

Wer braucht denn sowas?

Datenschutz in der Krise



Begriffsklärung „Datenschutz“

Im Sinne dieser **Verordnung** bezeichnet der Ausdruck:
„**personenbezogene Daten**“ alle Informationen, die sich auf eine **identifizierte oder identifizierbare natürliche Person** (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind;

„Ich habe doch nichts zu verbergen.“

Mindestens vier Irrtümer:

- 1) Man hat nur unredliche Dinge zu verbergen.
- 2) Ich habe nichts zu verbergen, also dürfen Sie auch nichts zu verbergen haben.
- 3) Ich habe tatsächlich nichts zu verbergen
 - 1) Ich brauche nicht darüber zu reden.
 - 2) Ich will nicht darüber reden.
 - 3) Ich darf nicht darüber reden.
- 4) Ich habe bis in alle Ewigkeit nichts zu verbergen.

Das neue Argument

Es geht um MENSCHENLEBEN!!!Eins11

(viele Mails an den CCC)

**In diesen schwierigen Zeiten scheint
uns aber die Beantwortung der
Frage, wie wir nah bei den Menschen
bleiben, wichtiger als der
Datenschutz zu sein.**

Rundschreiben des EKIR-LKA vom 16.3.2020

A propos

- Wirtschaft fordert **Lockerungen** bei Datenschutzverordnung wegen Coronakrise

Von welcher Gefahr reden wir?

- Kriminelle (greifen direkt an)
- Ermittlungsbehörden (überwachen)
- Wirtschaft (will Werbung schalten)

Gewöhnliche Kriminelle

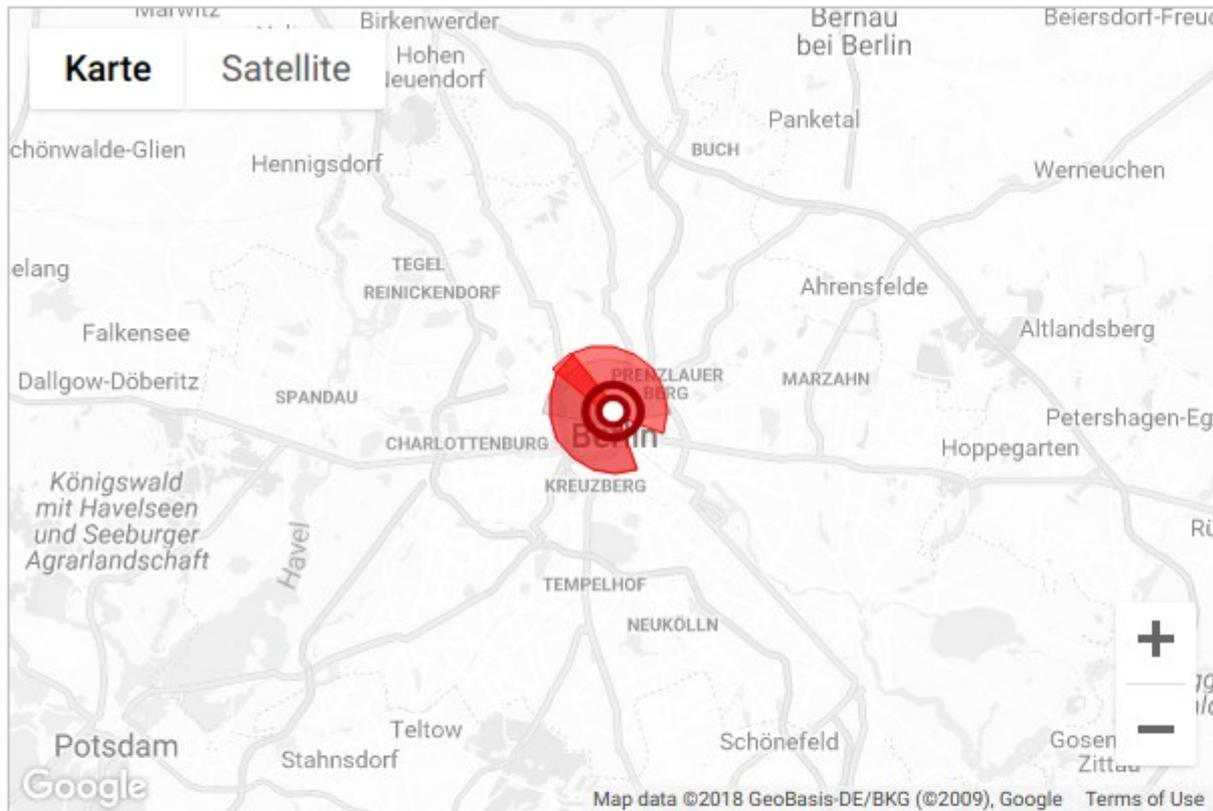
- Betreiben Phishing
- Installieren Trojanische Pferde
- Greifen Server an und saugen Nutzerdatenbanken ab
- Kaufen Passwortlisten und probieren sie aus
- Suchen Sicherheitslücken und verkaufen sie

Quelle: www.csonline.com

Ermittlungsbehörden

- Greifen Daten an Knotenpunkten (DE-CIX) ab
- Werten Metadaten aus (Vorratsdatenspeicherung)
- Installieren Trojanische Pferde (Quellen-TKÜ)
- Installieren Trojanische Pferde (Onlinedurchsuchung)
- Kaufen Sicherheitslücken auf dem Schwarzmarkt

Beispiel Vorratsdaten



Mittwoch, 2. September 2009



Malte Spitz ist am Nachmittag um 16 Uhr bei der VZ-Gruppe (SchülerVZ/StudiVZ) zu einem Gespräch über Daten- und Verbraucherschutz (Quelle: **Twitter**)



5 eingehende Anrufe
23 ausgehende Anrufe
Gesamtdauer: 0h 57min 40s



12 eingehende Nachrichten
14 ausgehende Nachrichten



Dauer der Verbindung mit dem Internet: 16h 19min 13s



Privatwirtschaft

- Installiert Apps
- Wertet Metadaten aus
- Die Nutzer liefern die Daten freiwillig (unter anderem Metadaten)

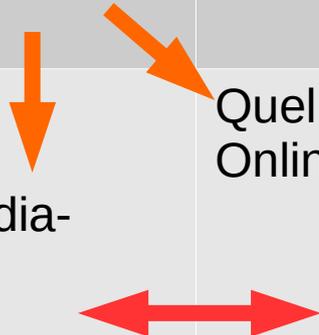
Allgemein oder gezielt?

- Allgemein
 - Man nimmt, was man bekommt
 - Geringe Trefferquote, Erfolg durch Masse
 - Abwehr relativ leicht
- Gezielt
 - Genaues Wissen über das Ziel
 - Hoher Aufwand
 - Abwehr schwer bis unmöglich

Klassische kriminelle Angriffe

- Schwache oder mehrfach verwendete Passworte
- Phishing
- Drive-by-Downloads
- Leichtfertig installierte Software

	Kriminelle	Staat	Wirtschaft
allgemein	Phishing Scam Verseuchte Mailanhänge Drive-By-Downloads Passwortlisten Trojanische Pferde Viren Fake-Hotspots	Vorratsdatenspeicherung	Big-Data-Analysen
spezifisch	Social Engineering Belauschen von WLANs Auswerten von Social-Media- Profilen	Quellen-TKÜ Online-Durchsuchung	Apps Nutzerprofile



Was geht?

- Mobilfunkanbieter haben unsere Positionsdaten
- Google erfasst Suchbegriffe und Positionsdaten
- Facebook erfasst, wann wir reden, mit wem wir reden, worüber wir reden und wie wir reden
- Schufa-Scoring erfasst nicht nur die Zahlungsmoral, sondern auch scheinbar sinnlose Daten wie die Wohngegend
- Big-Data-Analysen finden Zusammenhänge in scheinbar sinnlosen Datenbergen
- Es gibt faktisch keine größeren anonymen Finanztransaktionen mehr

Was geht?

- Kommunikationsanbieter (Internet, Telefon) wissen, wann wir wo mit wem wie lange reden.
- Gratis-Apps liefern in der Summe ein Komplettprofil
- Payback liefert Kundenprofile
- Gesundheits-Apps liefern Patientenprofile
- PNR liefern detaillierte Fluggastdatenprofile, die teilweise über Jahrzehnte gespeichert werden.

Die Android- Verwanzung

- Apps senden
Nutzerdaten
- Aus Puzzlestücken
wird beim
Drittanbieter ein
Gesamtbild
- Diebstahl-
sicherung

Beispiel Google Dashboard

The screenshot displays the Google My Activity dashboard. At the top, a blue header bar contains the text "Google Meine Aktivitäten > > Web & App". On the left side, there is a navigation menu with options: "Gruppierte Ansicht", "Einzelansicht", "Aktivitäten löschen nach", "Andere Google-Aktivitäten", "Aktivitätseinstellungen", "Mein Konto", "Hilfe", "Feedback geben", "Datenschutzerklärung", and "Nutzungsbedingungen". The main content area shows a list of activities. The first activity is from "google.com" with the search query "Gesucht nach Frank Herrmann Politiker". Below it is another search entry for "frank herrmann". A summary indicates "12 Einträge". The second activity is from "compliance-manager.net" at 14:23, accessed 2 times. The third activity is from "frischnetz.de" at 12:38, also accessed 2 times. On the right side, a "Details zum Eintrag" panel is open for the "compliance-manager.net" entry, showing it was used with the app "DB Navigator" at "Heute um 05:04" on an "Android" device, specifically a "Sony Xperia XZ". A map fragment is visible on the far right edge.

Google Meine Aktivitäten > > Web & App

2018

Gruppierte Ansicht

Einzelansicht

Aktivitäten löschen nach

Andere Google-Aktivitäten

Aktivitätseinstellungen

Mein Konto

Hilfe

Feedback geben

Datenschutzerklärung

Nutzungsbedingungen

google.com

Gesucht nach Frank Herrmann Politiker

Details • Google-Suche

Gesucht nach "frank herrmann"

Details • Google-Suche

→ 12 Einträge

14:23

compliance-manager.net 2-mal

12:38

frischnetz.de 2-mal

Details zum Eintrag

DB Navigator

Verwendet: DB Navigator

Details

Heute um 05:04

Android

DB Navigator

Sony Xperia XZ

A propos Google

[heise.de](https://www.heise.de), 1.9.2018: Google übermittelt Mastercard-Transaktionsdaten an seine Online-Werbekunden



(Bild: dpa, Oliver Berg/Archiv)

Im vergangenen Jahr konnten Werbekunden von Google prüfen, ob sich der Klick auf eine Online-Anzeige mit einem Offline-Kauf per Kreditkarte in einem US-Einzelhandelsgeschäft verknüpfen ließ. Dazu haben Google und Mastercard eine bislang geheim gehaltene Vereinbarung getroffen: Google kauft massenhaft Kreditkarten-Transaktionsdaten von Mastercard und korreliert sie mit den Klicks seiner Benutzer auf Online-Werbung. Darüber berichtet die Nachrichtenseite Bloomberg.

Mastercard-Kunden waren nicht informiert

Dieses Tracking soll ohne Kenntnis der Karteninhaber stattgefunden haben, weil

Was geht nicht?

- Instagram und Facebook können zwar heimlich auf das Mikrofon zugreifen, aber es gibt keine belastbare Untersuchung, dass dies auch wirklich geschieht – im **Gegenteil**.
- Der auf einigen Smartphone-Akkus verbaute NFC-Chip ist kein **verstecktes Mikrofon**.

Digitalisierung im Lockdown



Zwischen den Extremen

Sperrt
uns ein!

Ich will
hier raus!

Lass dich überraschen

- Die Pandemie hat die meisten Firmen, (Hoch-)Schulen, Veranstaltungs- und Seminarhäuser unvorbereitet erwischt.
- Folge: Wir haben improvisiert.

Improvisation

- Arbeit am eigenen Rechner statt im Büro
- Dateiaustausch per Dropbox
- Kollaboratives Arbeiten mit Google Docs
- Chats per Whatsapp
- Videokonferenzen per Zoom

Wenn die Kirche improvisiert

„So einfach die Umsetzung bei WhatsApp ist, so problematisch ist deren datenschutzrechtliche Dimension. Alternativ ließen sich zwar datenschutzrechtlich unbedenkliche Messengerdienste nutzen, die aber nur gering verbreitet sind und deren Nutzung für die meisten User zunächst ungewohnt ist. Die parallele Nutzung zweier Messengerdienste (WhatsApp und ein anderer unbedenklicher Dienst) empfiehlt sich nicht.“

Was ich gerne hätte

- Open Source
- Server in der EU oder auf eigenem Server installierbar
- Aufruf im Browser ohne Zusatzsoftware und auch mit eingeschränkten Rechten (unter Windows)
- DSGVO-konform
- Ende-zu-Ende-Verschlüsselung
- 20 bis 30 Personen in einer Konferenz
- Teilnahme ohne Anmeldung möglich

Was ist mit Zoom?

- Der **aktuelle Stand** bei Zoom
- Falschangaben bei Datenweiterleitung an Facebook und E2E-Verschlüsselung
- In der Gratisversion Datenverkehr über die USA
- Mehrere Sicherheitslücken im Client, bei Installation unter MacOS Aushebeln von Sicherheitsmechanismen
- Zoom-Bombing und Passworte auf dem Schwarzmarkt
- Fehler schnell behoben, Version 5.0 ausgerollt, der Vertrauensverlust bleibt
- Risiko beim AV-Verhältnis

Adobe Connect	USA	Privacy Shield	Auf Anfrage	Link
AnyMeeting	USA	Privacy Shield	Auf Anfrage	Link
Arkadin	DE	–	Auf Anfrage	Link
Cisco WebEx	USA	Privacy Shield und Standardschutz	In SCC enthalten	Link
ClickMeeting	PI	–	Im Kundenkonto	Link
Discord	USA	Privacy Shield	nicht angeboten	Link
edudip	De	–	Im Kundenkonto	Link
fastviewer	De	–	Link	Link
Google Hangouts	USA	Privacy Shield	Link (automatisch mit AGB akzeptiert)	Link
GoToMeeting	USA	Privacy Shield	Link	Link
Intercall Unified	USA	Privacy Shield	Link	Link
meetgreen	De	–	Auf Anfrage	Link
meetyoo	De	–	Auf Anfrage	Link
Microsoft Teams	USA	Privacy Shield	Link	Link, Link
Skype for Business	USA	Privacy Shield	Link	Link, Link
Slack	USA	Privacy Shield	Link	Link
TeamViewer	De	Nicht angeboten	Auf Anfrage	Link
Telekom – Connect	De	–	Link	Link
Twitch	USA	–	nicht angeboten	Link
Whereby	USA	Anerkanntes Datenschutzniveau, Standardschutz	In SCC enthalten (automatisch mit AGB akzeptiert)	Link
Zoom	USA	Privacy Shield und Standardschutz	In SCC enthalten	Link

Verschiedene Anbieter



- **Vergleichsmatrix** der GDD
- **Ende-zu-Ende-Verschlüsselung?**
 - Zoom? Vermutlich nicht
 - GoToMeeting? Nein
 - **WebEx? „Auf Anfrage“**
 - Blizz? Vermutlich nicht.
 - Skype? Vermutlich nicht
 - Teams? Vermutlich nicht
 - Meet? Vermutlich nicht
 - Lifesize? Vermutlich nicht
 - Big Blue Button? Nein
 - **Jitsi? Nur bei 1:1-Sitzungen**

Wiederholendes Muster

- Unter Handlungsdruck greifen wir zur ersten sich bietenden Lösung
- Das ist nicht unbedingt die langfristig beste
- Hat sich der Schnellschuss erst etabliert, will keiner mehr etwas daran ändern.
- Beispiel QWERTZ-Tastaturen

Beispiel Corona-App

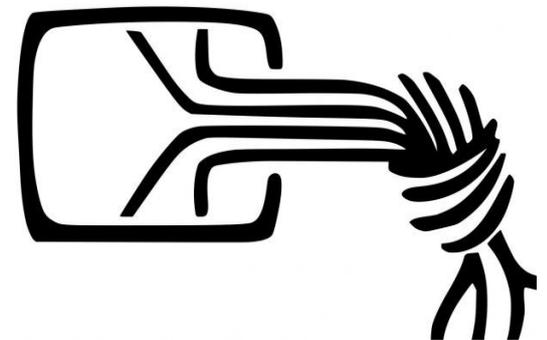
- Erste Idee: Alle Smartphones per GPS erfassen
- Zweite Idee: Funkzellenabfrage
- Intermezzo: RKI-Datenspende-App
- Dritte Idee: Bluetooth
 - zentrale Datensammlung
 - dezentral auf den Endgeräten
 - Pflicht
 - freiwillig
 - „Anreize“
 - Quarantäne-Überwachung



10 Prüfsteine des CCC

I. Gesellschaftliche Anforderungen

- 1) Epidemiologischer Sinn & Zweckgebundenheit
- 2) Freiwilligkeit & Diskriminierungsfreiheit
- 3) Grundlegende Privatsphäre
- 4) Transparenz & Prüfbarkeit



10 Prüfsteine des CCC

II. Technische Anforderungen

- 5) Keine zentrale Entität, der vertraut werden muss
- 6) Datensparsamkeit
- 7) Anonymität
- 8) Kein Aufbau von zentralen Bewegungs- und Kontaktprofilen
- 9) Unverkettbarkeit
- 10) Unbeobachtbarkeit der Kommunikation



Beispiel Namenslisten

- in NRW **freiwillig**
„Kundenkontaktdaten der Gäste sowie Zeiträume des Aufenthaltes in der Innen- und Außengastronomie sind für jede Tischgruppe mittels einfacher, auf den Tischen ausliegender Listen (einschließlich **Einverständniserklärung** zur Datenerhebung) zur Ermöglichung einer Kontaktpersonennachverfolgung zu erheben und durch die Inhaberin/den Inhaber, unter Wahrung der Vertraulichkeit, gesichert für 4 Wochen aufzubewahren und anschließend sicher zu vernichten.“
- auf **Kundgebungen** Pflicht – oder doch nicht?
- in Gottesdiensten der ev. Kirche Pflicht



Was tun?

- Gute Passworte
- Festplatte verschlüsseln
- Backups
- Vorsicht bei unbekannter Software
- Vorsicht in offenen WLANs
- Weg von den großen Datensammlern, hin zu Unternehmen mit anderem Geschäftsmodell (z.B. Posteo als Mailanbieter)
- Vor allem aber: politischen Einfluss ausüben

Zum Weiterlesen

- Malte Spitz: [Was macht ihr mit meinen Daten?](#)
- Katharina Nocun: [Die Daten, die ich rief](#)
- [Daten als Ware](#) – Spaß und Kurzweil im Überwachungsstaat
- [Cryptoparty](#) Köln-Bonn
- Cryptoparty [international](#)
- Linkliste zur [DSGVO](#)
- Verschiedene Messenger im [Vergleich](#)