinnen, was das nDSG für ihr Immobilienunternehmen bedeutet. Siehe dazu die Branchenempfehlung SVIT (4Link).
- Die wichtigsten Massnahmen auch tatsächlich umsetzen, vgl. Liste der Hilfsmittel und Arbeitsergebnisse auf Seite XY dieser Anleitung.
- Schrittweise vorgehen und sich periodisch auf dem Laufenden halten (5Link).

thebranch

ADB+

1.2023d, Version 1.0

Auftrag zur Datenbearbeitung

Vorlage für die schweizerische Immobilienwirtschaft zur Regelung der Datenbearbeitung durch dirtte unter dem per 1. September 2023 gültigen, revidierten Datenschutzgesetz.

ADB+ ist ein Mustervertrag mit vier Anhängen. Er ist als teilgeschütztes PDF-Formular aufgebaut, in welchem Firmenangaben und gewisse Textteile frei eingefügt und Textblöcke als gültig markiert werden können. Um zu erkennen, wann der Mustervertrag eingesetzt werden soll sowie für die inhaltlich korrekte Anwendung wird auf die ADB+ Anleitung von The Branche verwiesen

Für das generelle Verständnis des Datenschutzgesetzes und die praktische Umsetzung sollten sich betroffene Unternehmen der Immobilienwirtschaft zudem an der Branchenempfehlung des SVIT Schweiz orientieren (Branchenempfehlungen (svit.ch)

Inhalt

- Vereinbarung zur Bearbeitung von Daten im Auftrag 2
- Anhang A Zusätzliche Beschreibung der Auftragsbearbeitung 9
- Anhang B TOM, technische und organisatorische Massnahmen 13
- Anhang C Unter-Auftragnehmer 24
- Anhang D Datenhoheit 25

6. Die Ecke Datenhoheit:

Der Branch Anhang D) Datenhoheit

Anhang D: Datenhoheit

Mit diesem **Anhang D** regeln die Parteien die Bearbeitung von Personendaten durch den Auftragnehmer ausserhalb der Bearbeitung im Auftrag im Sinne der Vereinbarung, sowie die Verwendung von nicht-personenbezogenen Daten, insbesondere technische Daten, Maschinendaten, anonymisierte Personendaten (im Weiteren: „**Sachdaten**"), die der Auftragnehmer vom Auftraggeber erhält oder im Rahmen der Erfüllung des Hauptvertrages gewinnt. Die Regelungen der Vereinbarung gelten für diese eigenen Zwecke des Auftragnehmers nicht. „**Dritte**" im Sinne dieses **Anhang E** sind sämtliche Empfänger von Personendaten oder Sachdaten ausserhalb des Auftragnehmers und des Auftraggebers, einschliesslich verbundene Unternehmen oder Konzernangehörige Unternehmen des Auftragnehmers.

1. Sachdaten

☐ Der Auftragnehmer ist nicht berechtigt, Sachdaten des Auftraggebers zu eigenen Zwecken des Auftragnehmers zu bearbeiten oder zu verwenden.

☐ Der Auftragnehmer ist in eigener Verantwortung zu folgendem Umgang mit Sachdaten berechtigt:

☐	Auswertungen zum Zwecke der Produktverbesserung und Produktentwicklung, z.B. Erstellung von Leistungs- und Kostenstatistiken, Vornahme weiterer Analysen, Auswertung von Vergütungsmodellen, Messung von Kundenzufriedenheit etc. Der Auftragnehmer ist berechtigt, die Auswertungen auch Dritten zur Verfügung zu stellen.
☐	Auswertung von Nutzerverhalten. Der Auftragnehmer ist berechtigt, die Auswertungen auch Dritten zur Verfügung zu stellen.
☐	Erhebung von Nutzungsdaten. Der Auftragnehmer ist berechtigt, die Daten auch Dritten zur Verfügung zu stellen.
☐	Marktanalysen. Der Auftragnehmer ist berechtigt, die Analysen auch Dritten zur Verfügung zu stellen.
☐	[…]

2. Personendaten

☐ Der Auftragnehmer ist nicht berechtigt, Personendaten des Auftraggebers zu eigenen Zwecken des Auftragnehmers zu bearbeiten oder zu verwenden.

☐ Der Auftragnehmer ist in eigener Verantwortung zu folgendem Umgang mit Personendaten des Auftraggebers zu eigenen Zwecken des Auftragnehmers berechtigt, unter der Voraussetzung, dass der Auftragnehmer die Einhaltung des geltenden Datenschutzrechts garantiert:

☐	Anonymisierung der Daten
☐	Auswertungen zum Zwecke der Produktverbesserung und Produktentwicklung, z.B. Erstellung von Leistungs- und Kostenstatistiken, Vornahme weiterer Analysen, Auswertung von Vergütungsmodellen, Messung von Kundenzufriedenheit etc. Der Auftragnehmer ist berechtigt, die Auswertungen in anonymisierter Form auch Dritten zur Verfügung zu stellen.
☐	Auswertung von Nutzerverhalten. Der Auftragnehmer ist berechtigt, die Auswertungen in anonymisierter Form auch Dritten zur Verfügung zu stellen.
☐	Erhebung von Nutzungsdaten. Der Auftragnehmer ist berechtigt, die Daten in anonymisierter Form auch Dritten zur Verfügung zu stellen.
☐	Kommunikation zur Entwicklung und Pflege von Kundenbeziehungen, insbesondere

	Kontaktaufnahme per E-Mail, SMS, Telefon oder Post zu eigenen Zwecken des Auftragnehmers.
☐	Marktanalysen. Der Auftragnehmer ist berechtigt, die Analysen in anonymisierter Form auch Dritten zur Verfügung zu stellen.
☐	Marketingzwecke des Auftragnehmers und Dritten und verkaufsfördernde Massnahmen, insbesondere Newsletter, Online-Werbung, Push Notifications, Marktforschung, Durchführung Umfragen.
☐	[…]

3. Pflichten des Auftragnehmers

Sollte der Auftragnehmer im Rahmen einer ihm nach diesem Anhang E eingeräumten Berechtigung geltendes Recht, insbesondere datenschutzrechtliche Anforderungen, verletzen, stellt der Auftragnehmer den Auftraggeber von sämtlichen Ansprüchen Dritter, die gegen den Auftragnehmer aus und im Zusammenhang mit diesem Anhang E gegen den Auftragnehmer gestellt werden, in vollem Umfang frei. Die Geltendmachung eines darüber hinaus gehenden Schadens bleibt dem Auftraggeber vorbehalten.

7. Die Ecke Datenzugänglichkeit:

Das Reifegradmodell von the Branch für Interoperabilität

thebranch

Interoperability Maturity Matrix (IMM) v.06

Produkt: XXXXX

	DATA TANSFER MECHANISM	DOCUMENTATION	EXPLANATION
☐	Public API		API open for the public.
☐	Closed API		API not available for the public.
☐	No API (FTP. .csv, copy & paste)		Data exchange with other parties through FTP, .csv, copy & paste)
	API ARCHITECTURE		
☐	REST		A RESTful API is an architectural style for an application program interface (API) that uses HTTP requests to access and use data. That data can be used to GET, PUT, POST and DELETE data types, which refers to the reading, updating, creating and deleting of operations concerning resources.
☐	SOAP		SOAP (Simple Object Access Protocol) is a message protocol that enables the distributed elements of an application to communicate. SOAP can be carried over a variety of standard protocols, including the web-related Hypertext Transfer Protocol (HTTP).
☐	PRC (Procedural remote call)		Remote Procedure Call (RPC) is a software communication protocol that one program can use to request a service from a program located in another computer on a network without having to understand the network's details. RPC is used to call other processes on the remote systems like a local system.
☐	GRAPHQL		GraphQL is designed to make APIs fast, flexible, and developer-friendly. It can even be deployed within an integrated development environment (IDE) known as GraphiQL. As an alternative to REST, GraphQL lets developers construct requests that pull data from multiple data sources in a single API call.
☐	OTHERS (please list)		
	EXCHANGE TYPE		
☐	Unidirectional		
☐	Bidirectional		
	END POINTS / RESOURCES		
☐	Short business description		What is the business value of this api?
☐	Full functionality		Does the api provide full functionality regarding business objects / data?
☐	Limited functionality		Does the api provide limited functionalities regarding business objects / data ?
☐	API upgrade and developments		Is it planned to upgrade limited functionalities to full functionalities in the next 3-9 month ?
	List of key business objects	/ref_house:	What are the key data points that can be accessed or exchanged using this api?
		/street:	
		/email:	
	AUTHORIZATION		
☐	HTTP basic authentication		If a simple form of HTTP authentication is all an app or service requires, HTTP basic authentication might be a good fit. It uses a locally derived username and password and relies on Base64 encoding. Authentication uses the HTTP header, making it easy to integrate. Because this method uses shared credentials, however, it's important to rotate passwords on
☐	API access tokens / keys		API keys have unique identifiers for each user and for every time they attempt to authenticate. Access tokens are suitable for applications where many users require access. Access tokens are secure and easy to work with from an end-user perspective.
☐	OAuth with OpenID		Despite having auth in the name, OAuth is not an authentication mechanism. Instead, it provides authorization services to determine which users have access to various corporate resources. OAuth is used alongside OpenID, an authentication mechanism. Using OAuth and OpenID together provides authentication and authorization. With OAuth 2.0, OpenID can authenticate users and devices using a third-party authentication system. This combination is considered one of the more secure authentication/authorization options available today.
☐	SAML federated identity		Security Assertion Markup Language (SAML) is another tokenlike authentication method often used in environments that have federated single sign-on (SSO) implemented. This XML-derived open standard framework helps seamlessly authenticate users through the organization's respective identity provider. For larger organizations working to consolidate the number of authentication mechanisms within the company, the use of SAML and federated SSO is a great fit.

	ROLES BASED ACCESS CONTROL (RBAC)		
☐	All have same roles based access (RBAC)		
☐	Every user has RBAC		
☐	Every user has RBAC, own org. unit with access		
☐	Every user has RBAC, has access rules by each org.unit, hierarchy		
☐	Every user has RBAC, and Attribute Based Access Control (ABAC) and authorization can be done on any level (hierarchy, object)		
	PRICING MODEL		
☐	Free		
☐	Pay as you go		Pay as you go API pricing models charge developers based on how much they (or rather, their software product) use the API.One example of a pay as you go API pricing model is pay per use/call. This is where you pay individually each time you make an API call. (i.e., when the API gets a request and retrieves the data required.)
☐	Fixed API pricing / per month		When picturing fixed API pricing, think subscription model. This would have developers/users pay a fixed amount per month or year to use the API. This may or may not restrict the amount the developer or their users can make use of the API. For example, take a fixed quota API pricing strategy. In a fixed quota strategy, the flat rate paid per month will cover the use of the API for a set amount of time/use. This is known as the quota. Once the quota is met, the API would not be usable until the next payment is taken.
☐	Combination API pricing		The most popular of the API pricing models is an approach that combines the above two methods. They're often known as overage models. An overage model has a base amount that is paid to use the API, and it comes with a quota. If this quota is met, the API will still work. But, you'll swap to a pay as you go method for all the API calls or downloads that exceed the quota for the specified time.
☐	Partnership-based API pricing		This type relies on a kind of partnership between the developers using the API, and the API owners.The API pricing model in question is known as revenue share. This is where the API provider gets a share of the revenue generated by the developer's use of their API.
	RESTRICTIONS		
☐	API restrictions		Are there any general or specific restrictions regarding the use of the API? Please specify in the lines below.
☐	(restriction 1)		
☐	(restriction 2)		
	CONTACT ADDRESS		
Company address	xxxxxxxxxxxxxxxxxxxx		
Contact person	xxxxxxxxxxxxxxxxxxxx		
Contact e-mail	xxxxxxxxxxxxxxxxxxxx		
Contact phone	xxxxxxxxxxxxxxxxxxxx		

thebranch

8. Zutaten für den Erfolg:

a) Bestellerkompetenz und Verankerung in allen Verträgen

thebranch

9. Zutaten für den Erfolg:

b) neutrale Kooperationsgefässe

thebranch

10. Zutaten für den Erfolg:

c) Politischer Druck (hoffentlich nicht)

thebranch

Fragen

1. Was ist neu im nDSG?
2. Was kann man von der EU in Sachen Datenschutz und Zusammenarbeit unter Unternehmen lernen?
3. Wieso hatte Standardisierung in der Immobilienwirtschaft bis dato einen so schwierigen Stand?
4. Wieso ist Datenzugänglichkeit / Verfügbarkeit / Durchgängigkeit so essentiell?
5. Was kann man von Initiativen wie FRIDA betr. Datenaustausch / -Zugänglichkeit lernen?
6. Wer sind die wichtigsten Player, die man gewinnen muss?
7. Was muss im Q1 / 2023 geschehen, damit sich was ändert?
8. Soll man auf die Politik setzen?