Analysis and constructive criticism of the official DPIA of the German Corona-Warn-App (CWA)

Rainer Rehak, *Christian R. Kühne, Kirsten Bock*
24h of June 2022, APF 2022
Koźminski University, Warsaw, Poland

1) Introduction and background
2) CWA functionality & official DPIA
3) Critique of official DPIA
4) Impact and discussion

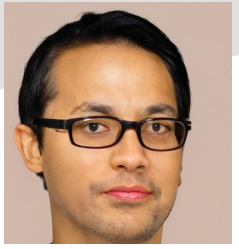
weizenbaum institut

10th Annual Privacy Forum

WZB
Wissenschaftszentrum Berlin für Sozialforschung

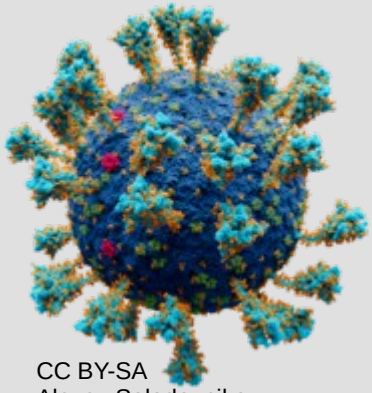
Authors

- Rainer Rehak, Weizenbaum Institute for the Networked Society – the German internet institute / Berlin Social Science Center (WZB), CS/Philosophy
- Christian R. Kühne, Forum Computer Scientists für Peace and Societal Responsibility (FIfF), CS/Social Sciences
- Kirsten Bock, Independent Centre for Privacy Protection Schleswig-Holstein (ICPP), Law/Philosophy



weizenbaum institut

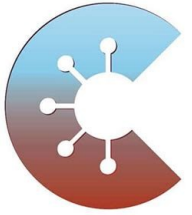
Introduction



- SARS-CoV-2 pandemic situation
  - Dangerous infectiousness before symptoms
- Manual to digital automated contact tracing
- German Ministry of Health -> T-Systems and SAP
- Corona-Warn-App came June 16, 2020
  - DPIA 10h before that
- We made a DPIA given public information in April 2020

The Coron-Warn-App

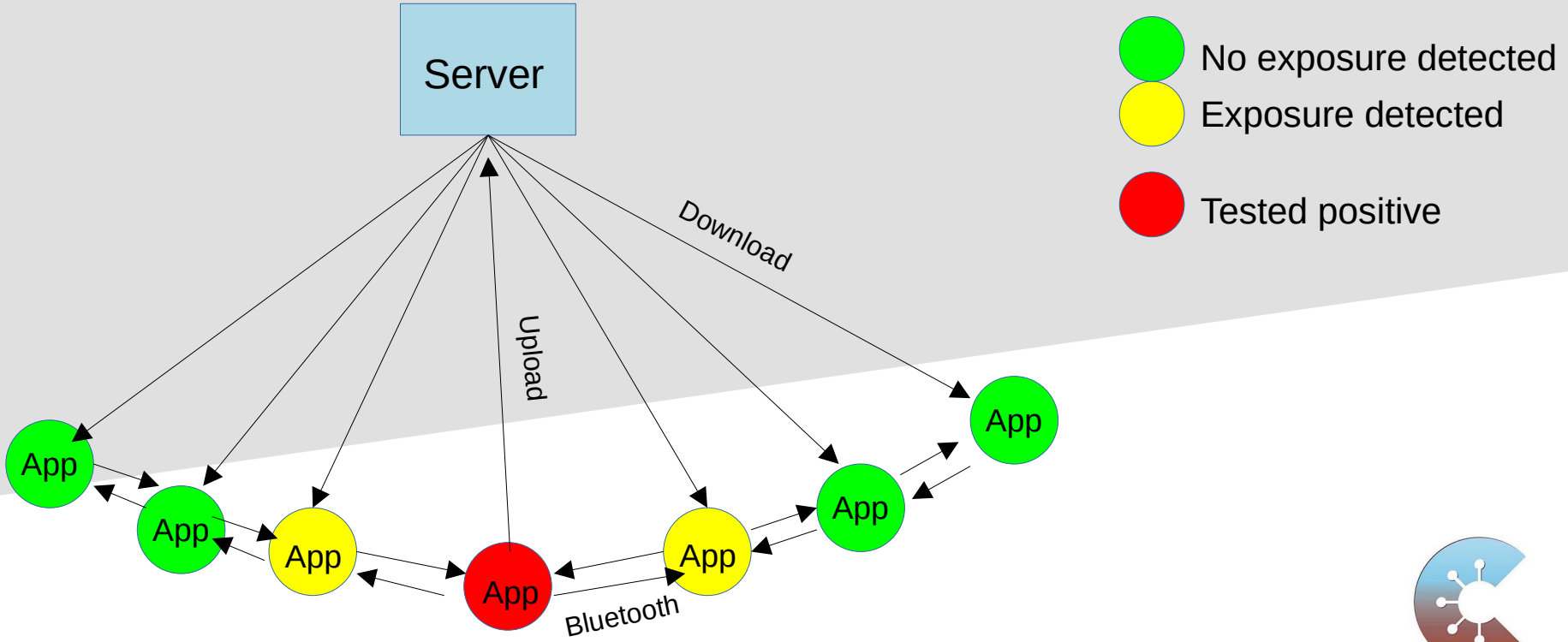
- BTLE-based, client-server arch, GAEN/ENF infrastructure
- Sending out regularly changing temporary identifiers (pseudonymous tempIDs), stored locally
- Receiving the temporary identifiers (tempIDs) of others, stored locally
- Regular download of all uploaded tempIDs
- Local matching, local warning for self-quarantine
- Upon positive test, upload of all IDs sent



CORONA
WARN-APP

weizenbaum
institut

CWA Architecture



weizenbaum institut

CORONA WARN-APP

Official DPIA – summary

- Describes the app
- Processing of health data
- Main attackers are hackers and deanonymising attempts
- Consent is acceptable as legal basis
- GAEN is a unilateral construct, but Google and Apple are trustworthy providers
- IP addresses are a problem

weizenbaum institut

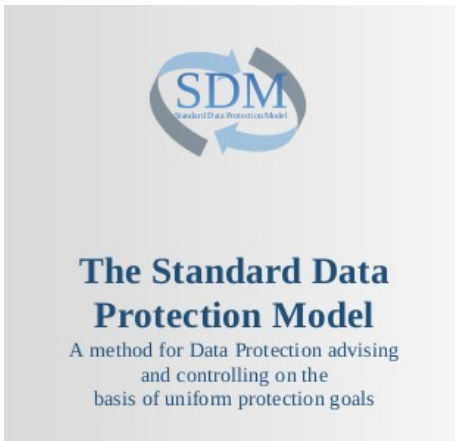
DPIA critique

- Analysed mainly "the App", not the processing (e.g. high risk: server)
- No mention of protecting (all) fundamental rights and freedoms
- Mixup of data protection and IT security
  - Main attacker is the organisation itself, then infra, then third parties
- Data processed locally or "offline" are not considered part of the controller's processing activity
- No systematic description of interfaces or communication
- No mitigation for IP address processing
- Difference of (actual) voluntariness and (legal) consent not discussed
- Generally so systematic approach used
- Discussion of responsibility and purpose limitation of processing missing

weizenbaum institut

Proper DPIA acc. to SDM

- Article 35 GDPR (Data Protection Impact Assessment)
  - Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data
- DPIA is a systematic and structured risk assessment
- Standard Data Protection Model / SDM (referenced by EDPB “Accountability on the ground”)
  - Threshold analysis
  - Context: actors and their interests, political and technical situation
  - Purpose definitions, assumptions and use cases
  - Processing activity in detail (not all will be technical)
  - Legal analysis and responsibility structure
  - Weaknesses, vulnerabilities and risks(!) of processing activity
  - Protective measures for processing activity reg. the rights of the data subjects
  - Recommendations for data controller



weizenbaum institut

Impact

Data Protection Impact Assessment

for the Corona App

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
denian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Möo R. Ott
moto.ott@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.6 – April 29, 2020

Forum InformatikerInnen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.

Contact: dsfa-corona@fiff.de
https://www.fiff.de/dsfa-corona

- Official DPIA was improved a lot
  - New standard set (method and detail)
  - Explicitly citing us several times on key aspects
- Our DPIA was widely cited and recommended (from German DPSAs and Turkish researchers to EDRi)
  - DPIA as GDPR tool became more visible
  - Meaning of “processing” in the discussion
  - The role of platforms and software infrastructure providers

weizenbaum institut

Summary and Discussion

- Still no critical stance to GAEN in official DPIA
- Still no law recommended, consent to a Ministry required
- How could the poor quality of the official DPIA happen?
- An open & responsive process is a good process!
- DPIAs should always be public!

weizenbaum
institut

Ceterum censeo

- Good data protection theory is necessary for a good data protection practice!
- *Data protection does not protect data as sun protection does not protect the sun. Data protection protects people and society from unwanted consequences of data processing.*

Art. 1 GDPR

Subject-matter and objectives

1. This Regulation lays down rules relating to the protection of natural persons with regard to the processing of personal data and rules relating to the free movement of personal data.

2. This Regulation protects fundamental rights and freedoms of natural persons and in particular their right to the protection of personal data.

weizenbaum institut

References

- Anderson R (2008) Security Engineering: A Guide to Building Dependable Distributed Systems, Wiley India
- Article 29 Working Party (2007): Opinion 4/2007 on the concept of personal data, https://ec.europa.eu/justice/article-29/documentation/opinion-recommendation/files/2007/wp136_en.pdf
- Article 35 GDPR (Data Protection Impact Assessment), https://gdpr-info.eu/art-35-gdpr/ (accessed 14th Jan 2022)
- Bock, K.; Kühne, C.; Mühlhoff, R.; Ost, M.; Pohle, J.; Rehak, R. (2020): Data Protection Impact Assessment for the Corona App, https://arxiv.org/abs/2101.07292
- Independent Data Protection Supervisory Authorities of the Federation and the Länder (2020) The Standard Data Protection Model – A method for Data Protection advising and controlling on the basis of uniform protection goals, https://www.datenschutzzentrum.de/uploads/sdm/SDM-Methodology_V2.0b.pdf (accessed 9/9/2021)
- Kröger J L, Lutz O H, Ullrich Stefan (2021), The Myth of Individual Control: Mapping the Limitations of Privacy Self-management, http://dx.doi.org/10.2139/ssrn.3881776 (accessed 14th Jan 2022)
- Rost M (2018) Risks in the context of data protection/Risiken im Datenschutz. In: vorgänge – Zeitschrift für Bürgerrechte und Gesellschaftspolitik, 57(1/2), pp. 79–92. English version: https://www.maroki.de/pub/privacy/Rost_Martin_2019-02_Risk:_8types_v1.pdf (accessed 14th Jan 2022)
- Steinmüller W (1972) Grundfragen des Datenschutzes, Gutachten, BT-Drucksache 6/3826, German Bundestag

Thank you

Rainer Rehak
rainer.rehak@wzb.eu
0496 A3A6 DC10 9851 A09F
04A3 FF25 0994 CE9E FB45
@Rainer_Rehak

10th Annual Privacy Forum

weizenbaum institut

WZB
Wissenschaftszentrum Berlin für Sozialforschung

Our DPIA findings

1) Not analysing the app, but the whole processing
2) **Processing of personal health data and anonymising procedures**
3) Ensuring voluntariness of use
4) The problem of informed consent
5) Ensuring the ability of data subjects to intervene
6) **The role of platforms and software infrastructure providers**

Data Protection Impact Assessment

for the Corona App

Kirsten Bock
kirsten.bock@fiff.de

Christian Ricardo Kühne
denian@fiff.de

Rainer Mühlhoff
rainer.muehlhoff@fiff.de

Mötö R. Ost
moto.ost@fiff.de

Jörg Pohle
joerg.pohle@fiff.de

Rainer Rehak
rainer.rehak@fiff.de

Version 1.6 – April 29, 2020

Forum Informatiker:Innen für Frieden und gesellschaftliche Verantwortung (FIfF) e. V.

Contact: dsfa-corona@fiff.de
https://www.fiff.de/dsfa-corona

weizenbaum institut