







JENNER

# 1 - Normalize

## 2 - Hash

Use  $\text{hash}(\text{salt} + \text{data})$  to prevent precomputing attacks. Use multiple iterations of hashing.

- ▶ *public salt*     $\Rightarrow$  treat hash as *pseudonymised*
- ▶ *secret salt*     $\Rightarrow$  treat hash as *anonymised*

COMPARE DATA



53

**Problem:** Securely compare two data items

**Solution:** Normalise & hash data, compare hashes



E.g. J. EDGAR HOOVER



HOOVER, JOHN EDGAR



H160, J500 E326



*\*Soundex-but whatever nomenclature you*



## COMPARE DATA

Hashed personal data sometimes is longer personal data!



Dr. Grace Nacimiento von der Kanzlei KLEINER: „Der Einsatz von Salt-Wert und kryptographischer Hashfunktion durch Posteo sorgt dafür, dass eine vom Kunden eingegebene Mobilfunknummer anonymisiert wird, bevor eine Übermittlung an Posteo erfolgt. **Für die bei Posteo allein gespeicherten Hashwerte fehlt es daher an einem Personenbezug [...]** Die gespeicherten Hashwerte sind daher kein Bestandsdatum im Sinne des § 95 TKG [...]" ()

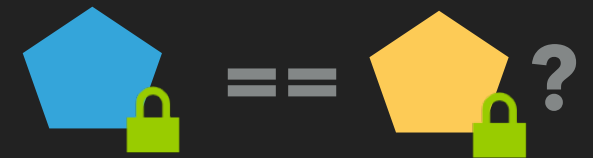
### Bundesdatenschutzbeauftragte Andrea Voßhof:

„Auch aus meiner Sicht ist der gespeicherte gesaltete Hashwert kein **personenbeziehbares Datum**. (...) Zusammenfassend stelle ich fest, dass Posteo im Sinne des § 95 TKG keine Bestandsdaten erhebt“.

[https://posteo.de/bfdi\\_pruefbericht.pdf](https://posteo.de/bfdi_pruefbericht.pdf)

<https://posteo.de/blog/bnetza-entscheidung-zu-posteo-kryptographisch-bearbeitete-daten-nicht-auskunftspflichtig>

# COMPARE DATA



**Problem:** Securely compare two data items

**Solution:** Normalise & hash data, compare hashes

## 1 - Normalize

E.g. **J. EDGAR HOOVER**  $\Rightarrow$  **HOOVER, JOHN EDGAR**  $\Rightarrow^*$  **H160, J500 E326**

## 2 - Hash

Use *hash(salt + data)* to prevent precomputing attacks. Use multiple iterations of hashing.

- ▶ *public salt*  $\Rightarrow$  treat hash as *pseudonymised*
- ▶ *secret salt*  $\Rightarrow$  treat hash as *anonymised*

\* *Soundex - but choose whatever normalisation works for you*