AI and the GDPR

– Principles to Remember –

Dominik Straßel[†,*]

[†] *Competence Center for High Performance Computing, Fraunhofer ITWM, Kaiserslautern, GERMANY*

[∗] *Fraunhofer Center Machine Learning*

ITWM Deep Learning Seminar,
29/08/2019,
Kaiserslautern, GERMANY

Fraunhofer
ITWM

Bundesministerium
für Bildung
und Forschung

RheinlandPfalz
MINISTERIUM FÜR BILDUNG,
WISSENSCHAFT, JUGEND
UND KULTUR

Conclusion

GDPR Principles to Remember...

- **fairness and discrimination**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**
- **data minimisation**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**
- **data minimisation**
- **transparency and the right to be informed**

Literature

Used Literature

- ✎ Datatilsinet *“Artificial intelligence and privacy”*
- ✎ Bitkom *“Machine Learning und die Transparenzanforderungen der DSGVO”*
- ✎ ICO *“Big data, artificial intelligence, machine learning and data protection”*
- ✎ EU Parliament *“General Data Protection Regulation”*
- ✎ Article 29 Working Party *“Guidelines on transparency under Regulation 2016/679”*
- ✎ Heise Developer *“Künstliche Intelligenz trifft Datenschutz”*
- ✎ F. Koushanfar *“Deep Learning on Private Data”*
- ✎ B.C. Stahl *“Ethics and Privacy in AI and Big Data”*
- ✎ S. Wachter *“Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR”*
- ✎ N. Papernot *“A Marauder’s Map of Security and Privacy in Machine Learning”*
- ✎ F. Pittaluga *“Learning Privacy Preserving Encodings through Adversarial Training”*

General Data Protection Regulation

The General Data Protection Regulation

- Regulation (EU) 2016/679

The General Data Protection Regulation

- Regulation (EU) 2016/679

- ***regulates*** the ***processing*** by
  - ➪ an *individual*
  - ➪ a *company*
  - ➪ an *organisation*

  of ***personal data*** relating to ***individuals*** in the EU

The General Data Protection Regulation

- Regulation (EU) 2016/679

- ***regulates*** the ***processing*** by
  - ➪ an *individual*
  - ➪ a *company*
  - ➪ an *organisation*

  of ***personal data*** relating to ***individuals*** in the EU

- enforced since 25 May 2018!

What are Personal Data?

Personal Data [GDPR Article 4 (1)]

- *any* information relating to an identified or identifiable natural person

Personal Data [GDPR Article 4 (1)]

- *any* information relating to an identified or identifiable natural person
- *directly linked*, e.g.
  - ➪ name
  - ➪ id number
  - ➪ location data

Personal Data [GDPR Article 4 (1)]

- *any* information relating to an identified or identifiable natural person

- *directly linked*, e.g.
  - ➪ name
  - ➪ id number
  - ➪ location data

- *indirectly linked*
  → you can be identified through a combination of elements
  - ➪ physical/physiological, genetic, mental features
  - ➪ economical actions
  - ➪ cultural or social identity

What means Processing?

Processing [GDPR Article 4 (2)]

- *any* operation or set of operations which is performed on personal data

Processing [GDPR Article 4 (2)]

- *any* operation or set of operations which is performed on personal data

- this includes, e.g.
  - ➪ collecting or recording
  - ➪ structuring or storing
  - ➪ aligning or combing
  - ➪ making them available
  - ➪ erasing or destructing

What are the Penalties?

Enforcements and Penalties [GDPR Article 83]

- ***up to €10 million or 2% of annual global turnover***
  - ➪ article 8 *(conditions for children’s consent)*
  - ➪ article 11 *(processing that doesn’t require identification)*
  - ➪ article 25–39 *(general obligations of processors and controllers)*
  - ➪ article 42 *(certification)*
  - ➪ article 43 *(certification bodies)*

Enforcements and Penalties [GDPR Article 83]

- ***up to €10 million or 2% of annual global turnover***
  - ➩ article 8 *(conditions for children's consent)*
  - ➩ article 11 *(processing that doesn't require identification)*
  - ➩ article 25–39 *(general obligations of processors and controllers)*
  - ➩ article 42 *(certification)*
  - ➩ article 43 *(certification bodies)*

- ***up to €20 million or 4% of annual global turnover***
  - ➩ article 5 *(data processing principles)*
  - ➩ article 6 *(lawfulness of processing)*
  - ➩ article 7 *(conditions for consent)*
  - ➩ article 9 *(processing of special categories of data)*
  - ➩ article 12–22 *(data subjects' rights)*
  - ➩ article 44–49 *(data transfers to third countries or international organisations)*

Where can I get Information?

Getting Information

- **GDPR**
  → `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`

Getting Information

- **GDPR**
  ⟶ `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`

- **European Data Protection Board** (EDPB)
  ⟶ `https://edpb.europa.eu`

Getting Information

- **GDPR**
  → `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`
- **European Data Protection Board** (EDPB)
  → `https://edpb.europa.eu`
- **Article 29 Working Party** *(closed but useful!)*
  → `https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358`

Getting Information

- **GDPR**
  → `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`
- **European Data Protection Board** (EDPB)
  → `https://edpb.europa.eu`
- **Article 29 Working Party** *(closed but useful!)*
  → `https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358`
- at **ITWM**
  → Dr. Markus Pfeffer and Holger Westing (Local Contact Persons)
  → Christian Peter (Information Security Officer)
  → Tino Labudda, Mathias Dalheimer (Deputy Information Security Officer)

Getting Information

- **GDPR**
  → `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`

- **European Data Protection Board** (EDPB)
  → `https://edpb.europa.eu`

- **Article 29 Working Party** *(closed but useful!)*
  → `https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358`

- at **ITWM**
  → Dr. Markus Pfeffer and Holger Westing (Local Contact Persons)
  → Christian Peter (Information Security Officer)
  → Tino Labudda, Mathias Dalheimer (Deputy Information Security Officer)

- at **Fraunhofer Central in Munich**
  → Dr. Ralph Harter (Data Protection Commissioner)

Getting Information

- **GDPR**
  → `https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX%3A32016R0679`
- **European Data Protection Board** (EDPB)
  → `https://edpb.europa.eu`
- **Article 29 Working Party** *(closed but useful!)*
  → `https://ec.europa.eu/newsroom/article29/news.cfm?item_type=1358`
- at **ITWM**
  → Dr. Markus Pfeffer and Holger Westing (Local Contact Persons)
  → Christian Peter (Information Security Officer)
  → Tino Labudda, Mathias Dalheimer (Deputy Information Security Officer)
- at **Fraunhofer Central in Munich**
  → Dr. Ralph Harter (Data Protection Commissioner)
- **Bavarian State Data Protection Institution**
  → `https://www.lda.bayern.de`

AI – the Past, the Present and the Future

The AI winter...

- “AI” is known since the 1950’s

The AI winter...

- “AI” is known since the 1950’s
- but little progress for decades

The AI winter...

- “AI” is known since the 1950’s
- but little progress for decades
- AI stayed in science finction

The AI spring...

- rise of “specialised AI”
  - ➪ e.g. image or speech recognition

The AI spring...

- rise of “specialised AI”
  - ➪ e.g. image or speech recognition
- thanks to
  - ➪ increase in processing power
  - ➪ access to cheap and big storage
  - ➪ and huge amounts of data

The AI summer??

- AI has the potential for
  - ➪ radical improved services
  - ➪ commercial breakthroughs
  - ➪ financial gains
  - ➪ ...

The AI summer??

- AI has the potential for
  - ➪ radical improved services
  - ➪ commercial breakthroughs
  - ➪ financial gains
  - ➪ ...
- AI needs data to be “smart”

The AI future

- people have to trust AI
  - ➯ ethics
  - ➯ security
  - ➯ legal responsibility

The AI future

- people have to trust AI
  - ➪ ethics
  - ➪ security
  - ➪ legal responsibility

- social advances with AI
  - ➪ climate protection?
  - ➪ safer society?
  - ➪ a cure for cancer?

AI meets the GDPR

The GDPR comes into play when AI...

- is ***under development*** with the help of personal data

The GDPR comes into play when AI...

- is ***under development*** with the help of personal data
- is used to ***analyse*** or ***reach decisions*** about individuals

Fundamental Principles [GDPR Article 5]

- *principle of legality, fairness and transparency*

  → `personal data is processed in a lawful, fair and transparent manner`

Fundamental Principles [GDPR Article 5]

- *principle of legality, fairness and transparency*

  → `personal data is processed in a lawful, fair and transparent manner`

- *principle of purpose limitation*

  → `personal data is collected for specific, expressly stated and justified purposes and not treated in a new way that is incompatible with these purposes`

Fundamental Principles [GDPR Article 5]

- *principle of legality, fairness and transparency*

  → personal data is processed in a lawful, fair and transparent manner

- *principle of purpose limitation*

  → personal data is collected for specific, expressly stated and justified purposes and not treated in a new way that is incompatible with these purposes

- *principle of data minimisation*

  → personal data is adequate, relevant and limited to what is necessary for fulfilling the purposes for which it is being processed

Fundamental Principles [GDPR Article 5]

- *accuracy principle*

  → `personal data is correct and, if necessary, updated`

Fundamental Principles [GDPR Article 5]

- *accuracy principle*

  → `personal data is correct and, if necessary, updated`

- *principle relating to data retention periods*

  → `personal data is not stored in identifiable form for longer periods than is necessary for the purposes`

Fundamental Principles [GDPR Article 5]

- *accuracy principle*

  → `personal data is correct and, if necessary, updated`

- *principle relating to data retention periods*

  → `personal data is not stored in identifiable form for longer periods than is necessary for the purposes`

- *principle of integrity and confidentiality*

  → `personal data is processed in a way that ensures adequate personal data protection`

Interesting for us are...

- principle of fairness
- principle of transparency
- principle of purpose limitation
- principle of data minimisation

"Fairness Principle"

- models are no more objective than
  - ➪ its developer
  - ➪ the used data

"Fairness Principle"

- models are no more objective than
  - ➪ its developer
  - ➪ the used data
- all processing is conducted with respect for the data subject's interests

"Fairness Principle"

- models are no more objective than
  - ➩ its developer
  - ➩ the used data
- all processing is conducted with respect for the data subject's interests
- data is used in accordance with what the users reasonably expect

"Fairness Principle"

- models are no more objective than
  - ➪ its developer
  - ➪ the used data

- all processing is conducted with respect for the data subject's interests

- data is used in accordance with what the users reasonably expect

- implement measures to prevent the arbitrary discriminatory treatment of individual persons

This means for a model that...

- it is trained using relevant and correct data

This means for a model that...

- it is trained using relevant and correct data
- it must learn which data to emphasise

This means for a model that...

- it is trained using relevant and correct data
- it must learn which data to emphasise
- must not emphasise information relating to
  - ➪ racial or ethnic origin
  - ➪ political opinion
  - ➪ religion or belief
  - ➪ trade union membership
  - ➪ genetic status
  - ➪ health status
  - ➪ sexual orientation

  if this would lead to arbitrary discriminatory treatment

“Purpose Limitation Principle”

- the reason for processing personal data must
  - ➪ *clearly established*
  - ➪ *fully explained to the data subject*
  - ➪ and *indicated*

  when the data is collected

“Purpose Limitation Principle”

- the reason for processing personal data must
  - *clearly established*
  - *fully explained to the data subject*
  - and *indicated*

  when the data is collected

- recycling data during development and application
  - is maybe useful
  - **but** can be illegal!

Can be illegal?

processing of data is considered to be allowed...

- if it takes place in connection with scientific or historical research

processing of data is considered to be allowed...

- if it takes place in connection with scientific or historical research
- for statistical and archival purposes in the public interest

Is developing AI scientific research?

research...

- Careful study of a given subject, field, or problem, undertaken to discover facts or principles.

✎ **The American Heritage Dictionary of the English Language**

research...

- Careful study of a given subject, field, or problem, undertaken to discover facts or principles.
- An act or period of such study.

✎ **The American Heritage Dictionary of the English Language**

scientific...

- Of, relating to, or employing the methodology of science.

✎ **The American Heritage Dictionary of the English Language**

scientific...

- Of, relating to, or employing the methodology of science.

science...

- The observation, identification, description, experimental investigation, and theoretical explanation of phenomena.

✎ **The American Heritage Dictionary of the English Language**

scientific...

- Of, relating to, or employing the methodology of science.

science...

- The observation, identification, description, experimental investigation, and theoretical explanation of phenomena.
- Such activities restricted to a class of natural phenomena.

✎ **The American Heritage Dictionary of the English Language**

scientific...

- Of, relating to, or employing the methodology of science.

science...

- The observation, identification, description, experimental investigation, and theoretical explanation of phenomena.
- Such activities restricted to a class of natural phenomena.
- A systematic method or body of knowledge in a given area.

✎ **The American Heritage Dictionary of the English Language**

scientific...

- Of, relating to, or employing the methodology of science.

science...

- The observation, identification, description, experimental investigation, and theoretical explanation of phenomena.
- Such activities restricted to a class of natural phenomena.
- A systematic method or body of knowledge in a given area.
- Knowledge, especially that gained through experience.

✎ **The American Heritage Dictionary of the English Language**

GDPR preface Recital 159...

- scientific research should be interpreted broadly

GDPR preface Recital 159...

- scientific research should be interpreted broadly
- include technological development and demonstration

GDPR preface Recital 159...

- scientific research should be interpreted broadly
- include technological development and demonstration
- basic research

GDPR preface Recital 159...

- scientific research should be interpreted broadly
- include technological development and demonstration
- basic research
- applied and privately financed research

So simply separate research and application?

offline vs. online models

- **offline models**
  - ➪ will not learn anything further from the personal data it is currently processing
  - ➪ will not develop “intelligence” once it has been put into use
  - ➪ separate development and application

offline vs. online models

- **offline models**
  - will not learn anything further from the personal data it is currently processing
  - will not develop “intelligence” once it has been put into use
  - separate development and application

- **online models**
  - develop and improve continuously as they are fed more personal data
  - provide decision support
  - *no* separate development and application?

Is there a clear statement?

Is there a clear statement?

"Data Minimization Principle"

- the data used shall be
  - ➪ *adequate*
  - ➪ *relevant*
  - ➪ and *limited*

  to what is necessary for achieving the purpose for which the data is processed

when developing AI tools...

- may be difficult to define the purpose
  - ➪ is it possible to predict what the algorithm will really learn

when developing AI tools...

- may be difficult to define the purpose
  - ➩ is it possible to predict what the algorithm will really learn
- the purpose may also be changed
  - ➩ the machine learns and develops

when developing AI tools...

- may be difficult to define the purpose
  - ➩ is it possible to predict what the algorithm will really learn
- the purpose may also be changed
  - ➩ the machine learns and develops
- examine the intended area of application

when developing AI tools...

- may be difficult to define the purpose
  - ➭ is it possible to predict what the algorithm will really learn
- the purpose may also be changed
  - ➭ the machine learns and develops
- examine the intended area of application
- document what you did

"Transparent Processing Principle"

- provide data subjects with process details

“Transparent Processing Principle”

- provide data subjects with process details
- data subjects must be informed about how the information will be used

"Transparent Processing Principle"

- provide data subjects with process details
- data subjects must be informed about how the information will be used
- the information must be easily available and be written in a clear and comprehensible language

when developing AI tools...

- black box approach
  - ➯ possible to explain how information is correlated and weighted in a specific process?

when developing AI tools...

- black box approach
  - ➪ possible to explain how information is correlated and weighted in a specific process?

- information about the model may reveal commercial secrets and intellectual property rights

when developing AI tools...

- black box approach
  - ➯ possible to explain how information is correlated and weighted in a specific process?
- information about the model may reveal commercial secrets and intellectual property rights
- *in general:*
  ➯ the transparent processing principle strikes with full force!

Are we lost?

in practice...

- the right to an explanation does not appear in the GDPR

  ✎ A. Burt "Is there a right to explanation for machine learning in the GDPR?"

  ✎ S. Wachter "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR"

in practice...

- the right to an explanation does not appear in the GDPR

  ✎ A. Burt "Is there a right to explanation for machine learning in the GDPR?"

  ✎ S. Wachter "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR"

- the decision must be explained in such a way that the data subject is able to understand the result

in practice...

- the right to an explanation does not appear in the GDPR

  ✎ A. Burt "Is there a right to explanation for machine learning in the GDPR?"

  ✎ S. Wachter "Why a Right to Explanation of Automated Decision-Making Does Not Exist in the GDPR"

- the decision must be explained in such a way that the data subject is able to understand the result

- not necessarily means to open the black box, *but* enable the data subject to understand why a particular decision was reached

  ✎ S. Wachter "Counterfactual explanations without opening the black box: automated decisions and the GDPR"

“Controlling” Algorithms

Who would “control” all these things?

The (responsible) Data Protection Authority

- can conduct investigations

The (responsible) Data Protection Authority

- can conduct investigations
- may ask for all the information needed to perform the task

The (responsible) Data Protection Authority

- can conduct investigations
- may ask for all the information needed to perform the task
- be given access to
  - ➩ premises
  - ➩ data processing equipment and means
  - ➩ the personal data that is being processed

Important Authorities for us

- The Institutes Information Security Officer

Important Authorities for us

- The Institutes Information Security Officer
- The Fraunhofer Data Protection Commissioner

Important Authorities for us

- The Institutes Information Security Officer
- The Fraunhofer Data Protection Commissioner
- The Bavarian State Data Protection Institution

Important Authorities for us

- The Institutes Information Security Officer
- The Fraunhofer Data Protection Commissioner
- The Bavarian State Data Protection Institution
- The German Data Protection Institution

Important Authorities for us

- The Institutes Information Security Officer
- The Fraunhofer Data Protection Commissioner
- The Bavarian State Data Protection Institution
- The German Data Protection Institution
- The European Data Protection Institution

Recommendations

always check that...

- data is not re-used for new purposes without an adequate processing basis

always check that...

- data is not re-used for new purposes without an adequate processing basis
- you do not process more personal data than needed

always check that...

- data is not re-used for new purposes without an adequate processing basis
- you do not process more personal data than needed
- measures are in place to ensure fair treatment

always check that...

- data is not re-used for new purposes without an adequate processing basis
- you do not process more personal data than needed
- measures are in place to ensure fair treatment
- data subjects are informed as required by law

Some Ideas to start...

- *Garbled Circuits*

  ✎ https://ieeexplore.ieee.org/document/4568207

- *Homomorphic Encryption*

  ✎ http://homomorphicencryption.org

- *Differential Privacy*

  ✎ https://arxiv.org/abs/1412.7584

- *Federated Learning*

  ✎ https://research.googleblog.com/2017/04/federated-learning-collaborative.html

- *SecureML*

  ✎ https://ieeexplore.ieee.org/document/7958569

- *DeepSecure*

  ✎ https://ieeexplore.ieee.org/document/8465894

- *Explainable AI*

  ✎ https://www.darpa.mil/program/explainable-artificial-intelligence

- *LIME*

  ✎ https://www.oreilly.com/learning/introduction-to-local-interpretable-model-agnostic-explanations-lime

Conclusion

GDPR Principles to Remember...

- **fairness and discrimination**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**
- **data minimisation**

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**
- **data minimisation**
- **transparency and the right to be informed**

☺

GDPR Principles to Remember...

- **fairness and discrimination**
- **purpose limitation**
- **data minimisation**
- **transparency and the right to be informed**

Thank you for your attention!!