Lufthansa Group

22.09.2015

Personal data secured

Angela Espinosa, Deutsche Lufthansa AG

Agenda

- Introduction
- Data protection
- Pillars of data protection
- Technical and organisational measures
- Requirements on database level
- Penalties

Lufthansa Group

Introduction

- Lufthansa Group operates worldwide in the aviation industry

- Organized in 4 business areas:
  - Passage Airline Group
  - Logistical services
  - Technical services
  - Catering

- 118.973 employees, 30 billion Euro annual turnover

- big demand on IT services through digitalisation and modernisation
- different provider are included

- not only flight data, also creditcard and personal data must be stored
  → subject of regulations by data privacy laws or PCI DSS etc.
  → control and contractual regulations with the provider

Data protection

- **The individual itself stands in the center**
  → protection of personal data

- data protection anchored indirectly in constitution law
  „fundamental right to self-determination“
  by court decision (population census judgement 1983)

Data protection – personal data

Personal data – detailed information about	
personal	**material circuumstances**
name, address, size, age	car-type, income, taxes
of a	
identified person	**identifiable individual**
address, telephone number, photo	userid, social security number
Special personal data (§ 6 BDSG)	
Racial and ethnic origin, political opinions, religious or philosophical convictions, union memberships	

Data protection

- **Every day we leave data marks…**

- Mobile devices make us more visible than we want…

Social networks, insurances, Finanzamt, bank, S Protection Association for General Credit Security, medical laboratory, clinic, doctor, employer, energy provider, online shops, library, school, customer card provider, etc…..

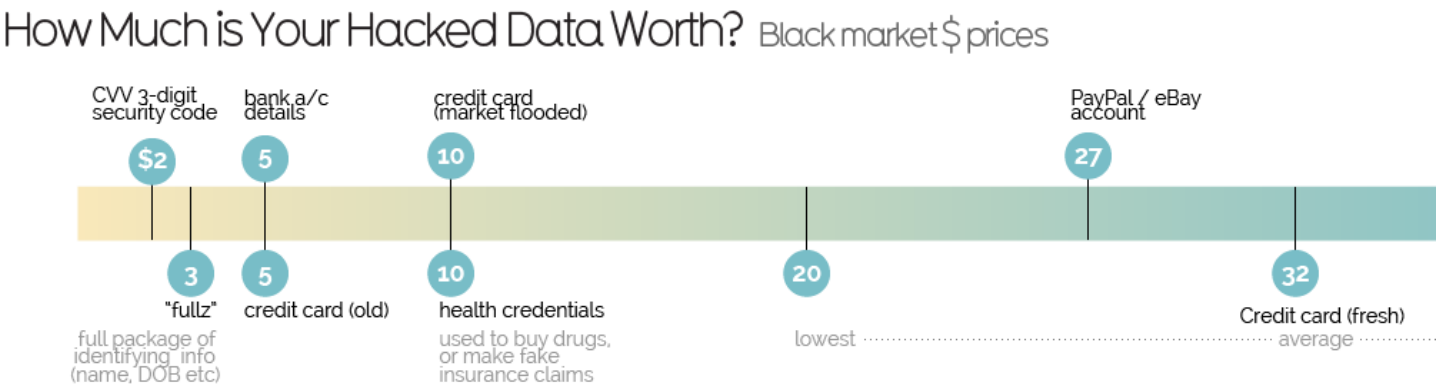
Data protection

- **….you can gain very interesting and useful information**

- Safety authorities → Improving the fight against crime
- Tax authorities → Detect tax offenses
- Companies → Surveilance of employees
- Customer profiles → Improve marketung and price differentiation
- Identity theft → Abuse of own data

You can earn a lot of money!

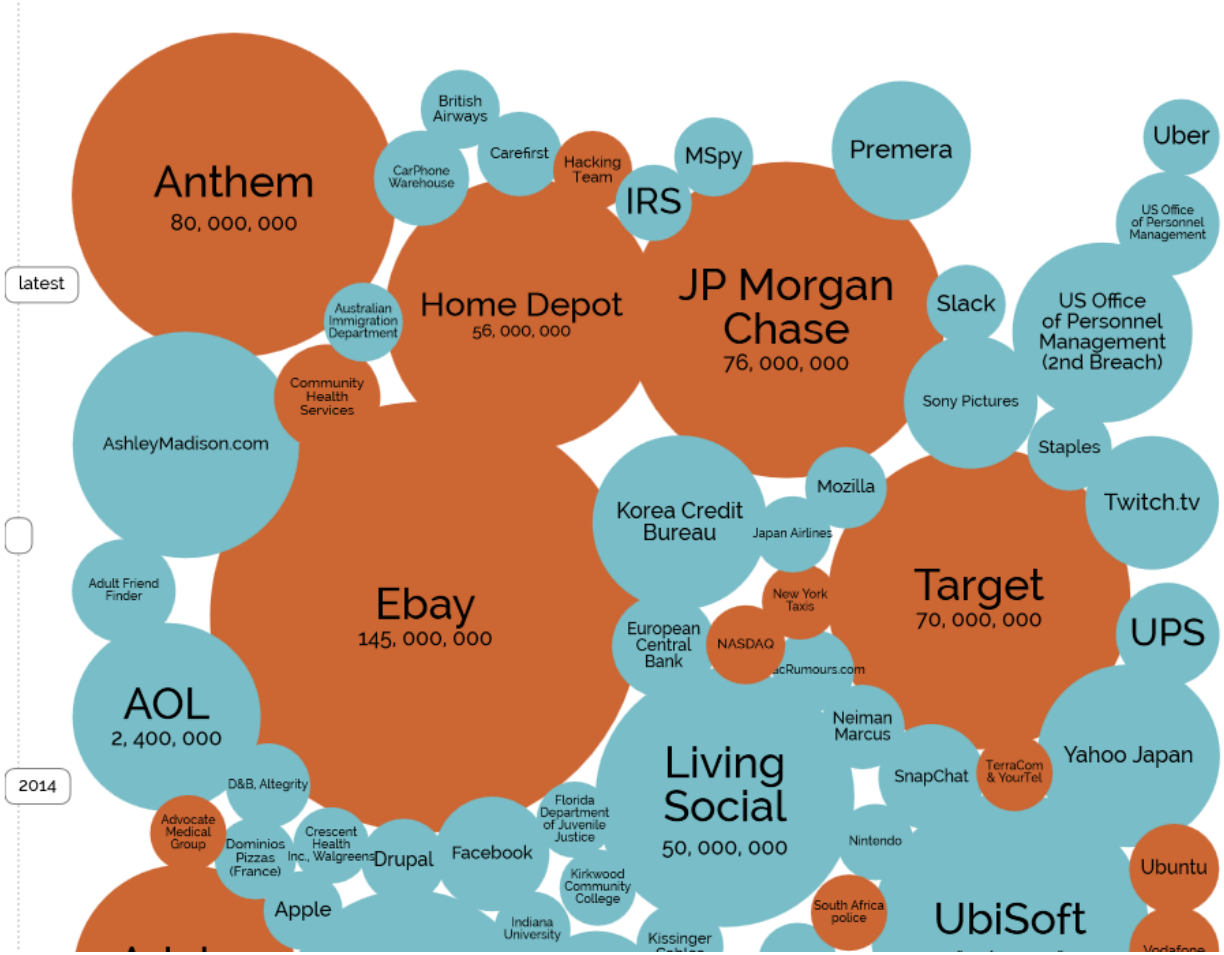
Source: http://www.trendmicro.de/infografiken/wie-viel-sind-ihre-daten-wert/



Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Data protection

- How many data breaches exist?



70
CONTRIBUTING ORGANIZATIONS

79,790
SECURITY INCIDENTS

2,122
CONFIRMED DATA BREACHES

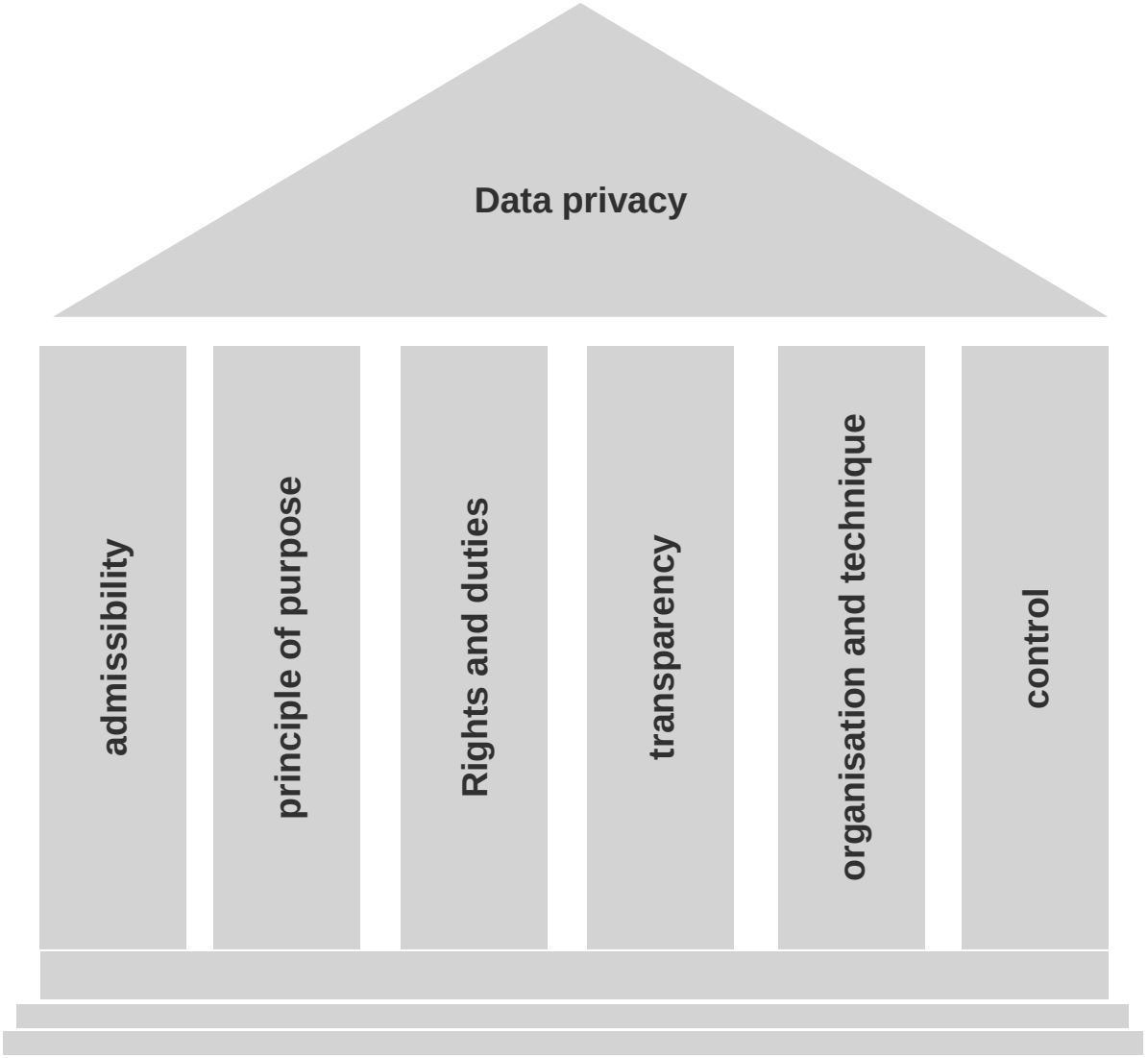
61
COUNTRIES REPRESENTED[1]

Source: http://www.verizonenterprise.com/de/DBIR/2015

Source: http://www.informationisbeautiful.net/visualizations/worlds-biggest-data-breaches-hacks/

Lufthansa Group

Pillars of data protection



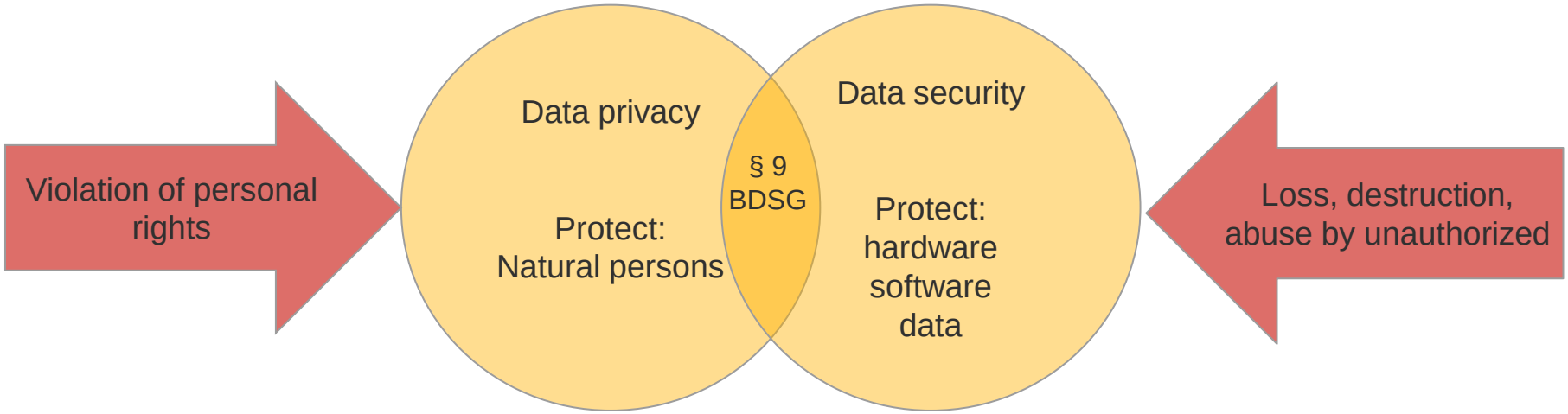
General requirements in advance

- Prior checking of data privacy law regulation for special personal data (§ 6, by DSB)
- Acceptability, appropriation (Processing and use)
- Legal basis documented in register of prcessing information
- Agreement creates transparency
- Check of necessity (data reduction)

- Appropriate technical and organizational measures:
  - protection requirement determination and risk analysis
  - protection level concept (depending on the protection requirement of the data)
  - Authorization concept
  - encryption
  - process management
  - data privacy management
  - dokumentation

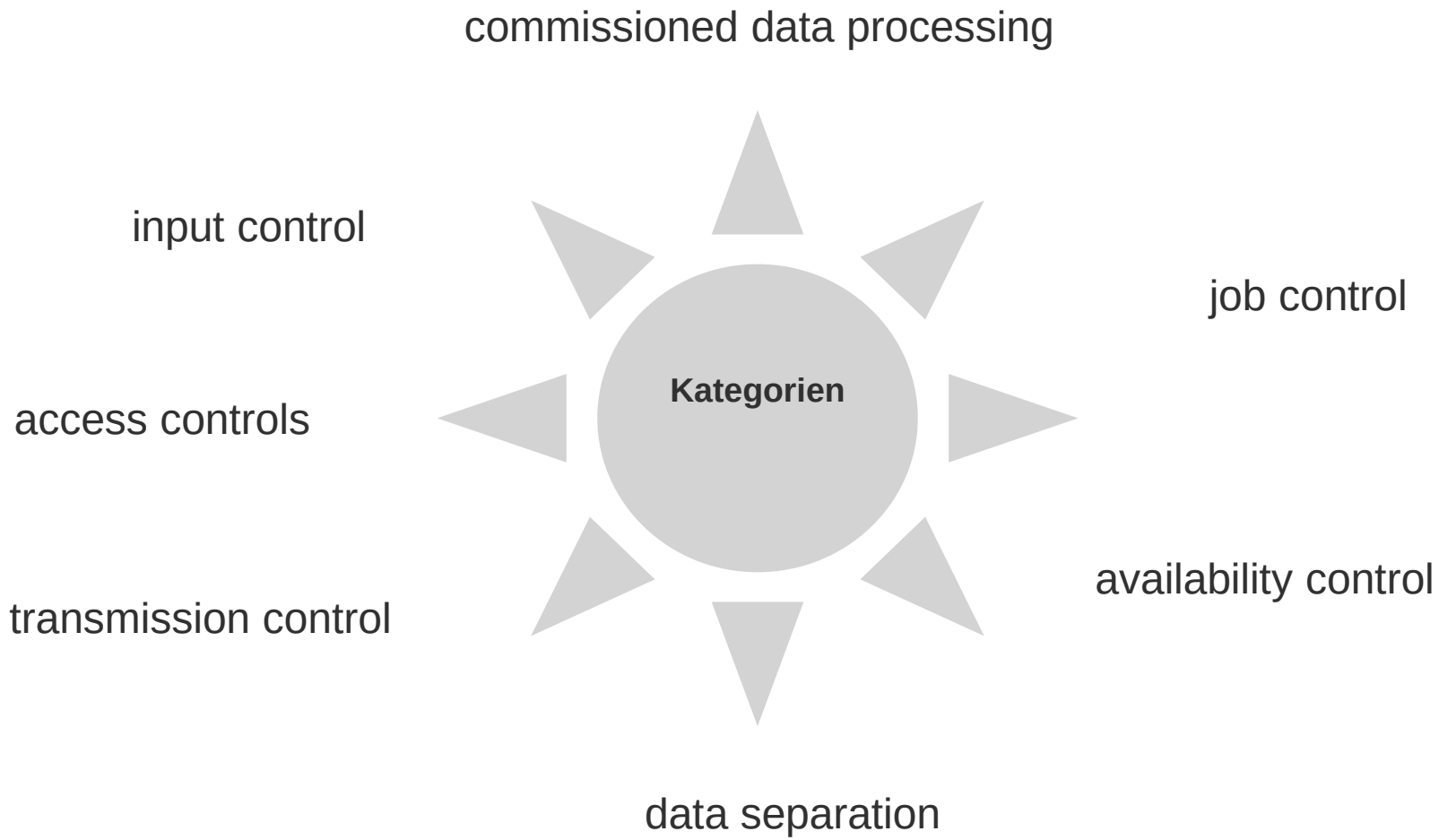
Technical and organizational measures § 9 BDSG

- **effort and desired protection level must be in a reasonable relation**



- **categories:** access control, transmission control, input control, job control, availability control, data separation, commissioned data processing

Technical and organizational measures § 9 BDSG



Requirements on database level

Access control

- Building security (fences, video surveillance, …)
- Room security (security lock, chip card reader, safety glazing, alarm system)

- → although not important for database level, also important fact

Access control (Authentication)

- Personalization
  → Oracle Enterprise User Security (use of AD, LDAP)
  → strong authentication via kerberos, radius, certificates and token

- safe passwords → passwort verify function (use own or provided)

Requirements on database level

- create profiles → assign to users THEN set the passwords
  (Password_Verify_Function, Password Lock Time, Failed Login Attempts)

- limit access to password store (sys.user$)

  REVOKE ALL on SYS.USER$/SYS.LINK$ from <username>;
  SELECT ANY DICTIONARY hat SELECT on sys.user$
  DROP TABLE SYS.USER$MIG;

- limit/delete password hash entries (sqlnet.ora)
  SQLNET.ALLOWED_LOGON_VERSION_SERVER = 12/12a

- change standard password of Oracle internal user (DBA_USERS_WITH_DEFPWD)

- lock unused users and SYS/SYSTEM

Requirements on database level

- change of default options (listener port 1521, db name ORCL, etc.)

- deactivate unused options and features (XML, JAVA, etc. (MOS 2001512.1))
- do not install demo- and testschemas (SCOTT, HR)

- regularly updates of Oracle software (check security alerts/patches)

  SELECT * FROM DBA_REGISTRY_HISTORY;

- change of the active listener only by restart (defined in listener.ora)

  ADMIN_RESTRICTIONS_<listener_name>=ON

- establish an approval process for new users, user changes, user deletion (Lock or delete a former employee promptly)

Requirements on database level

- limit (listener) protocols

  SECURE_REGISTER_<listener_name>=IPC/TCPS

- avoid TNS Poison Attack (permit only local connections)

  ALTER SYSTEM SET LOCAL_LISTENER=
  '(DESCRIPTION=(ADDRESS=(PROTOCOL=IPC)(KEY=REGISTER)))‘ SCOPE=BOTH;
  Since 11.2.0.4 VALID_NODE_CHECKING_REGISTRATION_<listener_name>=*ON*

- limit access (sqlnet.ora)

  TCP.VALIDNODE_CHECKING = YES
  TCP.INVITED_NODES = (hostname1, name2)

- use logon trigger (limited access by application user)

Requirements on database level

Access control (Authorization)

- authorization concept – which user has which privilege on which data
  → Virtual Private Database (new concept RAS; XS$NULL auditing)
  → Label Security (limitations down to row level)

- separate application user from application data schema

- PUBLIC has more than 10.000 privileges → every user inherits these privileges

- Important: Remove execution rights from PUBLIC to objects and packages
  REVOKE EXECUTE on DBMS_ADVISOR from PUBLIC;

  → Source: https://www.cisecurity.org/

Requirements on database level

- limit user privileges (also for Oracle internal user)

  REVOKE EXECUTE ANY PROCEDURE from OUTLN/DBSNMP;

- motto: „As less privileges as possible and as much as necessary" (ANY-, DBA-rights)

- Oracle 12c offers Privilege Analysis (Database Vault)

- avoid concentration of functions (root+DBA in one person) → Separation of duties

- limit access to objects in SYS schema by EXECUTE ANY PROCEDURE and SELECT ANY DICTIONARY privilege

  07_DICTIONARY_ACCESSIBILITY=FALSE

- limit access to OS-files $ORACLE_HOME/…

Requirements on database level

Transmission control

- data has to be encrypted, rendered anonymous
- use de facto standard
  - TLS 1.1/1.2 (electronic transmission via public nets)
  - Tunnel connections (Virtual Private Network)
  - S/MIME for email (electronic signatur)
  - X.509 V3 for coding of asymmetric keys

- encrypted backup (key management)

- immediately deletion of transport data storage medium
- deletion of the encryption and the keys

- documentation and control (protocols if media is changing)

Requirements on database level

Encryption (explicitly in access and transmission controls)

- access to database
  - transmission of passwords must be encrypted (not for UPDATE or ALTER USER)
  - network encryption (part of Enterprise Edition)

- access to data
  - encryption by application itself (key management)
  - encryption through DBMS_CRYPTO
  - encryption of tablespaces or columns (Tablespace Data Encryption)
  - Oracle Database Vault as additional security measure (limit access)

- transmission of data
  - application ensures encryption and auditing
  - Data Pump only encrypted (ENCRYPTION option)
  - render data anonymous (no relation to the real data)
  - backup encryption (key management)

Requirements on database level

Data separation

- save data for different purposes separately
- separate employee and customer data
- logical separation (own tablespaces)
  → different schema and using different users for access

- Other possibilities of data separation:
  – use different databases
  – use access control software and access rights
  – different encryption for single records
  – Different keys per client

- Separate test from productive environment and use only rendered data
  → if this is not possible, use only a set of data in the test environment
  → establish a gradual concept

Requirements on database level

Availability control (Protection of destruction and loss of data)

- detailed emergency plan (Desaster Recovery Plan)
- USV uninterruptible power supply, firewall
- mirroring of disks, RAID-method, virus protection (on OS-level)
- monitoring of database with appropriate alerting (eg. Oracle Enterprise Manager)
- backup-concept (full backup, inkremental backups)
- regularly and secure backup of archive logs and datafiles with RMAN
  → implement regularly restore- and recovery tests
- multiplexed controlfiles/redologs on different disks

Requirements on database level

Logging (purpose bound, data reducted, complete) – input control

- Logging data not for behaviour or performance control (!!)
- Important: limit type, duration and scope
- Who, when processed which personal data
- Executed operations, application/program, machine, individuals with time relation
- No manipulation afterwards, only limited number of people can access this data
- Test of the proper work - sampling
- Retention period is variable, depending on evaluation cycle

Requirements on database level

Solution for Oracle 12c → Unified Auditing (automatically activated)

- extensive in logging (Backup, Restore, Dumps, oradebug, read-only mounting etc.)
- logging table is only read-only accessible (unified_audit_trail in audsys schema)
- Logging entries can be collected by central protocol server
- Don`t forget the delete job:

```
exec DBMS_AUDIT_MGMT.CREATE_PURGE_JOB
(AUDIT_TRAIL_TYPE => DBMS_AUDIT_MGMT.AUDIT_TRAIL_UNIFIED,
AUDIT_TRAIL_PURGE_INTERVAL => Zeitintervall,
AUDIT_TRAIL_PURGE_NAME => ‚Purge_audit_tabelle',
USE_LAST_ARCH_TIMESTAMP => TRUE);
```

Requirements on database level

- Implement audit-policy
- Oracle 12c automatically has ORA-SECURECONFIG

```
CREATE AUDIT POLICY ORA_SECURECONFIG
 PRIVILEGES ALTER ANY TABLE, CREATE ANY TABLE, DROP ANY TABLE,
            CREATE ANY PROCEDURE, DROP ANY PROCEDURE, ALTER ANY PROCEDURE,
            GRANT ANY PRIVILEGE, GRANT ANY OBJECT PRIVILEGE, GRANT ANY ROLE,
            AUDIT SYSTEM, CREATE EXTERNAL JOB, CREATE ANY JOB,
            CREATE ANY LIBRARY,
            EXEMPT ACCESS POLICY,
            CREATE USER, DROP USER,
            ALTER DATABASE, ALTER SYSTEM,
            CREATE PUBLIC SYNONYM, DROP PUBLIC SYNONYM,
            CREATE SQL TRANSLATION PROFILE, CREATE ANY SQL TRANSLATION PROFILE,
            DROP ANY SQL TRANSLATION PROFILE, ALTER ANY SQL TRANSLATION PROFILE,
            CREATE ANY SQL TRANSLATION PROFILE, DROP ANY SQL TRANSLATION PROFILE,
            ALTER ANY SQL TRANSLATION PROFILE, TRANSLATE ANY SQL,
            EXEMPT REDACTION POLICY,
            PURGE DBA_RECYCLEBIN, LOGMINING,
            ADMINISTER KEY MANAGEMENT
ACTIONS     ALTER USER, CREATE ROLE, ALTER ROLE, DROP ROLE, SET ROLE,
            CREATE PROFILE, ALTER PROFILE, DROP PROFILE,
            CREATE DATABASE LINK, ALTER DATABASE LINK, DROP DATABASE LINK,
            LOGON, LOGOFF, CREATE DIRECTORY, DROP DIRECTORY;
```

- expansion by access on certain packages (DBMS_FGA and tables (sys.user$)

- log access to sensitive data with Fine Grained Auditing

Requirements on database level

SIEM USE CASES - definition of suspect and flashy events

- trigger alarming
- examples:
  - user changes database parameter
  - user creates another user
    different possibilities: create user, grant user identified by

- configuration should be extended

- examples how identity changes can be done without password:
  - DBMS_SYS_SQL (undocumented), DBMS_IJOB (undocumented)
  - sys.kupp$proc (undocumented), Alter User su (feature)
  - Proxy User (feature), Any Procedure (feature)
  - Become User (feature), KUPP_PROC_LIB (undocumented)

- logging of oradebug use in Oracle 12c possible (do it!)

Requirements on database level

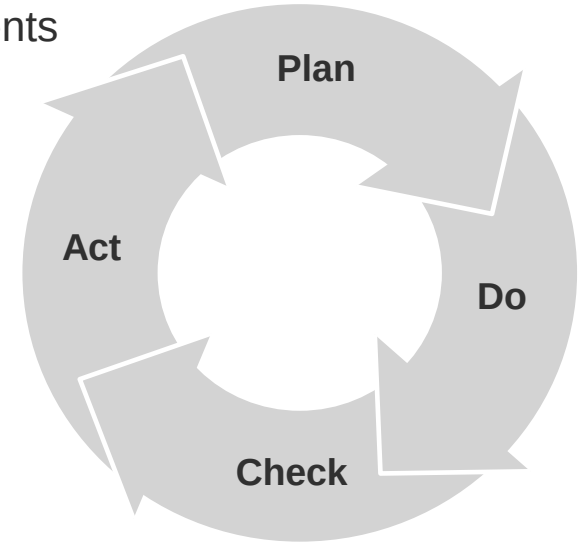
Commissioned data processing (§ 5 and § 11 BDSG)

- data secrecy obligation within the company (§ 5 BDSG)
- data processing of behalf → according to the instructions of the client
- warranty of data protection in outsourcing of data processing
- client is commited:
- conclusion by § 11 BDSG with contractor (ADV)
  → execute regularly controls
- not interesting on database level, but also important

Requirements on database level

Regularly checks

- not explicitly required: data protection management system
- control is the alpha and omega
- regularly checks of hardening and security measures
- development of new versions/features/security requirements



Be aware!

- Interesting requests:
  - Absence times of employees → visitations of addiction treatment of company
  - Workers council → Duration and frequency of trainings
  - How much earns my colleague

- Illegal inspection
  → transgression of purpose (eg. JOIN over certain tables)

- Affected individuals have to be informed
  → § 42a BDSG
  → reporting obligation if data is illegal accessed

- „reporting makes free“ contact data protection officer or authority

Penalties

- Privacy violations lead to fines § 43 BDSG

- fines of 50.000 – 300.000 Euro

- Every privacy violation is punished
- „Kleinvieh macht auch Mist“

- Examples from reality (amount of fines):
  - Retail chain 1.462.000 €
  - Bank 120.000 €
  - Drug store 137.500 €
  - Transport company 1.123.503,50 €

Thanks for the attention!