



Course material

Course:

Understanding the digital supply chain and its stakes for humanitarian actors

Video:

5.4 Obligations vis-à-vis affected persons

Concepts (extracted from automatically generated subtitles):

Data protection considerations. Personal data. Wealth of data. International organisations. Legal considerations. Personal data of the people. Sensitive data. Such organisations. Legal basis. Organisations. Process personal data. Home address. Prominent examples. Data of vulnerable persons. Medical data.



[to video sequence search](#)

(within Understanding the digital supply chain and its stakes for humanitarian actors.)



[to video](#)

Center for Digital Education. More educational support material here:

<https://www.epfl.ch/education/educational-initiatives/cede/educational-technologies-gallery/boocs-en/>

CYBERSECURITY

LEGAL CONSIDERATIONS



Obligations vis-à-vis Affected Persons

Andrea Raab-Gray

Legal Counsel, International Committee of the Red Cross (ICRC)



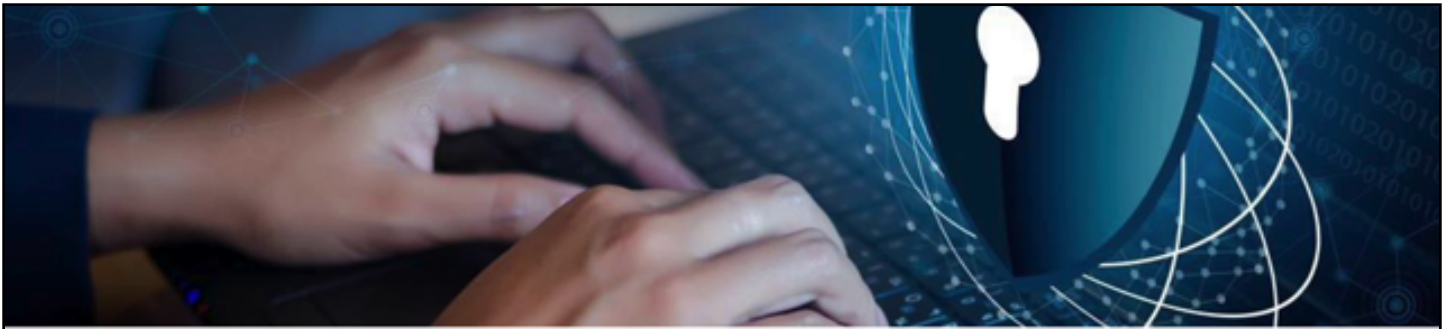
...

notes

summary

0m 0s





Personal data is any information that relates to an identified or identifiable living individual.

A data breach relating to personal data of affected persons can exacerbate their harms and compound stigmatization.

Might trigger reluctance to engage with humanitarians if:

- Data used for other purposes
- Data not safely handled

Welcome back to our last video on legal considerations related to cybersecurity. In this video, we will discuss data protection considerations. In carrying out their activities, organisations collect and process a wealth of data about affected persons who use their services. Much of that data constitutes personal data. That is, any information that relates to an identified or identifiable living individual. This includes name and surname, a home address, an email address such as name.surname@company.com, an identification card number, and even data held by a hospital or doctor, which could be a symbol that uniquely identifies a person. As they often handle data of vulnerable persons or particularly sensitive data such as medical data, it is crucial that organisations protect personal data of the people they seek to serve.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

.....

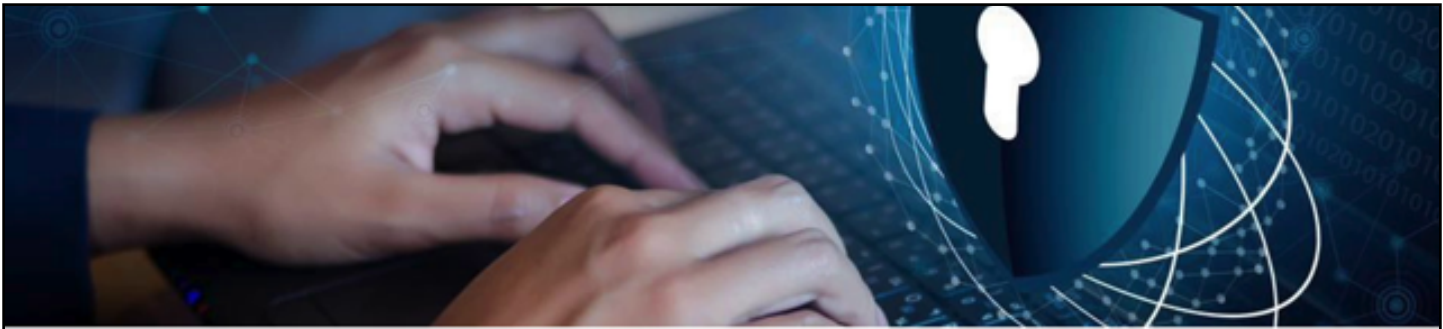
.....

.....

.....

.....





Personal data is any information that relates to an identified or identifiable living individual.

A data breach relating to personal data of affected persons can exacerbate their harms and compound stigmatization.

Might trigger reluctance to engage with humanitarians if:

- Data used for other purposes
- Data not safely handled

Indeed, a data breach relating to personal data of affected persons can exacerbate their harms and compound stigmatization.

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....


.....

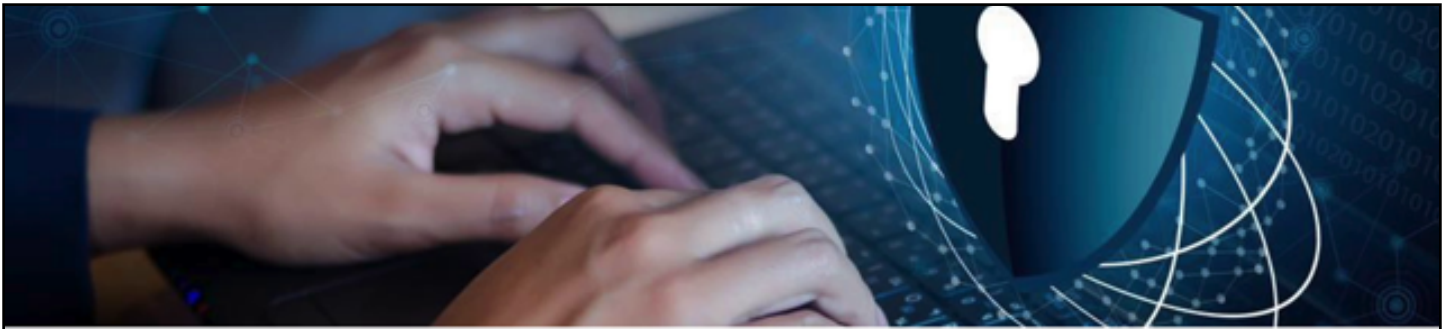
.....

.....

.....

1m 7s





Personal data is any information that relates to an identified or identifiable living individual.

A data breach relating to personal data of affected persons can exacerbate their harms and compound stigmatization.

Might trigger reluctance to engage with humanitarians if:

- Data used for other purposes
- Data not safely handled

Relatedly, affected populations might become reluctant to engage with organisations and accept the services if they were to consider that such organisations use their data for purposes other than those for which data was collected. They might also not wish to engage with the organisation if they perceived

notes

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....

summary

.....

.....

.....

.....

.....

.....

.....

.....

.....

.....





notes

1m 37s





Legislations on personal data protection:

- EU's General Data Protection Regulation – GDPR
- Council of Europe's Convention 108+

Given the importance of protecting personal data in the digital age, many states have developed legislations on personal data protection. These legislations impose obligations, particularly on companies in relation to the processing of personal data.

notes

summary

2m 13s





Legislations on personal data protection:

- EU's General Data Protection Regulation – GDPR
- Council of Europe's Convention 108+

Prominent examples are the EU's General Data Protection Regulation the GDPR, as well as the Council

notes

summary

2m 29s





Legislations on personal data protection:

- EU's General Data Protection Regulation – GDPR
- Council of Europe's Convention 108+

of Europe's Convention 108 plus, which was ratified by 55 states. For reasons of their independence, many international organisations have developed their own personal data protection frameworks.

notes

summary

2m 37s





Legislations on personal data protection:

- EU's General Data Protection Regulation – GDPR
- Council of Europe's Convention 108+

Yet, those different legislations and frameworks of international organisations share certain common data protection principles, which we will now go through.

notes

summary

2m 49s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

First, lawfulness. Organisations are typically only allowed to process personal data if a legal basis is given. National legislations and frameworks of international organisations typically recognise the following legal basis and require that at least one of them is fulfilled to lawfully process personal data. First, consent.

notes

summary

2m 59s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

This means that the individual gave their consent to processing the personal data. Consent is only valid if it is freely given, which in many conflict and violent

notes

summary

3m 24s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

settings is difficult to ascertain due to the power imbalance between effective populations and organisations working in these contexts. Second, contracts. This applies if there is a contract in place with the individual,

notes

summary

3m 37s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

and processing the personal data is necessary to fulfil this contract.

notes

summary

3m 49s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

Another legal basis are legal obligations. This is given if processing of the information is required to comply with local law. Moreover, vital interests can be a valid legal basis. This requirement is fulfilled if processing of personal data is required to protect an individual's life.

notes

summary

3m 53s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

Finally, legitimate or public interests.

notes

summary

4m 12s





Lawfulness - Types of legal bases

1

Consent

Must be freely given by individual.

2

Contract

Data processing necessary to fulfill agreement.

3

Legal obligation

Data processing is required by local law.

4

Vital interests

Data processing necessary to protect individual's life.

5

Legitimate or public interests

Data processing required in the legitimate interests of the organization or a public interest.

This means that the processing of personal data is required in the legitimate interests of the organisation or a public interest unless these interests are

notes

summary

4m 18s





- page 18/26 - 5.4 Obligations vis-a-vis affected persons



- | | | | |
|---|--------------------|---|------------------------|
| 1 | Transparency | 4 | Data Quality |
| 2 | Purpose Limitation | 5 | Storage Limitations |
| 3 | Data Relevance | 6 | Data Security |
| | | 7 | Rights of Data Subject |

notes

4m 37s



Further Data Protection Principles

- | | | | |
|---|--------------------|---|------------------------|
| 1 | Transparency | 4 | Data Quality |
| 2 | Purpose Limitation | 5 | Storage Limitations |
| 3 | Data Relevance | 6 | Data Security |
| | | 7 | Rights of Data Subject |

Moreover, data quality.

notes

summary

5m 19s





- Personal data must be as accurate and up to date as possible. There are also storage limitations. This means that data must only be held for such time as it is required for fulfilling the purpose, though there are some exceptions. Organisations must also ensure data security. This requires that organisations take legal, technical, and organisational measures to ensure the confidentiality and integrity of the personal data.





- page 22/26 - 5.4 Obligations vis-a-vis affected persons

Obligations vis-à-vis Affected Persons



I hope you now understand what to bear in mind when handling the personal data of affected populations and why this is important.

notes

summary

6m 12s





Key messages

- Consider regulatory risks when taking cybersecurity-related decisions.
- Contractual clauses are important in managing cybersecurity risks.
- Open-source software = respect IP rights.
- *Do no harm* – stick to data protection standards + ensure the data security.

With this, we conclude our module on legal considerations relating to cybersecurity. Thank you so much for watching these videos. Before you turn to the quiz, let me summarise the key messages for you. Take legal considerations into account when you take

notes

summary

6m 25s





Key messages

- Consider regulatory risks when taking cybersecurity-related decisions.
- Contractual clauses are important in managing cybersecurity risks.
- Open-source software = respect IP rights.
- *Do no harm* – stick to data protection standards + ensure the data security.

cybersecurity-related decisions. Specifically, think about your regulatory environment and the impact it can have on your organisation and specifically the confidentiality of its data. Remember that contractual clauses are important in managing cybersecurity risks. When you choose to engage with open-source software, be mindful to respect intellectual property rights and protect your own intellectual property.

notes

summary

6m 40s



Finally, whenever you choose or use digital solutions, don't harm the people you seek to serve. Stick to data protection standards and ensure the cybersecurity of the data which they entrust you with.

notes

summary

7m 10s

