EMPRI-DEVOPS

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

TRAPEZE

Horizon 2020 European Union funding for Research & Innovation

Beschäftigtendatenschutz bei Einführung neuer Software im Unternehmen – Ansätze aus der Forschung

Sommerakademie
am 12. September 2022
in Kiel

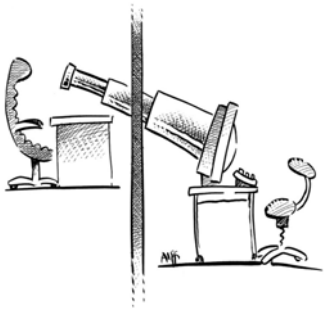
Matti Henning
0431 988-1225
ULD65@datenschutzzentrum.de
https://www.datenschutzzentrum.de/

ULD
Unabhängiges Landeszentrum für Datenschutz Schleswig-Holstein

Inferenzanalyse, Metadaten und Angreifermodell

Inferenzanalysen zu Beschäftigten:

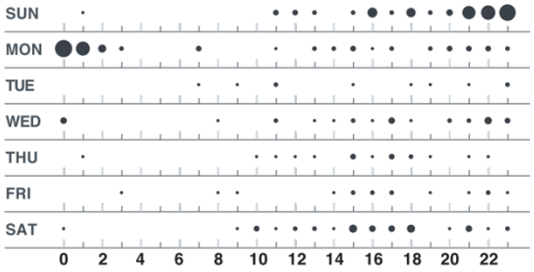
- Abschätzung der Risiken für die informationelle Selbstbestimmung der Beschäftigten
- Mittels gängiger Inferenz-Verfahren wurden repräsentativ gewonnene Datensätze aus DevOps-Tools (Development and Operations = Vorgänge) untersucht
- Fragestellung: Welche Aussagen lassen sich aus den Metadaten über Leistung und Verhalten der Beschäftigten ableiten?



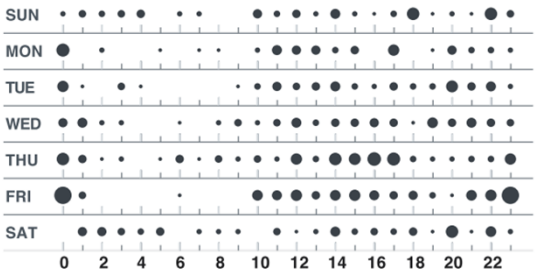
Inferenzanalyse, Metadaten und Angreifermodell

Beispiel Rückschlüsse auf die Arbeitsweise aus Timestamps von Änderungen

Wochenend-Projekt, das aber auch während der Arbeitszeit betreut wird:



Entwickler unter Zeitdruck, muss am Wochenende Arbeit nachholen:



Quelle: Radcliffe, D.: „What does your GitHub Punch-Card Graph say about You?" Medium, http://t1p.de/pmc2

Inferenzanalyse, Metadaten und Angreifermodell

Beispiel Rückschlüsse auf die Arbeitsweise aus Timestamps von Veröffentlichungen

Eine unterhaltsame Auf-den-Punkt-Einführung zum „Potential" (=Risiken) von Inferenzanalysen:

SpiegelMining: Wer, wann, was, mit wem? Das soziale Netz der SpiegelOnline-Redakteure

Quelle: D. Kriesel, „Spiegel Mining", Vortrag 33C3, https://www.dkriesel.com/spiegelmining

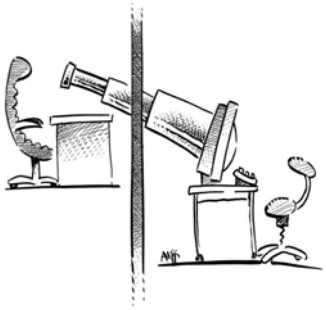
Video: https://media.ccc.de/v/33c3-7912-spiegelmining_reverse_engineering_von_spiegel-online#t=1926

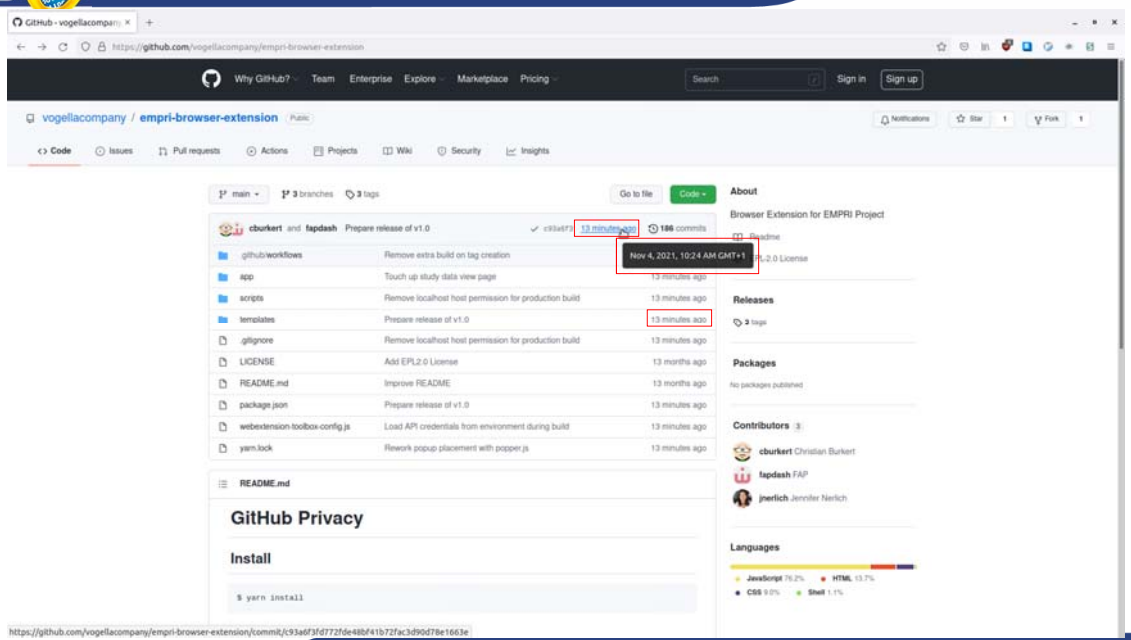
Inferenzanalyse, Metadaten und Angreifermodell

Metadaten:

- „Daten über Daten"
- Können personenbezogen oder personenbeziehbar sein
- Anwendung des Telekommunikation-Telemedien-Datenschutz-Gesetz (TTDSG) und/oder der DSGVO?
- Beispiel: Zeitstempel (timestamps) in Softwareanwendungen

  Sie reichern in Web-Anwendungen an vielen Stellen die in der Web-UI dargestellte Information an, indem sie eine zeitliche Einordnung des dargestellten Ereignisses oder der dargestellten Nutzerinteraktion für den Betrachter ermöglichen





Inferenzanalyse, Metadaten und Angreifermodell

Angreifermodell:

Wer kann potenzieller „Angreifer" sein?

- **Arbeitgeber**
- **Vorgesetzte**
- **Kollegen**

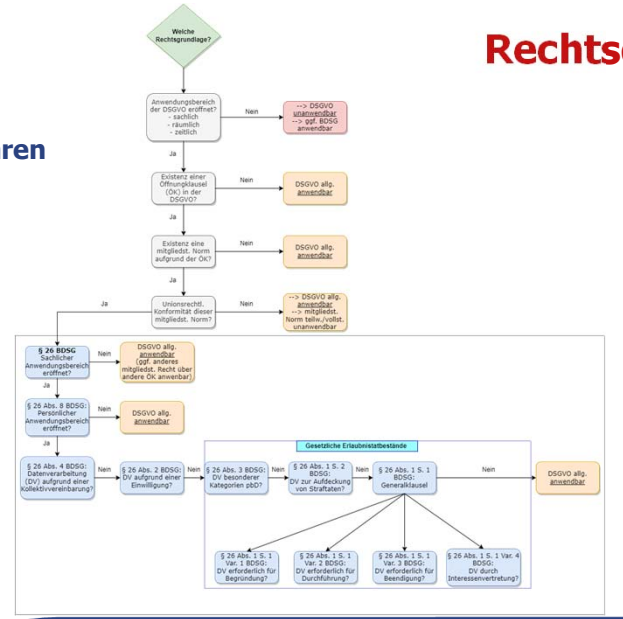
Angriffe:

Wie können Angreife aussehen?

- **Herausgreifen-Können (singling out)**
- **Verkettung (linkage)**
- **Schlussfolgerungen (inference)**

Rechtsgrundlagen

Ermittlung der anwendbaren Rechtsgrundlage



Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG

- Einordnung am Beispiel von Softwareentwicklern -

Beschäftigte sind gem. § 26 Abs. 8 BDSG:

- Arbeitnehmerinnen und Arbeitnehmer einschließlich Leiharbeiterinnen und Leiharbeiter
- Auszubildende
- Teilnehmerinnen und Teilnehmer an Leistungen zur Teilhabe am Arbeitsleben oder zur Abklärung der beruflichen Eignung oder Arbeitserprobung
- Beschäftigte in anerkannten Werkstätten für behinderte Menschen
- Jugend- oder Bundesfreiwilligendienstleistende
- Arbeitnehmerähnliche Beschäftigte (Merkmal: wirtschaftlich unselbstständig)
- Beamtinnen und Beamte, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten sowie Zivildienstleistende
- Bewerberinnen und Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist

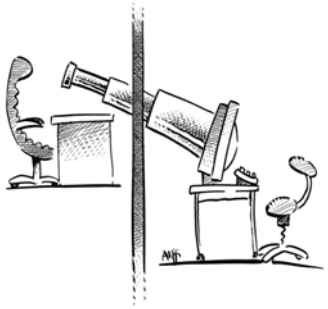
ULD www.datenschutzzentrum.de

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG

- Einordnung am Beispiel von Softwareentwicklern -

- Der persönliche Anwendungsbereich entscheidet bereits zu Beginn der Prüfung der Rechtmäßigkeit der Datenverarbeitung über die anwendbare Rechtsgrundlage
- Ist er nicht eröffnet, so findet die gesamte Norm keine Anwendung
- Folge: Anwendung der DSGVO (Artt. 6, 7, 9 DSGVO)



Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG
- Einordnung am Beispiel von Softwareentwicklern -

- Unterschiede:
  - Verarbeitung personenbezogener Daten des Entwicklers durch das Auftraggeber-Unternehmen
  - Verarbeitung personenbezogener Daten durch den Entwickler
- Entscheidend ist die rechtliche Einordnung als Arbeitnehmer oder selbstständiger freier Mitarbeiter

ULD www.datenschutzzentrum.de

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG
- Einordnung am Beispiel von Softwareentwicklern -

- Art. 88 DSGVO als Öffnungsklausel für den Beschäftigtendatenschutz
- Was sind Beschäftigte im unionsrechtlichen Sinne?
  - Keine Definition in der DSGVO oder der Rechtspr. des EuGH
  - Lediglich Rechtspr. zum Arbeitnehmer-Begriff
  - Selbstständige sollen hiervon jdf. nicht umfasst sein

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG
- Einordnung am Beispiel von Softwareentwicklern -

- Angestellte Softwareentwickler/Programmierer gelten als Arbeitnehmer und damit als Beschäftigte gem. § 26 Abs. 8 Nr. 1 BDSG
- „Echte" freie Mitarbeiter sind nicht vom persönlichen Anwendungsbereich von § 26 Abs. 8 BDSG iVm Art. 88 DSGVO umfasst

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG
- Einordnung am Beispiel von Softwareentwicklern -

- Besonderheit: „Scheinselbstständige"
  - Formal liegt ein „Freelancer-Vertrag" (Dienst-/Werkvertrag) vor
  - Tatsächlich besteht wirtschaftliche und soziale Abhängigkeit, Weisungsgebundenheit und/oder eine enge organisatorische Eingliederung in das Auftraggeber-Unternehmen (Verantwortlicher)

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG

- Einordnung am Beispiel von Softwareentwicklern -

- Sonderfall: „arbeitnehmerähnliche Personen", § 26 Abs. 8 Nr. 6 BDSG
  - Diese sind zwar grds. selbstständig, werden jedoch überwiegend nur für ein Unternehmen tätig
  - Folge: wirtschaftliche Abhängigkeit und dadurch bedingte soziale Schutzbedürftigkeit

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG

- Einordnung am Beispiel von Softwareentwicklern -

- Verarbeitet der Entwickler als freier Mitarbeiter selbst personenbezogene Daten, kommen verschiedene Konstellationen in Betracht:
  - Art. 29 DSGVO: „eine dem Verantwortlichen oder Auftragsverarbeiter unterstellte Person"
  - Artt. 4 Nr. 8, 28 DSGVO: Auftragsverarbeiter
  - Artt. 4 Nr. 7, 24, 26 DSGVO: Verantwortlicher oder gemeinsame Verantwortlichkeit
- Maßgeblich ist, ob bzw. inwieweit der Entwickler die Zwecke und Mittel der Datenverarbeitung im konkreten Fall selbst bestimmt

Rechtsgrundlagen

Persönlicher Anwendungsbereich des § 26 BDSG
- Einordnung von Softwareentwicklern -

- Die Datenübermittlung von Beschäftigtendaten des Verantwortlichen an den Freien Mitarbeiter erfordert eine eigenständige Rechtsgrundlage
- Diese wird i.d.R. in Art. 6 Abs.1 UAbs. 1 lit. f) DSGVO zu finden sein
- Die DSGVO und das BDSG kennen kein Konzernprivileg
- Rein juristische Betrachtungsweise

Lösungsansätze und -vorschläge

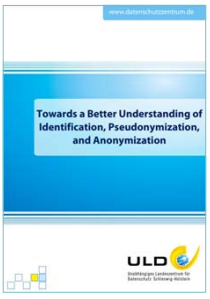
- Einbinden von Beschäftigten
- „Klassiker?" (Löschung, Anonymisierung, Pseudonymisierung)
- Verblassen

Einbindung von Beschäftigten

- Mitbestimmungsrecht des Betriebsrats gem. § 87 Abs. 1 Nr. 6 BetrVG bei Einführung nahezu jeder Software
- Die Inferenzrisiken durch Metadaten, welche auch bei Standardsoftware für den Arbeitsplatz bestehen, unterstützen Rspr.-Linie des BAG
- Bei KMU ohne Betriebsrat fehlt zusätzliches „Kontrollorgan"
- Sensibilisierung der Beschäftigten und Freelancer für Datenschutz und Risiken durch anfallende Metadaten wichtig
- Hier setzen auch entwickelte Lösungen an

Löschen / Anonymität / Pseudonymität

- Rechtslage: Datenschutz by Design, Art. 25 DSGVO
- Klassische Strategien zur Datenminimierung:
  Löschung, Anonymisierung, Pseudonymisierung
  - Für die Auslegung der DSGVO zu diesen Konzepten sind gegenwärtig die Leitlinien zu Anonymisierungs- und Pseudonymisierungstechniken des Europ. Datenschutzausschusses (EDSA) in Arbeit
  - Zum grundlegenden Verständnis siehe die Ausarbeitung zur Identifizierbarkeit, Pseudonymisierung und Anonymisierung aus der Projektarbeit am ULD



https://uld-sh.de/pseudoanon

Löschen / Anonymität / Pseudonymität

Bei Metadaten: **Löschung**

- Bereits bei Einführung der Verfahren Löschung definieren.
  - Zwischenergebnisse zeitnah löschen
  - Löschfristen definieren und/oder
  - Löschen bei Ereignis z.B. Fertigstellung der jeweils übernächsten Version (denkbar bei Software).

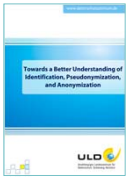
https://uld-sh.de/pseudoanon

Löschen / Anonymität / Pseudonymität

Bei Metadaten: **Anonymisierung**

- DSGVO stellt hohe Anforderungen an eine Anonymisierung
  - Daten sind anonym, wenn keine Person / Angreifer in der Lage ist, betroffene Personen direkt oder indirekt zu (re-)identifizieren, und zwar mit Mitteln, die jetzt oder in Zukunft nach allgemeinem Ermessen wahrscheinlich verwendet werden.
  - Bei Angreifern hier an Vorgesetzte und Kollegium denken. D.h. Vorgang, Sprach-/Programmier-Stile sind bekannt
  - Zukunft: Identifizierende Informationen von dritter Seite?

=> Anonymisierung im Kontext von Beschäftigten-Metadaten idR nicht hilfreich



https://uld-sh.de/pseudoanon

Löschen / Anonymität / Pseudonymität

Bei Metadaten: **Pseudonymisierung**

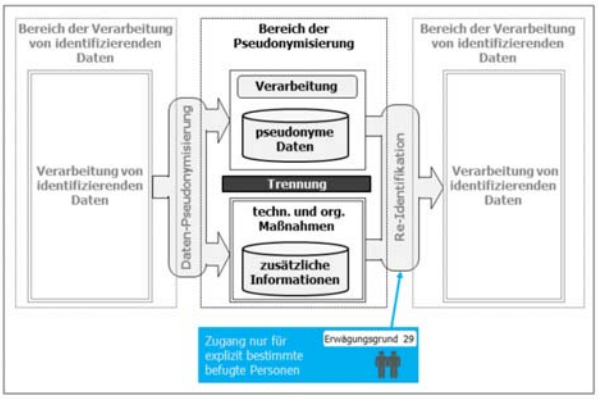
- Verlässliche Trennung der pseudonymisierten Daten (‚was') von den zur Identifizierung geeigneten „zusätzlichen Informationen" (‚wer')
- Technisch-organisatorische Maßnahmen erforderlich, sodass im Kreis legitimer Empfänger keine direkte Identifikation möglich ist.
- Eine direkte Identifizierung muss ausgeschlossen sein
- Mittels Pseudonymisierung wird das Risiko einer Re-Identifizierung reduziert. Denkbar als Zwischenlösung vor einem Löschen.

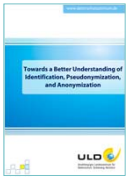
https://uld-sh.de/pseudoanon

ULD www.datenschutzzentrum.de

Löschen / Anonymität / Pseudonymität

Bei Metadaten: **Pseudonymisierung**



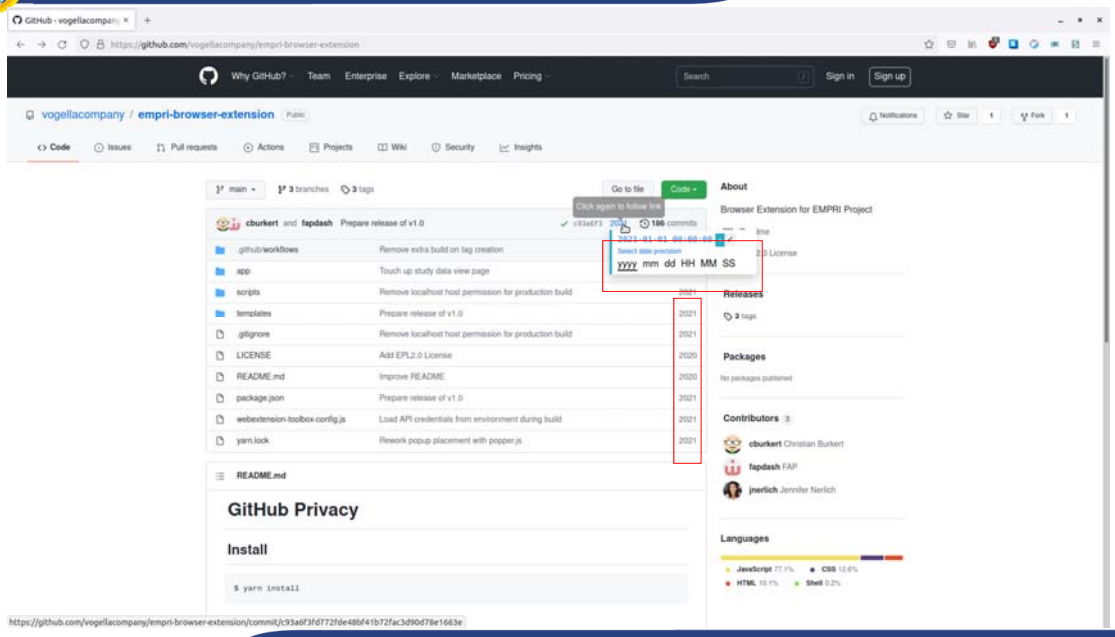


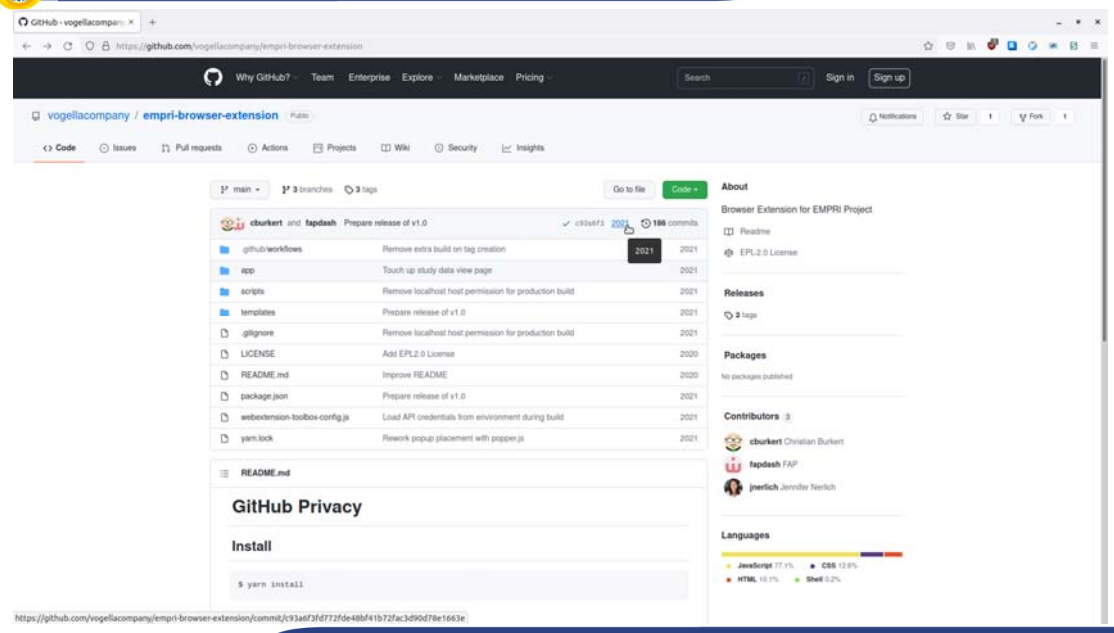
https://uld-sh.de/pseudoanon

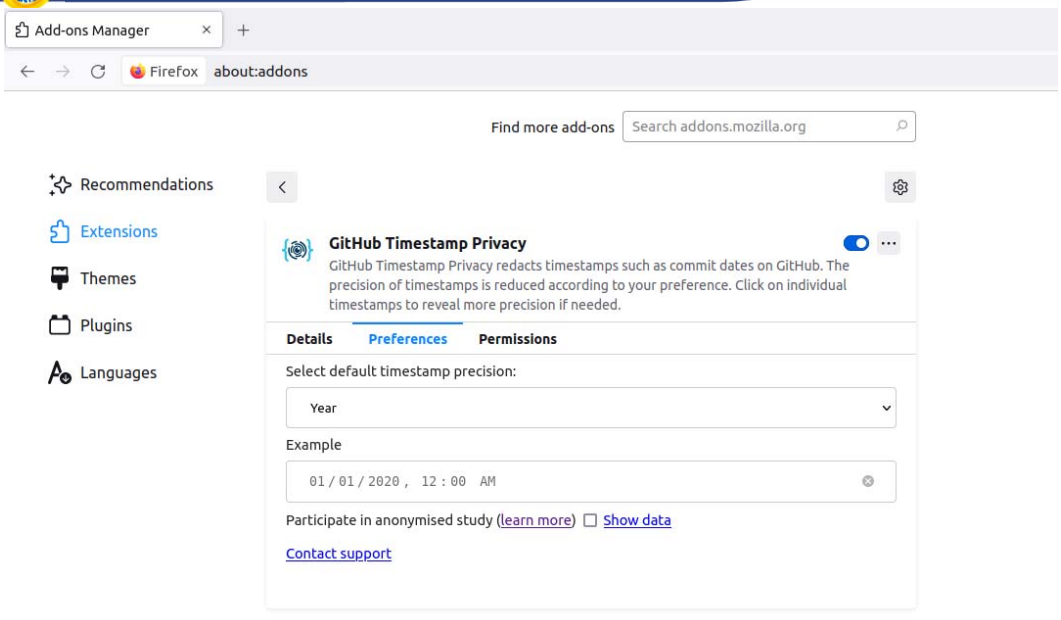
Lösungsansätze und -vorschläge

- Datenschutz by Design
  - Software auswählen, die gute Löschkonzepte unterstützt
  - Software auswählen, bei der nur wenige Metadaten mit Personenbezug anfallen oder jdf. Löschen dieser ermöglicht wird
  - Software auswählen, die datenschutzfreundliche Modifikationen unterstützt (z.B. durch Plug-ins für nutzerseitige Darstellung)
    Three identified Alternatives (=timestamp modifications) [1]
    1. Rough Date (Zeitstempel mit statisch reduzierter Genauigkeit)
    2. Vanishing Date (Zeitstempel mit dynamisch im Laufe der Zeit abnehmender Genauigkeit)
    3. Ordering Date (Pseudo-Zeitstempel, der lediglich die „Eingangsreihenfolge" erhält)

[1] *C. Burkert, J. Balack, H. Federrath, PrivacyDates*: A Framework for More Privacy-Preserving Timestamp Data Types , GI SICHERHEIT 2022




vogellacompany / empri-browser-extension
Why GitHub?
Team
Enterprise
Explore
Marketplace
Pricing
Sign in
Sign up
Code
Issues
Pull requests
Actions
Projects
Wiki
Security
Insights
About
Browser Extension for EMPRI Project
Releases
Packages
Contributors
Languages
README.md
GitHub Privacy
Install
$ yarn install


Add-ons Manager
Firefox about:addons
Find more add-ons
Search addons.mozilla.org
Recommendations
Extensions
Themes
Plugins
Languages
GitHub Timestamp Privacy
GitHub Timestamp Privacy redacts timestamps such as commit dates on GitHub. The precision of timestamps is reduced according to your preference. Click on individual timestamps to reveal more precision if needed.
Details
Preferences
Permissions
Select default timestamp precision:
Year
Example
01/01/2020, 12:00 AM
Participate in anonymised study (learn more)
Show data
Contact support

Lösungsansätze und -vorschläge

- Wenn Betriebsrat vorhanden: Verarbeitung von Beschäftigten-Metadaten in Betriebsvereinbarung regeln.

  → Beispielhafter Formulierungsvorschlag:

  § 2: Geltungsbereich

  Diese Vereinbarung gilt:

  Sachlich für die Einführung, den Betrieb und die Nutzung von Standardsoftware auf allen Servern und Endgeräten, die geeignet sind, auf Daten und Nutzungsverhalten der Beschäftigten im persönlichen Geltungsbereich zuzugreifen, unabhängig von den konkret verwendeten Produkten; zu diesen Daten zählen auch personenbezogene oder personenbeziehbare Metadaten der Beschäftigten.

  Räumlich(…).

  Zeitlich(…).

- Regelung in künftigem BeschäftDSG?

  → Beispielhafte Ergänzung einer Formulierung aus dem Entwurf des DGB (https://www.dgb.de/uber-uns/dgb-heute/recht/++co++82a3178c-88c4-11ec-b434-001a4a160123):

  § 5 Begriffsbestimmungen

  (…)

  (4) „Beschäftigtendaten" sind personenbeziehbare oder personenbezogene Daten zu Beschäftigten oder über diese Personen. Zusatz: Hierzu zählen auch personenbeziehbare oder personenbezogene Beschäftigtenmetadaten, die bei der Nutzung von betrieblichen Software-Anwendungen für die Erbringung der vertraglich geschuldeten Tätigkeiten oder Aufgaben automatisiert erzeugt werden/anfallen.

Vielen Dank!

Kontakt:

Matti Henning
uld65@datenschutzzentrum.de

EMPRI-DEVOPS

GEFÖRDERT VOM
Bundesministerium für Bildung und Forschung

TRAPEEZE

Horizon 2020
European Union funding for Research & Innovation