ECLIPSE® FOUNDATION

Webinar Series on CRA OSS Implementation

Open Regulatory Compliance Working Group (ORC WG)

Why a series of webinars on the CRA ?

Bring the community up to speed

Understand how the CRA is going to be implemented

Understand the impact on open source

Get aligned on the path forward

CRA Open Source Implementation Series

1

How to read the CRA: Identifying the key parts of the CRA for effective compliance

July 15, 2024

2

The CRA obligations: Identifying the relevant obligations for the OSS community

July 22, 2024

3

CRA Standards making: Understanding key standards and their production timeline

July 29, 2024

4

CRA OSS implementation: Guidelines, attestations and other key documents

August 29 2024,

ECLIPSE FOUNDATION

ECLIPSE® FOUNDATION

Webinar Series on CRA OSS Implementation

How to read the CRA: Identifying the key parts of the CRA for effective compliance

Enzo Ribagnac, *Associate Director for European Policy*

Today's session

1

How to read the CRA: Identifying the key parts of the CRA for effective compliance

July 15, 2024

Target of this session:

1. Help non-legal stakeholders to navigate a legal text without too much hurdles;
2. Help non-legal stakeholders to efficiently read the CRA;
   - Quickly access to relevant information;
   - Find answers already present in the text;
3. Identify relevant parts for the OSS community to focus on;
4. Identify elements that the ORC WG will work on.

Existing resources in the ORC WG

1

How to read the CRA: Identifying the key parts of the CRA for effective compliance

July 15, 2024

- Mailing list
- Office hours (every Tuesday at 4pm CEST)
- By popular demand: weekly calls soon (see community calendar)
- Gitlab (CRA-focused repository)
- Matrix Chat Service
- CRA information hub (gathering all info to read and understand the CRA and related procedures)

Today's Agenda

- The structure of an EU legislation
- Focusing on OSS in the CRA
- A CRA reading use-case
- Conclusion

Today's Agenda

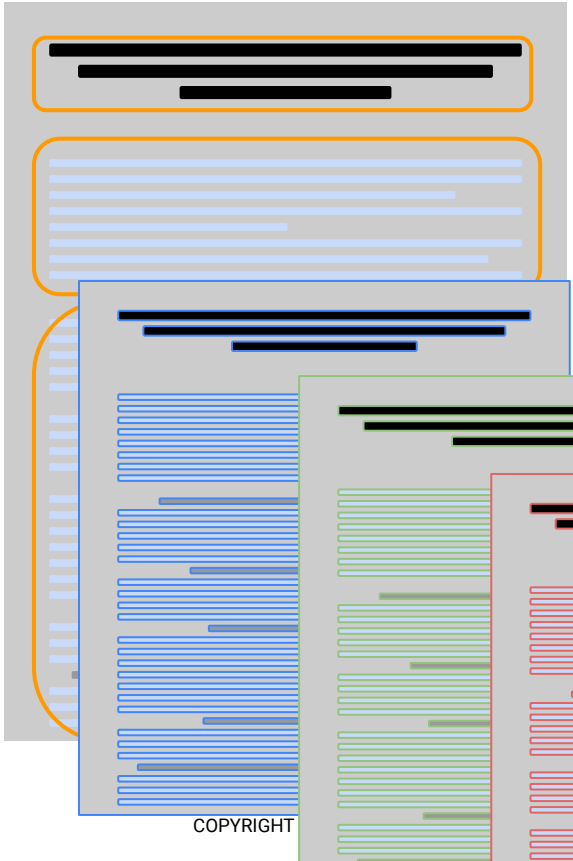
The structure of an EU legislation

Focusing on OSS in the CRA

A CRA reading use-case

Conclusion

The structure of an EU legislation 1/5



Title

(Citations e.g “Having regards…”)

Recitals

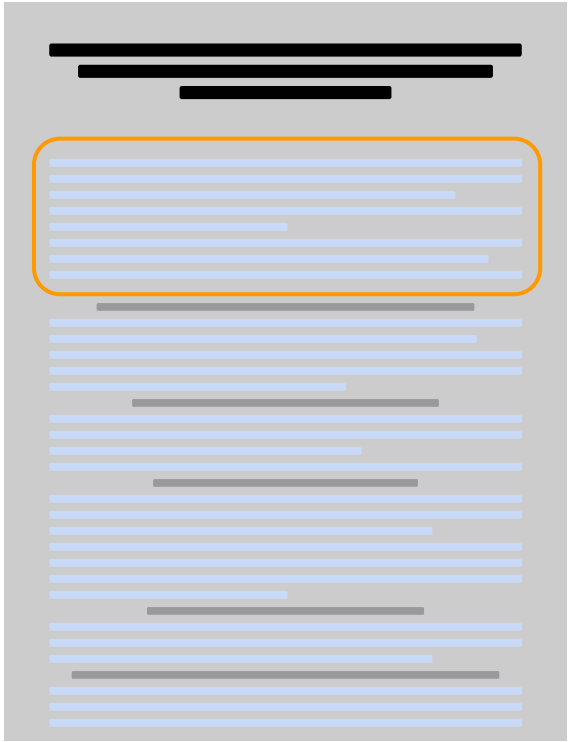
Annexes

Implementing Act/Delegated Act

Standards

Guidances and others

The structure of an EU legislation 2/5



“Recitals”
Set out concise reasons for the provisions/articles of the legislations without paraphrasing.

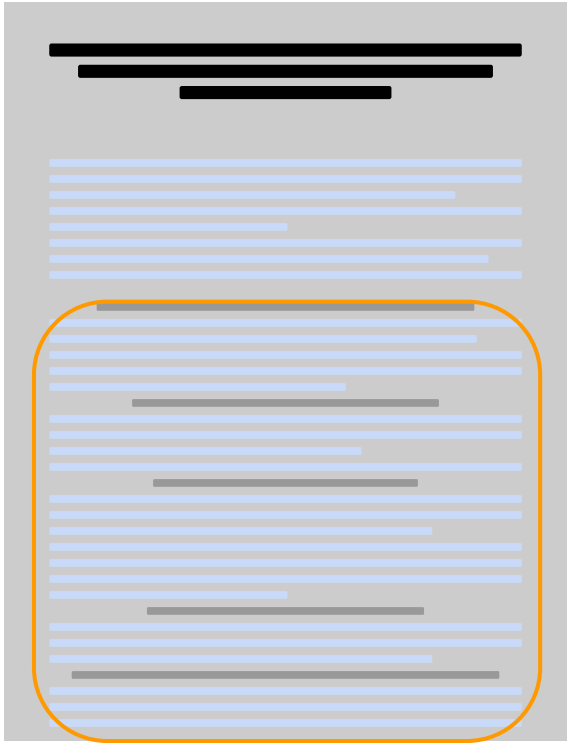
Some answers
- Reasoning
- Clarifications

Connecting recitals with the relevant articles

Order generally “chronologically” follows the text

Legally non-binding

The structure of an EU legislation 3/5



“Articles”

Set by Parts, Titles, Chapters ,Sections, Articles

Scope and definitions first

In case of doubts linking definition, recitals and articles is generally the right approach

Legally binding

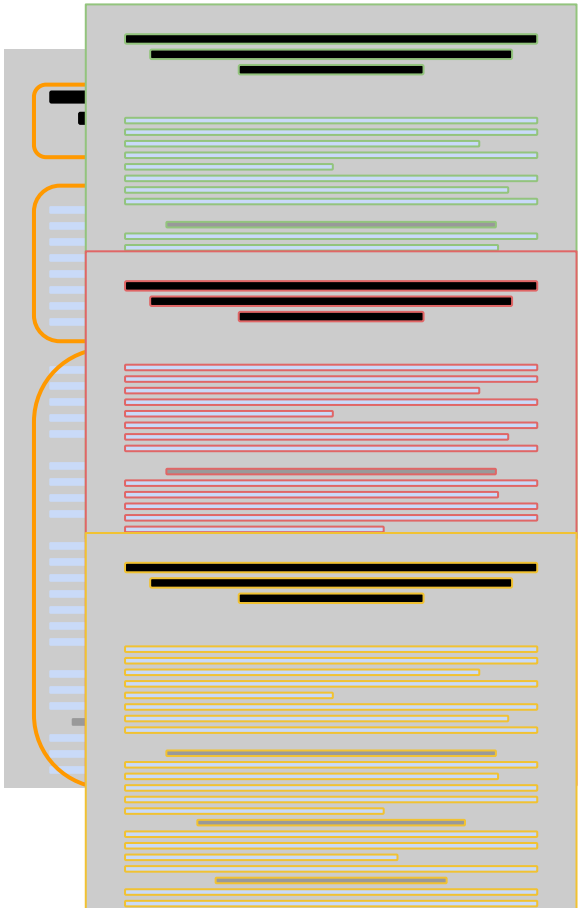
The structure of an EU legislation 4/5

Annexes

Generally used to present materials separately from the body of the text, because it is voluminous or technical or both.

Same value than articles = legally binding

The structure of an EU legislation 5/5



Implementing Act/Delegated Act

- IA:
  - aim to create uniform conditions for the implementation of the legislative act
  - Adopted by the EC after consultation with expert groups and other technical committees
- DA
  - to amend or supplement the non-essential elements of the legislation = legally binding

Standards

- Technical specifications defining requirements
- These specifications are voluntary but have the advantage of allowing presumption of conformity
- They are developed by industry and market actors following some basic principles such as consensus, openness, transparency and non-discrimination.
- Developed by European Standardisation Organisations

Guidances and others

Provide indications to organisations subject to the text on how to interpret and comply with the Act.

Today's Agenda

The structure of an EU legislation

Focusing on OSS in the CRA

A CRA reading use-case

Conclusion

Focusing on OSS in the CRA 1/4

Manufacturers:
Articles: All articles applicable to manufacturers of closed source also apply to OS product of an organisation if the OS product is made available on the market and supplied in the course of a commercial activity

- Article 3 - Definitions (manufacturer, CE marking, SBOMs etc.)
- Article 13 - Obligations of manufacturers
- Article 14 - Reporting obligations of manufacturers
- Article 15 - Voluntary reporting
- Etc.

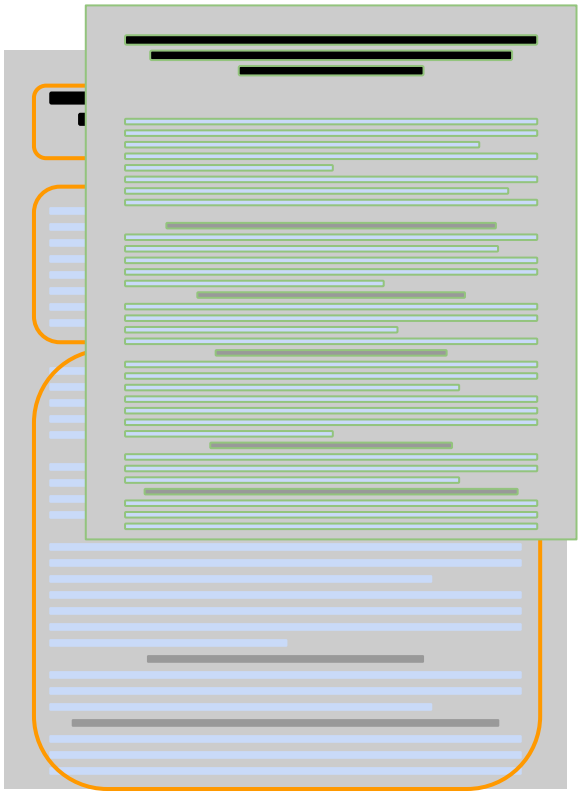
Recitals: 15 to 18 will give me more context commercial activity etc.
Annex: All relevant Annexes applicable to closed source also applyto OS product of an organisat, if the OS product is made available on the market and supplied in the course of a commercial activity

Stewards:
Articles:

Article 3(14) defines OS stewards
Article 24 defines my obligations
Some articles concerning presumption of conformity, and, guidance and attestations are useful to stewards as much as manufacturers

Recitals: 15 to 19 will give me more context helping to understand the scope and my obligations

Focusing on OSS in the CRA 2/4



Implementing Act/Delegated Act

IA:

Implementing act to specify the **technical description** of the categories of important products with digital elements (Article 7)

May adopt:

- implementing acts taking into account European or international standards and best practices, specify the format and elements of the software bill of materials *(Article 13 paragraph 24)*
- implementing acts, specify further the format and procedures for voluntary reporting *(Article 14 paragraph 10)*

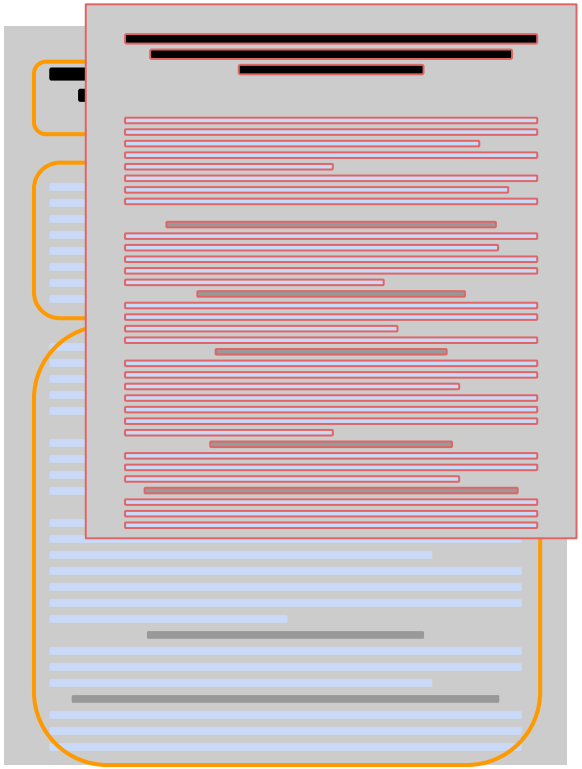
In case standards making - procedure and results - were not satisfactory:

- Implementing acts establishing common specifications covering technical requirements that **provide a means to comply with the essential requirements**

DA:

Delegated acts to establishing voluntary security attestation programmes allowing (...) **to assess the conformity of such products with all or certain essential requirements or other obligations laid down in this Regulation.**

Focusing on OSS in the CRA 3/4



Standards

Standards will allow manufacturers of OSS falling under the definition of products under the CRA to benefit from presumption of conformity upon adoption of standards following procedure dictated by the CRA

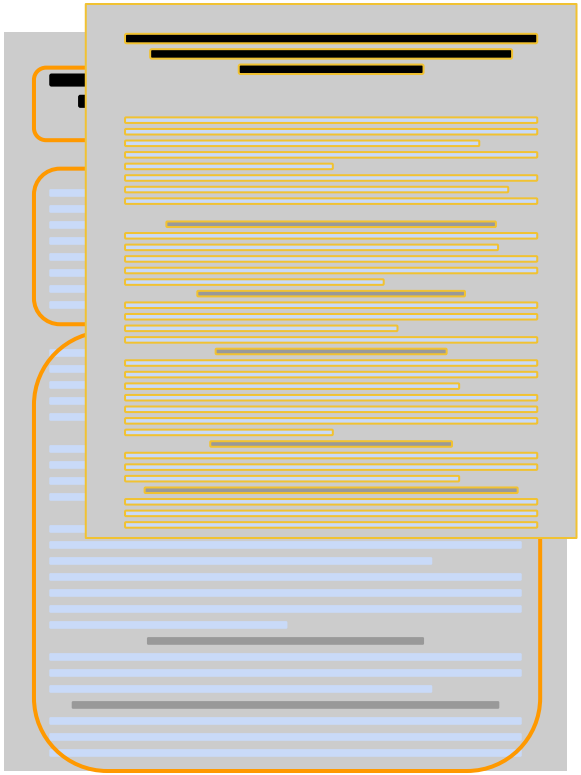
Draft Standardisation Request includes an element pushing for the consultation of the OSS community

Standards will be developed by ESOs such as CEN, CENELEC and ETSI

Draft standardisation request lists 44 standards

We will have a dedicated meeting on this topic on July 29, 2024

Focusing on OSS in the CRA 4/4



Guidances and other

Scope and nature defined Article 26 of the text together with relevant recitals.

A clear reference to OSS in the Article

An obligation to consult relevant stakeholders

Four types of guidance relevant to the OSS community:

1. the scope of this Regulation, with a particular focus on remote data processing solutions and free and open-source software;
2. the application of support periods in relation to particular categories of products with digital elements;
3. guidance targeted at manufacturers subject to this Regulation that are also subject to Union harmonisation legislation other than this Regulation or to other related Union legal acts;
4. the concept of substantial modification.

Today's Agenda

- The structure of an EU legislation
- Focusing on OSS in the CRA
- **A CRA reading use-case**
- Conclusion

Reading the CRA with a use case : OSS foundation 1/2

Case: An OSS foundation, releasing OSS projects developed by members and individual contributors

Relevant Articles

- **Article 3**
  - **(3)** Definition of software
  - **(14)** definition of OS stewards
  - Etc.
- **Article 24** defines my obligations
  - **Put in place and document in a verifiable manner a cybersecurity policy**
  - **Put in place and document effective handling of vulnerabilities by the developers of that product**
  - **Obligations on notification of exploitable vulnerabilities applies to me if I am involved in software development**
  - **In certain cases: obligations on communication of exploitable vulnerabilities to users + notification of severe incident to authorities**

  Article 25 will define the scope and procedure of adoption of the attestation I can apply for my software

Relevant recitals

- **(15) to (18)** give me more context and information about the definition of commercial activity
- **(19)** will give me more context in order to understand
  - If I fall under the definition of stewards based on my nature
  - If I fall under the definition of stewards based on my actions
- **(121)** will tell me about my relationship to fines

Reading the CRA with a use case : OSS foundation 2/2

Case: **An OSS foundation, releasing OSS projects developed by members and individual contributors**

Standards: There are no references to standards directly applicable to stewards in the text. But other documents such as guidance could in theory refer to existing standards and specifications to facilitate the compliance

Besides, when stewards are subjected to manufacturers obligations (e.g when involved in development) they could leverage standards for compliance

Implementing Acts will

- Technically define products that I release falling under the scope of the CRA
- define the format and procedure of SBOMs that I could potentially re-use

A Delegated Act will define the attestations I can apply for in order to facilitate the use of my software by manufacturers of products

Reading the CRA with a use case : Manufacturer of OS products in scope 1/1

Case: A company releasing OS products that constitute a part of commercial activities

Relevant Articles

- **All articles applicable to manufacturers of closed source products also apply to my organisations and products**
- **NB: My organisation is subjected to a due diligence obligation for OSS component present in my products**

Relevant recitals

- **(15) to (18)** give me more context and information about the definition of commercial activity

Standards:

- All articles related to standards applicable to manufacturers of closed source also apply to my OS products

A Delegated Act will define attestations applicable for OS components. My organisation can apply for such attestation for any OS components.

Challenge for articles and recitals:

- Some elements concerning the scope (commercial activities) will be defined in guidances after consultation of experts
- Standards defined for closed source software might not be suitable for open source software (e.g updates, communication with users, development process)
- My organisation depends on manufacturers of other OSS components and OS stewards to comply with the due diligence obligation

Conclusions

1. Articles define the requirements, scope etc. but **not all of them are applicable to my organisation;**
2. Recitals will give **missing context and additional information** in case something is not clear;
3. Annex will include **technical elements** and be clearly referred to in relevant Articles when applicable to my case;
4. Currently elements such as **standards, implementing act, guidance and attestation are still missing/being developed**
5. As a **manufacturer,** my **organisation depend on OSS implementation**
6. The **ORC WG provides for a space for the OSS community to work** on technical content and specifications that can contribute to the development of these missing pieces (E.g standards) are therefore facilitate my compliance

CRA Open Source Implementation Series

1

How to read the CRA: Identifying the key parts of the CRA for effective compliance

July 15, 2024

2

The CRA obligations: Identifying the relevant obligations for the OSS community

July 22, 2024

3

CRA Standards making: Understanding key standards and their production timeline

July 29, 2024

4

CRA OSS implementation: Guidelines, attestations and other key documents

August 29 2024,

Next webinar and ORC WG resources

2

The CRA obligations:
Identifying the relevant obligations for the OSS community

July 22, 2024

- Mailing list
- Office hours (every Tuesday at 4pm CEST)
- By popular demand: weekly calls soon (see community calendar)
- Gitlab (CRA-focused repository)
- Matrix Chat Service
- CRA information hub (gathering all info to read and understand the CRA and related procedures)

Sources

- https://eur-lex.europa.eu/EN/legal-content/glossary/implementing-acts.html
- https://www.europarl.europa.eu/RegData/etudes/BRIE/2021/690709/EPRS_BRI(2021)690709_EN.pdf