

Gefördert durch:



Bundesministerium
der Justiz und
für Verbraucherschutz

aufgrund eines Beschlusses
des Deutschen Bundestages



Projektträger Bundesanstalt
für Landwirtschaft und Ernährung



ISEngineering
Information Systems Engineering



Digital Autonomy Hub Tutorial

Neue technische Wege zur Erfüllung datenschutzrechtlicher Transparenzpflichten

Elias Grünewald, Dr.-Ing. Frank Pallas

21.01.2021

DaSKITA

Apple App Store

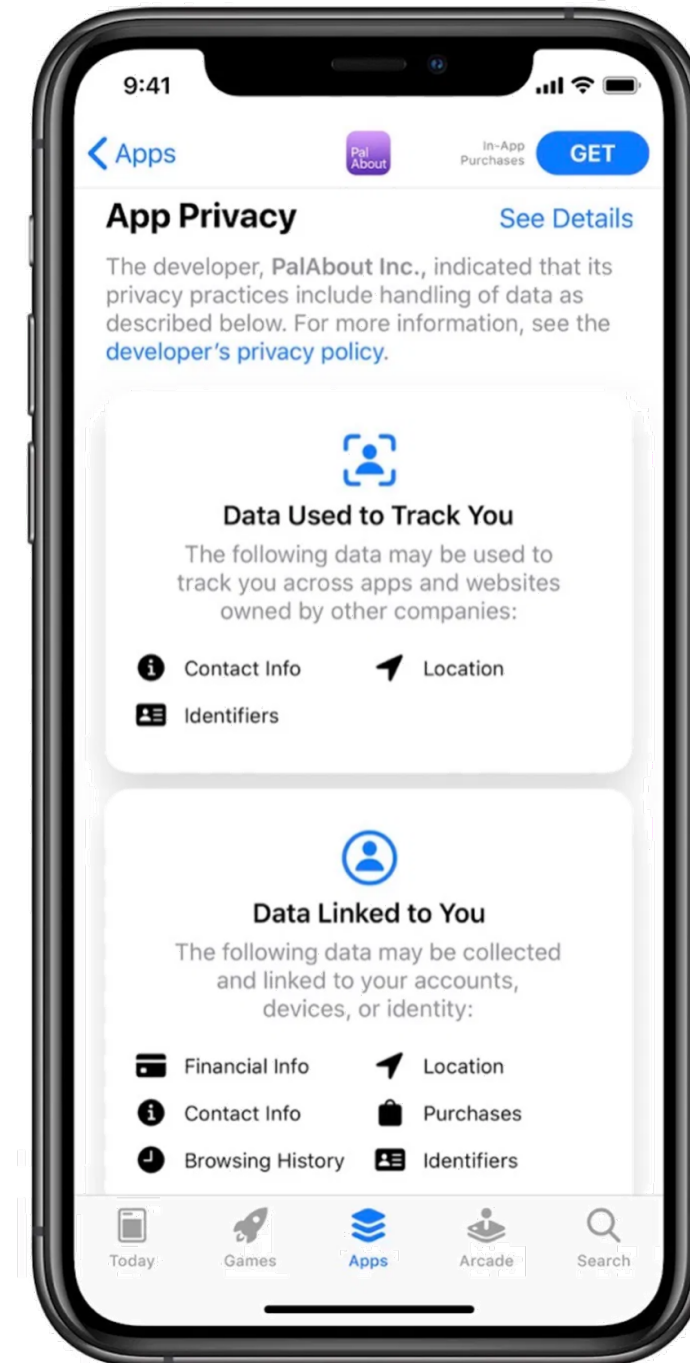
Schau mal, was die tracken

Welche App will welche Daten von mir? Im App Store müssen Entwickler nun anzeigen, welche Informationen sie sammeln. Apple will damit Transparenz für die Nutzer schaffen.

Von **Lisa Hegemann**14. Dezember 2020, 21:29 Uhr / [61 Kommentare](#) / 

Apps mögen nett aussehen, sammeln aber teils sehr viele Daten. © Benjamin Sow/unsplash.com

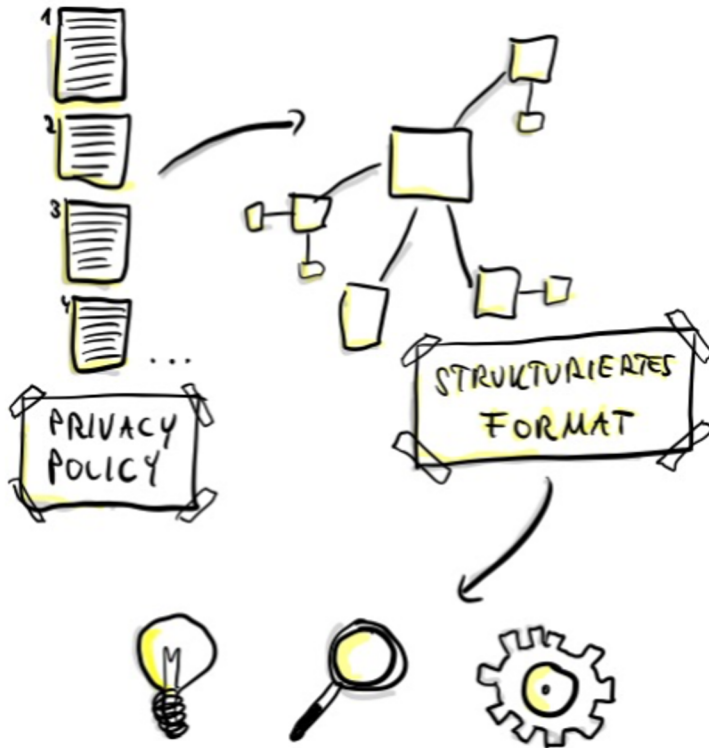
Apps können ganz schön neugierig sein. Wie heißen Sie? Wie lautet Ihre E-Mail-Adresse? Wo wohnen Sie und wo sind Sie gerade, wie lautet Ihre



Motivation

- ➔ **Standardisiertes maschinenlesbares Format für datenschutzrechtliche Transparenzinformationen**
 - im *vollen* rechtlich geforderten Umfang (Art. 12, 13, 14, [15, 30] DSGVO)
 - in einer **nachvollziehbaren und transparenten Form** (Art. 5 GDPR)
- ➔ Neue technische Wege für Nutzer*innen werden ermöglicht (adaptiv, kontextuell, nach Präferenz...)
- ➔ Verantwortliche Stellen können die Informationen intern und extern deutlich vielseitiger und effizienter verarbeiten

Agenda



- **Rechtliche Grundlagen**
- **Transparency Information Language**
 - Ausdrucksmächtigkeit
 - Design und Implementierung
- **Toolkit** und aufbauende Arbeiten
 - Hands-on
- **Ausblick**
- **Diskussion**

Rechtliche Grundlagen

4.5.2016	DE	Amtsblatt der Europäischen Union	L 119/1
I			
(Gesetzgebungsakte)			
VERORDNUNGEN			
VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES			
vom 27. April 2016			
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)			
(Text von Bedeutung für den EWR)			
DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —			
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,			
auf Vorschlag der Europäischen Kommission,			
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,			
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ⁽¹⁾ ,			
nach Stellungnahme des Ausschusses der Regionen ⁽²⁾ ,			
gemäß dem ordentlichen Gesetzgebungsverfahren ⁽³⁾ ,			
in Erwägung nachstehender Gründe:			
⁽¹⁾ Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.			
⁽²⁾ Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.			
⁽³⁾ Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ^(*) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.			
^(*) ABl. C 229 vom 31.7.2012, S. 90.			
⁽¹⁾ ABl. C 391 vom 18.12.2012, S. 127.			
⁽²⁾ Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.			
⁽³⁾ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).			

Fundstellen				Kurzbezeichnung
13(1a)	14(1a)		30(1a)	Verantwortliche*r
13(1b)	14(1b)		30(1a)	Datenschutzbeauftragte*r
13(1c)	14(1c)	15(1a)	30(1b)	Zwecke
13(1c)	14(1c)			Rechtsgrundlage
13(1d)	14(2b)			Berechtigte Interessen
13(1e)	14(1e)	15(1c)	30(1d)	Empfänger(-kategorien)
13(1f)	14(1f)	15(1c)	30(1e)	Drittland-Weitergabe
13(1f)	14(1f)	15(2)	30(1e)	Angemessenheit (Drittland)
13(1f)	14(1f)	15(2)	30(1e)	Auskunft und Datenportabilität
13(2a)	14(2a)	15(1d)	30(1f)	Dauer der Speicherung, Speicherkriterien
13(2b)	14(2c)	15(1e)		Recht auf Auskunft
13(2b)	14(2c)	15(1e)	16, 17	Recht auf Berichtigung oder Löschung
13(2b)	14(2c)	15(1e)	20	Recht auf Datenübertragbarkeit
13(2c)	14(2d)			Recht auf Widerruf der Einwilligung
13(2d)	14(2e)	15(1f)		Recht auf Beschwerde
13(2e)				Erforderlichkeit/Nichtpreisgabe
13(2f)	14(2g)	15(1h)	22	Automatisierte Entscheidungsfindung/Logik
14(2f)				Quellen
13(3)				Benachrichtigung bei Zweckänderung
			30(1c)	Kategorien der betroffenen Personen/Daten

	# Tabellenbl. Dienste	1 1A VW	2 1B RyanAir	3 1C MAN	4 2A Shire	5 2B BASF	6 2C Beiersdorf	7 3A Vinci	8 3B Viessmann	9 3C Stihl	10 4A Caritas	11 4B TK	12 4C Fresenius	13 5A Siemens	14 5B Telefónica	15 5C Lotto	16 6A REWE	17 6B nnes & Mau	18 6C Tesco	19 7A DHL	20 7B WEB.de	21 7C Repubblica	22 8A LTUR	23 8B Verivox	24 8C Enel	25 9A BNP Paribas	26 9B Otto	27 9C Carrefour	28 10A Qwant	29 10B XING	30 10C YouPorn	
Verantwortliche*r		+	~	~	+	+	+	-	~	~	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	~	+	+	+	+	+	
Datenschutzbeauftragte*r		+	~	+	+	+	+	+	+	~	+	+	~	+	+	+	+	+	+	+	+	+	~	~	+	+	+	+	+	+	+	~
Zwecke		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	~	+	+	+	+	+	+	+	~
Rechtsgrundlage		+	+	+	+	+	+	+	+	~	+	+	-	+	+	+	+	+	+	+	+	~	+	+	~	~	~	+	+	+	+	~
Berechtigte Interessen		+	+	+	~	~	+	-	+	+	-	+	+	+	+	+	+	+	+	+	+	~	+	+	~	~	~	+	+	+	+	+
Empfänger(kategorien)		+	~	~	~	~	~	+	+	~	~	~	~	~	~	+	+	+	~	~	+	~	+	~	~	-	~	+	+	+	+	~
Drittland-Weitergabe		~	~	+	+	+	+	?	+	+	+	?	+	~	~	~	~	+	+	+	+	-	+	~	+	?	~	~	+	?	+	~
Angemessenheit (Drittland)		?	?	+	?	?	?	?	+	+	+	?	+	~	+	~	~	+	+	+	+	?	+	+	+	+	+	+	+	?	+	+
Auskunft und Datenportabilität		+	+	-	~	~	-	-	+	-	-	+	~	~	~	+	~	-	+	-	~	+	+	+	+	+	+	+	~	+	+	+
Dauer der Speicherung bzw. Speicherkriterien		+	+	~	+	+	+	+	+	~	~	~	~	~	+	+	~	+	+	~	+	+	~	+	+	~	~	~	+	+	+	~
Recht auf Auskunft		+	+	+	+	+	+	+	+	+	+	+	~	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	~	+	+	+
Recht auf Berichtigung oder Löschung		+	+	+	+	+	+	+	+	+	+	+	+	+	-	~	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Recht auf Datenübertragbarkeit		+	+	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Recht auf Widerruf der Einwilligung		+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Recht auf Beschwerde		+	+	-	+	+	+	+	+	+	+	+	~	~	+	+	+	~	+	+	+	+	+	+	+	+	+	+	+	+	+	+
Erforderlichkeit und Konsequenzen bei Nichtpreisgabe		~	~	+	+	+	~	+	+	~	+	?	-	~	~	~	~	+	+	?	?	+	~	~	~	-	~	~	-	~	~	-
Automatisierte Entscheidungsfindung und Logik		?	?	+	?	?	?	?	~	?	?	+	?	?	?	~	+	~	+	?	?	~	~	+	~	?	+	+	?	?	+	?
Quellen		+	+	+	+	+	+	~	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	+	~	+	~	+	+	+	+
Benachrichtigung bei Zweckänderung		?	+	~	-	-	?	-	+	+	?	?	?	?	~	+	?	~	+	~	~	~	+	?	?	-	+	?	~	~	?	+
Kategorien der betroffenen Personen und Daten		+	+	+	+	+	+	-	+	+	+	+	-	+	+	+	+	+	+	+	+	~	+	~	-	+	+	-	+	+	+	~

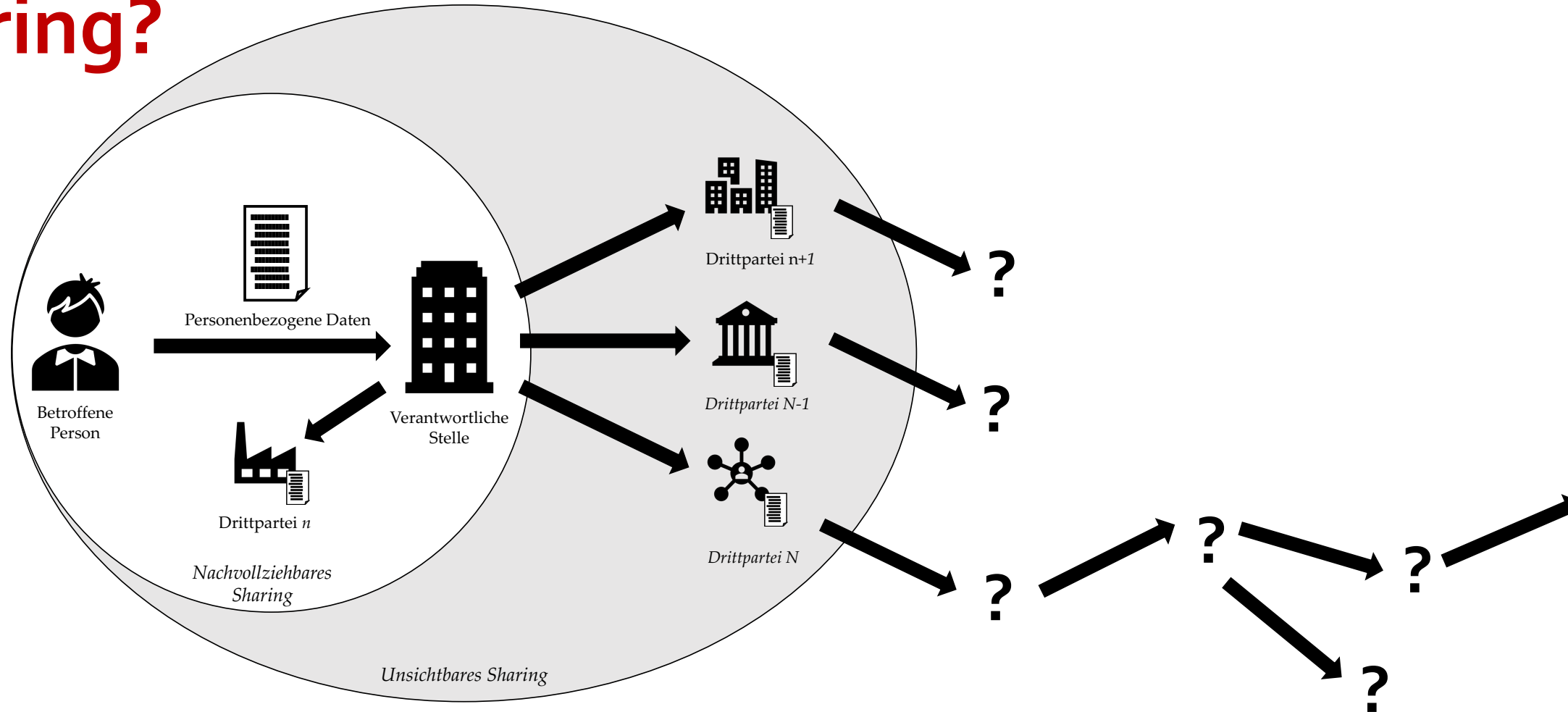
Legende: ? + ~ - Unklar | Erfüllt | Unvollständig | Nicht erfüllt

Rechtliche Grundlagen

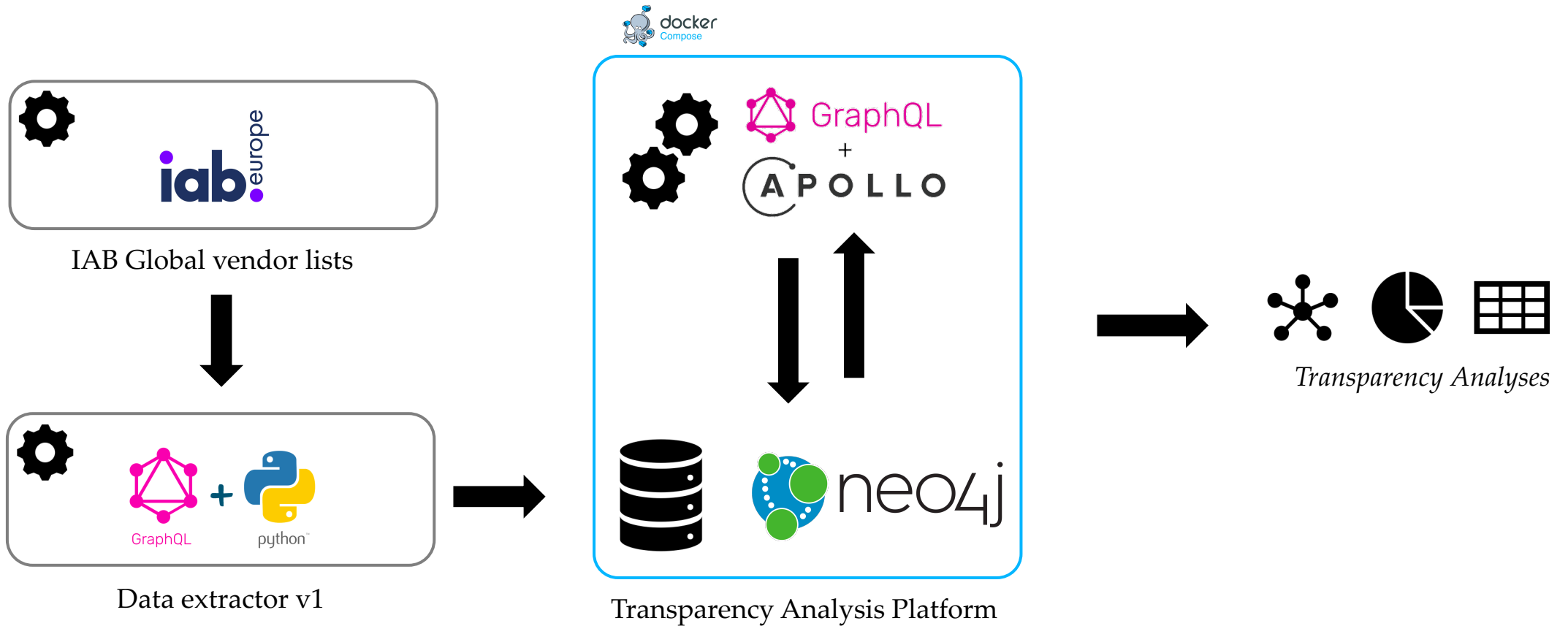
4.5.2016	DE	Amtsblatt der Europäischen Union	L 119/1
I			
(Gesetzgebungsakte)			
VERORDNUNGEN			
VERORDNUNG (EU) 2016/679 DES EUROPÄISCHEN PARLAMENTS UND DES RATES			
vom 27. April 2016			
zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung)			
(Text von Bedeutung für den EWR)			
DAS EUROPÄISCHE PARLAMENT UND DER RAT DER EUROPÄISCHEN UNION —			
gestützt auf den Vertrag über die Arbeitsweise der Europäischen Union, insbesondere auf Artikel 16,			
auf Vorschlag der Europäischen Kommission,			
nach Zuleitung des Entwurfs des Gesetzgebungsakts an die nationalen Parlamente,			
nach Stellungnahme des Europäischen Wirtschafts- und Sozialausschusses ⁽¹⁾ ,			
nach Stellungnahme des Ausschusses der Regionen ⁽²⁾ ,			
gemäß dem ordentlichen Gesetzgebungsverfahren ⁽³⁾ ,			
in Erwägung nachstehender Gründe:			
⁽¹⁾ Der Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten ist ein Grundrecht. Gemäß Artikel 8 Absatz 1 der Charta der Grundrechte der Europäischen Union (im Folgenden „Charta“) sowie Artikel 16 Absatz 1 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) hat jede Person das Recht auf Schutz der sie betreffenden personenbezogenen Daten.			
⁽²⁾ Die Grundsätze und Vorschriften zum Schutz natürlicher Personen bei der Verarbeitung ihrer personenbezogenen Daten sollten gewährleisten, dass ihre Grundrechte und Grundfreiheiten und insbesondere ihr Recht auf Schutz personenbezogener Daten ungeachtet ihrer Staatsangehörigkeit oder ihres Aufenthaltsorts gewahrt bleiben. Diese Verordnung soll zur Vollendung eines Raums der Freiheit, der Sicherheit und des Rechts und einer Wirtschaftsunion, zum wirtschaftlichen und sozialen Fortschritt, zur Stärkung und zum Zusammenwachsen der Volkswirtschaften innerhalb des Binnenmarkts sowie zum Wohlergehen natürlicher Personen beitragen.			
⁽³⁾ Zweck der Richtlinie 95/46/EG des Europäischen Parlaments und des Rates ^(*) ist die Harmonisierung der Vorschriften zum Schutz der Grundrechte und Grundfreiheiten natürlicher Personen bei der Datenverarbeitung sowie die Gewährleistung des freien Verkehrs personenbezogener Daten zwischen den Mitgliedstaaten.			
^(*) ABl. C 229 vom 31.7.2012, S. 90.			
⁽¹⁾ ABl. C 391 vom 18.12.2012, S. 127.			
⁽²⁾ Standpunkt des Europäischen Parlaments vom 12. März 2014 (noch nicht im Amtsblatt veröffentlicht) und Standpunkt des Rates in erster Lesung vom 8. April 2016 (noch nicht im Amtsblatt veröffentlicht). Standpunkt des Europäischen Parlaments vom 14. April 2016.			
⁽³⁾ Richtlinie 95/46/EG des Europäischen Parlaments und des Rates vom 24. Oktober 1995 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (ABl. L 281 vom 23.11.1995, S. 31).			

Fundstellen				Kurzbezeichnung
13(1a)	14(1a)		30(1a)	Verantwortliche*r
13(1b)	14(1b)		30(1a)	Datenschutzbeauftragte*r
13(1c)	14(1c)	15(1a)	30(1b)	Zwecke
13(1c)	14(1c)			Rechtsgrundlage
13(1d)	14(2b)			Berechtigte Interessen
13(1e)	14(1e)	15(1c)	30(1d)	Empfänger(-kategorien)
13(1f)	14(1f)	15(1c)	30(1e)	Drittland-Weitergabe
13(1f)	14(1f)	15(2)	30(1e)	Angemessenheit (Drittland)
13(1f)	14(1f)	15(2)	30(1e)	Auskunft und Datenportabilität
13(2a)	14(2a)	15(1d)	30(1f)	Dauer der Speicherung, Speichungskriterien
13(2b)	14(2c)	15(1e)		Recht auf Auskunft
13(2b)	14(2c)	15(1e)	16, 17	Recht auf Berichtigung oder Löschung
13(2b)	14(2c)	15(1e)	20	Recht auf Datenübertragbarkeit
13(2c)	14(2d)			Recht auf Widerruf der Einwilligung
13(2d)	14(2e)	15(1f)		Recht auf Beschwerde
13(2e)				Erforderlichkeit/Nichtpreisgabe
13(2f)	14(2g)	15(1h)	22	Automatisierte Entscheidungsfindung/Logik
14(2f)				Quellen
13(3)				Benachrichtigung bei Zweckänderung
			30(1c)	Kategorien der betroffenen Personen/Daten

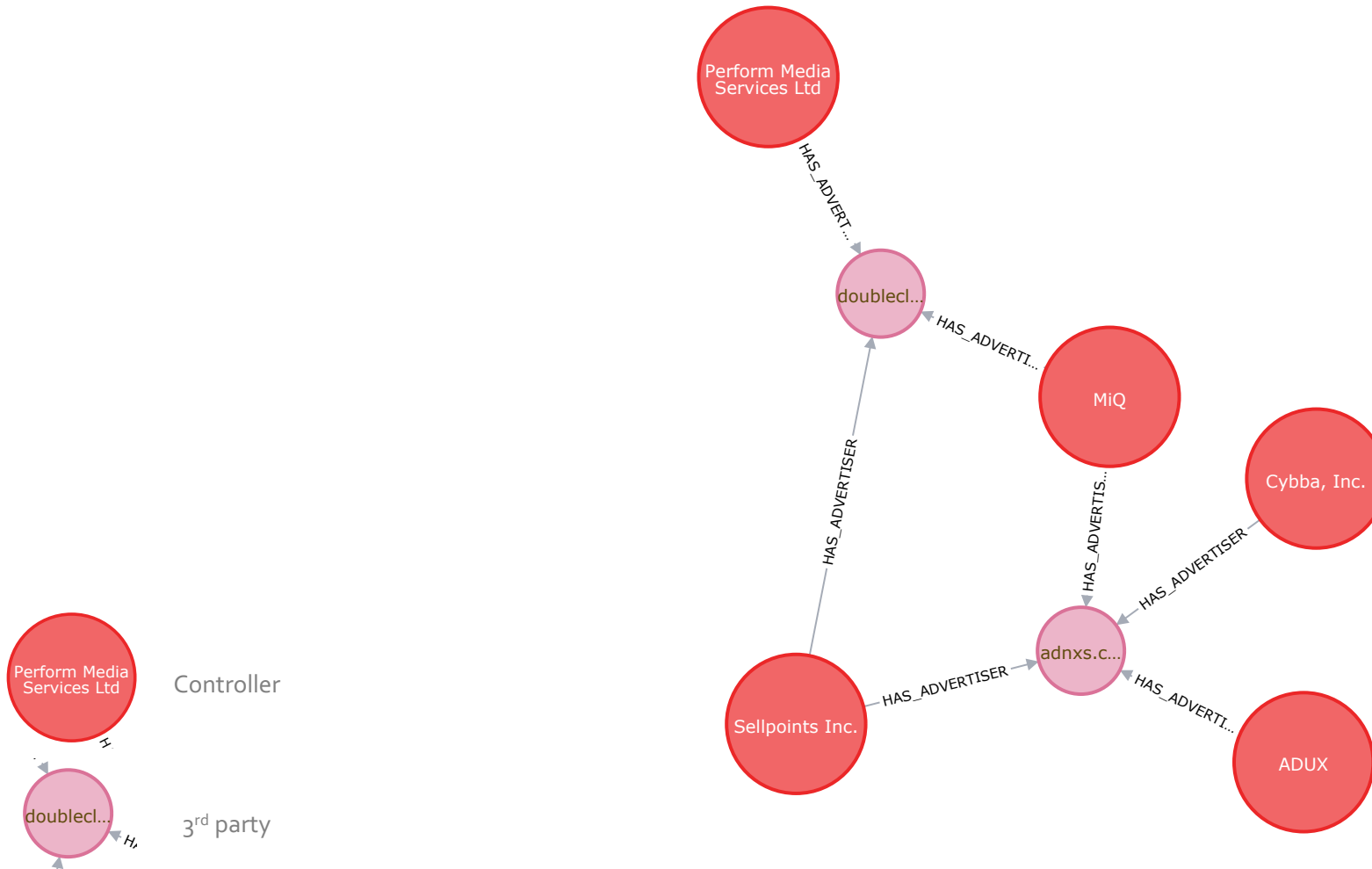
Sharing?



Transparency Analysis Platform (tap) für IAB Europe



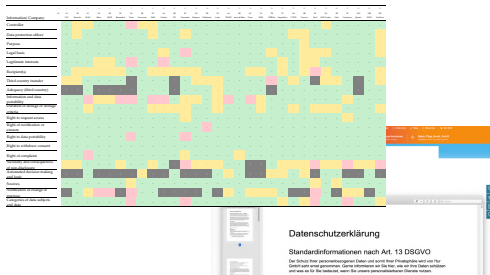
Aufdecken von Datenaustausch-Netzwerken*



* Mehr dazu später

Transparency Information Language (TIL)

Standstellen	Kurzbezeichnung
(1a) 14(1a)	30(1a) Verantwortliche*r
(1b) 14(1b)	30(1a) Datenschutzbeauftragte*r
(1c) 14(1c) 15(1a) 30(1b)	Zwecke
(1c) 14(1c)	Rechtsgrundlage
(1d) 14(1d)	Berechtigte Interessen



1. Rechtliche Anforderungen. 
2. Abgleich mit existierender Praxis in der Industrie. 
3. Austausch- und Weiterleitungsnetzwerke identifizieren können. 
4. Ausdrucksmächtigkeit der Sprache definieren. 

Notwendige Ausdrucksmächtigkeit

Kurzbezeichnung	Beschreibung	Beispiel	Anmerkungen
Meta-Informationen zur Identifikation und Verifikation des Dokuments	1. Identifikationsnummer* 2. Name* 3. Erstellungsdatum* 4. Änderungsdatum* 5. Version* 6. Sprachkürzel*⁶ 7. Status* 8. URL* 9. Hash*⁷	1. f1424f86-ca0f-4f0c-9438-43cc00509931⁸ 2. VW 3. 2020-04-03T15:53:05.929588 4. 2020-06-01T16:16:47.151300 5. 2 6. de 7. active 8. https://elektrowagen.de/datenschutz 9. d732a793562a3e5dc57645a8e9947a8a72af5ef6f64a247879cdfd3077725799	Die Identifikationsnummer ist global eindeutig.
Verantwortliche*r	1. Unternehmensbezeichnung* 2. Unternehmensbereich 3. Anschrift* 4. Landeskürzel*⁹ 5. Name (Vertreter)* 6. Email (Vertreter)* 7. Telefon (Vertreter)	1. Elektrowagen AG 2. Unternehmensbereich/Produktlinie E-Mobilität 3. Wolfsburger Ring 2, 38440 Berlin 4. DE 5. Hubert Deiss 6. kundenbetreuung@elektrowagen.de 7. 0151 1234 5678	2 dient der Unterscheidung verschiedener Bereiche eines Unternehmens; besonders relevant für Großunternehmen.
Datenschutzbeauftragte*r	1. Name* 2. Anschrift* 3. Landeskürzel* 4. Email* 5. Telefon	1. Datenschutzbeauftragter der Elektrowagen AG 2. Wolfsburger Ring 2, 38440 Berlin 3. DE 4. datenschutz@elektrowagen.de 5. 0171 1234 5678	Wenn möglich, ist eine natürliche Person anzugeben.

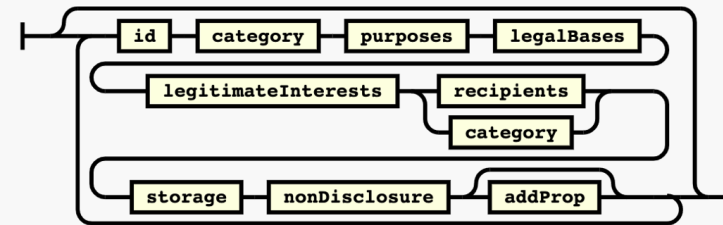
Formale Sprachdefinition

```

16 tilt = header, properties, [addProp];
17
18 header = schema, identification, title, description, examples, [addProp];
19 schema = "http://json-schema.org/draft-07/schema";
20 identification = "https://github.com/Transparency-Information-Language/schema";
21 title = "Transparency Information Language";
22 description = string;
23 examples = { properties };
24
25 properties = meta,
26   controller,
27   dataProtectionOfficer,
28   dataDisclosed,
29   thirdCountryTransfers,
30   accessAndDataPortability,
31   sources,
32   rightToInformation,
33   rightToRectificationOrDeletion,
34   rightToDataPortability,
35   rightToWithdrawConsent,
36   rightToComplain,
37   automatedDecisionMaking,
38   changesOfPurpose,
39   [addProp];
40 (* Note: Each of these properties can have any additional "subproperties" which are not shown *)
41
42 meta = id, name, created, modified, version, language, status, url, hash;
43 id = string;
44 created = stringDate;
45 modified = stringDate;
46 version = string;
47 language = string;
48 status = string;
49 url = stringUrl;
50 hash = stringHash;
51
52 controller = name, division, address, country, representative;
53 name = string;
54 division = string;
55 address = string;
56 country = stringCountryCode;
57
58 representative = name, email, [phone];

```

dataDisclosed



```

dataDisclosed = { ( id , category , purposes ,
  legalBases , legitimateInterests , ( recipients | category ) ,
  storage , nonDisclosure , [ addProp ] ) };

```

Items referencing **dataDisclosed**:

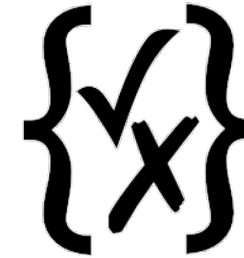
- properties

dataDisclosed is referencing:

- id
- category
- purposes
- legalBases
- legitimateInterests
- recipients
- storage
- nonDisclosure
- addProp

Technische Implementierung (i)

```
"name": {  
  "$id": "#/properties/controller/properties/name",  
  "type": "string",  
405  "title": "Name",  
  "description": "Name of the controller.",  
  "examples": [  
    "Green Company AG"  
  ]  
410 },
```



JSON Schema

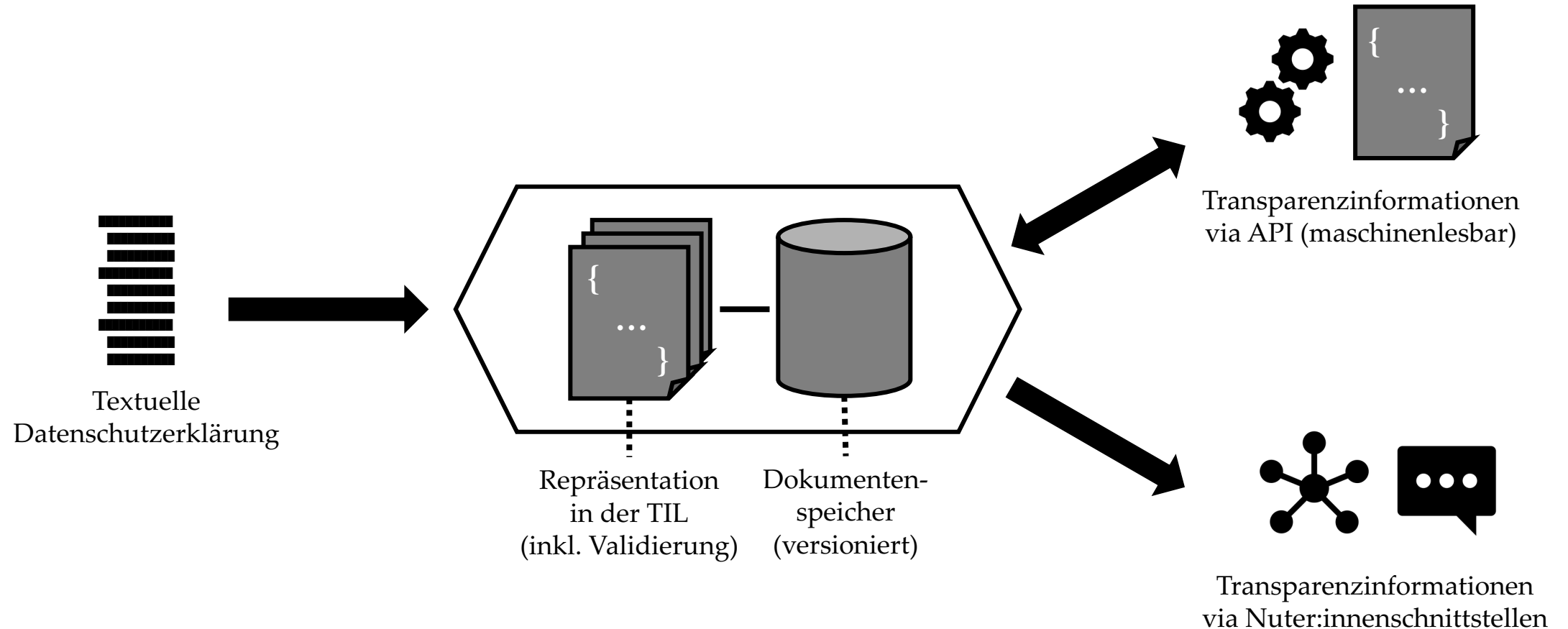
Technische Implementierung (ii)

- **JSON** als plattformunabhängiges Datenformat
- **JSON Schema** für sofortige Validierung (syntaktisch, tlw. semantisch)
- Reguläre Ausdrücke und definierte Typen für gängige Standards
- Zahlreiche `if-then-else/anyOf`-Konstrukte für rechtlichen Kontext
 - `"if (automatedDecisionMaking) { then descriptionOfInvolvedLogic }"`
 - `"either temporal or conditional data retention"`

Beispiel

```
15  },
    "controller": {
      "name": "Green Company AG",
      "division": "Product line e-mobility",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "representative": {
        "name": "Jane Super",
        "email": "contact@greencompany.de",
        "phone": "0049 151 1234 5678"
      }
    },
    "dataProtectionOfficer": {
      "name": "Jane Super",
      "address": "Wolfsburger Ring 2, 38440 Berlin",
      "country": "DE",
      "email": "contact@greencompany.de",
      "phone": "0049 151 1234 5678"
    },
    "dataDisclosed": [
      {
        "_id": "f1424f86-ca0f-4f0c-9438-43cc00509931",
        "category": "E-mail address",
        "purposes": [
          {
            "purpose": "Marketing",
            "description": "Newsletter will be sent out once a month."
          }
        ]
      }
    ],
    "legalBases": [
      {
        "reference": "GDPR-99-1-a",
        "description": "The data are processed on the basis of Art. 99 GDPR which states..."
      },
      {
        "reference": "BDSG-42-5",
        "description": "BDSG-42-5 refers to the processing of personal data within..."
      }
    ],
    "legitimateInterests": [
      {
        "exists": false,
        "reasoning": "There is an legitimate interest based on ... and is not overwritten because ..."
      }
    ],
    "recipients": [
      {
        "name": "Yellow Company AG",
        "division": "Product line e-mobility",
        "address": "Triana 123, 9999 Seville",
        "country": "ES",
        "representative": {
```

Language (✓) and Toolkit (tilt)



Bibliotheken



`pom.xml + mvn install`

```
// Generate new Tilt instance from scratch
Tilt tilt = new Tilt();

Controller controller = new Controller();
controller.setName("Example Company SE");
tilt.setController(controller);
```

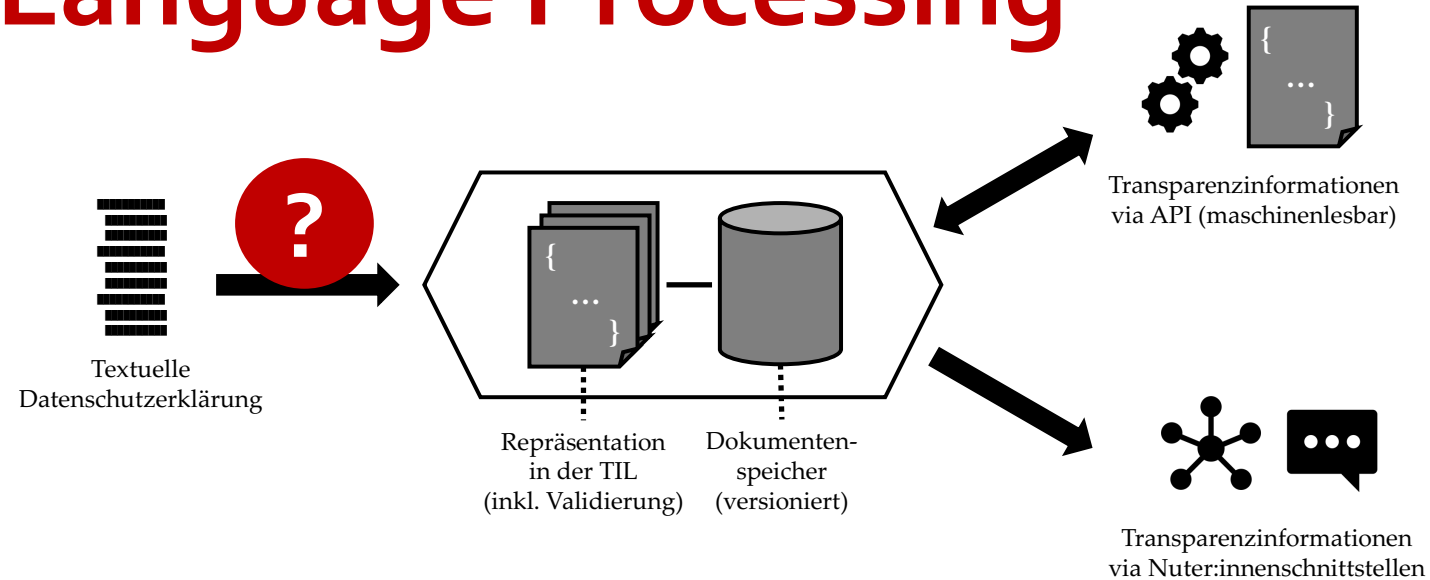


`pip install tilt`

```
for element in list(instance.data_disclosed):
    for recipient in element.recipients:
        print(recipient.category)
# Marketing content provider
# Responsible Statistical Institutes

instance.controller.name = 'Yellow Company Ltd.'
print(instance.controller.to_dict())
# {'address': 'Wolfsburger Ring 2, 38440 Berlin',
```

Natural Language Processing



1

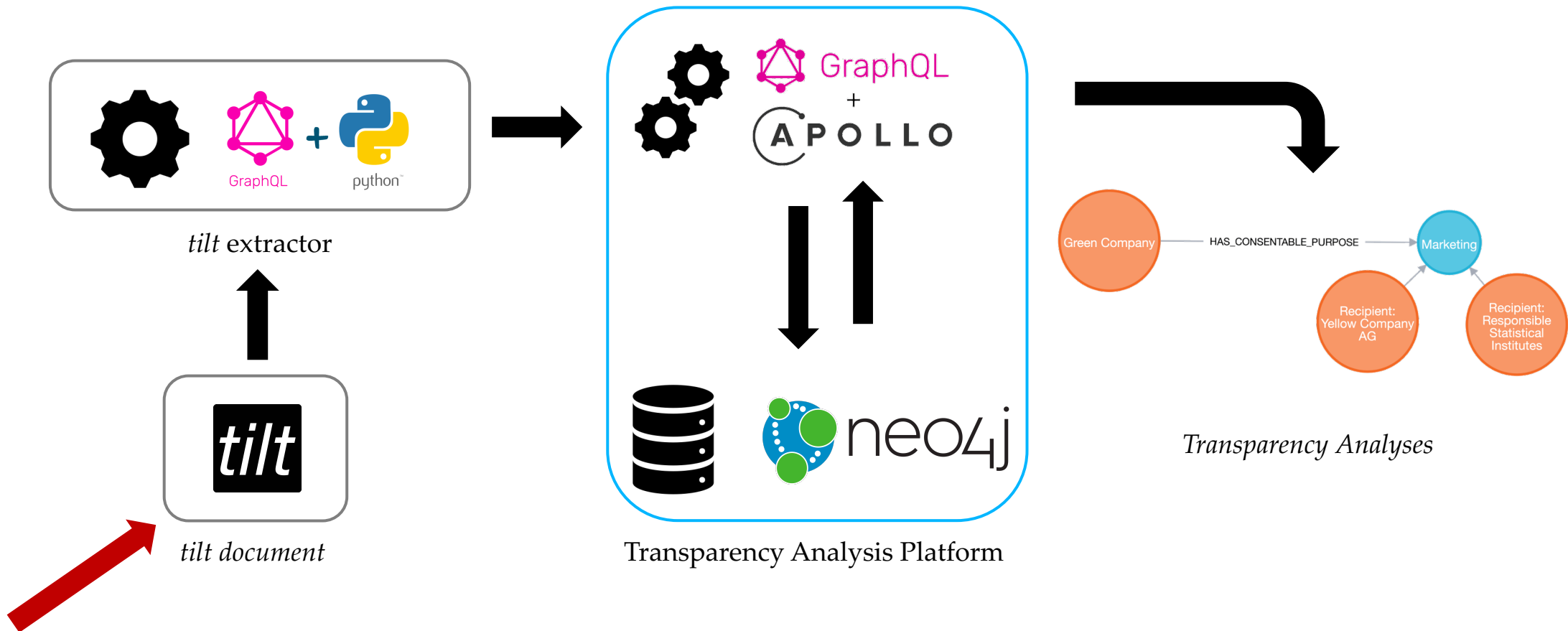
(i) Welcome to the web site (the "Site") of **Zapier, ORG** Inc. ("Zapier", "we", "us" and/or "our").

(ii) Privacy Policy This Policy was last updated on **May 29, 2018 DATE** . Visit **Alexandria GPE** has created this statement in order to demonstrate our

2

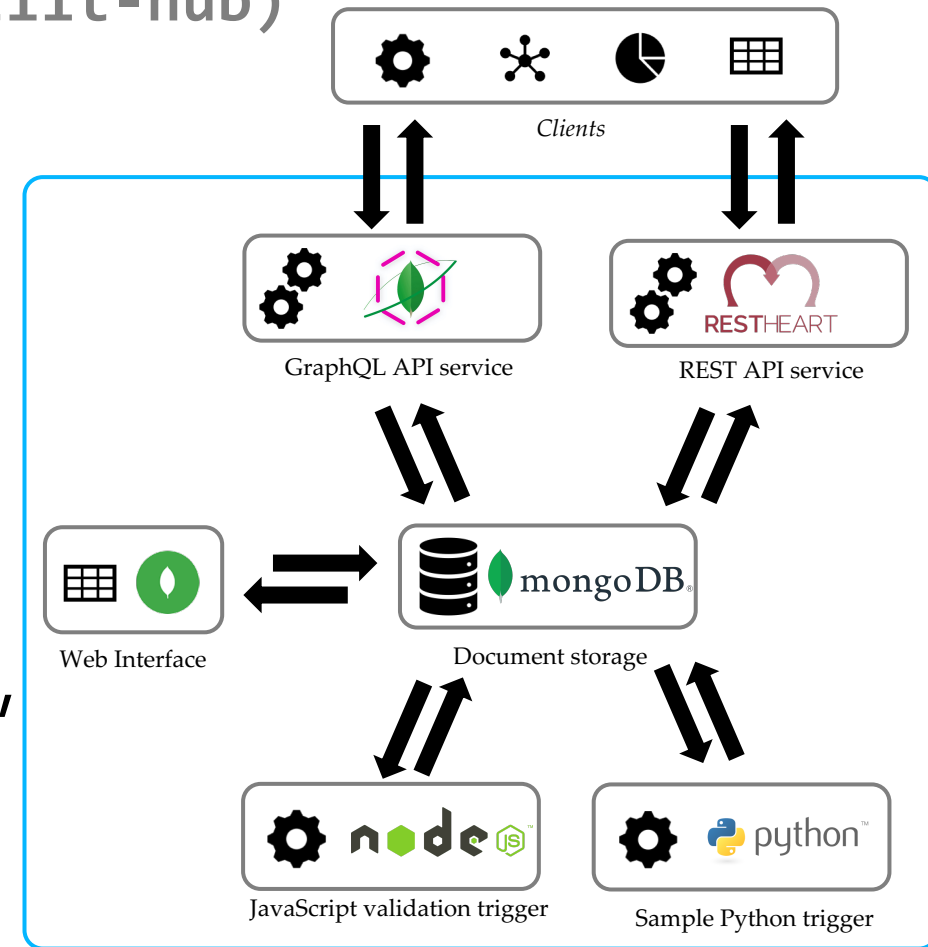
<tilt.tilt.Controller object at 0x1153c85b0>

Transparency Analysis Platform



Dokumentenspeicher (tilt-hub)

1. Erstellung von *TIL*-Dokumenten.
2. Verwaltung und Speicherung im *tilt-hub*.
3. Anfragen via **APIs**.
4. Konzeption **aufbauender Anwendungen** (z.B. Privacy Agents), verbesserte Kollaboration und neue interne Prozesse oder Auditierung.

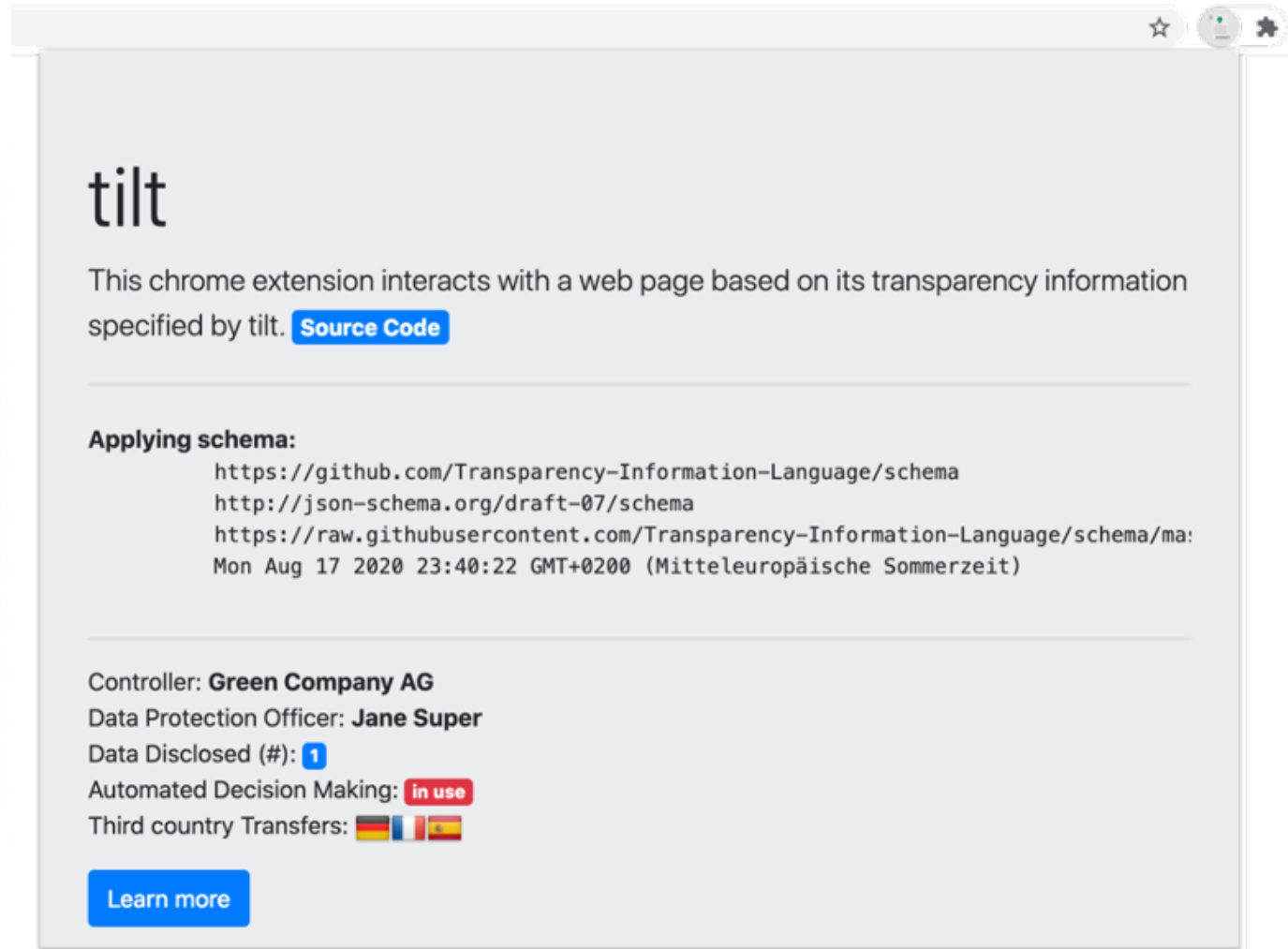
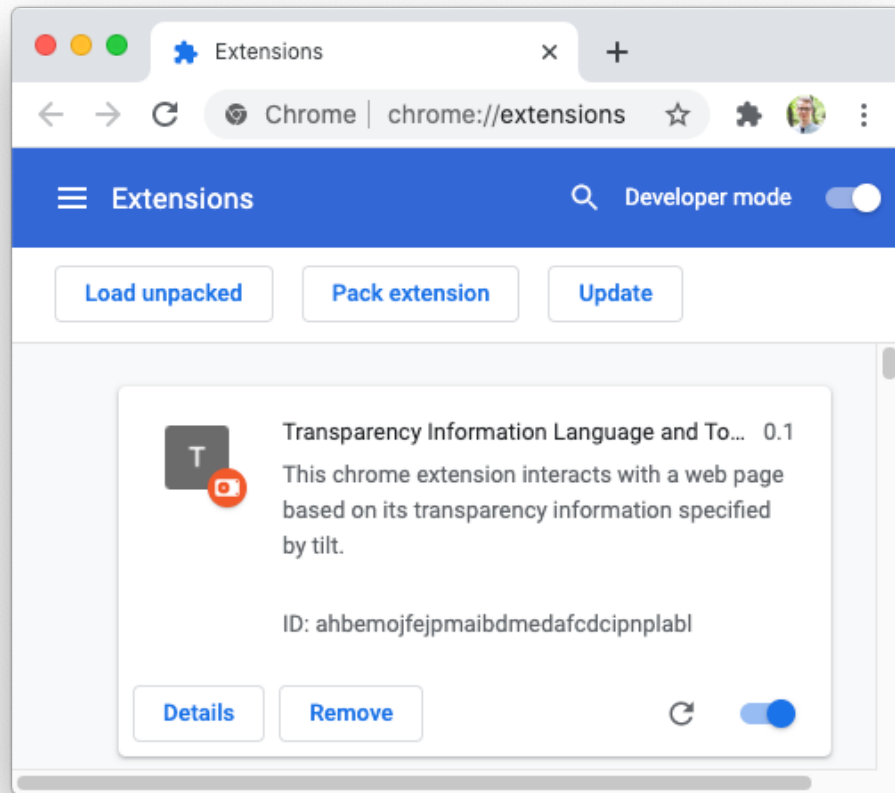


API/GraphQL

```
{
  Tilt {
    controller {
      name
    }
    dataProtectionOfficer {
      name
    }
    thirdCountryTransfers {
      country
      adequacyDecision {
        available
      }
    }
  }
}
```

```
{
  "data": {
    "Tilt": {
      "controller": {
        "name": "Green Company AG"
      },
      "dataProtectionOfficer": {
        "name": "Jane Wonderwomen"
      },
      "thirdCountryTransfers": [
        {
          "country": "ES",
          "adequacyDecision": {
            "available": true
          }
        }
      ]
    }
  }
}
```

Browser-Erweiterung (chrome-tilt)



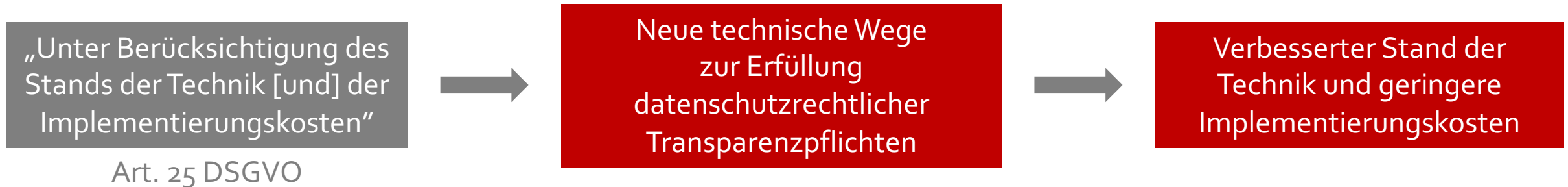


Interesse geweckt?

Verwandte Arbeiten

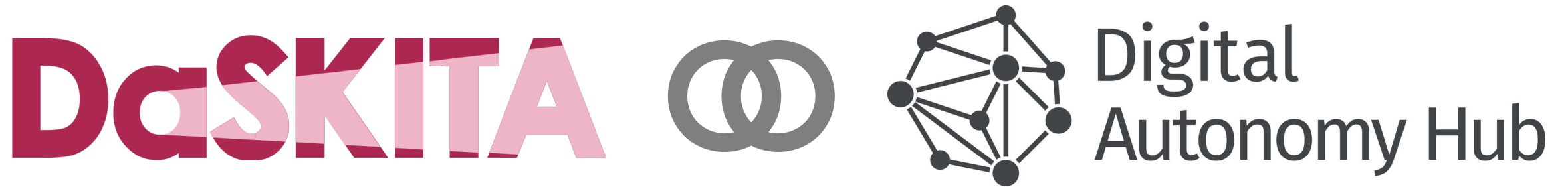
	Ansatz	Anwendungsbereich der Transparenz	DSGVO-Ansprüche	Interoperabilität und Tooling	Flexible Vokabulare	Unternehmenskontext	Privater Kontext
Zhao et al. 2016							
Cranor et al. 2002	P3P	✓	✗	(✗), nur Privacy Bird	✗	✓	✓
Ardagna et al. 2009	PrimeLife Policy Language	(✓)	✗	✗	✓	✓	(✓)
Gerl et al. 2018	LPL	(✓) + De-Identifikation	(✓), bestenfalls nach Revision	(✗), nur „Visualizer“	✓	(✗), nur rudimentärer Speicher	✓
Bonatti et. al. 2019	SPECIAL	(✓) + Konsent	(✓), nicht alle	✓	✗	✓	(✓), Dashboard
Grünewald und Pallas 2021	TILT	✓	✓	✓	✓	✓	✓

„Okay, aber warum sollte ein Unternehmen *das* machen?“



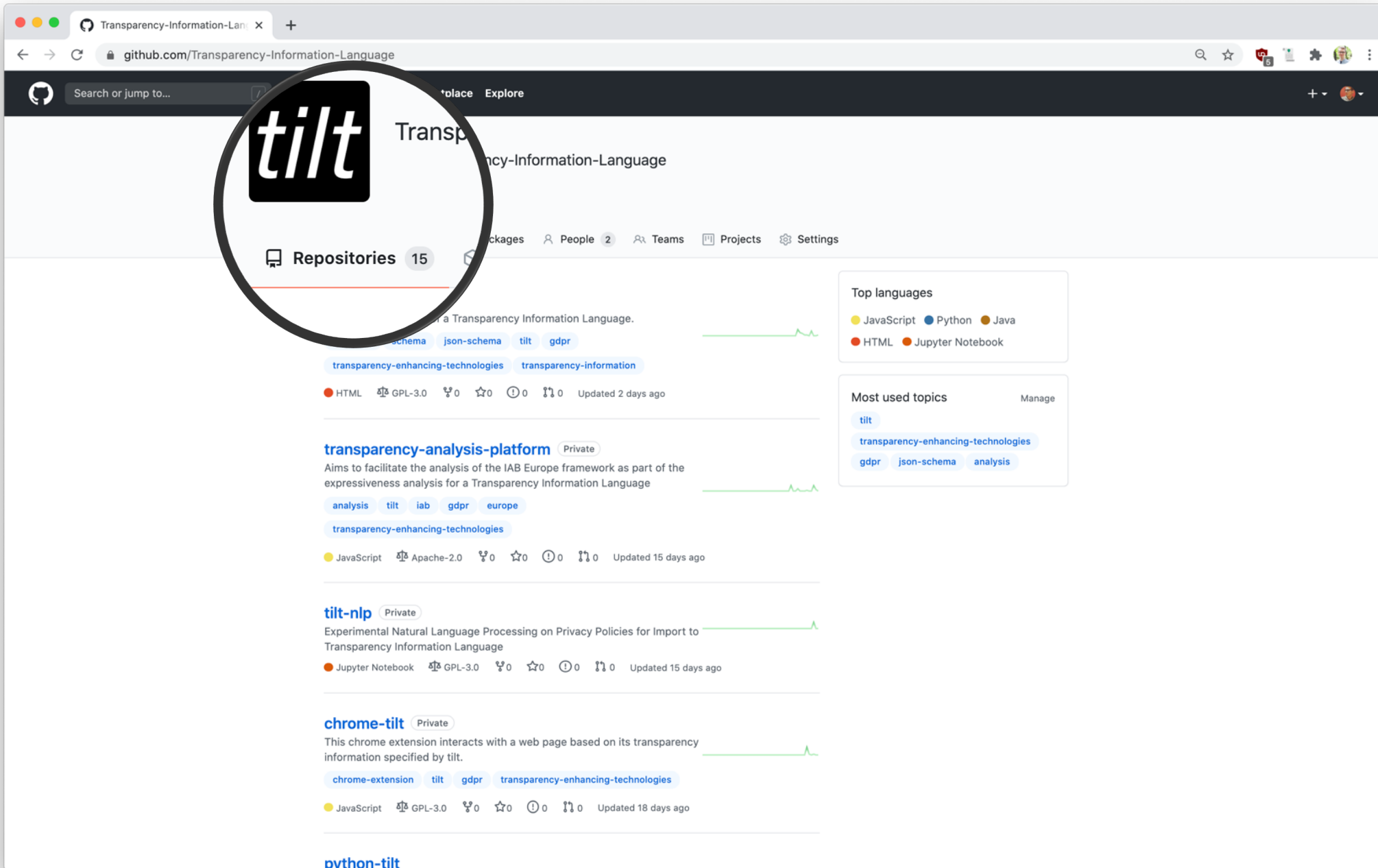
Datenschutz durch Technikgestaltung (PbD)

Folge: Verantwortliche müss(t)en* vergleichbare Technik nutzen,
da der Machbarkeitsbeweis erbracht wurde



Erwünschtes Ergebnis:

1. Iterative Verbesserungen + **Anwendungsfälle**
2. Adaption für **reale Szenarien**



Transparency-Information-Language

Repositories 15

Top languages

- JavaScript
- Python
- Java
- HTML
- Jupyter Notebook

Most used topics

- tilt
- transparency-enhancing-technologies
- gdpr
- json-schema
- analysis

transparency-analysis-platform (Private)

Aims to facilitate the analysis of the IAB Europe framework as part of the expressiveness analysis for a Transparency Information Language

analysis tilt iab gdpr europe

transparency-enhancing-technologies

JavaScript Apache-2.0 0 0 0 0 Updated 15 days ago

tilt-nlp (Private)

Experimental Natural Language Processing on Privacy Policies for Import to Transparency Information Language

Jupyter Notebook GPL-3.0 0 0 0 0 Updated 15 days ago

chrome-tilt (Private)

This chrome extension interacts with a web page based on its transparency information specified by tilt.

chrome-extension tilt gdpr transparency-enhancing-technologies

JavaScript GPL-3.0 0 0 0 0 Updated 18 days ago

python-tilt

<https://github.com/Transparency-Information-Language/>

TILT: A GDPR-Aligned Transparency Information Language and Toolkit for Practical Privacy Engineering

Elias Grünewald
Technische Universität Berlin
Information Systems Engineering Research Group
Berlin, Germany
gruenewald@tu-berlin.de

Frank Pallas
Technische Universität Berlin
Information Systems Engineering Research Group
Berlin, Germany
frank.pallas@tu-berlin.de

ABSTRACT

In this paper, we present TILT, a transparency information language and toolkit explicitly designed to represent and process transparency information in line with the requirements of the GDPR and allowing for a more automated and adaptive use of such information than established, legalese data protection policies do.

We provide a detailed analysis of transparency obligations from the GDPR to identify the expressiveness required for a formal transparency language intended to meet respective legal requirements. In addition, we identify a set of further, non-functional requirements that need to be met to foster practical adoption in real-world (web) information systems engineering. On this basis, we specify our formal language and present a respective, fully implemented toolkit around it. We then evaluate the practical applicability of our language and toolkit and demonstrate the additional prospects it unlocks through two different use cases: *a)* the inter-organizational analysis of personal data-related practices allowing, for instance, to uncover data sharing networks based on explicitly announced transparency information and *b)* the presentation of formally represented transparency information to users through novel, more comprehensible, and potentially adaptive user interfaces, heightening data subjects' actual informedness about data-related practices and, thus, their sovereignty.

Altogether, our transparency information language and toolkit allow – differently from previous work – to express transparency information in line with actual legal requirements and practices of modern (web) information systems engineering and thereby pave the way for a multitude of novel possibilities to heighten transparency and user sovereignty in practice.

CCS CONCEPTS

• Applied computing → Law; • Information systems → Information systems applications; Web data description languages; • Software and its engineering → Formal language definitions; Context specific languages; • Security and privacy → Privacy protections;

Permission to make digital or hard copies of part or all of this work for personal or classroom use is granted without fee provided that copies are not made or distributed for profit or commercial advantage and that copies bear this notice and the full citation on the first page. Copyrights for third-party components of this work must be honored. For all other uses, contact the owner/author(s).
FAccT '21, March 3–10, 2021, Virtual Event, Canada
© 2021 Copyright held by the owner/author(s).
ACM ISBN 978-1-4503-8309-7/21/03.
<https://doi.org/10.1145/3442188.3445925>

KEYWORDS

Data transparency, GDPR, data protection, privacy, privacy by design, legal tech, privacy engineering, web privacy, privacy law

ACM Reference Format:

Elias Grünewald and Frank Pallas. 2021. TILT: A GDPR-Aligned Transparency Information Language and Toolkit for Practical Privacy Engineering. In *Conference on Fairness, Accountability, and Transparency (FAccT '21)*, March 3–10, 2021, Virtual Event, Canada. ACM, New York, NY, USA, 12 pages. <https://doi.org/10.1145/3442188.3445925>

1 INTRODUCTION

Transparency has been a core principle in philosophical, legal, and technical deliberations around privacy¹ for decades. This particularly applies to data privacy in everyday digital life: To be able to act in a sovereign and self-determined way and actually make *informed* choices, individuals need to have sufficient knowledge about the actual facts and givens regarding the processing of personal data, including, e.g., which party collects what personal data for which purposes, how long this data is (going to be) stored, et cetera. Data protection laws and regulations around the world – such as the European General Data Protection Regulation (GDPR) [8] or the California Consumer Privacy Act (CCPA) [38] – therefore explicitly include transparency rules for data processing parties, obligating them to reveal respective information to the data subjects.

These obligations are today typically fulfilled through respective transparency parts of written privacy policies. Such privacy policies do, however, exhibit several shortcomings that severely limit their actual reception and comprehension on the side of data subjects: First of all, privacy policies are often long, complex, and written in legalese language, making it hard for data subjects to locate transparency-related information and actually understand them correctly [25, 35]. Second, different privacy policies employ different logical structures and vocabularies for factually similar statements, causing significant reading and decoding efforts for every new policy to be understood [26]. Such practice structurally discriminates people who are less privacy-literate [39]. Finally, data transfers towards other parties are now a broadly established practice. Data subjects wanting to see “the whole picture” in such contexts therefore have to read and understand multiple policies and establish the logical interdependencies between them themselves.

Together with the ever-increasing number of services used (and, thus, of privacy policies to be read), this leads to a state where privacy policies, including respective transparency statements, are not read anymore before using a particular service and/or consenting to

¹Being well aware of the slightly different notions between “Privacy” and “Data Protection”, we use these terms interchangeably herein.



Digital Autonomy Hub Tutorial

Neue technische Wege zur Erfüllung datenschutzrechtlicher Transparenzpflichten

Elias Grünewald

Dr.-Ing. Frank Pallas



eg@ise.tu-berlin.de

fp@ise.tu-berlin.de



@eliasgruenewald

@sallapf

DaSKITA

daskita.github.io

Interaktiver Teil

1

`pip3 install tilt`

2

`touch app.py`

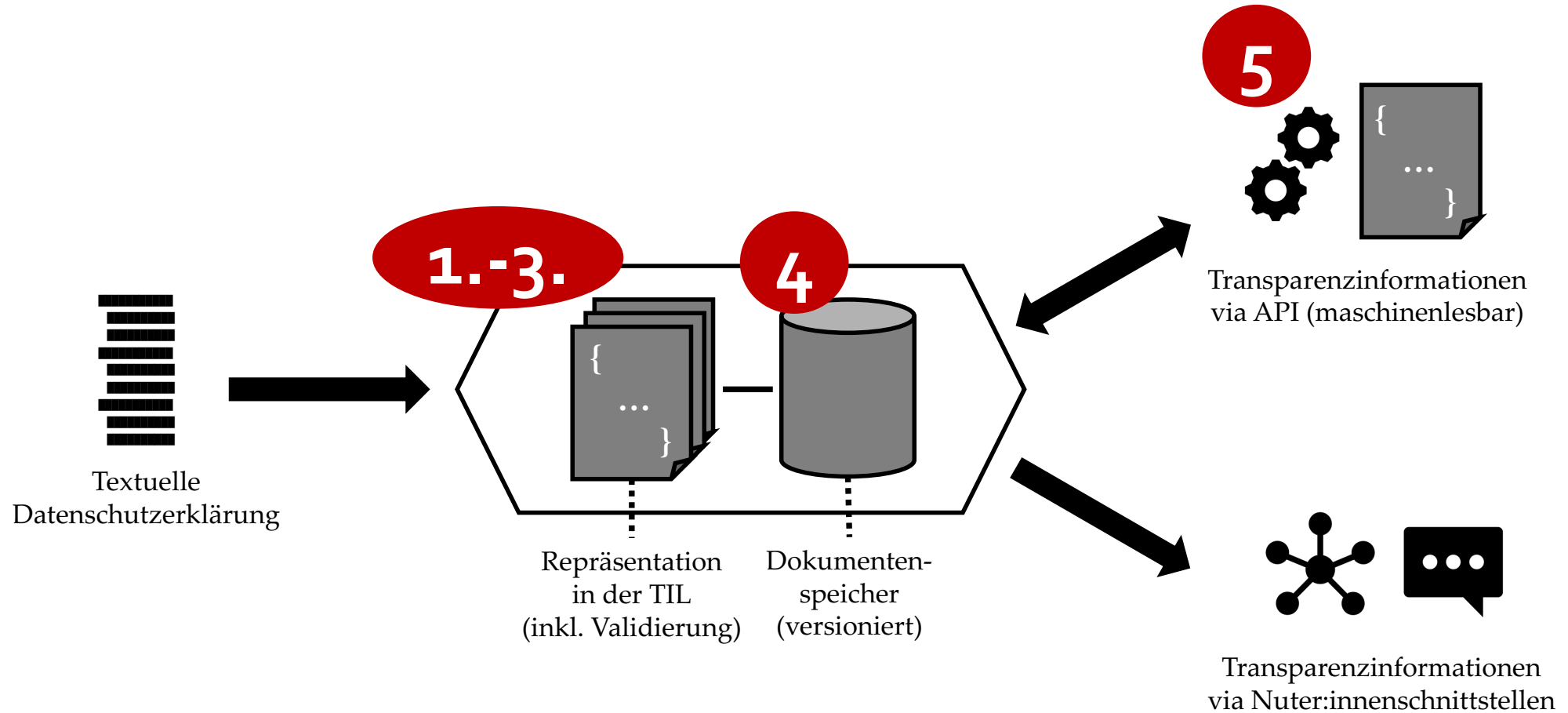
3

<https://github.com/Transparency-Information-Language/python-tilt>
<https://t1p.de/TIL> (Short-Link)

Basic usage

See here for an interactive playground  launch , in which you can run

1. Import the transparency information language binding/library.
2. Create your first object, e.g. a Data Protection Officer with their contact information.



Digital Autonomy Hub Tutorial

Neue technische Wege zur Erfüllung datenschutzrechtlicher Transparenzpflichten

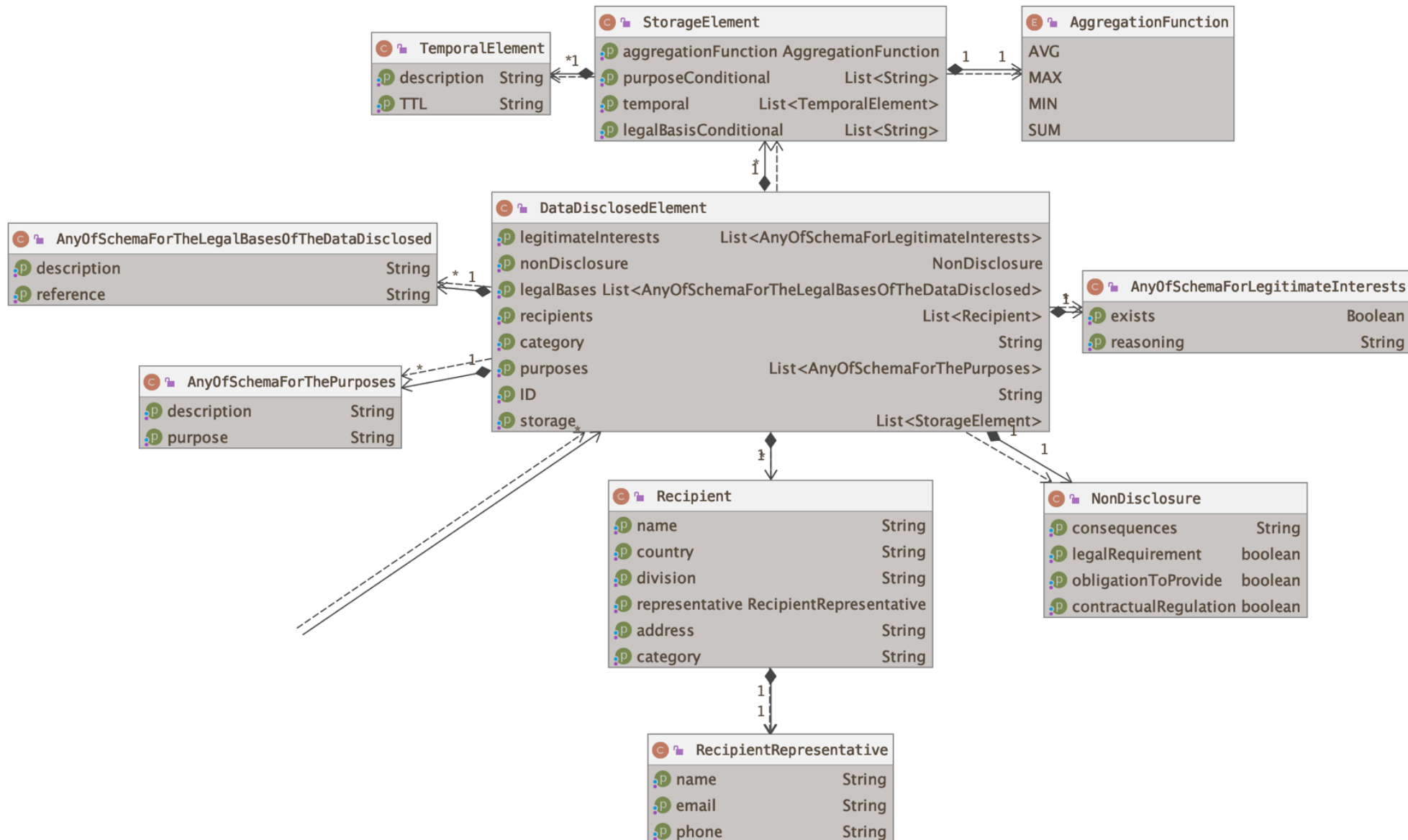


Digital
Autonomy Hub

DaSKITA

Addendum





Vocabularies

```

{
  "$schema" : "http://json-schema.org/draft-07/schema#",
  "type" : "object",
  "properties" : { "purpose" : { "$ref":"#/definitions/purpose" } },
5  "required" : [ "purpose" ],
  "definitions" : {
    "purpose" : {
      "type" : "string",
      "allOf" : [
10      {
        "anyOf" : [
          { "const": "Apple" },
          { "enum" : [ "Cat", "Dog" ] }
        ]
      },
15      {
        "not" : {
          "enum" : [ "Earth", "Water", "Air", "Fire" ]
        }
      }
    ]
  }
}

```

1. Research / Marketing / ...
2. Clinical research / Advertising / ...
3. COVID19 research / Targeted advertising / ...
4. Polymerase chain reaction testing / Mouse movement tracking / ...

Storage

```

▼ "storage": [
  ▼ {
    ▼ "temporal": [
      ▼ {
        "description": "Creating backups.",
        "ttl": "P3Y6M4DT12H30M5S"
      },
      ▼ {
        "description": "Finishing ordering process.",
        "ttl": "2020-08-09T18:31:42P3Y6M4DT12H30M17S"
      }
    ],
    ▼ "purposeConditional": [
      "Data is stored until the end of the ordering process."
    ],
    ▼ "legalBasisConditional": [
      "SGB-100-42"
    ],
    "aggregationFunction": "max"
  }
],

```

tilt schema

```

268     "required": [
269         "_id",
270         "name",
271         "created",
272         "modified",
273         "version",
274         "language",
275         "status",
276         "url",
277         "_hash"
278     ],
279     "additionalProperties": true,
280     "properties": {
281         "_id": {
282             "$id": "#/properties/meta/properties/_id",
283             "type": "string",
284             "title": "_id",
285             "description": "The ID follows the database-specific implementation and does not have to be set in advance; but should offer as much entropy as possible",
286             "examples": [
287                 "f1424f86-ca0f-4f0c-9438-43cc00509931"
288             ]
289         },
290         "name": {
291             "$id": "#/properties/meta/properties/name",
292             "type": "string",
293             "title": "Name",
294             "description": "Name of the data controller.",
295             "examples": [
296                 "Green Company"
297             ]
298         },
299         "created": {
300             "$id": "#/properties/meta/properties/created",
301             "type": "string",
302             "title": "Created",
303             "description": "Creation date of the document as an ISO-8601 time code.",
304             "pattern": "^(\\+|\\-)?\\d{4}(?!\\d{2}\\b)((-)?((0[1-9]|1[0-2])(\\3{12}\\d|0[1-9]|3[01]))?|W([0-4]\\d|5[0-2])(-?[1-7])?|(00[1-9]|0[1-9]\\d|[12]\\d{2}
305             "examples": [
306                 "2020-04-03T15:53:05.929588"
307             ]
308         },

```

<https://github.com/Transparency-Information-Language/schema/blob/master/tilt-schema.json>

Deployment models

D1 Internal deployment for a single data controller.

D2 Internal deployment w/ external access.

D3 Deployment at DPO's site

D4 Public transparency platform

