# Consistency checking of legal norms using LegalRuleML

## A case study on the consistency between GDPR and BDSG-E

Chun Tian

Scuola di Scienze, Università di Bologna
chun.tian@studio.unibo.it
Numero di matricola: 0000735539

**Abstract.** The consistency checking problem between two legal norms in which a child norm tried to adopt the parent norm, can be reduced to a series of small legal reasoning problems, with help of OASIS LegalRuleML, determined in defeasible reasoning engines. In this paper, we discuss the related theories and practices, and do a case study between European Union General Data Protection Regulation and its adoption in Germany, the draft Federal Data Protection Act (BDSG-E).

## 1 Introduction

Modern legal systems in any country or region usually consist of multiple legal norms regulating the same area. The most common example is the relationship between the constitution and other codes, in which a fundamental requirement for the latter is to not violate anything regulated in the constitution. Unite States of America (USA) is a federal republic composed of 50 states, each member states has their own legal subsystem, which is further under control of federal laws and U. S. constitution. European Union, on the other side, has also its united legal system: there're regulations and directives submitted by the European Parliament and the Council, and each Member States (Italy, Germany, etc.) must either directly obey or adopt them into their own legal systems. It's natural to ask if there's a convincing way to know (and fix) the potential consistencies between two legal norms which one adopts another, before they actually enforce. Any satisfied solution to this important problem could save huge time and legal resources in daily life.

The initial goal of the current exam project was to check the consistency between the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) [1], and a draft law (BDSG-E [2]) submitted by the German Federal Government in February 2017 for adapting the GDPR in Germany. Beside the Wikipedia page of GDPR, no other information including referenced papers was given, but the overall methodology is to have these laws rewritten in RuleML (or LegalRuleML) first, and then use whatever techniques from Computer Science to finish the task. The resulting work could be useful for checking the consistencies between GDPR and related laws submitted by other EU member states (e.g. Italy) in short future, and provide experiences to academic for generally checking the consistencies between any two legal norms in which one tries to adopt the other.

Unfortunately, as we'll see in the rest of this paper, such a complex task requires deep knowledges from both Computer Science and Legal Science, and the potential huge amount of work for manually (or semi-automatically) rewriting any complete legal norm into machine-readable formats is infeasible in scope of a course project which should be finished in a short time (e.g. one month) by a small group (less than 4 students) or single person. Thus, in short words *the given task is not completed*. However, in this paper, the author tried his best to explore all relevant materials (software, legal books, Internet blogs, academic papers) related to this task and have made a stage progress in combining several *state-of-art* technologies to provide a partial answer to the initial consistency question and have proposed a feasible path to a complete answer. We believe that, the *combination* itself, including the software and technologies involved in this project is creative

and unique insofar as the author can see.[1] At least the bibliography collection in this paper shall be useful for later scholars who are willing to attack the same problem.

## 2 Background and related work

In normal monotonic formal systems, e.g. Proposition Logic and first-order predicate logic, the concept 'consistency' can be defined in the following way [3]:

**Definition 1.** *A set $\Gamma$ of propositions is* consistent *if $\Gamma \nvdash \bot$. (and we call $\Gamma$* inconsistent *if $\Gamma \vdash \bot$)*

In words: one cannot derive a contradiction from $\Gamma$. The consistency of $\Gamma$ can be expressed in various other forms:

**Lemma 1.** *The following three conditions are equivalent:*

*(i)* *$\Gamma$ is consistent,*
*(ii)* *For no $\phi$, $\Gamma \vdash \phi$ and $\Gamma \vdash \neg\phi$,*
*(iii)* *There is at least one $\phi$ such that $\Gamma \nvdash \phi$.*

RuleML is nothing but a XML-based interchange format for representing rules, which can be roughly seen as a simple form of propositions in the underlying formal systems, so the problems of 'consistency checking of RuleML' is actually the consistency checking of underlying formal systems, in which the word 'consistency' has various different meanings (but share the same characteristic as above definition for propositional logic). And the work is usually done by transform RuleML into the statements in the underlying formal system in native formats, and then either use specially designed algorithms to finish the task, or the underlying rule engine may already provide a way to check the rule consistency.

The reasoning of legal rules, on the other side, is generally defeasible [4] in the sense that, a previously derivable conclusion may be later retracted when additional information were available. What philosophers call 'defeasible reasoning' is roughly the same as non-monotonic reasoning in AI. In other words, if legal rules can be transform into propositions in any kind of logic system, that logic system must be non-monotonic, otherwise it would be easily inconsistent and then any proposition, no matter truth or false, will be derivable. The concept of 'consistency' In defeasible reasoning must be weakened to *deductively consistency*, and a set of propositions is deductively consistent if and only if it does not have an explicit contradiction as a deductive consequence. In another words, Two propositions (or beliefs) $p$ and $\neq p$ may be both derivable, but their 'weight' or 'strength' must be different, so that one of the two conflicting conclusions can be finally chosen as the final conclusion.

This may sound arbitrary but actually reasonable and common. In legal norms, it's quite common that one article asserts that certain behavior is legal in general, while another article says it's illegal under particular conditions. Now under one of these particular conditions we got two applicable articles with completely different conclusion. Here the conflicts can be easily resolved by the implicit principle of specificity in legal norms: norms talking about particular cases in general has high priorities than articles regulating general cases. Sometimes such a specificity cannot be decided from the coverage of each norms, than other principles should be considered, e.g. later appeared norms usually have higher priority. This is how people actually interpret laws and also how people who wrote the law think it will be interpreted.

Here, again, the representation form of legal norms is essentially irrelevant. LegalRuleML, or any other similar format, as long as they include all necessary information for legal reasoning, can be used equally, because the first stage of any consistency checking task is to abandon the XML format and transform the contents into other native formats supported by the underlying reasoner (unless they natively supports some XML-based formats, but it's still hard to believe that any practical reasoner can use XML internally as primitive data structures). For general

[1] Actually the author sees this project as a great opportunity to learn and use the related software and underlying technologies in this project. It's an intention for the author to choose the most general framework among several candidates, so that the resulting learnt skills could be later applied to other research topics falling outside of legal domain.

concepts and framework of legal reasoning, our knowledge mainly comes from [5]. The only paper we found, related to legal reasoning in LegalRuleML is [6], in which the authors use XSLT to translate LegalRuleML documents into the native formats of a underlying defeasible reasoner called SPINdle (created by the same author in 2009).

The consistency between two legal norms (and the related consistency checking problem), surprisingly, is yet another different problem. And so far we didn't find any published papers in this area (with or without LegalRuleML). To understand this problem we had to consider some examples. GDPR and BDSG-E are two laws in which one adopts the other, before we formally introduce them in later sections of this paper, it's possible to use them to understand the core task that we're facing.

GDPR is an European Union regulation (or simply a 'law') that all member states must obey. One of the primary objectives of the GDPR is to simplify the regulatory environment for international business by unifying the regulation within the EU. That is to say, if certain data processing activities of an agent (individual, public authority, international organization or company, etc.), are *conclusively legal* according to GDPR, such activities should be automatically legal in all EU member states. And only in case any activity is unspecified in GDPR, or is defeasible due to the "open clauses" in related articles which has left flexibility to member states, the agent must also refer to member state laws (e.g. BDSG-E if it's in Germany) to get a more clear vision. This make perfect senses, as the following proposition:

**Proposition 1.** *An EU regulation is* consistent (in a member state) *if all its conclusions are not retracted by its adoptions in that member state, unless the regulation clearly states that it's defeasible.*

Such a requirement seems enough. If one actually looks into BDSG-E, he may pointed out that, since many articles of GDPR are explicitly mentioned, is it possible to just include those articles into BDSG-E as extra rules and the consistency checking between two legal norms now becomes the the consistency checking inside one legal norm? We think the answer is *no*: although such an extended version of BDSG-E is internally consistent, in the sense that any activity can be uniquely decided as legal or not (assume that anything unspecified is by default legal), but we still don't know if any legal activity according to this extended version of BDSG-E has violated GDPR, simply because not all contents of GDPR are included and considered. This lead to the next additional proposition:

**Proposition 2.** *Any conclusion made by a member state law, should be doubly checked in related EU regulations, and the member state law is* consistent (within EU) *only when the EU regulation makes the same conclusion or no conclusion.*

With these ideas in mind, now we proceed with our little research in LegalRuleML, Legal Reasoning (theory in Legal Science and Computer Science, tools in Computer Science) and the contents of two actual laws: GDPR and BDSG-E.

## 3 GDPR and BDSG-E

In this section we formally introduce the two legislations that we're going to look into deeply in the rest of this paper.

### 3.1 GDPR

According to the Wikipedia [1], "the General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a regulation by which the European Parliament, the Council of the European Union and the European Commission intend to strengthen and unify data protection for all individuals within the European Union (EU). It also addresses the export of personal data outside the EU. The primary objectives of the GDPR are to give control back to citizens and residents over their personal data and to simplify the regulatory environment for international business by unifying the regulation within the EU."

The regulation was adopted on 27 April 2016. It becomes enforceable from 25 May 2018 after a two-year transition period and, unlike a directive, it does not require any enabling legislation to be passed by national governments and is thus directly binding and applicable.

Regulation (EU) 2016/679 is available on Internet as part of the Official Journal L 119 of the European Union [7], published on May 4, 2016. It's available in 24 different languages and two formats (PDF and XHTML). The whole Official Journal L 119 actually contains one regulation (2016/679) and two directives (2016/680 and 2016/681), with the following full titles:

- Regulation (EU) 2016/679 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation);
- Directive (EU) 2016/680 of the European Parliament and of the Council of 27 April 2016 on the protection of natural persons with regard to the processing of personal data by *competent authorities* for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, and on the free movement of such data, and repealing Council Framework Decision 2008/977/JHA;
- Directive (EU) 2016/681 of the European Parliament and of the Council of 27 April 2016 on *the use of passenger name record (PNR) data* for the prevention, detection, investigation and prosecution of terrorist offences and serious crime.

There're a few things that must be noticed first:

1. On the differences between "regulations" and "directives", according to Wikipedia:
   - "A *regulation* is a legal act of the European Union that becomes immediately enforceable as law in all member states simultaneously. Regulations can be distinguished from *directives* which, at least in principle, need to be transposed into national law." [8]
   - "A *directive* is a legal act of the European Union which requires member states to achieve a particular result without dictating the means of achieving that result. It can be distinguished from *regulations* which are self-executing and do not require any implementing measures. Directives normally leave member states with a certain amount of leeway as to the exact rules to be adopted." [9]

   Both regulations and directives "can be adopted by means of a variety of legislative procedures depending on their subject matter." Thus, on the "consistencies" between European Union laws and member state laws, there's little to check on "directives", because by definition it's impossible for any behavior (of individuals or enterprises) to violate an EU directive which is essentially not enforced by itself.
2. It is indeed possible that a member state law transposed from an EU directive, may not be consistent with the original directive. But such a "consistency" has a different meaning as what we're going to study in this project. By actually looking into a directive (e.g. Directive (EU) 2016/680), we found that most articles have forms like "Member States shall provide for ..." associated with a situation. It seems that a member state law can only be inconsistent by regulate something not covered by all situations mentioned in the original EU directive, that is to say, the member state law must be talking about something completely different. But this is quite impossible to happen.
3. Among these 2 legal norms, only Regulation (EU) 2016/679 concerns about the behavior of normal legal agents (individuals, enterprises and international organisations, etc.), which is mostly interesting for us. For the other two directives, Directive (EU) 2016/680 concerns about behavior of "competent authorities" [2], and Directive (EU) 2016/681 concerns on a special kind of personal data, passenger name record (PNR) data, a very narrow area of little interests for us.

[2] Here 'competent authority' means: (a) any public authority competent for the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security; or (b) any other body or entity entrusted by Member State law to exercise public authority and public powers for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the execution of criminal penalties, including the safeguarding against and the prevention of threats to public security. [7]

Therefore, in this project, our research scope is limited in the consistency checking between Regulation (EU) 2016/679 and corresponding member state laws adopting it (as we will see, the Germany BDSG-E actually adopts all three parts of L 119). And when we refer to GDPR, it has the strict sense as the "regulation" part.

It's also worth noting that, GDPR is not created fully from the ground. It's actually based on the old Data Protection Directive [10] (officially Directive 95/46/EC on the protection of individuals with regard to the processing of personal data and on the free movement of such data), a European Union directive adopted in 1995 which regulates the processing of personal data within the European Union. Then on 25 January 2012, the European Commission (EC) announced it would attempt to unify data protection law across a unified European Union via proposed legislation called the "General Data Protection Regulation." It may be interesting to be noticed that, GDPR supersedes the old Data Protection Directive at not only the underlying legal contents, but also achieved a better legal rigor. As a proof, we have found in the book [5] of Giovanni Sartor some discussions on the difficulties when checking rule specificity in Directive 95/46/EC:

In legal reasoning, the so-called "specificity-based priority" is based on "the idea that more specific rules prevail over more general ones, according to the traditional saying that *lex specialis derogat legi generali* (a special law prevails over a general one). This way of reasoning is very frequently adopted in common-sense reasoning both in practical and in epistemic domains. This seems to correspond to a rational reasoning-pattern: If we know that something normally holds for a certain set of entities, but that something incompatible holds for a subset of such entities (which includes the case we are interested in), we had better focus on the features of the subset. Notwithstanding the ubiquity of the idea of specificity, it is very difficult to exactly characterise what it means for a rule to be more specific than another rule. For our purposes it is sufficient to remark that usually the test for specificity consists in checking whether the precondition of one rule entails the precondition of the other rule.

"This means that for rule [if $A1$ then $B1$] to be more specific than rule [if $A2$ then $B2$] it must be that both of the following conditions obtain:

- in every case where $A1$ is satisfied also $A2$ is, and
- there is some case where $A2$ is satisfied and $A1$ is not.

"There are a number of technical problems which are linked to performing a specificity check, but what we need to stress here is that when lawyers speak of specificity they are referring to a broader (and vaguer) concept, which is not limited to what emerges from a syntactically defined specificity-check. In particular, it seems that in some cases one needs to selectively identify—within the preconditions of the competing rules—what elements to focus on, for establishing specificity.

"Consider, for example art. 7 and 8 or the European Data Protection directive:

> Directive 95/46/EC, Art. 7 [P]ersonal data may be processed [...] if:
> a. the data subject has unambiguously given his consent; or
> b. processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract; or
> c. processing is necessary for compliance with a legal obligation to which the controller is subject; or
> d. processing is necessary in order to protect the vital interests of the data subject; or
> e. processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller or in the interest of a third party to whom the data are disclosed; or
> f. processing is necessary for the purposes of the legitimate interests pursued by the controller or by the third party or parties to whom the data are disclosed, except where such interests are overridden by the interests for fundamental rights and freedoms of the data subject which require protection under Art. 1 (1).
>
> Directive 95/46/EC, Art. 8
> 1. [It is prohibited] the processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life.

"When sensitive data (the types of data listed in Art. 8) are processed under the conditions listed in Art. 7, a conflict seems to arise: According to Art. 7 the data may be processed, while according to Art. 8 the data should not be processed.[3] It may seem that the solution is provided by specificity: specificity should favour Art. 8 over Art. 7 since the concept of sensitive personal data is certainly more specific that the concept of personal data in general (sensitive personal data are always personal data, while personal data may not be sensitive). Unfortunately this is not the case. Art. 7 makes the permission to process personal data dependent upon specific conditions (such as the fact that the data subject has consented) that do not necessarily hold for all sensitive data as specified in Art. 8: Sensitive personal data do not always fall under one of the conditions listed in Art. 8, and thus Art. 8 is not syntactically more specific than Art. 7."

It seems that, all such legal reasoning difficulties have been identified and fixed in the new GDPR. Above two articles 7 and 8 in Directive 95/46/EC correspond to the Art. 6 (Lawfulness of processing) and Art. 9 (Processing of special categories of personal data) in GDPR. The Art. 6 of GDPR looks like a strict superset of Art. 7 of Directive 95/46/EC, which now becomes the first part of Art. 6 of GDPR:

GDPR, Art. 6 (Lawfulness of processing)

1. Processing shall be lawful only if and to the extent that at least one of the following applies:
   (a) the data subject has given consent to the processing of his or her personal data for one or more specific purposes;
   (b) processing is necessary for the performance of a contract to which the data subject is party or in order to take steps at the request of the data subject prior to entering into a contract;
   (c) processing is necessary for compliance with a legal obligation to which the controller is subject;
   (d) processing is necessary in order to protect the vital interests of the data subject or of another natural person;
   (e) processing is necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;
   (f) processing is necessary for the purposes of the legitimate interests pursued by the controller or by a third party, except where such interests are overridden by the interests or fundamental rights and freedoms of the data subject which require protection of personal data, in particular where the data subject is a child.

   Point (f) of the first subparagraph shall not apply to processing carried out by public authorities in the performance of their tasks.
2. Member States may maintain or introduce more specific provisions to adapt the application of the rules of this Regulation with regard to processing for compliance with points (c) and (e) of paragraph 1 by determining more precisely specific requirements for the processing and other measures to ensure lawful and fair processing including for other specific processing situations as provided for in Chapter IX.
3. The basis for the processing referred to in point (c) and (e) of paragraph 1 shall be laid down by:
   (a) Union law; or
   (b) Member State law to which the controller is subject.

   The purpose of the processing shall be determined in that legal basis or, as regards the processing referred to in point (e) of paragraph 1, shall be necessary for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller. That legal basis may contain specific provisions to adapt the application of rules of this Regulation, inter alia: the general conditions governing the lawfulness of processing by the controller; the types of data which are subject to the processing; the data subjects concerned; the entities to, and the purposes for which, the personal data may be disclosed; the purpose limitation; storage periods; and processing operations and processing procedures, including measures to ensure lawful and fair processing such as those for other specific processing situations as provided for in Chapter IX. The Union or the Member State law shall meet an objective of public interest and be proportionate to the legitimate aim pursued.
4. Where the processing for a purpose other than that for which the personal data have been collected is not based on the data subject's consent or on a Union or Member State law which

[3] Further provisions of the data-protection directive, which we cannot consider here, specify particular conditions under which even sensitive data can be legally processed.

constitutes a necessary and proportionate measure in a democratic society to safeguard the objectives referred to in Article 23(1), the controller shall, in order to ascertain whether processing for another purpose is compatible with the purpose for which the personal data are initially collected, take into account, inter alia:

(a) any link between the purposes for which the personal data have been collected and the purposes of the intended further processing;
(b) the context in which the personal data have been collected, in particular regarding the relationship between data subjects and the controller;
(c) the nature of the personal data, in particular whether special categories of personal data are processed, pursuant to Article 9, or whether personal data related to criminal convictions and offences are processed, pursuant to Article 10;
(d) the possible consequences of the intended further processing for data subjects;
(e) the existence of appropriate safeguards, which may include encryption or pseudonymisation.

while the new Art. 9 of GDPR now stands on its own, it has no specificity relationship with above article any more:

GDPR, Art. 9 (Processing of special categories of personal data)

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
   (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject; the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
   (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;
   (c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
   (d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
   (e) processing relates to personal data which are manifestly made public by the data subject;
   (f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
   (g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;

(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;

(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;

(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

We can imagine the potential difficulties and complexity when translating even the above single GDPR article into machine-readable formats like LegalRuleML, but the new GDPR, seems to be carefully designed for easier legal reasoning. Such a belief forms the basis of any potential achievements in the computer-based processing of GDPR.

### 3.2 BDSG-E

In February 2017, the German Federal Government submitted a draft law (BDSG-E)[4] for adapting the GDPR in Germany. The administration wants to push the draft quickly through the Federal Parliament. After a hearing of experts for data protection on the 27th of March, the final enacting is planned for April. The law will likely come into force in May 2017 without significant further changes.

Following the full title of BDSG-E:

> Entwurf eines Gesetzes zur Anpassung des Datenschutzrechts an die Verordnung (EU) 2016/679 und zur Umsetzung der Richtlinie (EU) 2016/680 (Datenschutz-Anpassungs- und -Umsetzungsgesetz EU — DSAnpUG-EU)

or in English:

> Draft Law on the adaptation of the Data Protection Act into line with Regulation (EU) 2016/679 and implementing Directive (EU) 2016/680 (EU Data Protection Policy and Implementation Act)

we can see that, BDSG-E concerns not only Regulation (EU) 2016/679 but also Directive (EU) 2016/680. As we have explained in previous section, in this project we'll focus on the consistency checking between Regulation (EU) 2016/679 and its adoptions in member states. Thus certain parts of BDSG-E is out of our current reasearch scopes.

[4] 'BDSG' stands for 'BundesDatenSchutzGesetz' (Federal Data Protection Act) in German language. The appending letter 'E' should be 'Entwurf' which means 'draft' in English.

The full text of BSDG-E in PDF is available as a download link inside an Internet news [2] about the submission of BSDG-E. We have made an English translation for the structure (i.e. the title of all sections and articles) of this law as appendix of this paper. The translation work was done by the author who has basic German language knowledge with help of Google Translate and an old version of SDL Trados Studio[5]. What we can learn immediately here is the four parts of which BDSG-E consists:

1. Common provisions;
2. Implementing provisions for processing for the purposes of § 2 of Regulation (EU) 2016/679;
3. Provisions for processing as referred to in § 1 (1) of Directive (EU) 2016/680;
4. Specific provisions for processing under activities not covered by the scope of application of Regulation (EU) 2016/679 and Directive (EU) 2016/680

We can imagine that, if there's any potential "conflicts" or "inconsistencies" (in whatever sense) between GDPR (the regulation part) and BDSG-E, it should be mainly in Part 2 and Part 4, and we can completely ignore Part 3. However, so far we haven't clarified the precise definition for the "consistency" between these two legal norms. For this important question, an Internet blog titled "Data Protection: Does the German Implementation Act (BDSG-E) undermine the GDPR?" [11] has given us important clues:

> "The aim of the government is to make use of certain opening clauses in the GDPR in order to retain some well proven provisions of the German Data Protection Act (BDSG). However, it is sometimes unclear whether a national provision is still covered by an opening clause or whether it may violate European Law. According to German media coverage, the European Commission is already pressing for a number of changes in the draft law. A high-ranked representative of the DG Justice is quoted, constituting that some changes in the draft law are not covered by the opening clauses, and blaming the Geman government for undermining the original goal of the GDPR, full harmonisation."

## 4 Methodology in this project

The discovery of [11] has lead the author to the following researching approach in this project:

1. Analyze the cases mentioned in and work out a precise definition of "consistency" between two legal noms;
2. Rewrite GDPR and BDSG-E articles related to these cases into LegalRuleML, as GDPR and BDSG-E fragments;
3. Evaluate possible reasoning engine which is capable for legal reasoning and choose one for use in this project;
4. Extend the chosen reasoning engine when necessary (in case it's not designed for legal reasoning);
5. Formalize the informal consistency definition and all related things in the chosen legal reasoning engine;
6. Use XSLT 2.0 to transform LegalRuleML representations of GDPR and BDSG-E fragments into valid statements in the legal reasoning engine;
7. Make sure the legal reasoning engine produce the same results as the informal consistency analysis.

This sounds already a huge plan with many uncertain factors, but is still far from a complete solution. But that's all we can do in the scope of current project. The path to the final answer of the initial question should at least consist of the following extra steps:

1. Make full translations of GDPR and BDSG-E into LegalRuleML;
2. Find a suitable formalizations for the consistency between two entire legal norms.
3. Transform LegalRuleML to a legal reasoning engine and produce the checking results.

[5] `http://www.sdl.com/software-and-services/translation-software/sdl-trados-studio/`

However, even the above first-stage plans have shown the following central ideas in the kind of legal research in Computer Science:

1. we assume the correctness of the existing opinions from legal experts and try to use Computer Science to verify and reproduce these opinions;
2. then we use the resulting tools established in previous step to assert more results not covered by existing legal experts;
3. the details of any machine-based reasoning and intermediate steps/results should be preserved for the examination by legal experts, since any simple yes/no result is not convincing at all.

## 5 LegalRuleML

LegalRuleML [12] is XML-base a legal rule interchange format proposed by OASIS, which extends RuleML with features specific to legal domain. It aims to bridge the gap between natural language descriptions and semantic norms, and can be used to model various laws, rules and regulations by translating the compliance requirements into a machine readable format.

LegalRuleML is built on top of RuleML (or more specifically, ConsumerRuleML [13]), and the objective of the LegalRuleML Technical Committee (TC) is to extend RuleML with formal features specific to legal norms, guidelines, policies and reasoning. That is, the TC defines a standard that is able to represent the particularities of the legal normative rules with a rich, articulated, and meaningful markup language. The features are:

- defeasibility of rules and defeasible logic;
- deontic operators (e.g., obligations, permissions, prohibitions, rights);
- semantic management of negation;
- temporal management of rules and temporality in rules;
- classification of norms (i.e., constitutive, prescriptive);
- jurisdiction of norms;
- isomorphism between rules and natural language normative provisions;
- identification of parts of the norms (e.g. bearer, conditions);
- authorial tracking of rules.

According to LegalRuleML's OASIS repository[6], it has three sub-standards: the basic, normalized and compact LegalRuleML formats. Such a design has led to a lot of confusions in practical uses. They're essentially different XML-based standards defined by different DTD or XML Schema files, while they also share a large set of common elements (but the same element may not have the same grammar rules in different LegalRuleML sub-formats). The normative variant contains some elements (`<has-*>`) which has single valid child element, and this has made their existences meaningless. The compact variant, on the other side, has adopted also the 'compact' variant of RuleML, which is essential a flat representation of rules in which the level of XML elements were slightly smaller. But we think such a design will finally lead to more complicated XSLT rules when actually translating LegalRuleML documents into logical clauses in an actual reasoner. So we wanted to adopt the 'basic' variant as the only LegalRuleML formats in the project, however, it's funny that there's no examples provided by LegalRuleML TC: the official examples were either normative or compact! Finally we have decided to support all three formats in the structural authoring environment (see next section for details) that we built in Adobe FrameMaker, while only the normative variant was extensively developed with text formatting rules carefully defined and maintained. And since we're not manually writing any low-level XML tags, the size or levels in the LegalRuleML documents seems irrelevant. As a result, all LegalRuleML code appears int this paper, are actually normative.

Currently there's little knowledge on representing any complete legal norm into LegalRuleML. It's not surprised, because academic publications usually concern on theory and tools, while large applications are supposed to be done in scope of legal engineering by legal domain experts. But even for small examples, there're very few publications in which such information can be obtained. Beside the "U.S. Code 504" example described in [12], the only relevant paper the author has found

[6] `https://tools.oasis-open.org/version-control/svn/legalruleml/trunk`

so far, is the sample representation of a small business contract in [6], which further came from [14].

Here we omit the general introduction of node elements defined in LegalRuleML, which the latest version can be found from OASIA web site [7], but before we actually represent our work in translating GDPR and BSDG-E fragments into LegalRuleML, we briefly discuss the general principles of representing legal norms into LegalRuleML, with same XML code from [12] and [6], in a bottom-up approach.

The fundamental differences between legal texts and other literature, is that the former are made by norms, which can be represented by rules with the form

$$\text{if } A_1, \ldots, A_n \text{ then } C$$

where $A_1, \ldots, A_n$ are the conditions (or premises) of the norm, $C$ is the conclusion of the norm. In LegalRuleML, such a norm can be represented by the derivation rules in RuleML, i.e. a `<ruleml:Rule>` node, which usually consists of a `<ruleml:if>` and a `<ruleml:then>` parts. Inside the conditions and conclusions, any logically meaningful sentences should be presented by predicate, i.e. a relation operator with several arguments, which are either variables or individuals. In RuleML, a predicate can be defined as a `<ruleml:Atom>` node. Variables are represented as `<ruleml:Var>` nodes, while individuals are represented as `<ruleml:Ind>` nodes. With help of logical connectors (`<ruleml:And>`, `<ruleml:Or>`, `<ruleml:Neg>`, ...), first-order logic quantifiers (`<ruleml:Forall>`, `<ruleml:Exists>`) and many other basic RuleML ingredients, it's not hard to imagine that any legal text should be representable.

The relation and individuals used in `<ruleml:Rule>` nodes are generally from an ontology used in the LegalRuleML document. With different choice of Ontology, the resulting LegalRuleML representations for the same legal norm may looks very different.[8]

However, there're two extensions to the contents of `<ruleml:Rule>` node for proper representation of legal contents:

1. In legal domain, a rule/norm can be *defeasible*, or have other properties. LegalRuleML uses `<lrml:hasStrength>` to declare special properties for a single rule.
2. Deontic operators, i.e. obligations, prohibitions, permission, etc., which can be used around the core predicates, are represented by special LegalRuleML nodes: `<lrml:Obligation>`, `<lrml:Prohibition>`, `<lrml:Permission>`, etc.

with these two extra features, the core IF-THEN rule in any legal norm is in theory representable. They are core building blocks for legal norms in LegalRuleML.

The next upper level are statements. Below are types of statements supported in LegalRuleML: (c.f. [6] for more details)

- Norm Statements (Constitutive Statements, Prescriptive Statements);
- Factual Statement;
- Override Statement;
- Violation-Reparation Statements (Reparation Statements, Penalty Statements).

Constitutive Statements, Prescriptive Statements represent constitutive rules and prescriptive rules in legal norms. Factual Statement is a special case of norm statements without specification of premises. Override statements are used to handle defeasibility. Finally, a Violation-Reparation Statement is the type of statement concerning what actions are required when an obligation is violated.

Going to upper level, a rule (or a set of rules) may have further properties which can not be expressed inside the rules, such as the temporal characteristics, modality, authority, jurisdiction, etc. LegalRuleML introduce higher level constructions like `<lrml:Context>` which permits the description of all the characteristics that are linked to a particular rule.

[7] `http://docs.oasis-open.org/legalruleml/legalruleml-core-spec/v1.0/csprd01/legalruleml-core-spec-v1.0-csprd01.html`

[8] This means we can't simply translate *all* contents of GDPR into LegalRuleML first (no matter how long it is) and then expect to find a reasoning software to handle the resulting machine-readable XML documents, because we don't know at what fine level and use what set of ontology to make the reasoning feasible.

### 5.1 Structural Authoring of LegalRuleML

So far the only structural authoring tool for LegalRuleML is the RAWE online editor [15] which is not accessible to us. But we think that, a offline, free, desktop-based authoring environment for LegalRuleML shall be useful for legal authoring purposes. In this project, we have developed such an authoring environment based on Adobe FrameMaker [9]. It's free in the sense that we're releasing all code into public, but it's still a cost to retrieve Adobe FrameMaker as a commercial software. We have built our structural application [10] in FrameMaker 2015 but in theory we can provide installation files in FrameMaker versions ranged from 10 to 2015.

Adobe FrameMaker supports XML-based structural authoring, which is highly customizable by structural application developers. In FrameMaker, a structural application consists of a document template, an element definition document (EDD) file and optional read/write rules and XSLT transformers, advanced applications can even have C-based plugins handling arbitrary tasks. FrameMaker is unique in this area, as it's in theory possible for supporting the structural authoring of any XML-based format. Below is a screenshot when editing a LegalRuleML document:

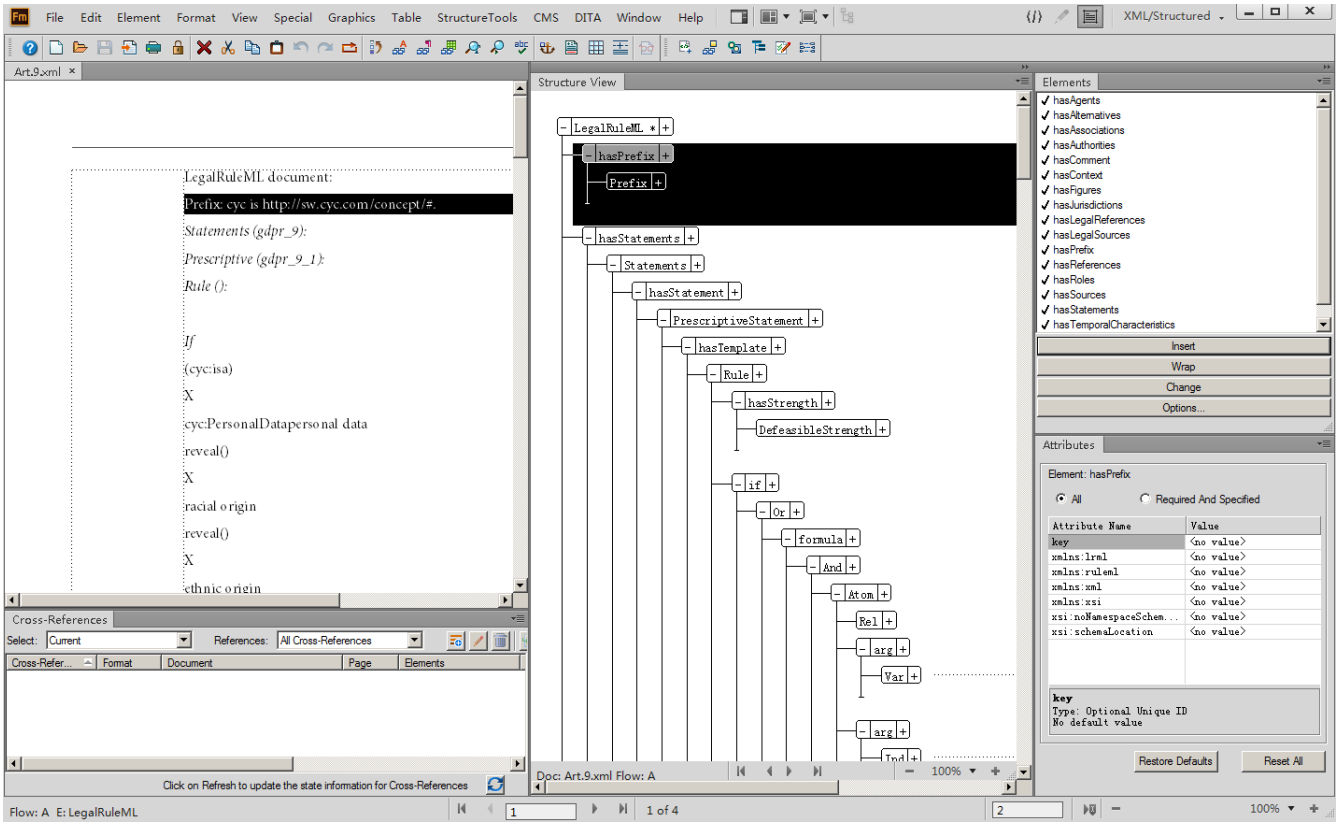


**Fig. 1.** default

We have made efforts to convert LegalRuleML `key` and `keyref` attributes into native FrameMaker cross-reference tags. To achieve this goal, we have used pre- and post-processing XSLs to process the LegalRuleML documents, here is the current version of the preprocessing XSL sheet:

```
<?xml version="1.0" encoding="UTF-8"?>
<xsl:stylesheet xmlns:xsl="http://www.w3.org/1999/XSL/Transform"
    xmlns:xs="http://www.w3.org/2001/XMLSchema"
    exclude-result-prefixes="xs"
    version="2.0">
    <xsl:output method="xml" version="1.0" encoding="UTF-8" indent="yes" />
```

[9] `http://www.adobe.com/products/framemaker.html`

[10] `https://github.com/binghe/fm-legalruleml`

```
    <xsl:preserve-space elements="*"/>

    <xsl:template match="@*|node()">
        <xsl:copy>
            <xsl:apply-templates select="@*|node()" />
        </xsl:copy>
    </xsl:template>

    <xsl:template match="@keyref">
        <xsl:attribute name="keyref">
            <xsl:analyze-string select="." regex="^#(.+)$">
                <xsl:matching-substring>
                    <xsl:value-of select="regex-group(1)" />
                </xsl:matching-substring>
                <xsl:non-matching-substring>
                    <xsl:value-of select="." />
                </xsl:non-matching-substring>
            </xsl:analyze-string>
        </xsl:attribute>
    </xsl:template>

    <xsl:template match="@hasCreationDate">
        <xsl:attribute name="hasCreationDate">
            <xsl:analyze-string select="." regex="^#(.+)$">
                <xsl:matching-substring>
                    <xsl:value-of select="regex-group(1)" />
                </xsl:matching-substring>
                <xsl:non-matching-substring>
                    <xsl:value-of select="." />
                </xsl:non-matching-substring>
            </xsl:analyze-string>
        </xsl:attribute>
    </xsl:template>

    <xsl:template match="@under">
        <xsl:attribute name="under">
            <xsl:analyze-string select="." regex="^#(.+)$">
                <xsl:matching-substring>
                    <xsl:value-of select="regex-group(1)" />
                </xsl:matching-substring>
            </xsl:analyze-string>
        </xsl:attribute>
    </xsl:template>

    <xsl:template match="@over">
        <xsl:attribute name="over">
            <xsl:analyze-string select="." regex="^#(.+)$">
                <xsl:matching-substring>
                    <xsl:value-of select="regex-group(1)" />
                </xsl:matching-substring>
            </xsl:analyze-string>
        </xsl:attribute>
    </xsl:template>
</xsl:stylesheet>
```

Currently we did't make special efforts on the natural language representations of LegalRuleML in the main editing area. What we have right now is the following benefits:

1. Grammar checking and XML validations;
2. There's no need to member LegalRuleML elements and attributes as they're selectable from a list;
3. Automatic insertion of elements in certain cases.
4. Automatic tracking of cross-references.

### 5.2 Problems of LegalRuleML

LegalRuleML lacks the support for legal document fragments. Unlike other well-designed XML-based document formats (e.g. DITA), a LegalRuleML document cannot include any pointer to other LegalRuleML documents. This is mainly because the node `<lrml:LegalRuleML>` is the only valid root element which contains everything else. Consider a huge LegalRuleML document representing all contents of GDPR, which consists of 99 articles. Such a XML document could have at least 10,000 lines, given the complexity of each single articles. Legal engineers may want to divide each single article into separated XML files, but current LegalRuleML specification has no support on cross-references from external files.

However, using our structural application, it's possible to combine large LegalRuleML document from related small fragments, because we have loosed the possible root elements. Here is the basic approach:

1. Put each article into separated document in FrameMaker native format (`*.fm`) with first-level child elements of `<lrml:LegalRuleML>` as root elements;
2. Create a root document in FrameMaker native format with `<lrml:LegalRuleML>` as root element, then use FrameMaker's text insert facility to include each article document into the root document.

3. Export the root document into XML format as the final interchangeable LegalRuleML document.

We propose the LegalRuleML TC should consider adding supports for referencing external document. For example, the `keyref` should have a general syntax `file#key`, in which `file` is another LegalRuleML document containing a node with `key` as the key.

## 6 Ontology

LegalRuleML is independent from any legal ontology and logic framework. In this project, all vocabularies as ontology entries were based on Cyc ontology [16]. As a direct result, all arithmetic functions that RuleML didn't define as part of its syntax, now has their names from Cyc ontology. Below is a short list:

- `(isa LogFn ArithmeticFunctions-Math-Topic)`
- `(isa SquaredFn ArithmeticFunctions-Math-Topic)`
- `(isa DifferenceFn ArithmeticFunctions-Math-Topic)`
- `(isa AbsoluteValueFn ArithmeticFunctions-Math-Topic)`
- `(isa SuccessorFn ArithmeticFunctions-Math-Topic)`
- `(isa TimesFn ArithmeticFunctions-Math-Topic)`
- `(isa MinusFn ArithmeticFunctions-Math-Topic)`
- `(isa MathematicalFunctionOnScalars ArithmeticFunctions-Math-Topic)`
- `(isa PlusAll ArithmeticFunctions-Math-Topic)`
- `(isa QuotientFn ArithmeticFunctions-Math-Topic)`
- `(isa ReciprocalFn ArithmeticFunctions-Math-Topic)`
- `(isa inverseQuantFunctions-Nonsymmetric ArithmeticFunctions-Math-Topic)`
- `(isa Minimum ArithmeticFunctions-Math-Topic)`
- `(isa SquareRootFn ArithmeticFunctions-Math-Topic)`
- `(isa ExpFn ArithmeticFunctions-Math-Topic)`
- `(isa PlusFn ArithmeticFunctions-Math-Topic)`
- `(isa Maximum ArithmeticFunctions-Math-Topic)`

To use Cyc entries in LegalRuleML documents, it's enough to declare a `lrml:hasPrefix` entry at the beginning of the XML document:

```
1  <lrml:hasPrefix>
2        <lrml:Prefix pre="cyc" refID="http://sw.cyc.com/concept/#"/>
3  </lrml:hasPrefix>
```

## 7 Legal Reasoning tools

The reasoning and consistency checking of RuleML are usually based on the translations of rules into formulae of propositional or first order logic. LegalRuleML, however, in general cannot be translated into these monotonic logic, because legal rules can be defeasible.

We have reviewed several defeasible reasoning implementations [17] (as in Table 1). Not all software in the list is available. And most of the prolog-based tools are C-based re-implementation of prolog-like languages, not anything can be ran in existing prolog implementations (SWI-prolog or SICStus Prolog). The author is a Common Lisp programmer, so LISP-based implementation is particularly interesting. But John Pollock's OSCAR [18] was chosen not only because it's a LISP-based solution, but also because its author is theorist in this area.

Reasoning in LegalRuleML has been partially researched in [6], in which LegalRuleML were translated into a simple Defeasible Logic (DL) with denotic operators. In this project, we have tried a different, more general approach. We have followed the cognitive approach of Giovanni Sartor on Legal reasoning [5] and consider legal reasoning as part of general human cognition behavior, i.e. the so-called "Practical Reasoning". Giovanni Sartor's approach is heavily influenced by John L. Pollock's theory on Defeasible Reasoning [4] , which is the so-far most complete theory on defeasible reasoning. In theory it's possible to map all information of LegalRuleML into Pollock's framework. Now we briefly introduce Pollock's defeasible reasoning theory [19], which consists of two levels: epistemic reasoning and practical reasoning.

**Table 1** Defeasible Reasoning Engines Overview

| System Name (ref) | Reasoning | Lang Supported | Technology | Interface | Complexity Analysis | Empirical Eval | Extra Notes |
|---|---|---|---|---|---|---|---|
| Nathan ([47]) | Defeasible | First order | Prolog meta | Command line | None | Simple benchmarks | None |
| d-Prolog ([55]) | Defeasible | First order | Prolog meta | Command line | None | Simple benchmarks (See [51] and [4]) | None |
| EVID ([16]) | Defeasible | First order | Prolog meta | Command line | None (although discussed) | Simple benchmark | *howdefeatit* query |
| OSCAR ([60]) | Defeasible | First order | LISP program | Command line | None (although considered) | Unavailable | Used within "rational agent" implementation |
| Deimos ([51, 62]) | Defeasible | Propositional | Haskell | Web and Command line | Undertaken (available in seperate paper) | Comprehensive benchmarking with DTScale | Only supports query answering |
| Delores ([51]) | Defeasible | Propositional | C | Command line | Undertaken (but not detailed) | Comprehensive benchmarking with DTScale | Only supports total answering and requires preprocessing of theory |
| Phobos ([64, 65]) | Plausible | Propositional | Haskell | Web and Command line | Undertaken (but not included) | Comprehensive benchmarking with custom tools | None |
| DeLP ([40]) | Defeasible (dialectic argumentation) | First order | Prolog/JAM | Web, Agent component and command line | See [20] | Simple benchmarks and anecdotal evidence | None |
| DR-PROLOG ([4]) | Defeasible | First order | Prolog meta | Web and command line | None | Comprehensive benchmarking with DTScale | RuleML support and ambiguity propogation |
| IACAS ([74]) | Argumentation | First order | LISP program | Command line | None | Simple benchmarks | Chisholms Theory of Knowledge support |
| AS ([76]) | Argumentation | First order | Ruby | Web (command line) | None | Benchmarks | Produces diagram of argument structure |
| Vreeswijk's Admissible Defence Sets ([75]) | Argumentation | First order | Ruby | Web (command line) | Detailed complexity analysis | Comprehensive examples | Discussion of empirical complexity analysis |
| Argue tuProlog ([12]) | Argumentation | First order | Java | Software Component and GUI | None | None (although discussed) | API to allow integration |
| CaSAPI ([37]) | Argumentation | First order | Prolog meta | Command line | None | Simple examples | Translation (by-hand) from a given formalism possibly required |

### 7.1 OSCAR

The OSCAR project [11] has implemented a sophisticated system of defeasible reasoning that enables it to deal defeasibly with:

1. perception
2. change and persistence
3. causation
4. probabilities
5. plan construction and evaluation

OSCAR is written in Common LISP. It has been tested in a variety of LISP environments. The preferred environment is Macintosh Common LISP, [12] where it supports graphics not available in other environments. OSCAR is capable to resolve problems described as a piece of text:

```
Problem #1
This is a case of collective rebutting defeat
Given premises:
     P    justification = 1.0
     A    justification = 1.0
Ultimate epistemic interests:
     R    interest = 1.0

    FORWARDS PRIMA FACIE REASONS
      pf-reason_1:   {P} ||=> Q   strength = 1.0
      pf-reason_2:   {Q} ||=> R   strength = 1.0
```

[11] http://johnpollock.us/ftp/OSCAR-web-page/oscar.html
[12] https://github.com/binghe/mcl

```
pf-reason_3:   {C} ||=> ~R   strength = 1.0
pf-reason_4:   {B} ||=> C   strength = 1.0
pf-reason_5:   {A} ||=> B   strength = 1.0
```

and below is the reasoning result:

```
================== ULTIMATE EPISTEMIC INTERESTS ==================
  Interest in R
  is unsatisfied.
--------------------------------------------------

Elapsed time = 0.001 sec
Cumulative size of arguments = 7
Size of inference-graph = 8 of which 0 were unused suppositions.
87% of the inference-graph was used in the argument.
12 interests were adopted.
1 suppositions were made.
```

Unfortunately OSCAR cannot be used directly as a legal reasoning tools. As a rational agent framework it must be further developed with deontic operators and related rules defined. In this project, what's done by the author is to make initial port work to get OSCAR runnable in modern Common Lisp platforms. We think it's worth to keep researching OSCAR as a general rational agent framework, and it may be useful not only for legal reasoning, but also as a general framework to implement Strong Artificial Intelligence. In next section we introduce the basic concepts used in OSCAR and Pollock's defeasible reasoning theory.

### 7.2 The logical structure of epistemic reasoning

Most rational thought involves reasoning that is *defeasible*, in the sense that the reasoning can lead not only to the adoption of new beliefs but also to the retraction of previously held beliefs.

Reasoning proceeds by constructing arguments, where *reasons* provide the atomic links in arguments. *Conclusive reasons* are reasons that are not defeasible. Conclusive reasons logically entail their conclusions. Those that are not conclusive are *prima facie reasons*. Prima facie reasons create a presumption in favor of their conclusion, but it can be defeated. A reason will be encoded as an ordered pair $\langle \Gamma, p\rangle$, where $G$ is the set of premises of the reason and $p$ is the conclusion. Considerations that defeat prima facie reasons are *defeaters*. The simplest kind of defeater for a prima facie reason $\langle \Gamma, p\rangle$ is a reason for denying the conclusion. Let us define '$\neg$' as follows: if for some $\theta$, $\varphi = \lceil\sim \theta\rceil$, let $\neg\varphi = \theta$, and let $\neg\varphi = \lceil\sim \varphi\rceil$ otherwise. Then we define:

**Definition 2.** *(Rebutting defeater) If $\langle \Gamma, p\rangle$ is a prima facie reason, $\langle \Lambda, q\rangle$ is a* rebutting defeater *for $\langle \Gamma, p\rangle$ iff $\langle \Lambda, q\rangle$ is a reason and $q = \lceil\neg p\rceil$.*

Every prima facie reason has associated *undercutting defeaters*, and these are the most important kinds of defeaters for understanding any complicated reasoning. Undercutting defeaters attack a prima facie reason without attacking its conclusion. They accomplish this by attacking the connection between the premises and the conclusion. For instance, '*x looks red to me*' is a prima facie reason for an agent to believe '*x is red*'. But if we know not only that x looks red but also that x is illuminated by red lights and red lights can make things look red when they are not, then it is unreasonable for us to infer that x is red. Consequently, '*x is illuminated by red lights and red lights can make things look red when they are not*' is a defeater, but it is not a reason for thinking that x is not red, so it is not a rebutting defeater. Instead, it attacks the connection between '*x looks red to me*' and '*x is red*', giving us a reason for doubting that x wouldn't look red unless it were red. '*P wouldn't be true unless Q were true*' is some kind of conditional, and we will symbolize it as $\lceil P \gg Q\rceil$ . If $\langle \Gamma, p\rangle$ is a prima facie reason, then where $\Pi\Gamma$ is the conjunction of the members of $\Gamma$, any reason for denying $(\Pi\Gamma \otimes p)$ is a defeater. Thus Pollock proposes to characterize undercutting defeaters as follows:

**Definition 3.** *(Undercutting defeater) If $\langle \Gamma, p\rangle$ is a prima facie reason, $\langle \Lambda, q\rangle$ is an* undercutting defeater *for $\langle \Gamma, p\rangle$ iff $\langle \Lambda, q\rangle$ is a reason and $q = \sim (\Pi\Gamma \gg p)$.*

It will be convenient to abbreviate $\lceil \sim (P \gg Q) \rceil$ as $\lceil (P \otimes Q) \rceil$, and we will henceforth represent undercutting defeaters as reasons for $\lceil (\Pi\Gamma \otimes p) \rceil$

The concept of undercutting defeater doesn't exist in most defeasible reasoners, nor ever been mentioned in the specification of LegalRuleML, however it exists in many legal norms. Correctly identifying undercutting defeaters may be the key for a successful legal reasoning. Here we omit most of details about how reasoning actually proceed. Interesting reader should take a look at [18]. The higher level consists of the system of practical cognition, and it is implemented in the lower level via *doxastification*.

## 8 A case study on the consistency between GDPR and BDSG-E

In this section, we discuss the four consistency cases mentioned in [11]. Fortunately, we have both positive and negative cases. We will list the original articles from GDPR and BDSG-E corresponding to each case, then try to analyze their consistency from the view of legal reasoning [5], and these articles will be the main targets for manually translating to LegalRuleML and further processing in the rest of this paper.

According to [11], "The aim of the government is to make use of certain opening clauses in the GDPR in order to retain some well proven provisions of the German Data Protection Act (BDSG). However, it is sometimes unclear whether a national provision is still covered by an opening clause or whether it may violate European Law. According to German media coverage, the European Commission is already pressing for a number of changes in the draft law. A high-ranked representative of the DG Justice is quoted, constituting that some changes in the draft law are not covered by the opening clauses, and blaming the Geman government for undermining the original goal of the GDPR, full harmonisation. "

Then the author took a closer look upon the most relevant sections of the German draft law, as illustrated in the following sub-sections:[13], Art. 45 and the rest articles belong to Part 3 (and an extra Art. 85 for Part 4), which aim to implement Directive (EU) 2016/680.

### 8.1 Case 1: Administrative fines and Penalties

The first case is a positive one. Let's first quote the original words from [11]:

> "Art. 83 GDPR provides for the opportunity to impose fines up to 20 million Euros or up to 4 % of the total worldwide annual turnover of the preceding financial year. While the fines primarily apply to companies, the member states can determine 'different penalties'. The German legislator makes use of this opportunity by creating rules also allowing for the sanctioning of individuals, leading to a risk of liability for managers, employees and in-house data protection officers. Section 42 BDSG-E even foresees a punishment of up to three years imprisonment.
> Thus, an effective and well organised compliance-structure is more crucial than ever."

Our goal here is to find a way to use computer to do legal reasoning with related articles and reach the same conclusion. To get a closer look at above arguments, let's first take a look at the full text of Art. 83 GDPR, which is long and complicated:

> Art. 83 (GDPR) (General conditions for imposing administrative fines)
> 1. Each supervisory authority shall ensure that the imposition of administrative fines pursuant to this Article in respect of infringements of this Regulation referred to in paragraphs 4, 5 and 6 shall in each individual case be effective, proportionate and dissuasive.
> 2. Administrative fines shall, depending on the circumstances of each individual case, be imposed in addition to, or instead of, measures referred to in points (a) to (h) and (j) of Article 58(2). When deciding whether to impose an administrative fine and deciding on the amount of the administrative fine in each individual case due regard shall be given to the following:

[13] The author also mentioned that, "It contains 84 sections. Compared to the old law that only had 48 sections, this alone indicates the complexity of the future German regulation." However, as we can see from Appendix B, only the first 44 articles (Part 1 and Part 2) are adopting Regulation (EU) 2016/679

(a) the nature, gravity and duration of the infringement taking into account the nature scope or purpose of the processing concerned as well as the number of data subjects affected and the level of damage suffered by them;
(b) the intentional or negligent character of the infringement;
(c) any action taken by the controller or processor to mitigate the damage suffered by data subjects;
(d) the degree of responsibility of the controller or processor taking into account technical and organisational measures implemented by them pursuant to Articles 25 and 32;
(e) any relevant previous infringements by the controller or processor;
(f) the degree of cooperation with the supervisory authority, in order to remedy the infringement and mitigate the possible adverse effects of the infringement;
(g) the categories of personal data affected by the infringement;
(h) the manner in which the infringement became known to the supervisory authority, in particular whether, and if so to what extent, the controller or processor notified the infringement;
(i) where measures referred to in Article 58(2) have previously been ordered against the controller or processor concerned with regard to the same subject-matter, compliance with those measures;
(j) adherence to approved codes of conduct pursuant to Article 40 or approved certification mechanisms pursuant to Article 42; and
(k) any other aggravating or mitigating factor applicable to the circumstances of the case, such as financial benefits gained, or losses avoided, directly or indirectly, from the infringement.

3. If a controller or processor intentionally or negligently, for the same or linked processing operations, infringes several provisions of this Regulation, the total amount of the administrative fine shall not exceed the amount specified for the gravest infringement.
4. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 10 000 000 EUR, or in the case of an undertaking, up to 2 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the obligations of the controller and the processor pursuant to Articles 8, 11, 25 to 39 and 42 and 43;
(b) the obligations of the certification body pursuant to Articles 42 and 43;
(c) the obligations of the monitoring body pursuant to Article 41(4).
5. Infringements of the following provisions shall, in accordance with paragraph 2, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher:
(a) the basic principles for processing, including conditions for consent, pursuant to Articles 5, 6, 7 and 9;
(b) the data subjects' rights pursuant to Articles 12 to 22;
(c) the transfers of personal data to a recipient in a third country or an international organisation pursuant to Articles 44 to 49;
(d) any obligations pursuant to Member State law adopted under Chapter IX;
(e) non-compliance with an order or a temporary or definitive limitation on processing or the suspension of data flows by the supervisory authority pursuant to Article 58(2) or failure to provide access in violation of Article 58(1).
6. Non-compliance with an order by the supervisory authority as referred to in Article 58(2) shall, in accordance with paragraph 2 of this Article, be subject to administrative fines up to 20 000 000 EUR, or in the case of an undertaking, up to 4 % of the total worldwide annual turnover of the preceding financial year, whichever is higher.
7. Without prejudice to the corrective powers of supervisory authorities pursuant to Article 58(2), each Member State may lay down the rules on whether and to what extent administrative fines may be imposed on public authorities and bodies established in that Member State.
8. The exercise by the supervisory authority of its powers under this Article shall be subject to appropriate procedural safeguards in accordance with Union and Member State law, including effective judicial remedy and due process.
9. Where the legal system of the Member State does not provide for administrative fines, this Article may be applied in such a manner that the fine is initiated by the competent supervisory authority and imposed by competent national courts, while ensuring that those legal remedies are effective and have an equivalent effect to the administrative fines imposed by supervisory authorities. In any event, the fines imposed shall be effective, proportionate and dissuasive.

Those Member States shall notify to the Commission the provisions of their laws which they adopt pursuant to this paragraph by 25 May 2018 and, without delay, any subsequent amendment law or amendment affecting them.

The kernel of Art. 83 (GDPR) are the penal provisions made by paragraph 4, 5 and 6, which regulated the upper bound of administrative fines according to the violation of the obligation pursuant to different group of articles. On the other side, paragraph 7 and 9 are a open clauses which gives each Member State rights to lay down further rules. Paragraph 9 is more specific than paragraph 7 because it's applicable to only Member States whose legal system does not provide for administrative fines. But this is not the case for German, because Section 41 of BDSG-E clearly admitted the administrative fines regulated by GDPR, with further provisions of the Act on Administrative Offenses:

Section 41 (BDSG-E) (Application of the legislation of the fines and criminal proceedings)

(1) The provisions of the Act on Administrative Offenses shall apply mutatis mutandis to infringements pursuant to Article 83 (4) to (6) of Regulation (EU) 2016/679, unless this law provides otherwise. Sections 17, 35 and 36 of the Act on Administrative Offenses shall not apply.

(2) The provisions of the Act on Administrative Offenses and the General Laws on Criminal Procedure, including the Code of Criminal Procedure and the Court of Appeals Act, shall apply to proceedings for an infringement under Article 83 (4) to (6) of Regulation (EU) 2016/679, accordingly. Sections 56 to 58, 87, 88, 99 and 100 of the Act on Administrative Offenses shall not apply. Section 69 (4) sentence 2 of the Act on Administrative Offenses applies with the proviso that the public prosecutor's office can terminate the proceedings only with the consent of the supervisory authority which issued the fine.

The details of such Administrative Offenses were regulated by Section 42 of BDSG-E, concerning the imprisonment individuals:

Section 42 (BDSG-E) (Penal provisions)

(1) A penalty of up to three years or with a fine will be punished, who is not knowledgeable in general accessible personal data of a large number of persons, without being entitled to do so,
   (a) transmitted to a third party;
   (b) in a different way and commercial activity.

(2) A penalty of up to two years, or a fine, shall be imposed on persons who are subject to personal data, which are not generally accessible,
   (a) without being authorized to do so, or
   (b) misrepresented by incorrect information and in doing so for consideration or for the purpose of enriching himself or another or another to damage.

(3) The act is only pursued upon request. The person concerned, the person responsible, the Federal Commissioner and the supervisory authority are entitled to submit proposals.

(4) A notification pursuant to Article 33 of Regulation (EU) 2016/679 and notification pursuant to Article 34 (1) of Regulation (EU) 2016/679 may, in criminal proceedings against the notifiable person or one of their relatives named in Section 52 (1) of the Code of Criminal Procedure shall be used with the consent of the police become.

Thus, if a German company as data controller has violated any kind of personal data protecting obligation, according to GDPR the company should be punished with administrative fines, then, according to BSDG-E, the person who is actually responsible for the infringements may be further punished of up to two or three years of imprisonment.

Here we have observed cumulative penalty statements formed by the combination of GDPR and BDSG-E. The additional penalties regulated by BDSG-E didn't supersede the penalty regulated by GDPR, thus from legal aspect we agree that BDSG-E is consistent with GDPR in this part.

```
1  <?xml version="1.0" encoding="UTF-8"?>
2  <lrml:LegalRuleML xmlns:lrml="http://docs.oasis-open.org/legalruleml/ns/v1.0/"
3                    xmlns:ruleml="http://ruleml.org/spec"
4                    xmlns:rulemlmm="http://ruleml.org/1.0/metamodel#"
5                    xmlns:xs="http://www.w3.org/2001/XMLSchema"
6                    xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
7     <lrml:hasStatements>
8        <lrml:Statements key="GDPR_83">
9           <lrml:hasStatement>
10             <lrml:PenaltyStatement key="gdpr-ps1">
11                <lrml:hasTemplate>
12                   <ruleml:Atom>
```

```
                        <ruleml:Rel iri="cyc:AdministrativeFine"/>
                        <ruleml:Expr>
                            <ruleml:op>
                                <ruleml:Fun iri="cyc:Maximum"/>
                            </ruleml:op>
                            <ruleml:arg>
                                <ruleml:Data>10000000 Euro</ruleml:Data>
                            </ruleml:arg>
                            <ruleml:arg>
                                <ruleml:Expr>
                                    <ruleml:op>
                                        <ruleml:Fun iri="cyc:TimesFN"/>
                                    </ruleml:op>
                                    <ruleml:arg>
                                        <ruleml:Data xsi:type="xs:real">2%</ruleml:Data>
                                    </ruleml:arg>
                                    <ruleml:arg>
                                        <ruleml:Expr>
                                            <ruleml:op>
                                                <ruleml:Fun iri="cyc:AnnualTurnover"/>
                                            </ruleml:op>
                                            <ruleml:arg>
                                                <ruleml:Var>X</ruleml:Var>
                                            </ruleml:arg>
                                            <ruleml:arg>
                                                <ruleml:Expr>
                                                    <ruleml:op>
                                                        <ruleml:Fun iri="cyc:DifferenceFN"/>
                                                    </ruleml:op>
                                                    <ruleml:arg>
                                                        <ruleml:Var>year</ruleml:Var>
                                                    </ruleml:arg>
                                                    <ruleml:arg>
                                                        <ruleml:Data xsi:type="xs:integer">1</ruleml:Data>
                                                    </ruleml:arg>
                                                </ruleml:Expr>
                                            </ruleml:arg>
                                        </ruleml:Expr>
                                    </ruleml:arg>
                                </ruleml:Expr>
                            </ruleml:arg>
                        </ruleml:Expr>
                    </ruleml:Atom>
                </lrml:hasTemplate>
            </lrml:PenaltyStatement>
        </lrml:hasStatement>
        <lrml:hasStatement>
            <lrml:PenaltyStatement key="gdpr-ps2">
                <lrml:hasTemplate>
                    <ruleml:Atom>
                        <ruleml:Rel iri="cyc:AdministrativeFine"/>
                        <ruleml:Expr>
                            <ruleml:op>
                                <ruleml:Fun iri="cyc:Maximum"/>
                            </ruleml:op>
                            <ruleml:arg>
                                <ruleml:Data>20000000 Euro</ruleml:Data>
                            </ruleml:arg>
                            <ruleml:arg>
                                <ruleml:Expr>
                                    <ruleml:op>
                                        <ruleml:Fun iri="cyc:TimesFN"/>
                                    </ruleml:op>
                                    <ruleml:arg>
                                        <ruleml:Data xsi:type="xs:real">4%</ruleml:Data>
                                    </ruleml:arg>
                                    <ruleml:arg>
                                        <ruleml:Expr>
                                            <ruleml:op>
                                                <ruleml:Fun iri="cyc:AnnualTurnover"/>
                                            </ruleml:op>
                                            <ruleml:arg>
                                                <ruleml:Var>X</ruleml:Var>
                                            </ruleml:arg>
                                            <ruleml:arg>
                                                <ruleml:Expr>
                                                    <ruleml:op>
                                                        <ruleml:Fun iri="cyc:DifferenceFN"/>
                                                    </ruleml:op>
                                                    <ruleml:arg>
                                                        <ruleml:Var>year</ruleml:Var>
                                                    </ruleml:arg>
                                                    <ruleml:arg>
                                                        <ruleml:Data xsi:type="xs:integer">1</ruleml:Data>
                                                    </ruleml:arg>
                                                </ruleml:Expr>
                                            </ruleml:arg>
                                        </ruleml:Expr>
                                    </ruleml:arg>
                                </ruleml:Expr>
                            </ruleml:arg>
                        </ruleml:Expr>
                    </ruleml:Atom>
                </lrml:hasTemplate>
            </lrml:PenaltyStatement>
        </lrml:hasStatement>
    </lrml:Statements>
</lrml:hasStatements>
</lrml:LegalRuleML>
```

```
<?xml version="1.0" encoding="UTF-8"?>
<lrml:LegalRuleML xmlns:lrml="http://docs.oasis-open.org/legalruleml/ns/v1.0/"
                  xmlns:ruleml="http://ruleml.org/spec"
                  xmlns:rulemlmm="http://ruleml.org/1.0/metamodel#"
                  xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
    <lrml:hasStatements>
        <lrml:Statements key="BDSG_42">
            <lrml:hasStatement>
                <lrml:PenaltyStatement key="bdsg-ps1">
```

```
                <lrml:hasTemplate>
                    <lrml:SuborderList>
                        <ruleml:formula>
                            <ruleml:Or>
                                <ruleml:formula>
                                    <ruleml:Atom>
                                        <ruleml:Rel iri="cyc:PrisonSentencePunishment"/>
                                        <ruleml:arg>
                                            <ruleml:Data xsi:type="xs:integer">3 years</ruleml:Data>
                                        </ruleml:arg>
                                        <ruleml:arg>
                                            <ruleml:Var>X</ruleml:Var>
                                        </ruleml:arg>
                                    </ruleml:Atom>
                                </ruleml:formula>
                                <ruleml:formula>
                                    <ruleml:Atom>
                                        <ruleml:Rel iri="cyc:AdministrativeFine"/>
                                        <ruleml:arg>
                                            <ruleml:Data>Y</ruleml:Data>
                                        </ruleml:arg>
                                    </ruleml:Atom>
                                </ruleml:formula>
                            </ruleml:Or>
                        </ruleml:formula>
                    </lrml:SuborderList>
                </lrml:hasTemplate>
            </lrml:PenaltyStatement>
        </lrml:hasStatement>
        <lrml:hasStatement>
            <lrml:PenaltyStatement key="bdsg-ps2">
                <lrml:hasTemplate>
                    <lrml:SuborderList>
                        <ruleml:formula>
                            <ruleml:Or>
                                <ruleml:formula>
                                    <ruleml:Atom>
                                        <ruleml:Rel iri="cyc:PrisonSentencePunishment"/>
                                        <ruleml:arg>
                                            <ruleml:Data xsi:type="xs:integer">2 years</ruleml:Data>
                                        </ruleml:arg>
                                        <ruleml:arg>
                                            <ruleml:Var>X</ruleml:Var>
                                        </ruleml:arg>
                                    </ruleml:Atom>
                                </ruleml:formula>
                                <ruleml:formula>
                                    <ruleml:Atom>
                                        <ruleml:Rel iri="cyc:AdministrativeFine"/>
                                        <ruleml:arg>
                                            <ruleml:Data>Y</ruleml:Data>
                                        </ruleml:arg>
                                    </ruleml:Atom>
                                </ruleml:formula>
                            </ruleml:Or>
                        </ruleml:formula>
                    </lrml:SuborderList>
                </lrml:hasTemplate>
            </lrml:PenaltyStatement>
        </lrml:hasStatement>
    </lrml:Statements>
  </lrml:hasStatements>
</lrml:LegalRuleML>
```

### 8.2 Case 2: Change of purpose of processing

We quote the original words from [11]:

> "Section 22 BDSG-E states a number of exceptions for the lawful processing of special categories of personal data according to Art. 9 GDPR, e.g. in the area of health and social services. Those exceptions are safeguarded by a number of requirements regarding appropriate and specific measures on a technical and organizational level.
> Interestingly, the high level of protection for special categories of personal data experiences another dilution: In case of scientific or historic research, even special categories of personal data can be processed without consent of the data subject, provided it is necessary for the relevant purpose and no overriding interests of the data subject are given. Although the controller has to provide appropriate measures to safeguard the data subjects interests (without further specification), this seems to be a quite generous exemption that allows for a flexible interpretation."

Below is the full contents of Section 22 BDSG-E:

Section 22 (BDSG-E) (Processing of special categories of personal data)

(1) By way of derogation from Article 9 (1) of Regulation (EU) 2016/679, the processing of specific categories of personal data within the meaning of Article 9 (1) of Regulation (EU) 2016/679 shall be permitted
  1. by public and non-public bodies,
     a) from the right to social security and social protection, and to comply with the relevant obligations,

b) for the assessment of the employability of the employee, medical care, healthcare or social services, or the management of health and social services systems and services, or a contract of the person concerned with a health professional, and such data are provided by medical personnel or by other persons , which are subject to a corresponding obligation of secrecy, or are processed under their responsibility, or
c) for reasons of public interest in the field of public health such as protection serious cross-border health risks or to ensure high quality and safety standards for health care and medicines and medical devices is required; In addition to the measures referred to in paragraph 2, professional and criminal requirements for the protection of professional secrecy,

2. by public authorities, if they
   a) are compulsory for reasons of a substantial public interest,
   b) in order to prevent a significant threat to public security,
   c) to prevent significant disadvantages for the public good or to safeguard significant interests of the public good is compulsory or
   d) for compelling reasons of defense or fulfillment of over- or inter-state obligations a public body of the Confederation in the field of crisis management or conflict prevention or for humanitarian action

   And insofar as the interests of the person responsible for the data processing in the cases of the number 2 are the interests of the data subject.

(2) In the cases referred to in paragraph 1, appropriate and specific measures shall be taken to safeguard the interests of the data subject. Considering the state of the art, the cost of implementation and the nature, extent, circumstances and purpose of processing, as well as the different probability of occurrence and the severity of the risks of the rights and freedoms of natural persons involved in processing:

1. Technical organizational measures to ensure that processing is carried out in accordance with the Regulation (EU) 2016/679,
2. Measures which ensure that it can be subsequently verified and ascertained whether and by whom personal data has been entered, modified or removed,
3. Raising the awareness of the stakeholders involved in processing operations,
4. Name of a data protection officer,
5. Restriction of access to the personal data within the responsible body and order processors,
6. Pseudonymization of personal data,
7. Encrypting personal data,
8. Ensuring the ability, confidentiality, integrity, availability and resilience of the systems and services related to the processing of personal data, including the ability to rapidly recover availability and access in the case of a physical or technical incident,
9. To ensure the safety of processing, the establishment of a procedure for periodic review, evaluation and evaluation of the effectiveness of the technical and organizational measures;
10. Specific procedural rules which ensure compliance with the provisions of this Act and Regulation (EU) 2016/679 in the case of transmission or processing for other purposes.

Paragraphs 1 and 2 shall not apply in the cases referred to in paragraph 1 (1) (b).

We have given the full content of Art 6 GDPR in previous section, here is the full content of Art 9 GDPR:

Art. 9 (GDPR) (Processing of special categories of personal data)

1. Processing of personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of genetic data, biometric data for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation shall be prohibited.
2. Paragraph 1 shall not apply if one of the following applies:
   (a) the data subject has given explicit consent to the processing of those personal data for one or more specified purposes, except where Union or Member State law provide that the prohibition referred to in paragraph 1 may not be lifted by the data subject;
   (b) processing is necessary for the purposes of carrying out the obligations and exercising specific rights of the controller or of the data subject in the field of employment and social security and social protection law in so far as it is authorised by Union or Member State law or a collective agreement pursuant to Member State law providing for appropriate safeguards for the fundamental rights and the interests of the data subject;

(c) processing is necessary to protect the vital interests of the data subject or of another natural person where the data subject is physically or legally incapable of giving consent;
(d) processing is carried out in the course of its legitimate activities with appropriate safeguards by a foundation, association or any other not-for-profit body with a political, philosophical, religious or trade union aim and on condition that the processing relates solely to the members or to former members of the body or to persons who have regular contact with it in connection with its purposes and that the personal data are not disclosed outside that body without the consent of the data subjects;
(e) processing relates to personal data which are manifestly made public by the data subject;
(f) processing is necessary for the establishment, exercise or defence of legal claims or whenever courts are acting in their judicial capacity;
(g) processing is necessary for reasons of substantial public interest, on the basis of Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject;
(h) processing is necessary for the purposes of preventive or occupational medicine, for the assessment of the working capacity of the employee, medical diagnosis, the provision of health or social care or treatment or the management of health or social care systems and services on the basis of Union or Member State law or pursuant to contract with a health professional and subject to the conditions and safeguards referred to in paragraph 3;
(i) processing is necessary for reasons of public interest in the area of public health, such as protecting against serious cross-border threats to health or ensuring high standards of quality and safety of health care and of medicinal products or medical devices, on the basis of Union or Member State law which provides for suitable and specific measures to safeguard the rights and freedoms of the data subject, in particular professional secrecy;
(j) processing is necessary for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) based on Union or Member State law which shall be proportionate to the aim pursued, respect the essence of the right to data protection and provide for suitable and specific measures to safeguard the fundamental rights and the interests of the data subject.

3. Personal data referred to in paragraph 1 may be processed for the purposes referred to in point (h) of paragraph 2 when those data are processed by or under the responsibility of a professional subject to the obligation of professional secrecy under Union or Member State law or rules established by national competent bodies or by another person also subject to an obligation of secrecy under Union or Member State law or rules established by national competent bodies.
4. Member States may maintain or introduce further conditions, including limitations, with regard to the processing of genetic data, biometric data or data concerning health.

We're not legal experts for the discussion of any new legal conclusions. But it should be obvious that, paragraph 1 of Art. 9 (GDPR) is a defeasible rule, and paragraph 2 is a list of rebutting defeaters. A direct translation of paragraph 1 and the first case of paragraph 2 in LegalRuleML could be the following one:

```
<?xml version="1.0" encoding="UTF-8"?>
<lrml:LegalRuleML xmlns:lrml="http://docs.oasis-open.org/legalruleml/ns/v1.0/"
                  xmlns:ruleml="http://ruleml.org/spec"
                  xmlns:rulemlmm="http://ruleml.org/1.0/metamodel#"
                  xmlns:xs="http://www.w3.org/2001/XMLSchema"
                  xmlns:xsi="http://www.w3.org/2001/XMLSchema-instance">
   <lrml:hasPrefix>
      <lrml:Prefix pre="cyc" refID="http://sw.cyc.com/concept/#"/>
   </lrml:hasPrefix>
   <lrml:hasStatements>
      <lrml:Statements key="gdpr_9">
         <lrml:hasStatement>
            <lrml:PrescriptiveStatement key="gdpr_9_1">
               <lrml:hasTemplate>
                  <ruleml:Rule>
                     <lrml:hasStrength>
                        <lrml:DefeasibleStrength/>
                     </lrml:hasStrength>
                     <ruleml:if>
                        <ruleml:Or>
                           <ruleml:formula>
                              <ruleml:And>
                                 <ruleml:Atom>
                                    <ruleml:Rel iri="cyc:isa"/>
                                    <ruleml:arg index="1">
                                       <ruleml:Var>X</ruleml:Var>
                                    </ruleml:arg>
                                    <ruleml:arg index="2">
                                       <ruleml:Ind iri="cyc:PersonalData">personal
data</ruleml:Ind>
```

```
                                    </ruleml:arg>
                                 </ruleml:Atom>
                                 <ruleml:Or>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>racial origin</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>ethnic origin</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>political opinion</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>religious belief</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>philosophical belief</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                    <ruleml:formula>
                                       <ruleml:Atom>
                                          <ruleml:Rel>reveal</ruleml:Rel>
                                          <ruleml:arg index="1">
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:arg>
                                          <ruleml:arg index="2">
                                             <ruleml:Ind>trade union membership</ruleml:Ind>
                                          </ruleml:arg>
                                       </ruleml:Atom>
                                    </ruleml:formula>
                                 </ruleml:Or>
                              </ruleml:And>
                           </ruleml:formula>
                           <ruleml:formula>
                              <ruleml:Atom>
                                 <ruleml:Rel iri="cyc:isa"/>
                                 <ruleml:arg index="1">
                                    <ruleml:Var>X</ruleml:Var>
                                 </ruleml:arg>
                                 <ruleml:arg index="2">
                                    <ruleml:Ind>genetic data</ruleml:Ind>
                                 </ruleml:arg>
                              </ruleml:Atom>
                           </ruleml:formula>
                           <ruleml:formula>
                              <ruleml:Atom>
                                 <ruleml:Rel iri="cyc:isa"/>
                                 <ruleml:arg index="1">
                                    <ruleml:Var>X</ruleml:Var>
                                 </ruleml:arg>
                                 <ruleml:arg index="2">
                                    <ruleml:Ind>biometric data for the purpose
of uniquely identifying a natural person</ruleml:Ind>
                                 </ruleml:arg>
                              </ruleml:Atom>
                           </ruleml:formula>
                           <ruleml:formula>
                              <ruleml:Atom>
                                 <ruleml:Rel iri="cyc:isa"/>
                                 <ruleml:arg index="1">
                                    <ruleml:Var>X</ruleml:Var>
                                 </ruleml:arg>
                                 <ruleml:arg index="2">
                                    <ruleml:Ind>data concerning health</ruleml:Ind>
                                 </ruleml:arg>
                              </ruleml:Atom>
                           </ruleml:formula>
                           <ruleml:formula>
                              <ruleml:Atom>
                                 <ruleml:Rel iri="cyc:isa"/>
                                 <ruleml:arg index="1">
                                    <ruleml:Var>X</ruleml:Var>
```

```
                                 </ruleml:arg>
                                 <ruleml:arg index="2">
                                    <ruleml:Ind>data concerning a natural person?s
sex life or sexual orientation</ruleml:Ind>
                                 </ruleml:arg>
                              </ruleml:Atom>
                           </ruleml:formula>
                        </ruleml:Or>
                     </ruleml:if>
                     <ruleml:then>
                        <lrml:Prohibition>
                           <ruleml:Atom>
                              <ruleml:Rel>process</ruleml:Rel>
                              <ruleml:Var>X</ruleml:Var>
                           </ruleml:Atom>
                        </lrml:Prohibition>
                     </ruleml:then>
                  </ruleml:Rule>
               </lrml:hasTemplate>
            </lrml:PrescriptiveStatement>
         </lrml:hasStatement>
         <lrml:hasStatements>
            <lrml:Statements>
               <lrml:hasStatement>
                  <lrml:PrescriptiveStatement key="gdpr_9_2a">
                     <lrml:hasTemplate>
                        <ruleml:Rule>
                           <lrml:hasStrength>
                              <lrml:Defeater/>
                           </lrml:hasStrength>
                           <ruleml:if>
                              <ruleml:Atom>
                                 <ruleml:Rel>consent</ruleml:Rel>
                                 <ruleml:arg index="1">
                                    <ruleml:Expr>
                                       <ruleml:op>
                                          <ruleml:Fun>data
subject</ruleml:Fun>
                                       </ruleml:op>
                                       <ruleml:arg>
                                          <ruleml:Var>X</ruleml:Var>
                                       </ruleml:arg>
                                    </ruleml:Expr>
                                 </ruleml:arg>
                                 <ruleml:arg>
                                    <ruleml:Var>X</ruleml:Var>
                                 </ruleml:arg>
                              </ruleml:Atom>
                           </ruleml:if>
                           <ruleml:then>
                              <lrml:SuborderList>
                                 <ruleml:formula>
                                    <lrml:Permission>
                                       <ruleml:formula>
                                          <ruleml:Atom>
                                             <ruleml:Rel>process</ruleml:Rel>
                                             <ruleml:Var>X</ruleml:Var>
                                          </ruleml:Atom>
                                       </ruleml:formula>
                                    </lrml:Permission>
                                 </ruleml:formula>
                              </lrml:SuborderList>
                           </ruleml:then>
                        </ruleml:Rule>
                     </lrml:hasTemplate>
                  </lrml:PrescriptiveStatement>
               </lrml:hasStatement>
            </lrml:Statements>
         </lrml:hasStatements>
         <lrml:hasStatements>
            <lrml:Statements>
               <lrml:hasStatement>
                  <lrml:OverrideStatement>
                     <lrml:hasTemplate>
                        <lrml:Override under="#gdpr_9_1" over="#gdpr_9_2a"/>
                     </lrml:hasTemplate>
                  </lrml:OverrideStatement>
               </lrml:hasStatement>
            </lrml:Statements>
         </lrml:hasStatements>
      </lrml:Statements>
   </lrml:hasStatements>
</lrml:LegalRuleML>
```

### 8.3 Case 3: Information Obligations

This is a negative case (inconsistency).

> "While the GDPR requires comprehensive information where personal data is collected from the data subject, the BDSG-E aims at creating exceptions for such information in specific cases. Section 32 and 33 BDSG-E will restrict the obligations according to Article 13 and 14 of the GDPR.
> The requirement for additional information of the data subject, if the controller intends to further process data for a purpose other than that for which the data was collected (Art. 13 (3) GDPR), will not apply if it would require a disproportional effort or presumably preclude or seriously compromise the realization of the processing-objectives and therefore the interest of the data subject for information is not overriding.

Here, Germany makes use of the opening clause according of Art. 23 GDPR, allowing restrictions for specific purposes. Again, some critics from Brussels already rate these exemptions as a violation of EU law.
Also, the right to obtain information from the controller according to Art. 15 GDPR is limited by Section 34 of the draft law. Amongst other exemptions, the right does not exist in cases where personal data has been stored only for the purpose of data security or data supervision, if providing the required information to the data subject would mean disproportionate effort. As a further safeguard, the processing for further purposes has to be excluded by technical and organisational measures.
This surely does not contribute to legal certainty, and legal disputes are easy to predict, regardless of whether the GDPR gives room for theses exemptions.
And as if this was not enough, Section 29 BDSG-E restricts the obligation of the controller to provide the data subject with information granted by Article 14 GDPR in cases where confidentially interests of the controller are overriding.
Finally, even the 'right to be forgotten', considered to be the sacred cow of the GDPR for some stakeholders during the legislative process, is limited by the German draft law: Section 35 BDSG-E codifies that an obligation to erase certain personal data does not take effect if erasure is not possible due to a particular way of data storage or only possible with a disproportionate effort. What sounds like an exemption for the blockchain technology might nevertheless conflict with the goal of the GDPR."

Section 35 (BDSG-E) (Right to be forgotten)
(1) If the deletion is not possible or is only possible with a disproportionate effort because of the special nature of the storage, the right of the data subject is the responsibility of the person responsible for the deletion of personal data pursuant to Article 17 (1) of Regulation (EU) 2016/679 in Article 17 (3) of Regulation (EU) 2016/679. In this case, the restriction of processing in accordance with Article 18 of Regulation (EU) 2016/679 shall be replaced by a deletion. Sentences 1 and 2 shall not apply if the personal data have been processed illegally.
(2) In addition to Article 18 (1) (b) and (c) of Regulation (EU) 2016/679, the first and second sentences of paragraph 1 shall apply mutatis mutandis[14] to Article 17 (1) (a) and (d) of Regulation (EU) 2016/679 Is responsible for the assumption that a deletion would jeopardize the interests of the data subject. The person responsible shall inform the data subject of the restriction of the processing, provided that such information does not prove impossible or would require disproportionate expenditure.
(3) In addition to Article 17 (3) (b) of Regulation (EU) 2016/679, paragraph 1 applies mutatis mutandis in the case of Article 17 (1) (a) of Regulation (EU) 2016/679 where cancellation is prohibited by contractual or contractual retention periods.

### 8.4 Case 4: Data Protection Officer

"With regard to the obligation to appoint a data protection officer, the draft law keeps the current provisions of the German Data Protection Act and obliges every company with at least ten persons employed with the automatic processing of personal data to appoint a data protection officer. The GDPR only obliges companies to do so in exceptional cases.
The controller or the processor will also have to appoint a data protection officer if they deal with processing subject to a data protection impact assessment according to Article 35 GDPR. The same applies if personal data is processed for the purpose of commercial transfer of data or for marketing and market research purposes."

Section 38 (BDSG-E) (Data protection officers of non-public bodies)
(1) In addition to Article 37 (1) (b) and (c) of Regulation (EU) 2016/679 the responsible person and the order processor appoint a data protection officer or a data protection officer, as long as they usually deal at least ten persons with the automated processing of personal data. Take the person in charge or the processors processing that are subject to a privacy impact assessment in accordance with Article 35 of Regulation (EU) 2016/679, or process them personal information business for the purpose of transmission, the anonymous transmission or for the purpose of market or opinion research, they have to appoint a data protection officer or a data protection officer, regardless of the number of workers with processing people.

[14] 'Mutatis mutandis' is a Medieval Latin phrase meaning "the necessary changes having been made" or "once the necessary changes have been made".

(2) Section 6 (4) and (5) sentence 2 and paragraph 6 shall apply, but Section 6 (4) shall apply only if the appointment of one or a data protection officer is compulsory.

## 9 From LegalRuleML to OSCAR problems

Due to time limits we didn't make any effort on transforming LegalRuleML to OSCAR problems, mostly because it's not ready at the side of OSCAR to accept legal problems. However, it must be noticed that, if we have known what's exactly to transform, writing XSL sheets to actually do the job, is purely an engineering problem. Any scientific research, once being reduced to pure engineering problem, becomes relatively "easy". What's really hard, is to work out the theory of solving the initial task.

But here we want to emphasize the position of LegalRuleML in the whole project. As an rule interchange format it seems unnecessary in the whole process: why didn't we just skip LegalRuleML and manually translate the original legal text into OSCAR problems or acceptable formats by any other defeasible reasoner? The answer is obvious: we're not choosing just one such reasoner, and having LegalRuleML as intermediate format will enable us for easily switching to alternative reasoners whenever we want.

## 10 Conclusions

In this project, we have learnt a lot in scope of the consistency checking between two legal norms. The author first learnt legal reasoning from books written by famous scholar, then LegalRuleML and the whole theory of defeasible reasoning in framework of human cognitive reasoning. The author has built a Structured Application in Adobe FrameMaker for easily authoring of LegalRuleML, and has has ported John Pollock's OSCAR project to modern Common Lisp platforms for future use. Two long legislations, GDPR and BDSG-E, were researched and compared in this work, and a small piece of them were translated in LegalRuleML as a proof-of-concept. By studying the opinions from legal experts on the consistency between GDPR and BSSG-E, the precise definition of "consistency" in this context was found and defined, and an systematic approach for solving the consistency checking problem was proposed, but due to time limits it remains unsolved.

Thanks to Prof. Danilo Montesi for the proposal of this project. And the author wants to point out that, both the author of legal reasoning book (Giovanni Sartor[15]) or the core creator of LegalRuleML (Monica Palmirani[16]) are current professors in University of Bologna. The author is proud for studying in the same university which has long tradition and is strength in the mixed areas between Legal Science and Computer Science.

## References

1. Wikipedia: General Data Protection Regulation (2016) https://en.wikipedia.org/wiki/General_Data_Protection_Regulation.
2. Deutscher Bundestag: Drucksache 18/11325. https://datenschutzbeauftragter-hamburg.de/2017/02/bdsg-neu-kabinett-beschliesst-entwurf-dsanpug-eu/ (March 2017) 1–134
3. van Dalen, D.: Logic and Structure. Springer Science & Business Media (November 2012)
4. Pollock, J.L.: Defeasible Reasoning. Cognitive Science **11**(4) (October 1987) 481–518
5. Sartor, G., Pattaro, E.: Legal Reasoning: A Cognitive Approach to the Law. Treatise of legal philosophy and general jurisprudence / ed.-in-chief Enrico Pattaro. Springer (2005)
6. Lam, H.P., Hashmi, M., Scofield, B.: Enabling reasoning with legalruleml. In: International Symposium on Rules and Rule Markup Languages for the Semantic Web, Springer (2016) 241–257
7. European Union: Official Journal L 119 of the European Union. http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=OJ:L:2016:119:TOC (May 2016) 1–156
8. Wikipedia: Regulation (European Union) https://en.wikipedia.org/wiki/Regulation_(European_Union).

[15] https://www.unibo.it/sitoweb/giovanni.sartor
[16] https://www.unibo.it/sitoweb/monica.palmirani

9. Wikipedia: Directive (European Union) https://en.wikipedia.org/wiki/Directive_(European_Union).
10. Wikipedia: Data Protection Directive (1995) https://en.wikipedia.org/wiki/Data_Protection_Directive.
11. Süme, O.: Data Protection: Does the German Implementation Act (BDSG-E) undermine the GDPR? http://privacylawblog.fieldfisher.com/2017/data-protection-does-the-german-implementation-act-bdsg-e-undermine-the-gdpr/ (April 2017)
12. Athan, T., Governatori, G., Palmirani, M., Paschke, A., Wyner, A.: Legalruleml: Design principles and foundations. In: Reasoning Web International Summer School, Springer (2015) 151–188
13. Boley, H., Tara Athan, e.: Consumer RuleML Specification 1.02 http://wiki.ruleml.org/index.php/Specification_of_Consumer_RuleML_1.02.
14. Governatori, G.: Representing business contracts in RuleML. International Journal of Cooperative Information Systems **14** (2005) 181–216
15. Palmirani, M., Cervone, L., Bujor, O., Chiappetta, M.: Rawe: a web editor for rule markup in legalruleml. In: CEUR workshop proceedings.< http://ceur-ws. org. Volume 1004. (2013)
16. Lenat, D.B.: Cyc: A large-scale investment in knowledge infrastructure. Communications of the ACM **38**(11) (1995) 33–38
17. BRYANT, D., KRAUSE, P.: A review of current defeasible reasoning implementations. The Knowledge Engineering Review **23**(3) (September 2008) 227–260
18. Pollock, J.L.: The OSCAR Manual. (August 1995) 1–240
19. Pollock, J.L.: Cognitive Carpentry. A Blueprint for how to Build a Person. MIT Press (1995)

## Appendix A: The outline of GDPR (Regulation (EU) 2016/679)

CHAPTER I
General provisions

§ 1 Subject-matter and objectives
§ 2 Material scope
§ 3 Territorial scope
§ 4 Definitions

CHAPTER II
Principles

§ 5 Principles relating to processing of personal data
§ 6 Lawfulness of processing
§ 7 Conditions for consent
§ 8 Conditions applicable to child's consent in relation to information society services
§ 9 Processing of special categories of personal data
§ 10 Processing of personal data relating to criminal convictions and offences
§ 11 Processing which does not require identification

CHAPTER III
Rights of the data subject

Section 1
Transparency and modalities

§ 12 Transparent information, communication and modalities for the exercise of the rights of the data subject

Section 2
Information and access to personal data

§ 13 Information to be provided where personal data are collected from the data subject
§ 14 Information to be provided where personal data have not been obtained from the data subject
§ 15 Right of access by the data subject

Section 3
Rectification and erasure

§ 16 Right to rectification
§ 17 Right to erasure ('right to be forgotten')
§ 18 Right to restriction of processing
§ 19 Notification obligation regarding rectification or erasure of personal data or restriction of processing
§ 20 Right to data portability

Section 4
Right to object and automated individual decision-making

§ 21 Right to object
§ 22 Automated individual decision-making, including profiling

Section 5
Restrictions

§ 23 Restrictions

CHAPTER IV
Controller and processor

Section 1
General obligations



Section 2
Security of personal data



Section 3
Data protection impact assessment and prior consultation



Section 4
Data protection officer



Section 5
Codes of conduct and certification



CHAPTER V
Transfers of personal data to third countries or international organisations



CHAPTER VI
Independent supervisory authorities

Section 1
Independent status

CHAPTER IX
Provisions relating to specific processing situations



CHAPTER X
Delegated acts and implementing acts



CHAPTER XI
Final provisions

## Appendix B: The outline of BDSG-E (translated in English)

Part 1
Common provisions

Chapter 1
Scope and definitions

§ 1 Scope of application of the law
§ 2 Definitions

Chapter 2
Legal basis of the processing of personal data

§ 3 Processing of personal data by public authorities
§ 4 Video surveillance of publicly accessible areas

Chapter 3
Data Protection Officer of public authorities

§ 5 Naming
§ 6 Position
§ 7 Duties

Chapter 4
The Federal Commissioner for Data Protection and Information Freedom

§ 8 Establishment
§ 9 Jurisdiction
§ 10 Independence
§ 11 Appointment and tenure
§ 12 Office relationship
§ 13 Rights and obligations
§ 14 Tasks
§ 15 Activity report
§ 16 Powers

Chapter 5
Representation in the European Data Protection Committee, focal point, cooperation of supervisory Visual authorities of the Federal and State Governments in European Union Affairs

§ 17 Representation in the European Data Protection Committee, central point of contact
§ 18 Procedure of cooperation of the supervisory authorities of the Federal and State Governments
§ 19 Responsibilities

Section 6
Appeals

§ 20 Judicial protection
§ 21 The request of the supervisory authority on the judicial decision when assuming the illegality of a decision of the European Commission

Part 2
Implementing provisions for processing for the purposes of § 2 of Regulation (EU) 2016/679

Chapter 1
Legal basis of the processing of personal data

Chapter 7
Liability and sanctions



Part 4
Specific provisions for processing under activities not covered by the scope of application of Regulation (EU) 2016/679 and Directive (EU) 2016/680