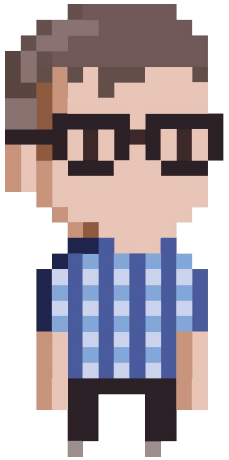


Databunker

PARANOID DATA PRIVACY

Address book on steroids for web and mobile apps

Address book on steroids

- UI and API access.
- Encrypted storage of user personal data (PII JSON).
- Secure user session storage for web applications.
- DPO management tool.
- User token / Pseudonymized user identity.
- Privacy portal for customers.
- Built-in node.js support.
- **Privacy by design (GDPR).**

Privacy is extremely important

CW Compliance Week

British Airways banking on drastic reduction of record GDPR fine

On July 8, 2019, the ICO issued a notice of its intention to fine BA $230 million for GDPR-related infringements following a cyber-attack that saw ...

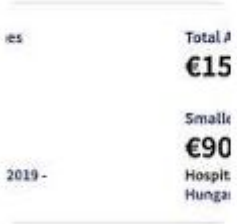
2 days ago

Help Net Security

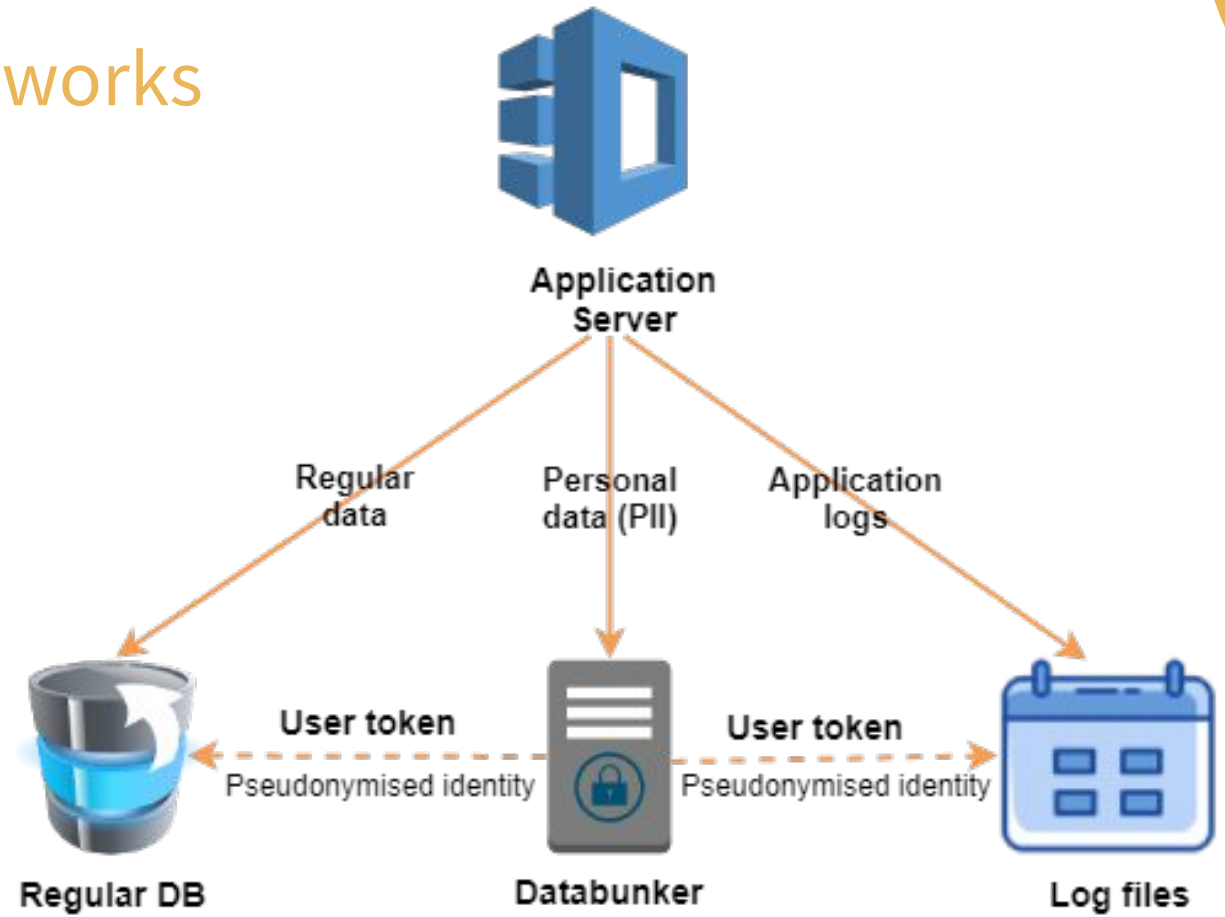
340 GDPR fines for a total of €158135806 issued since May ...

Every one of the 28 EU nations, plus the United Kingdom, has issued at least one GDPR fine, Privacy Affairs finds. GDPR fines. Whilst GDPR sets ...

3 weeks ago



How it works


Application Server
Regular data
Personal data (PII)
Application logs
User token
Pseudonymised identity
User token
Pseudonymised identity
Regular DB
Databunker
Log files

Use cases

1. Schrems II compatible cross-border personal data transfer when user token is used as a pseudonymized user identity.
2. Encrypted storage of personal and user session data.
3. Streamline data minimization:
    a. Cleanup for expired user accounts or the users that have left the service.
    b. Personal data consolidation.
4. DPO management tool and user Privacy Portal.
5. Automatic or semi-automation execution of user forget-me request and other user requests.
6. Boost privacy by design compliance.
7. Many more.

Current state

1. Production ready
2. https://privacybunker.io/ full production
3. https://bitbaza.io/ is using databunker as secure backend server.
4. Support for Node.JS.
5. Node.js example with Passport.JS and Magic.Link.
6. 107 ⭐ on git: https://github.com/securitybunker/databunker

Out of the box compliance with the following GDPR individual rights

Right to be informed	✗
Right of access	✓
Right to rectification	✓
Right to erasure	✓
Right to restrict process	✓
Right to data probability	✓
Rights related to automated decision making including profiling	✓
Right to object	✓

Future plans

1. Add support for different popular libraries and backends like python django, etc...
2. Promotion product for developer communities.
3. Add new features as requested by users.

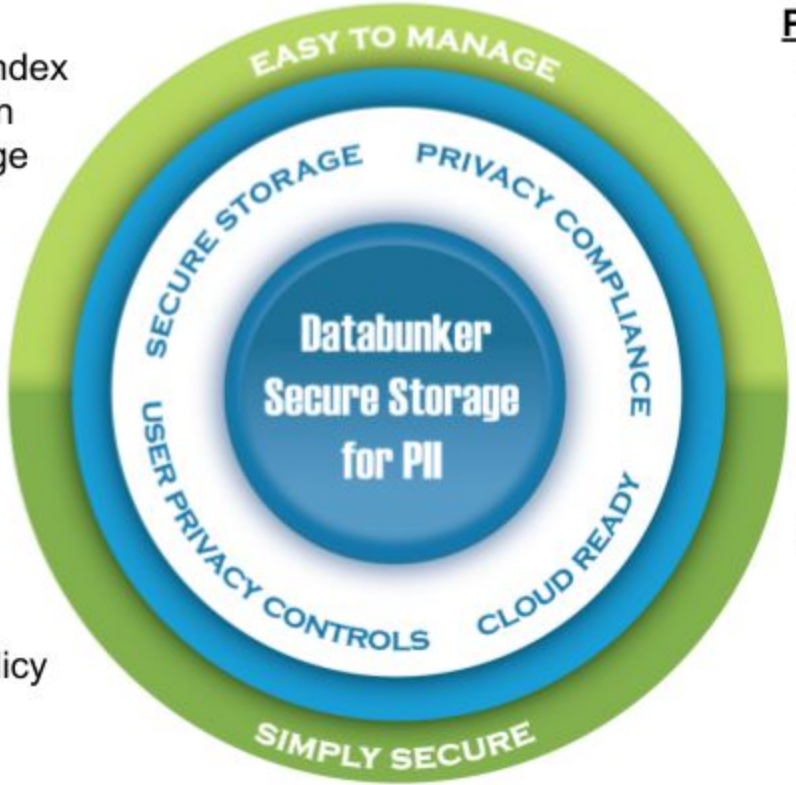
Product tech stack

1. Native code (go-lang)
2. Built-in user interface (compiled as one file)
3. Out of the box supports for clustering
4. Docker containers and AWS friendly
5. Backend database:
    a. SQLite
    b. MySQL
    c. PostgreSQL
    d. AWS Aurora PostgreSQL

Databunker solution

Secure storage

- Encrypted search index
- Encryption is motion
- Encryption in storage
- No SQL injections



Privacy compliance

- Audit trail of all operations
- GDPR compliance
- User control
- DPO friendly

User privacy controls

- User access
- Change records
- Change sharing policy
- Forget me request

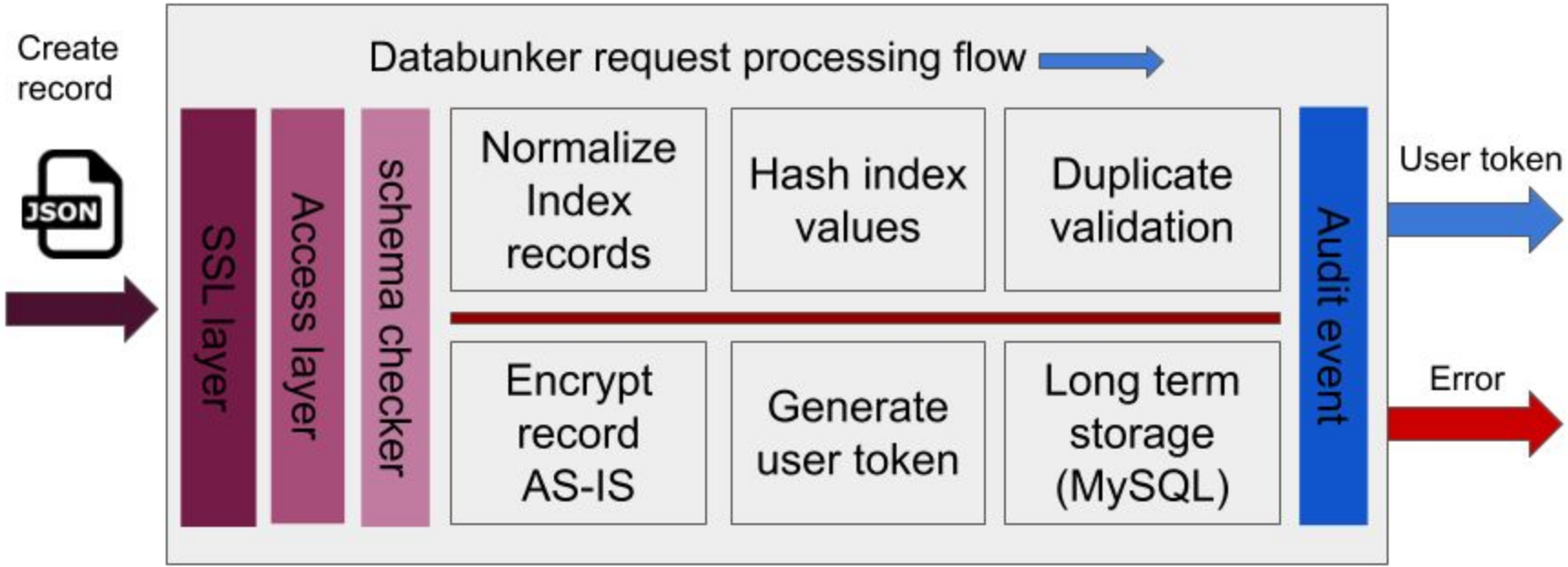
Cloud ready

- Docker containers
- MySQL backend
- GCP/AWS/Azure ready
- Setup scripts

Encrypted PII storage

1. Storage of JSON structure containing personal records
2. Automatic secure indexing without exposing original index value
3. Optional strict data model
4. Multi-tenancy in professional version
5. Encryption of all records containing PII: data, audit, sessions
6. Backend: SQLite, MySQL, PostgreSQL, AWS Aurora PostgreSQL

Create record API request



DEMO

https://demo.databunker.org/

Phone: 4444, Code: 4444, Admin token: DEMO

Node.JS support

Node.JS libraries

- npm install --save @databunker/store
- npm install --save @databunker/session-store

Databunker + Passport.JS + Magic.Link

https://github.com/securitybunker/databunker-nodejs-example

Founder: Yuli Stremovsky

- Previous significant role: Kesem.IO blockchain payments startup CTO.
- Hands-on cybersecurity architect & technology blogger.
- Filed a security vulnerability in Microsoft Azure Active Directory that revealed a privacy bug.
- Founder of database security company GreenSQL (Hexatier) that helped companies to become PCI compliant. The company was acquired by Huawei and now is a part of Huawei cloud.
- Various roles in RSA Security, Checkpoint.
- https://www.linkedin.com/in/stremovsky/

From the Deloitte report.

"As for the future, organisations should strive for a **data protection by design** approach."

THE FUTURE IS HERE

Thank you!

yuli@privacybunker.io