GDPR for Back Office

Frankfut, 4.12.2018

Udo Milkau, Chief Digital Officer, Transaction Banking
DZ BANK AG, Frankfurt

Agenda

1. The GDPR – Half Way to a Data Ownership Right
2. Robotics and RPA - Governance of Automated Decisions
3. Blockchains and the Right to be Forgotten
4. Algorithms and AI - Explicability as Challenges

Harmonisation across Europe vs. Data Protection Authorities (DPA): The Strange Case of Doorbell Nameplates at a German Federal DPA

TLfDI Thüringer Landesbeauftragter für den Datenschutz und die Informationsfreiheit

Pressemitteilung

Klingelschilder - ein Fall für die Datenschutz-Grundverordnung!

Erfurt, 19.10.2018

Derzeit herrscht in den Medien im Hinblick auf die Namensnennung auf Klingelschildern und Briefkästen große Verunsicherung. Aus diesem Anlass erläutert der Thüringer Landesbeauftragte für den Datenschutz (TLfDI) die Rechtslage:

Source: https://www.tlfdi.de/mam/tlfdi/presse/pm_klingelschilder.pdf

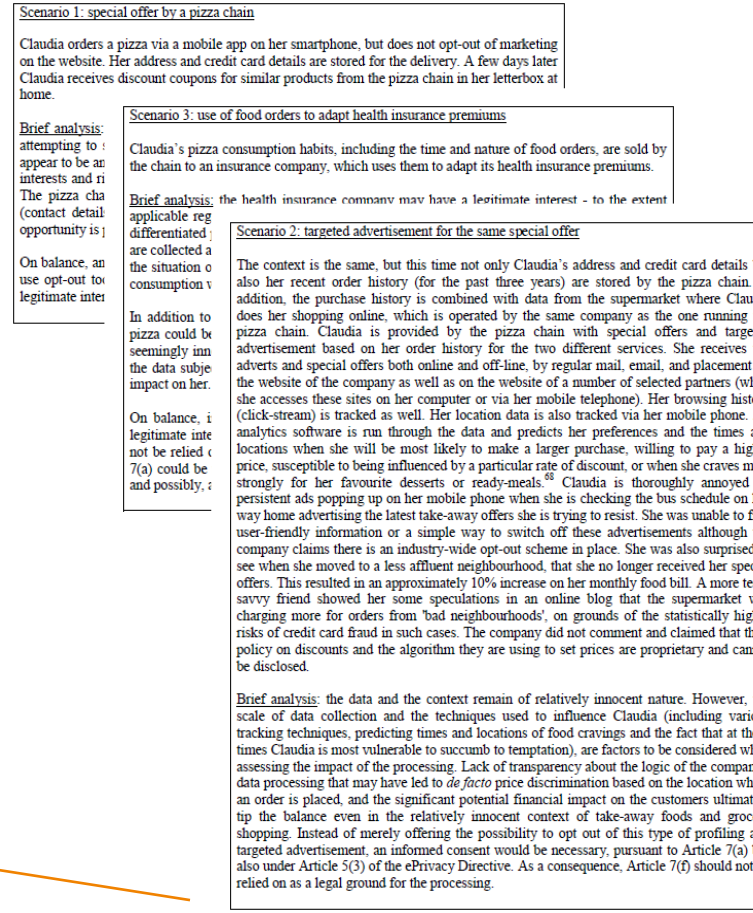
Art. 6 GDPR: Lawfulness of Processing – an Example for Marketing

1. the data subject has given consent to the processing of his or her personal data for one or more specific purposes
2. 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
3. processing is necessary for compliance with a legal obligation to which the controller is subject
4. processing is necessary in order to protect the vital interests of the data subject or of another natural person
5. 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
6. 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

Legitimate Interests – GDPR recital 47

- The legitimate interests of a controller … may provide a legal basis for processing […]
- Such legitimate interest could exist for example where … the data subject is a client or in the service of the controller. […]
- The processing of personal data strictly necessary for the purposes of preventing fraud also constitutes a legitimate interest of the data controller concerned.
- The processing of personal data for direct marketing purposes may be regarded as carried out for a legitimate interest.

Art. 29 Working Party* – Opinion 06/2014 on the notion of legitimate interests of the data controller (9.4.2014; * now: EDPB)



Scenario 1: special offer by a pizza chain

Claudia orders a pizza via a mobile app on her smartphone, but does not opt-out of marketing on the website. Her address and credit card details are stored for the delivery. A few days later Claudia receives discount coupons for similar products from the pizza chain in her letterbox at home.

Brief analysis: attempting to … appear to be an … interests and ri… The pizza cha… (contact detail… opportunity is …

On balance, an… use opt-out to… legitimate inter…

Scenario 3: use of food orders to adapt health insurance premiums

Claudia's pizza consumption habits, including the time and nature of food orders, are sold by the chain to an insurance company, which uses them to adapt its health insurance premiums.

Brief analysis: the health insurance company may have a legitimate interest - to the extent … applicable reg… differentiated … are collected a… the situation o… consumption …

In addition to … pizza could be … seemingly inn… the data subje… impact on her.

On balance, … legitimate inte… not be relied … 7(a) could be … and possibly, …

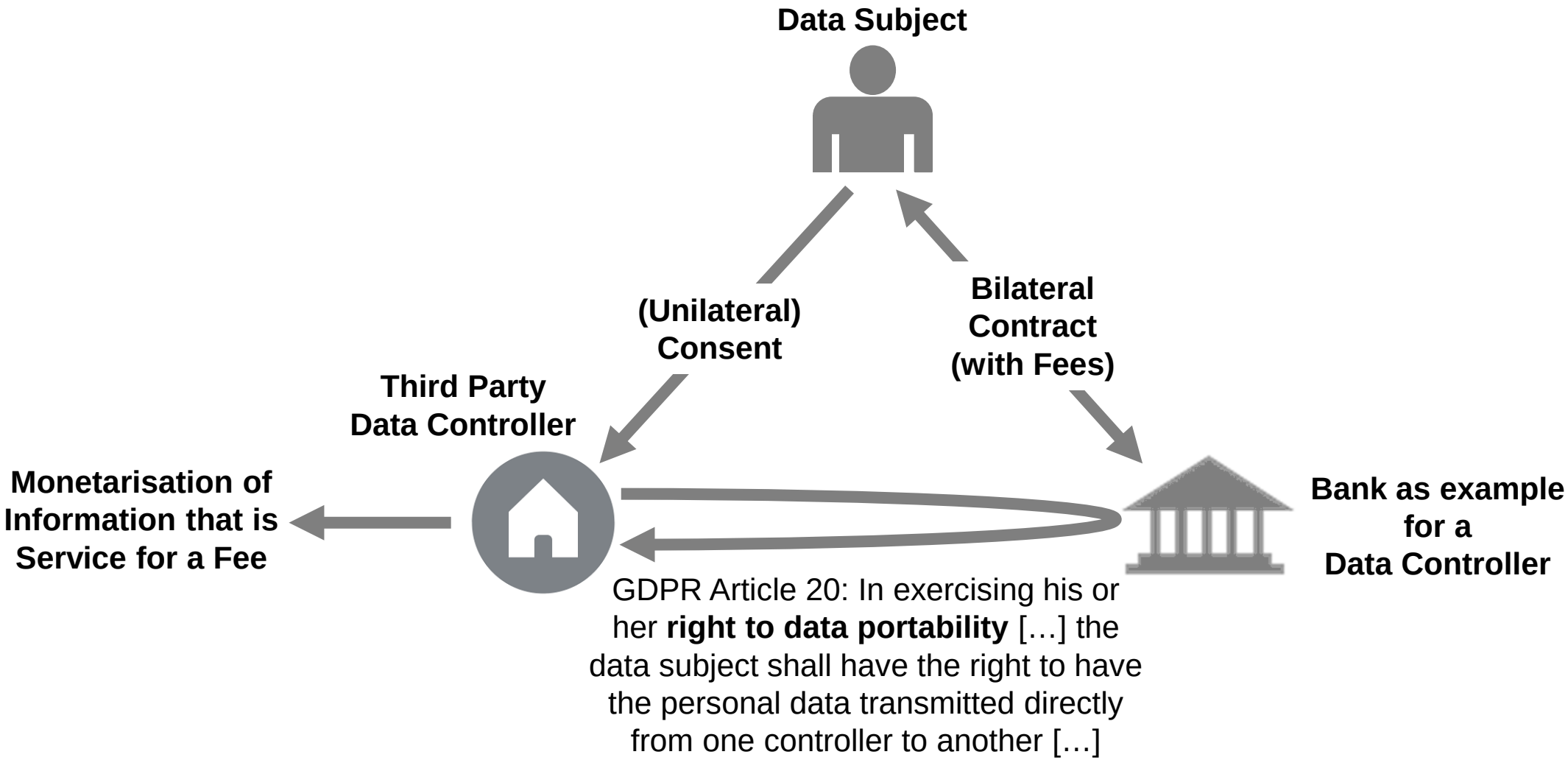
Scenario 2: targeted advertisement for the same special offer

The context is the same, but this time not only Claudia's address and credit card details … also her recent order history (for the past three years) are stored by the pizza chain. … addition, the purchase history is combined with data from the supermarket where Clau… does her shopping online, which is operated by the same company as the one running … pizza chain. Claudia is provided by the pizza chain with special offers and targe… advertisement based on her order history for the two different services. She receives … adverts and special offers both online and off-line, by regular mail, email, and placement … the website of the company as well as on the website of a number of selected partners (wl… she accesses these sites on her computer or via her mobile telephone). Her browsing hist… (click-stream) is tracked as well. Her location data is also tracked via her mobile phone. … analytics software is run through the data and predicts her preferences and the times … locations when she will be most likely to make a larger purchase, willing to pay a hig… price, susceptible to being influenced by a particular rate of discount, or when she craves m… strongly for her favourite desserts or ready-meals.[68] Claudia is thoroughly annoyed … persistent ads popping up on her mobile phone when she is checking the bus schedule on … way home advertising the latest take-away offers she is trying to resist. She was unable to f… user-friendly information or a simple way to switch off these advertisements although … company claims there is an industry-wide opt-out scheme in place. She was also surprised … see when she moved to a less affluent neighbourhood, that she no longer received her spec… offers. This resulted in an approximately 10% increase on her monthly food bill. A more te… savvy friend showed her some speculations in an online blog that the supermarket … charging more for orders from 'bad neighbourhoods', on grounds of the statistically hig… risks of credit card fraud in such cases. The company did not comment and claimed that th… policy on discounts and the algorithm they are using to set prices are proprietary and can… be disclosed.

Brief analysis: the data and the context remain of relatively innocent nature. However, … scale of data collection and the techniques used to influence Claudia (including vari… tracking techniques, predicting times and locations of food cravings and the fact that at th… times Claudia is most vulnerable to succumb to temptation), are factors to be considered wl… assessing the impact of the processing. Lack of transparency about the logic of the compar… data processing that may have led to *de facto* price discrimination based on the location wh… an order is placed, and the significant potential financial impact on the customers ultimat… tip the balance even in the relatively innocent context of take-away foods and groc… shopping. Instead of merely offering the possibility to opt out of this type of profiling … targeted advertisement, an informed consent would be necessary, pursuant to Article 7(a) … also under Article 5(3) of the ePrivacy Directive. As a consequence, Article 7(f) should not … relied on as a legal ground for the processing.

DZ BANK
Die Initiativbank

Art. 20 GDPR: Right to Data Portability vs. Data Ownership Rights



Sources: i) GDPR Article 20: the General Data Protection Regulation and (ii) Article 29 Working Party (WP29) (2017) 'Guidelines on the right to data portability', adopted on 13th December, 2016/As last Revised and adopted on 5th April, 2017, WP242 rev.01

DZ BANK
Die Initiativbank

Agenda

1. The GDPR – Half Way to a Data Ownership Right
2. Robotics and RPA - Governance of Automated Decisions
3. Blockchains and the Right to be Forgotten
4. Algorithms and AI - Explicability as Challenges

Art. 22 GDPR

Article 22

Automated individual decision-making, including profiling

1. The data subject shall have the right not to be subject to a decision based solely on automated processing, including profiling, which produces legal effects concerning him or her or similarly significantly affects him or her.

2. Paragraph 1 shall not apply if the decision:

(a) is necessary for entering into, or performance of, a contract between the data subject and a data controller;

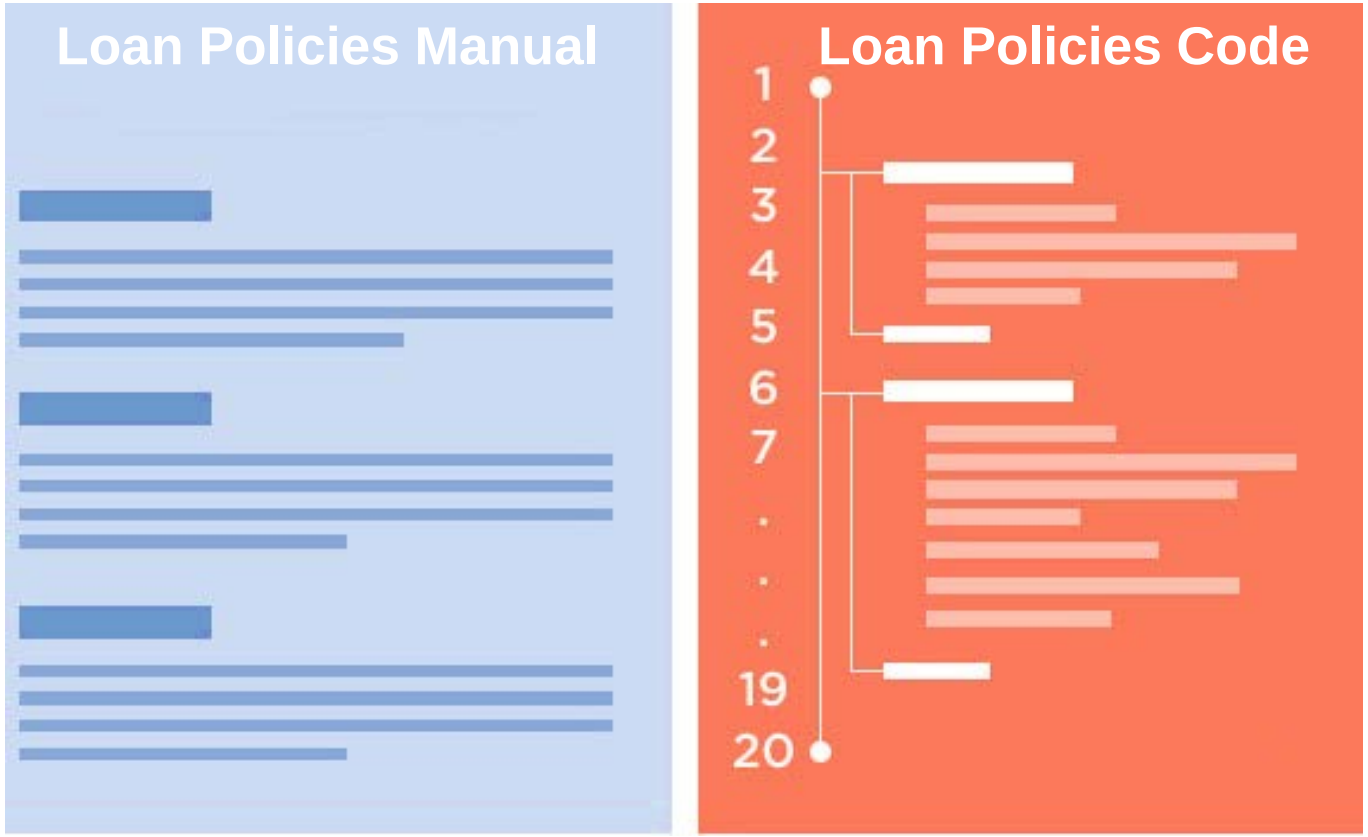
(b) is authorised by Union or Member State law to which the controller is subject and which also lays down suitable measures to safeguard the data subject's rights and freedoms and legitimate interests; or

(c) is based on the data subject's explicit consent.

L 119/14 EN Official Journal of the European Union 4.5.2016

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

What is “Automated Individual Decision-Making”?



DZ BANK
Die Initiativbank

Agenda

1. The GDPR – Half Way to a Data Ownership Right
2. Robotics and RPA - Governance of Automated Decisions
3. Blockchains and the Right to be Forgotten
4. Algorithms and AI - Explicability as Challenges

Art. 17 GDPR: Right to be Forgotten

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;

(b) the data subject withdraws consent on which the processing is based according to point (a) of Article 6(1), or point (a) of Article 9(2), and where there is no other legal ground for the processing;

(c) the data subject objects to the processing pursuant to Article 21(1) and there are no overriding legitimate grounds for the processing, or the data subject objects to the processing pursuant to Article 21(2);

(d) the personal data have been unlawfully processed;

(e) the personal data have to be erased for compliance with a legal obligation in Union or Member State law to which the controller is subject;

(f) the personal data have been collected in relation to the offer of information society services referred to in Article 8(1).

2. Where the controller has made the personal data public and is obliged pursuant to paragraph 1 to erase the personal data, the controller, taking account of available technology and the cost of implementation, shall take reasonable steps, including technical measures, to inform controllers which are processing the personal data that the data subject has requested the erasure by such controllers of any links to, or copy or replication of, those personal data.

3. Paragraphs 1 and 2 shall not apply to the extent that processing is necessary:

(a) for exercising the right of freedom of expression and information;

(b) for compliance with a legal obligation which requires processing by Union or Member State law to which the controller is subject or for the performance of a task carried out in the public interest or in the exercise of official authority vested in the controller;

(c) for reasons of public interest in the area of public health in accordance with points (h) and (i) of Article 9(2) as well as Article 9(3);

(d) for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes in accordance with Article 89(1) in so far as the right referred to in paragraph 1 is likely to render impossible or seriously impair the achievement of the objectives of that processing; or

(e) for the establishment, exercise or defence of legal claims.

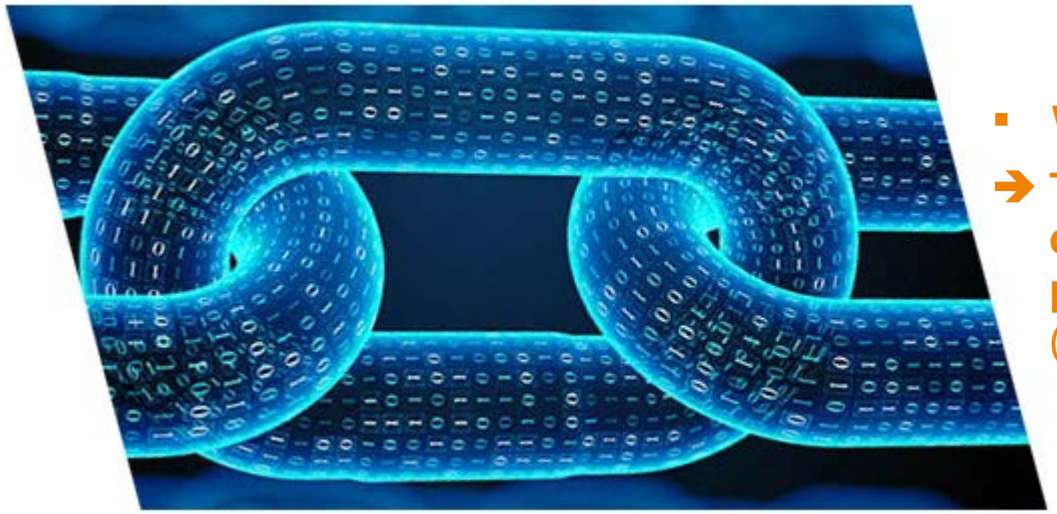
Art. 17 GDPR: Right to be Forgotten vs. Blockchain

Article 17

Right to erasure ('right to be forgotten')

1. The data subject shall have the right to obtain from the controller the erasure of personal data concerning him or her without undue delay and the controller shall have the obligation to erase personal data without undue delay where one of the following grounds applies:

(a) the personal data are no longer necessary in relation to the purposes for which they were collected or otherwise processed;



- **What is the purpose of using the blockchain?**

➔ **Traceability of a token from the beginning of the chain (recording) to the current status and prevention of duplicates**
(i.e. Byzantine Generals Problem and Double Spending Problem)

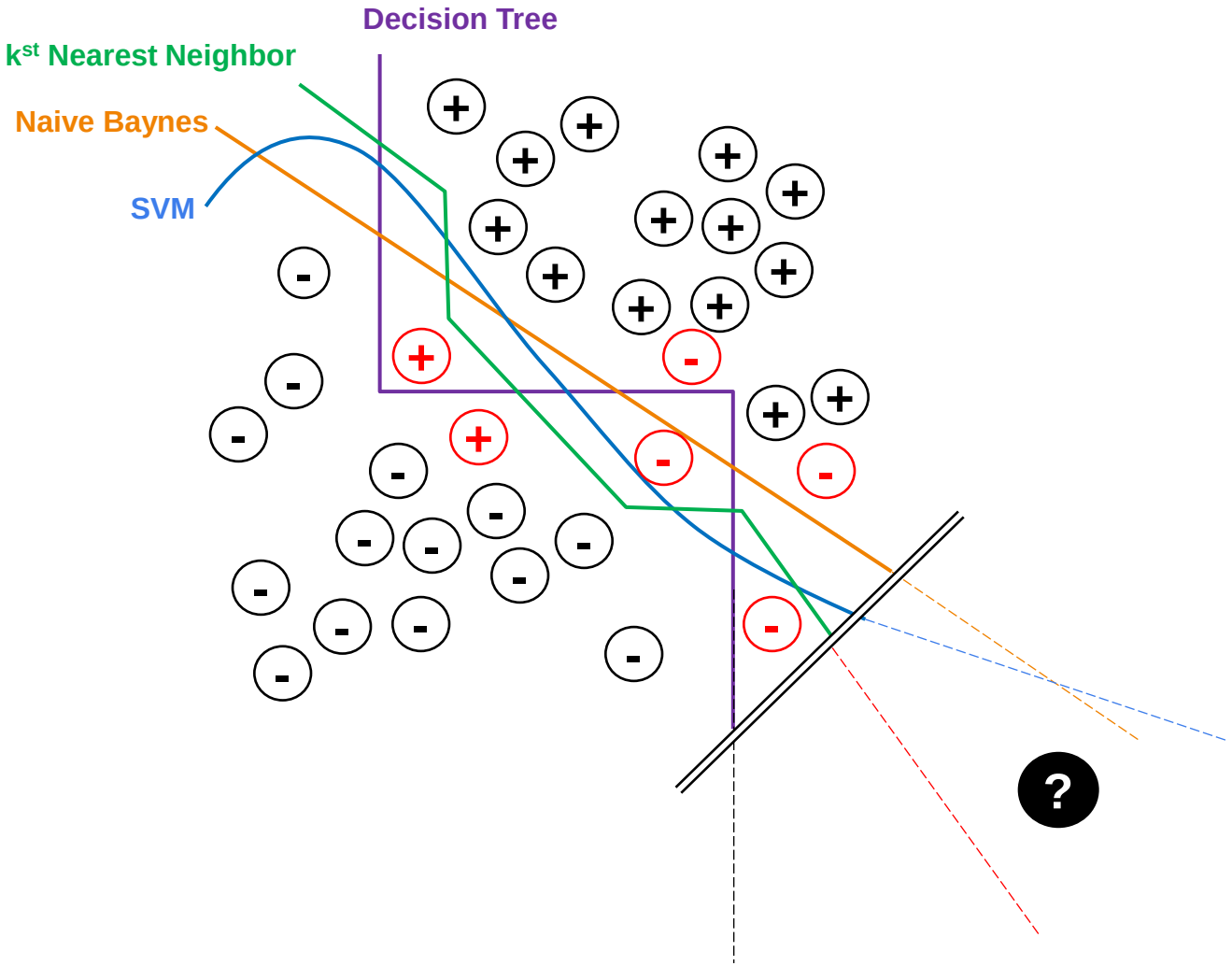
Agenda

1. The GDPR – Half Way to a Data Ownership Right
2. Robotics and RPA - Governance of Automated Decisions
3. Blockchains and the Right to be Forgotten
4. Algorithms and AI - Explicability as Challenges

Again Art. 22 GDPR

(71) The data subject should have the right not to be subject to a decision, which may include a measure, evaluating personal aspects relating to him or her which is based solely on automated processing and which produces legal effects concerning him or her or similarly significantly affects him or her, such as automatic refusal of an online credit application or e-recruiting practices without any human intervention. Such processing includes 'profiling' that consists of any form of automated processing of personal data evaluating the personal aspects relating to a natural person, in particular to analyse or predict aspects concerning the data subject's performance at work, economic situation, health, personal preferences or interests, reliability or behaviour, location or movements, where it produces legal effects concerning him or her or similarly significantly affects him or her. However, decision-making based on such processing, including profiling, should be allowed where expressly authorised by Union or Member State law to which the controller is subject, including for fraud and tax-evasion monitoring and prevention purposes conducted in accordance with the regulations, standards and recommendations of Union institutions or national oversight bodies and to ensure the security and reliability of a service provided by the controller, or necessary for the entering or performance of a contract between the data subject and a controller, or when the data subject has given his or her explicit consent. In any case, such processing should be subject to suitable safeguards, which should include specific information to the data subject and the right to obtain human intervention, to express his or her point of view, to obtain an explanation of the decision reached after such assessment and to challenge the decision. Such measure should not concern a child.

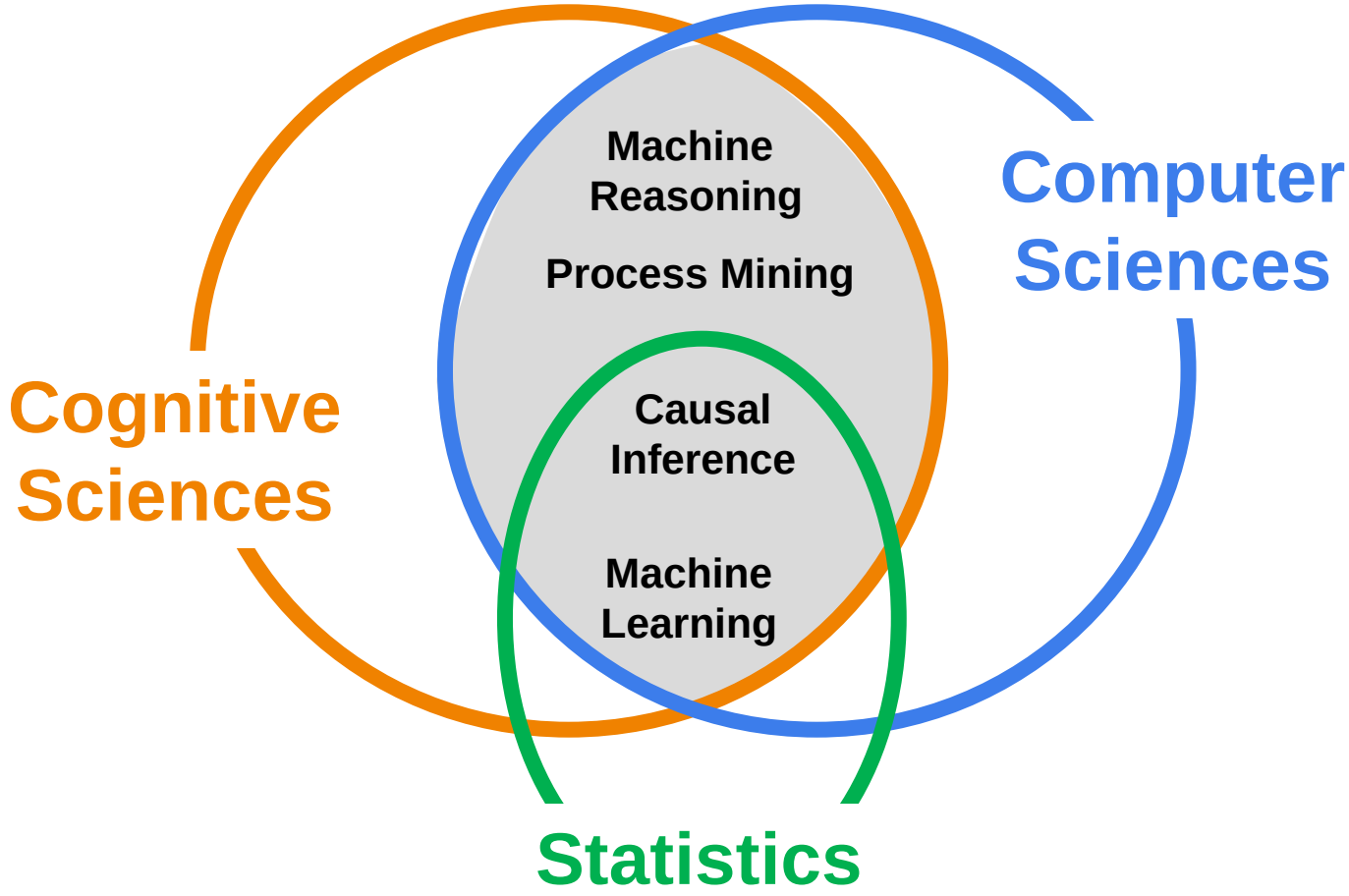
The Generic Problem of Explicability of Statistical Classifiers …



Angelehnt an: Domingos, Pedro. 2012. A few useful things to know about machine learning. Communications of the ACM CACM Homepage archive, Volume 55 Issue 10, pp 78-87.
Anmerkung: Siehe auch: Im Krankenhaus fällt Watson durch (F.A.S. vom 3.6.2018)

DZ BANK
Die Initiativbank

… Especially Machine Learning is Statistics!



DZ BANK
Die Initiativbank

Conclusion

1. A Digital Economy Needs a Data Ownership Right
2. Misunderstanding of “Decisions” and Man/Machine Complement
3. Blockchains as an Example for (logical) Erasure vs (technical) Deletion
4. Misunderstanding of Explicability in all Statistical Classifications