Daten, Datenbanken, Datenschutz

Alvar C.H. Freude
Referent beim Landesbeauftragten für Datenschutz und Informationsfreiheit Baden-Württemberg

Landesbeauftragter für
Datenschutz und
Informationsfreiheit
Baden-Württemberg

Vorstellung

- Alvar C.H. Freude
- Referent im Referat V, Technisch-Technisch-organisatorischer Datenschutz, Datensicherheit beim Landesbeauftragten für den Datenschutz und die Informationsfreiheit Baden-Württemberg (LfDI BW)
  https://www.baden-wuerttemberg.datenschutz.de/
- Zuvor Freiberufler im Bereich Datenbanken, Software-Entwicklung, IT-Sicherheit

DSGVO-Fake-Horror-Meldungen

Österreich

Wiener müssen wegen Datenschutz Klingelschilder entfernen

Wegen EU-Datenschutzverordnung

Kita schwärzt Erinnerungsfotos

ANGST VOR DER DSGVO

Schule verbietet Eltern das Fotografieren

Stadt Roth

DSGVO: Wunschzettel-Aktion für Kinder zu Weihnachten gestoppt

Fotographie

DSGVO-Chaos

Datenschutz-Wahnsinn Stehen bald auf Klingelschildern keine Namen mehr?

Was ist Datenschutz?

Grundrecht!

- „Das Grundrecht auf informationelle Selbstbestimmung gewährleistet die Befugnis des Einzelnen, grundsätzlich selbst über die Preisgabe und Verwendung seiner persönlichen Daten zu bestimmen.“
- [Die DS-GVO] schützt die Grundrechte und Grundfreiheiten natürlicher Personen und insbesondere deren Recht auf Schutz personenbezogener Daten.
- vgl. Artikel 1 GG, Artikel (7 und) 8 EU-GRCh

Gesetzliche Vorgaben

Was die DS-GVO von DBAs und Entwicklern fordert

Rechtmäßigkeit der Verarbeitung

- Verarbeitung muss **rechtmäßig** sein
- Und braucht eine Rechtsgrundlage
  - z.B. Einwilligung, Vertrag, gesetzliche Verpflichtung *oder* berechtigtes Interesse
- Zweckbindung & Datenminimierung
- Sicherheit der Verarbeitung (=> IT-Sicherheit)
- …

Rechte der Betroffenen

* Transparenz
* Auskunftsrechte
* Recht auf Löschung
* Datenübertragbarkeit
* Beschwerderecht
* …

Privacy by Design & Default

- Artikel 25 DS-GVO verlangt *Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen*
- Verfahren müssen von Anfang an so gestaltet werden, dass möglichst wenig Daten anfallen und die vorhandenen gut geschützt werden

IT-Sicherheit

- Artikel 32 DS-GVO:
  - Technische und organisatorische Maßnahmen zum angemessen Schutz und zur *Sicherheit der Verarbeitung*
  - u.a. Pseudonymisierung, Verschlüsselung
  - Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste im Zusammenhang mit der Verarbeitung müssen auf Dauer sichergestellt werden

Datenpannen

- Datenpannen sind meldepflichtige Vorkommnisse (siehe Artikel 33 DS-GVO), bei denen der Schutz personenbezogener Daten verletzt wurde
- Frist: unverzüglich, jedoch binnen 72 Stunden
- Meldepflicht unabhängig von Höhe des Risikos!

Exkurs: Tracking

- Darf ich Cookies setzen?
- Brauche ich Cookie-Banner?
- Darf ich Google Analytics oder Facebook-Plug-Ins nutzen?
- Wann brauche ich eine Einwilligung?
- Wie muss eine Einwilligung aussehen?
- *https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/04/FAQ-zu-Cookies-und-Tracking.pdf*

Exkurs: Einwilligung

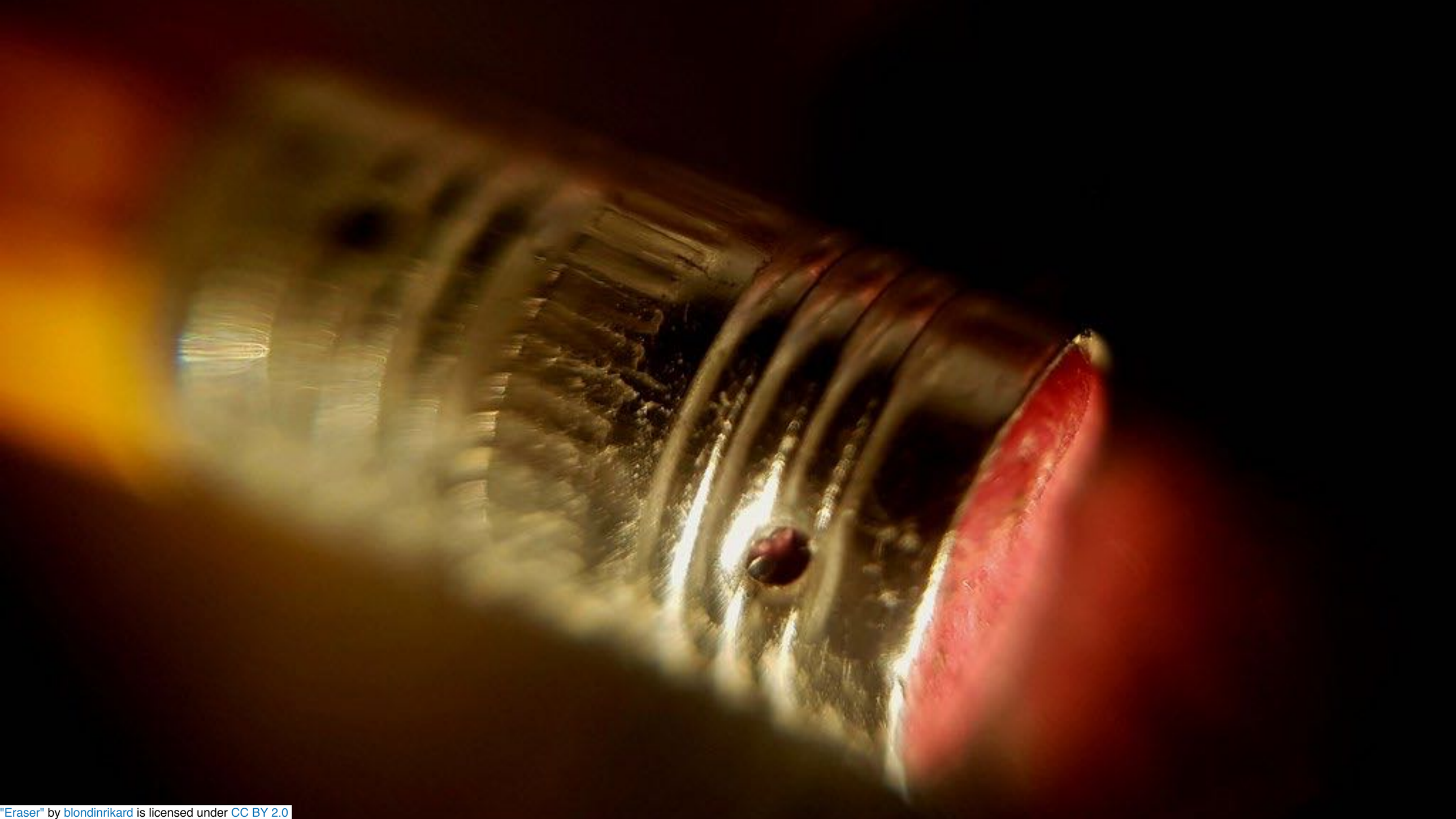
- Eine Einwilligung muss:
  - Aktiv vom Nutzer erteilt werden,
  - informiert erfolgen (Nutzer muss alles wissen, was mit seinen Daten geschieht),
  - wirklich Freiwillig sein (ohne Nachteile bei Ablehnung),
  - jederzeit und einfach widerrufbar sein,
  - und natürlich vor der Verarbeitung erfolgen!

Und nun?!?

Was können Entwickler und PostgreSQL-Admins tun?

Bei Planung & Design

* Datensparsamkeit!
* Löschen vorsehen; u.U. auch Teil-Löschungen
* Auskunftsrechte vorsehen
* Internen DSB und Aufsichtsbehörde beteiligen
* …



Bußgeld-Beispiel

- Erstes Bußgeld gegen ein Unternehmen in Deutschland: 20 000 € für Klartext-Passwörter!
- Für Verstöße gegen technisch-organisatorische Maßnahmen: bis zu 10 Millionen € oder 2% des weltweiten Jahresumsatzes
- Für andere Verstöße bis zu 20 Millionen € oder 4% …
- *https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2019/02/Hinweise-zum-Umgang-mit-Passwoertern-1.0.1.pdf*

Datenpannen vermeiden!

- Angreifer auch dann abwehren, wenn sie schon drin sind!
  - z.B. Passwörter nicht im Klartext speichern
    - Und auch nicht *md5*, sondern *scram-sha-256!*
- Sensible Daten?
  - Auch der Admin darf keine Möglichkeit des Zugriffs haben
  - Kommt aber immer ran
  - Also: Nutzdaten wie Dokumente Verschlüsseln!

z.B. Berechtigungen!

- Webserver läuft als *root* und kann */etc/passwd* ändern? Nein!
- Aber Datenbanken: Viele Anwendungen haben Vollzugriff!
- Besser:
  - Owner von Datenbanken und Tabellen ist ein Admin!
  - Reader-User darf nur lesen
  - Spezieller User darf nur einfügen
  - usw …

Beispiel (stark vereinfacht)

```
CREATE TABLE foo (…….);
ALTER  TABLE foo OWNER TO foo_admin;

REVOKE ALL             ON foo FROM PUBLIC;
REVOKE ALL             ON foo FROM current_user;

GRANT INSERT           ON foo TO   foo_inserter;
GRANT SELECT           ON foo TO   foo_reader;
GRANT DELETE, SELECT ON foo TO   foo_cleaner;

-- usw. auch mit Datenbanken und Schemas
```

Zugriffe feiner steuern

- PostgeSQLs und *row level security*
- BSI Empfiehlt (in Grundschutzkatalog M 2.134):
  - „Anfragen an die Datenbank sollten möglichst nicht direkt auf Tabellen, sondern über *Views* und *Prozeduren* ausgeführt werden.“
  - Und wie sieht das dann aus?

Beispiel: Zugriffe via Funktion

```
CREATE OR REPLACE FUNCTION latest_foo()
    RETURNS SETOF foo
    AS
    $code$
      SELECT * FROM foo LIMIT 10 ORDER BY last_changed;
    $code$
    LANGUAGE sql STABLE
    SECURITY DEFINER
    SET search_path = foo_schema, pg_temp;

  ALTER FUNCTION              latest_foo() OWNER TO foo_admin;
  REVOKE ALL     ON FUNCTION latest_foo() FROM PUBLIC;
  GRANT  EXECUTE ON FUNCTION latest_foo() TO foo_reader;

  -- Ausführen kann nur foo_reader, ohne Rechte auf Tabelle!
  SELECT * FROM latest_foo();
```

Umsetzungsbeispiel

Neues Postgres-Monitoring-Framework:
Posemo – PostgreSQL Secure Monitoring

https://github.com/alvar-freude/Posemo

Beispiel: Posemo, PostgreSQL Secure Monitoring

* Ziele:
  * Einfach erweiterbar, Monitoring-Checks einfach schreibbar, hohe Performance, …
  * Sicher, also Zugriff via Funktionen
  * Flexibel anbindbar an beliebige (Monitoring-) Frontends (z.B. von Nagios über Check_MK, Icinga und Zabbix bis zu Grafana und Prometheus)

Definition eines Checks

```
package PostgreSQL::SecureMonitoring::Checks::BackupAge;

use PostgreSQL::SecureMonitoring::ChecksHelper;
extends "PostgreSQL::SecureMonitoring::Checks";

check_has
    return_type => 'integer',
    result_unit => 'seconds',
    code        => "SELECT CASE WHEN pg_is_in_backup()
                                THEN CAST(extract(EPOCH FROM statement_timestamp()
                                                             - pg_backup_start_time())
                                          AS integer)
                                ELSE NULL
                           END
                           AS backup_age;";


1;
```

Intern generierte Funktion

```
CREATE OR REPLACE FUNCTION posemo.backup_age()
  RETURNS  integer
  AS
  $code$
    SELECT CASE WHEN pg_is_in_backup()
                THEN CAST(extract(EPOCH FROM statement_timestamp()
                                             - pg_backup_start_time())
                          AS integer)
                ELSE NULL
           END
           AS backup_age;
  $code$
  LANGUAGE sql
  STABLE
  SECURITY DEFINER
  SET search_path = posemo, pg_temp;

ALTER FUNCTION             posemo.backup_age() OWNER TO posemo_admin;
REVOKE ALL     ON FUNCTION posemo.backup_age() FROM PUBLIC;
GRANT  EXECUTE ON FUNCTION posemo.backup_age() TO posemo;
```

Posemo

- PostgreSQL-Lizenz
- *https://github.com/alvar-freude/Posemo*
- Nutzbar, Ausgabe-Module für JSON, Check_MK; Postgres-interne Speicherung und Grafana-Ausgabe angedacht
- Bisher 16 Checks fertig
- Patches und Ideen Willkommen!

Fragen und Diskussion

Danke!

Kontakt:

https://www.baden-wuerttemberg.datenschutz.de/

https://alvar.a-blast.org/ | https://blog.alvar-freude.de/

alvar@a-blast.org

Der Datenschutz-Song!

https://www.baden-wuerttemberg.datenschutz.de/datenschutz-mit-ohrwurmqualitaet/

oder https://www.youtube.com/watch?v=M-407cLRpzU