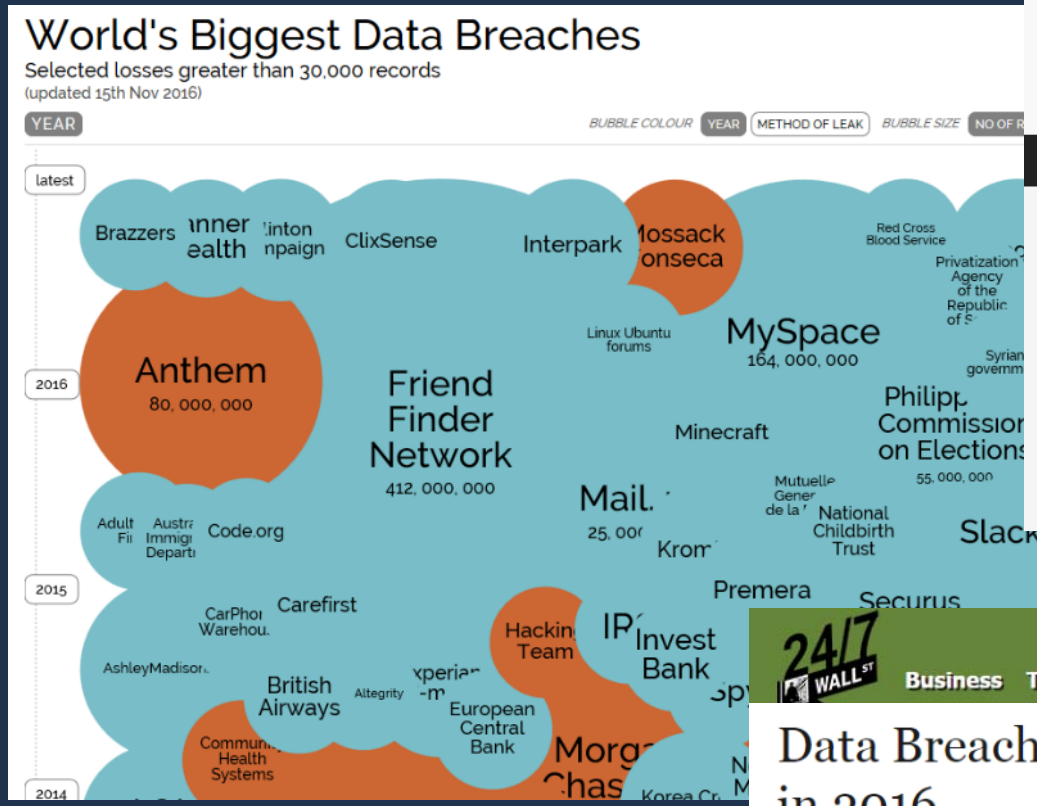
SAS
Personal Data Protection
How do you protect your data?

Presented by:

Casper Pedersen
Thought Leader & Certified DPO
SAS Global Data Management



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

http://www.itgovernance.co.uk/blog/list-of-data-breaches-and-cyber-attacks-in-142160000-records-leaked/

http://247wallst.com/technology-3/2016/09/21/data-breaches-up-16-to-date-in-2016/

INDEPENDENT.IE NEWS BUSINESS SPORT LIFE STYLE ENTERTAINMENT TRAV

Brexit | Irish | World | Technology | Personal Finance | Small Business | Farming | Jobs |

From Independent.ie

Yahoo's data privacy woes may cost it €1bn

BBC Sign in News Sport Weather iPlayer TV Radi

NEWS

Home UK World Business Politics Tech Science Health Education Enterta

Business Your Money Market Data Markets Companies Economy

TalkTalk fined £400,000 for theft of customer details

5 October 2016 | Business Share

FRIENDFINDER® NETWORKS

In May, TalkTalk revealed that the attack had cost it £42m and that 101,000 subscribers had left in the aftermath of the attack.

computing

Britain on the hook for £122bn in fines under European Union GDPR, claims PCI Security Standards Council

SMEs on the hook for £52bn, while large organisations could be forced to pay up £70bn

British businesses and other organisations could be fined as much as £122bn under the European Union's General Data Protection Regulation (GDPR) if they don't get their act together before it becomes law in less than two years.

That is the warning of the PCI Security Standards Council (PCI-SSC), which claims that if the level of cyber security incidents against organisations in the UK in 2015 is the same or worse after the GDPR comes into force, then British businesses, charities and government bodies could be fined as much as £122bn.

http://www.computing.co.uk/ctg/news/2474369/britain-on-the-hook-for-gbp122bn-in-fines-under-european-union-gdpr-claims-pci-security-standards-council

sas

Up to 20,000,000 EUR or up to 4% of global turnover

(whichever is the greater)

What's it about?

EU General Data Protection Regulation (GDPR)

- The Regulation will enter into force on 24 May 2016 and it shall apply from 25 May 2018
- The reform strengthens citizens' fundamental rights in the Digital Market and focuses on Personal Data
- The Regulation promotes techniques such as anonymization (removing PD*), pseudonymization (replacing DP*), and encryption (encoding PD*)
- Sanctions: Up to 20,000,000 EUR or up to 4% of the annual worldwide turnover
- http://europa.eu/rapid/press-release_MEMO-15-6385_en.htm

Go to webpage

*Personal Data

What's it about?

1. Responsibility and accountability
    a. Data Protection Impact Assessments (DPIA)
    b. Privacy by Design and Privacy by Default
2. Consent
    a. Valid consent must be explicit for data collected and purposes data used
    b. Data controllers must be able to prove consent (opt-in) and consent may be withdrawn
3. Data Protection Officer
    a. Ensure compliance within organization
4. Data Breaches
    a. How will you react to a data security breach?
    b. Legal obligation to notify the Supervisory Authority without undue delay
5. Right to erasure
    a. Right to be forgotten / deleted
6. Data portability
    a. Transfer their personal data from one electronic processing system to and into another
    b. Cross-border data transfers

What are the challenges?

Towards Authorities

- Do we have an overview of all data sources?
- What is the risk level for each data source?
- Can we show a report where Personal data are located?
- Can we show that processes are in place?
- Do you have documentation and audit trails?

Internal Challenges

- What is Personal Data?
- And how do we identify Personal Data?
- Do we control access rights?
- Do we log user activity for each and every data store?
- Does duplication and poor data quality make it difficult to “be erased and forgotten”?

sas

The changing organization

Towards authorities

Data flow analysis

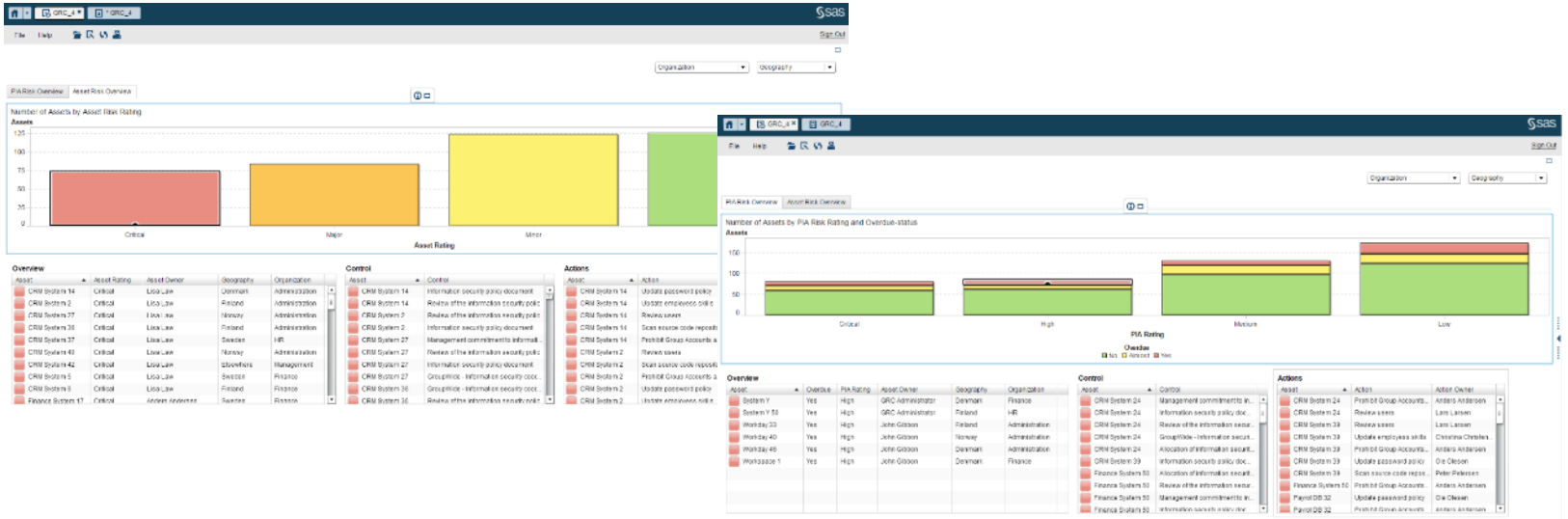
- Identify, categorize and risk assess data flows
- Recommend and describe control measures
- Report measures based on prioritized risks

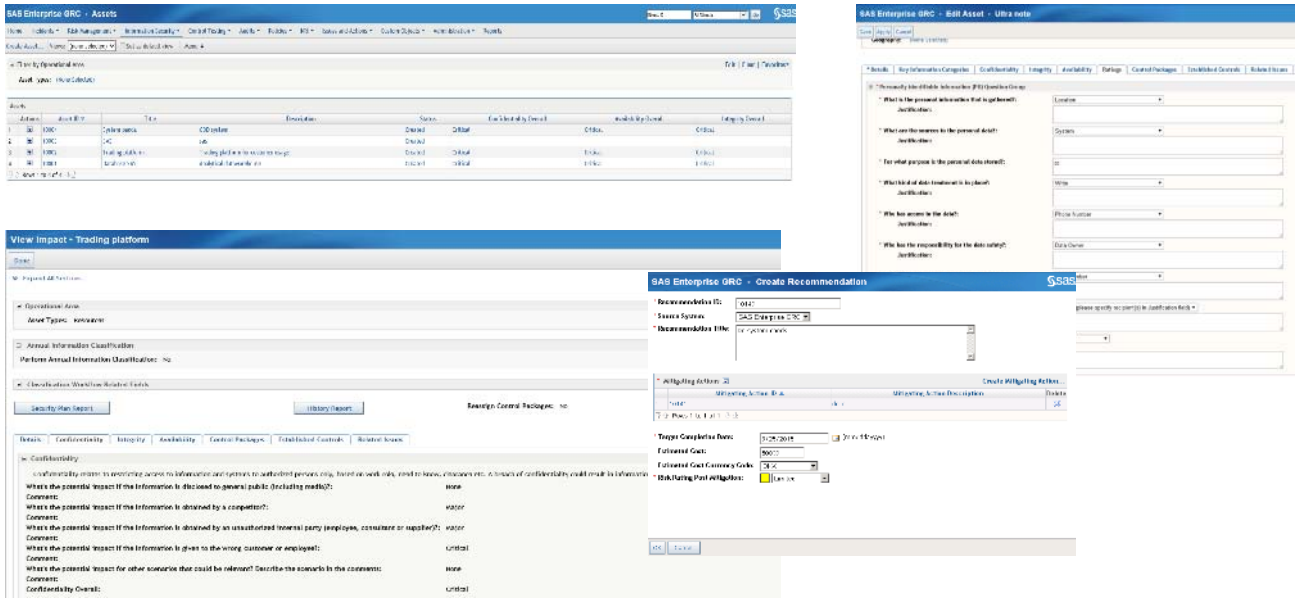
Incident management

- Standard automated process
- Identify, categorize and add measures. Link to risk assessment and policies

Policy management

- Standard process
- Policy lifecycle
- Link together with incidents and risk assessment from the data flow analysis





Internal challenges

Personal Data Identification

- Parsing
- Extraction
- Pattern Analysis
- Identification Analysis
- Gender Analysis
- Standardization, Casing
- Matching

Supported PD

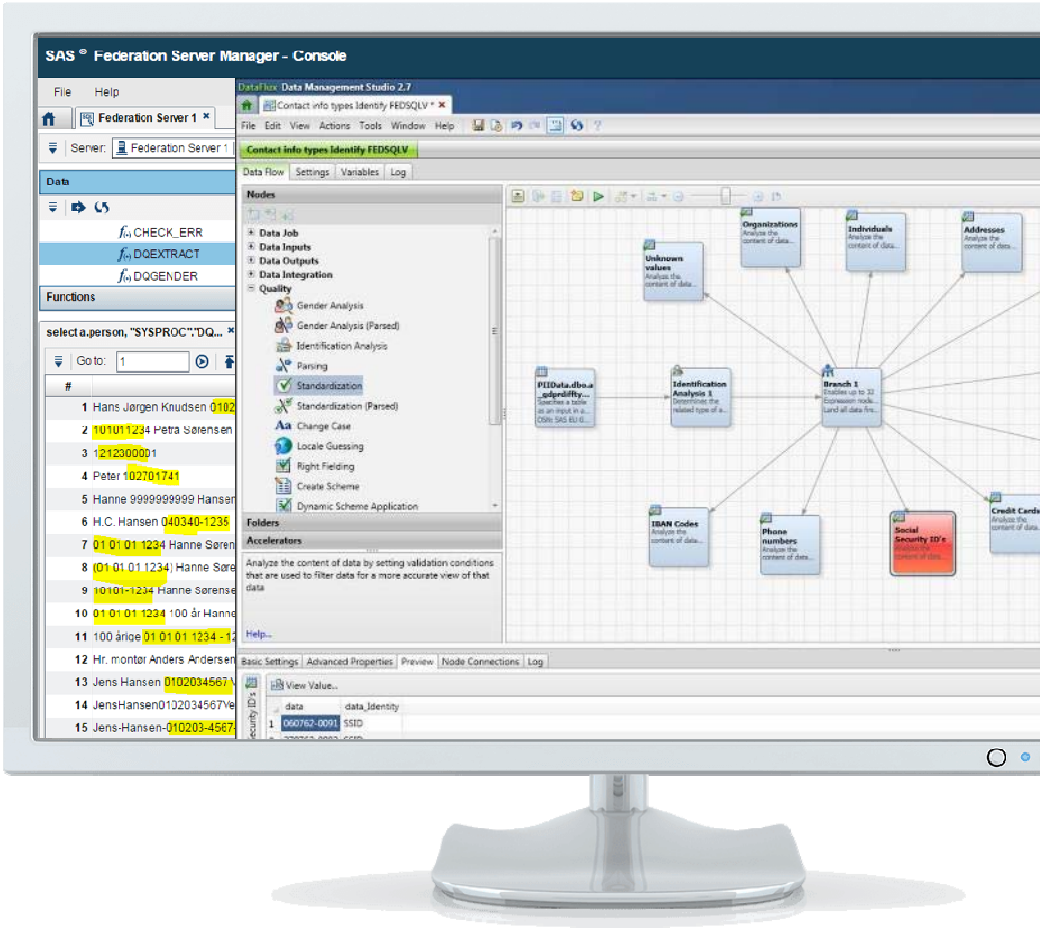
- Names
- Phone numbers
- 4-digit zip codes
- E-mail addresses
- Street addresses
- IP address
- Health data
- DOB
- Gender
- HR data
- Personal files
- Social security numbers
- IBAN (International Bank Account Number)
- Credit card numbers
  - VISA (4571)
  - MasterCard (55XX)
  - American Express

Personal Data Protection Tokens

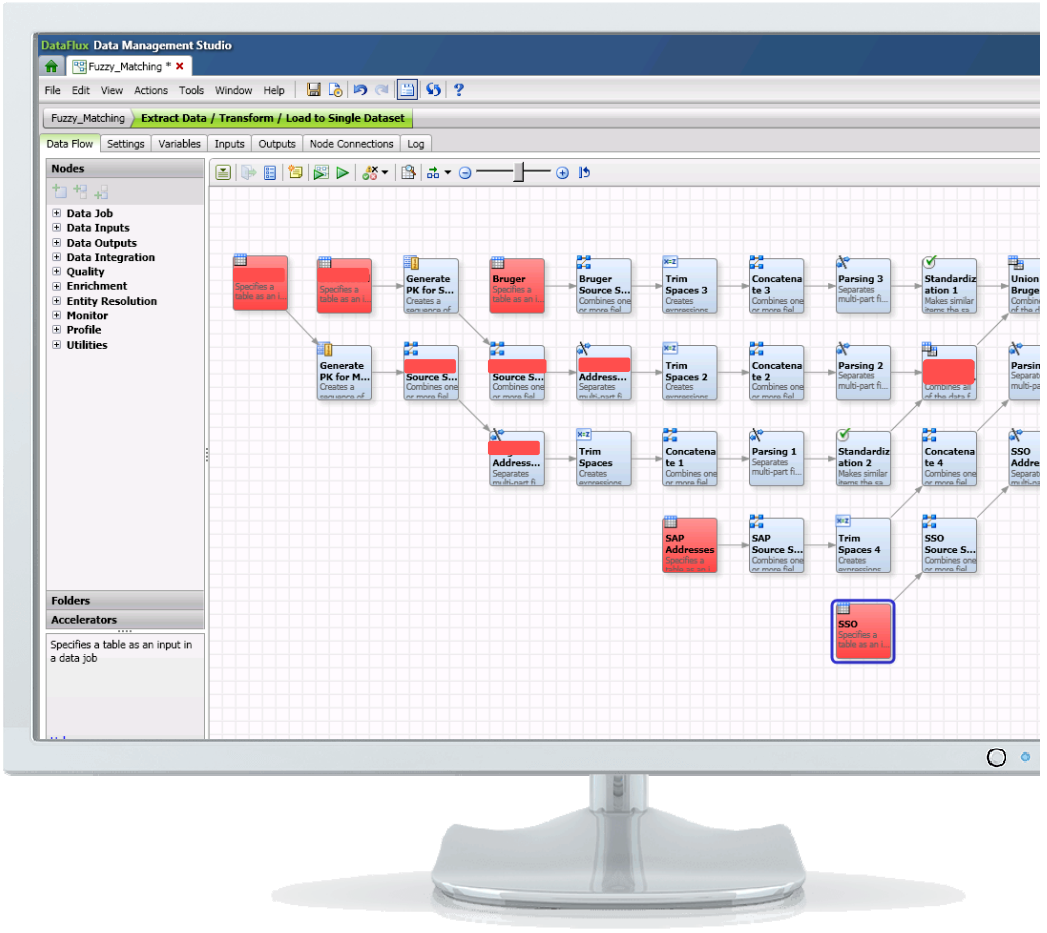
- Bank Account
  - Bank Identifier Code (BIC)
  - IBAN
- Credit Card Number
  - American Express
  - VISA
  - MasterCard
  - Dinners Club
  - Discover
  - JCB
- Demographic Data
  - Name
  - Gender
  - Date of Birth
  - Age
  - Nationality
- Channels
  - Phone Number
  - Postal Address
    - City
    - Country
  - Email Address
- Government Identifiers
  - National Id
  - Passport Number
  - Social Security Number
  - Vehicle Registration Number
  - Driver License
- Digital Identifiers
  - IP Address (V4, V6)
  - MAC Address
  - X/Y Geographic Coordinate
- Social Media
  - Twitter Account
  - URL FaceBook
  - URL Linkedin
  - URL Pinterest
  - URL Instagram
- Organization
- Sensitive Data
  - Health, Sex
  - Political
  - Religious
  - Philosophical
  - Trade union member info
  - Genetic
  - Biometric
  - Race
  - Gender
  - Ethnicity
  - Children

Example: Extracting social security numbers using the Quality Knowledge Base for Personal Data.

The same technique applies for ALL Personal Data Types …

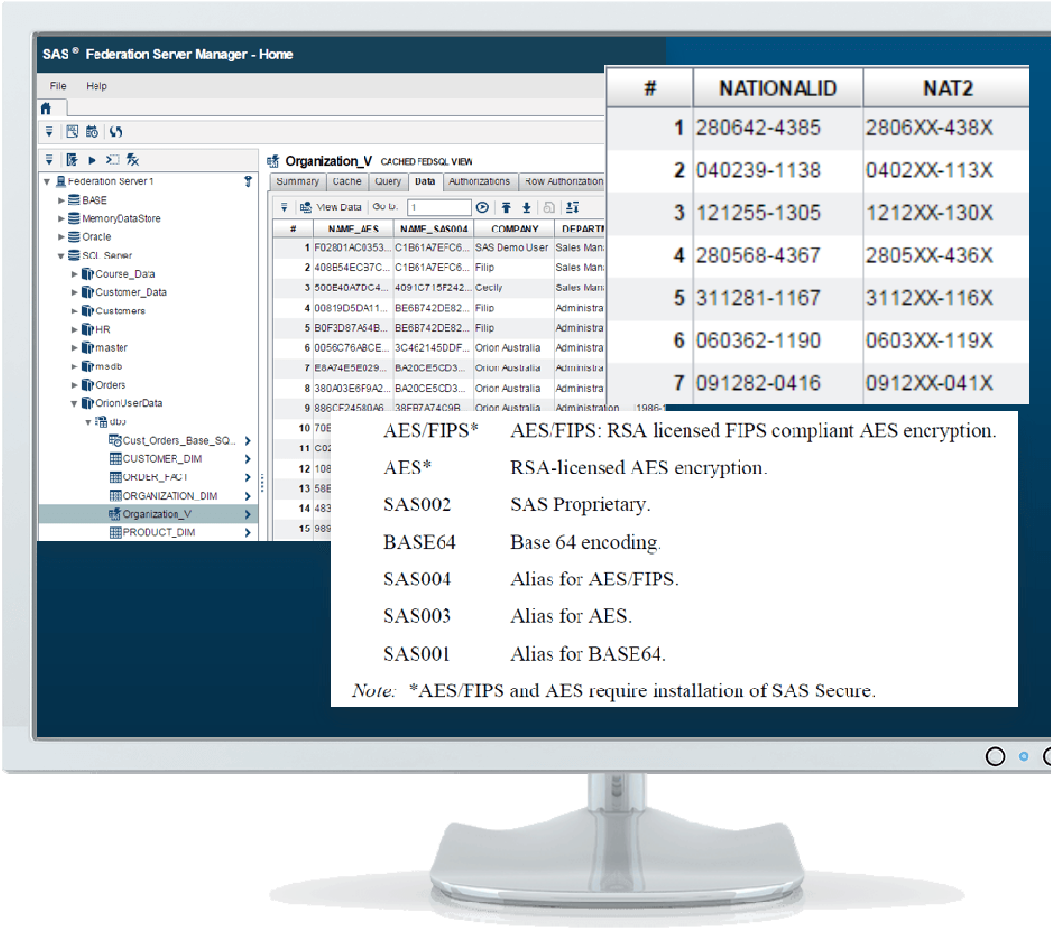


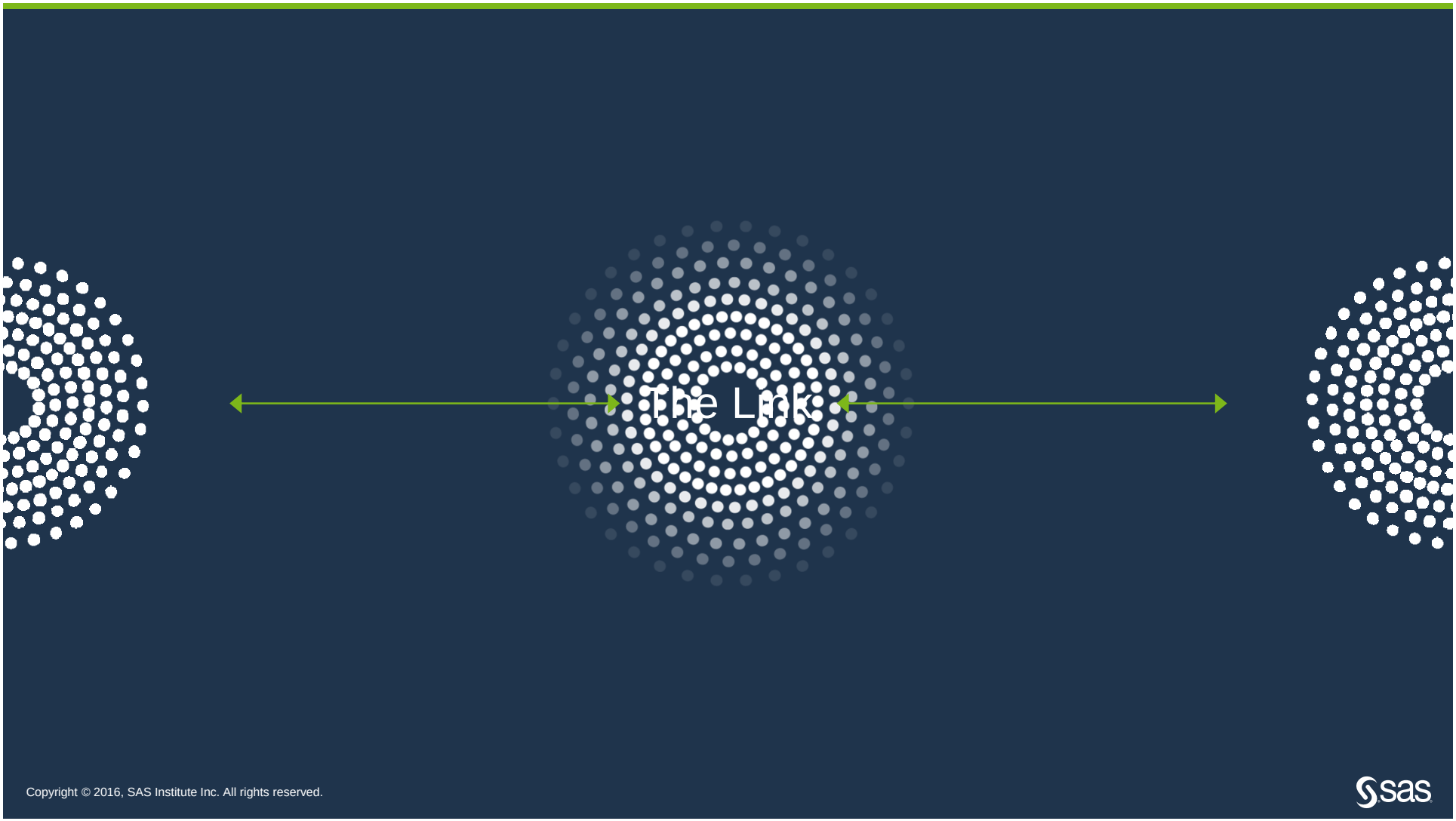
- Business Identity check
- Why?
- Easily find Personal Data where data is mixed and messy



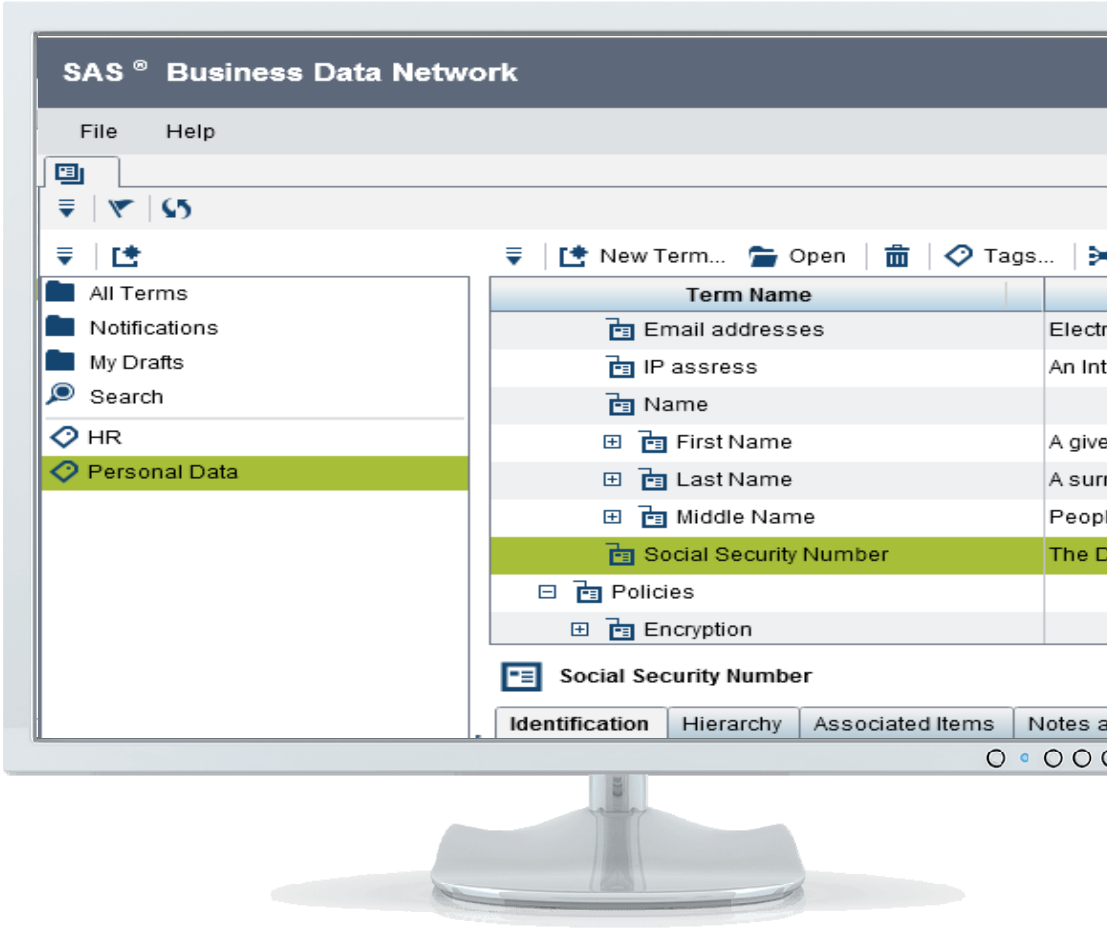
The Regulation promotes techniques such as:

- Anonymization (removing PD)
- Pseudonymization (replacing PD)
- Encryption (encoding PD)

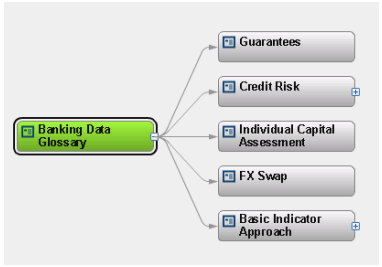


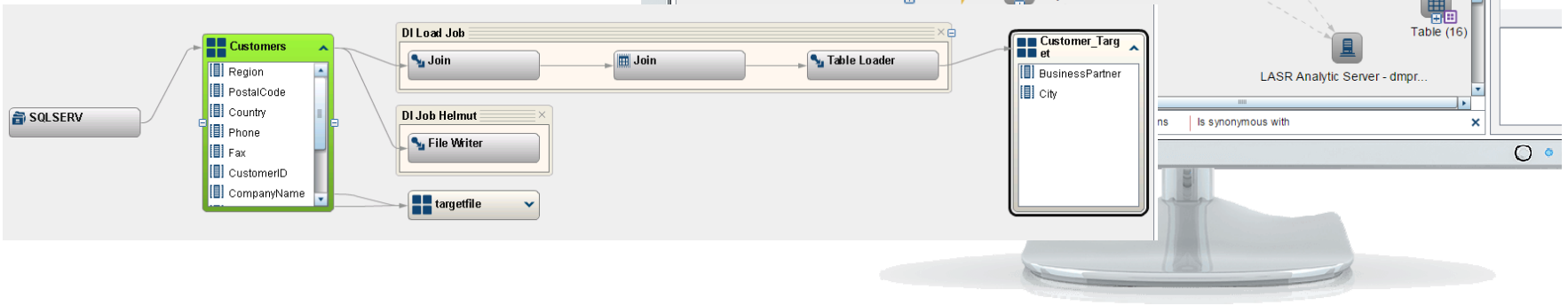


- Automated Personal Data glossary
- Define Business Terms in order to align Business & IT
- Get a clear overview on roles & responsibility!



- Link Systems, Processes and Business Owners in data flows

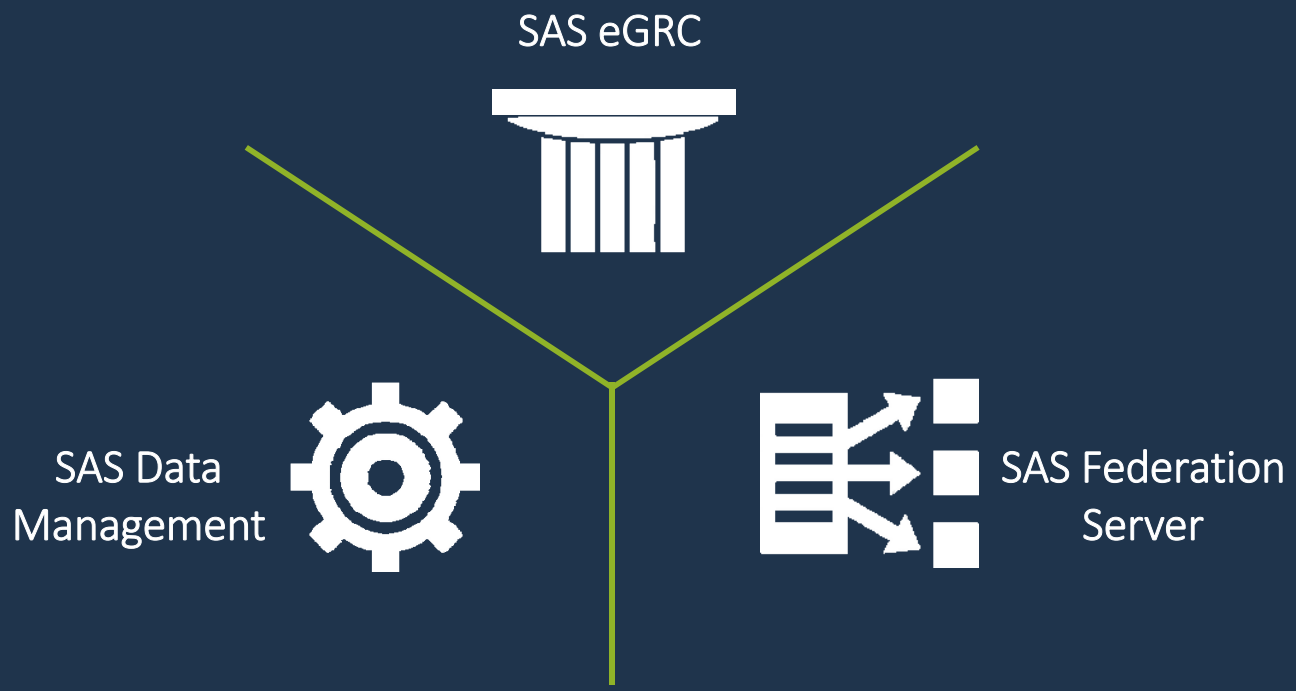




Yes… Data Quality issues also need to be a part of the reporting! (show & shame)

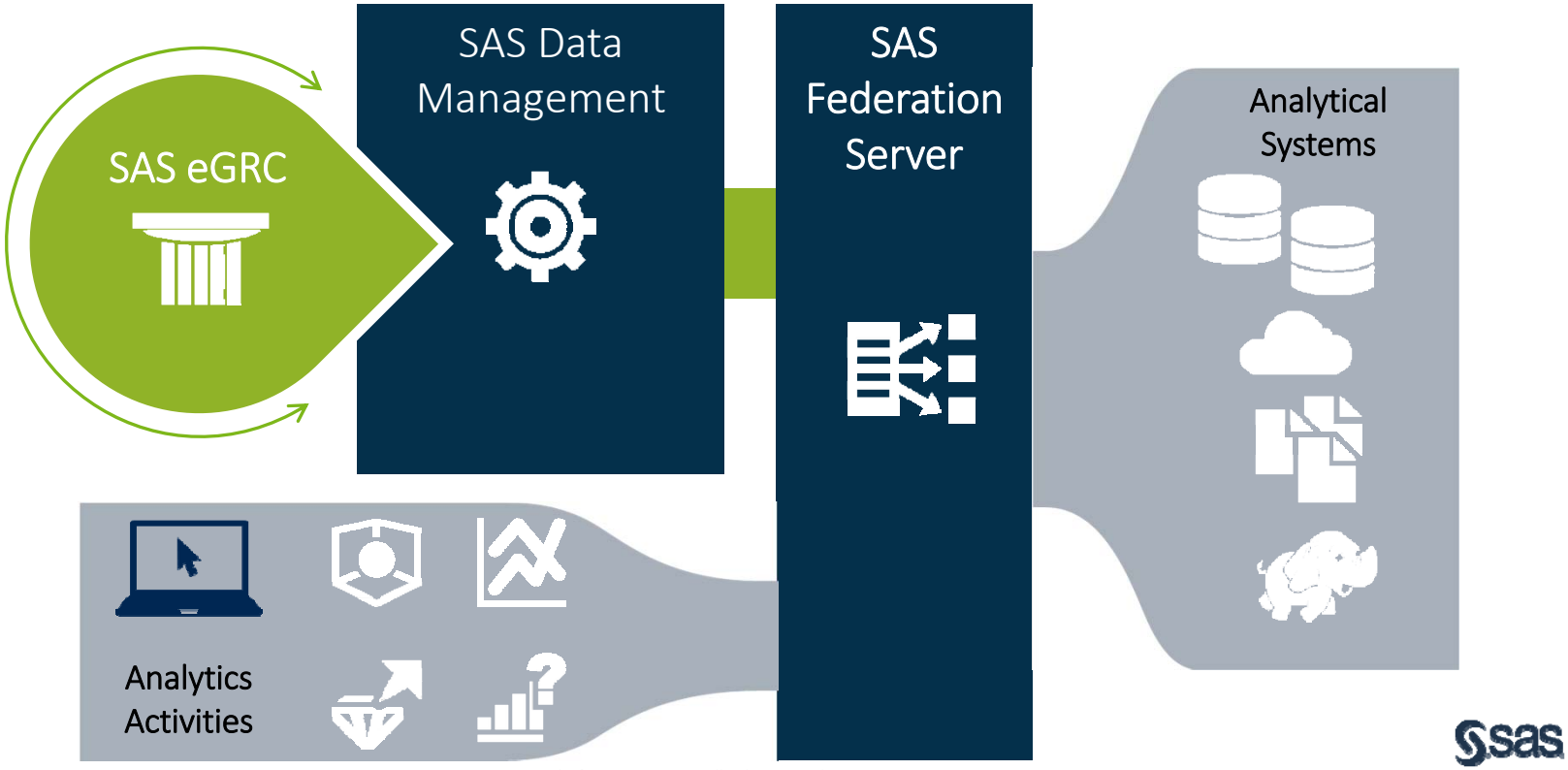
SAS for Personal Data Protection

SAS Components



SAS for Personal Data Protection

SAS Components



P

SAS Enterprise Governance Risk & Compliance

- Develop an enterprise view of your risk exposure throughout all common risk management stages risk identification, assessment, response and monitoring
- Automate the management of governance, risk, and compliance (GRC) data.

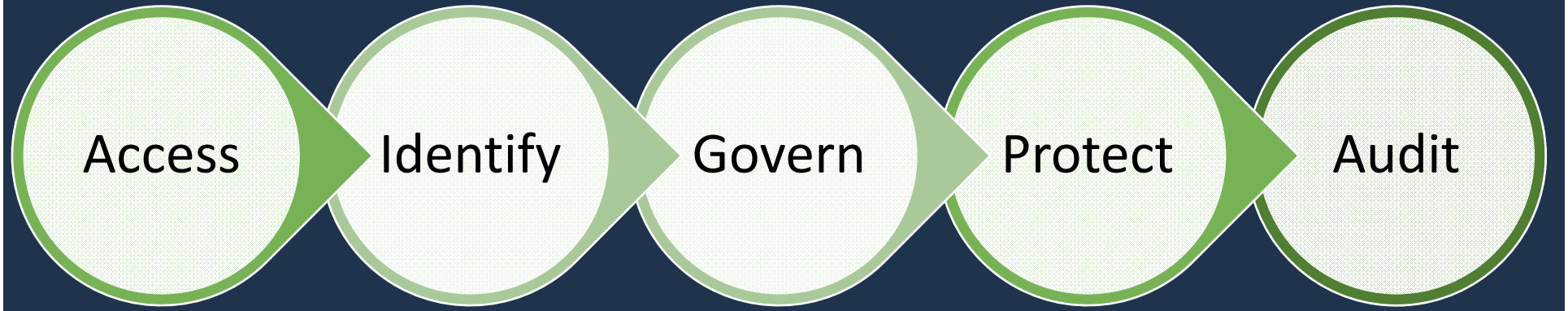
SAS Data Management

- Discover Personal Data (Identification & Extraction)
- Define Business Terms in order to align Business & IT
- Link Systems, Processes & Business Owners in data flows
- Monitor Personal Data Over time & Retention

SAS Federation Server

- Manage & Secure Access to Personal Data
- Mask Personal Data
- Minimize Personal Data
- Report on Personal Data Access

Getting started…



- Connect to all relevant DB and systems

- Profile data to get a structure and format overview.
- Identify Personal Data, in DB, tables and fields.
- Start looking at deduplication
- Catalogue findings on field, table and DB level

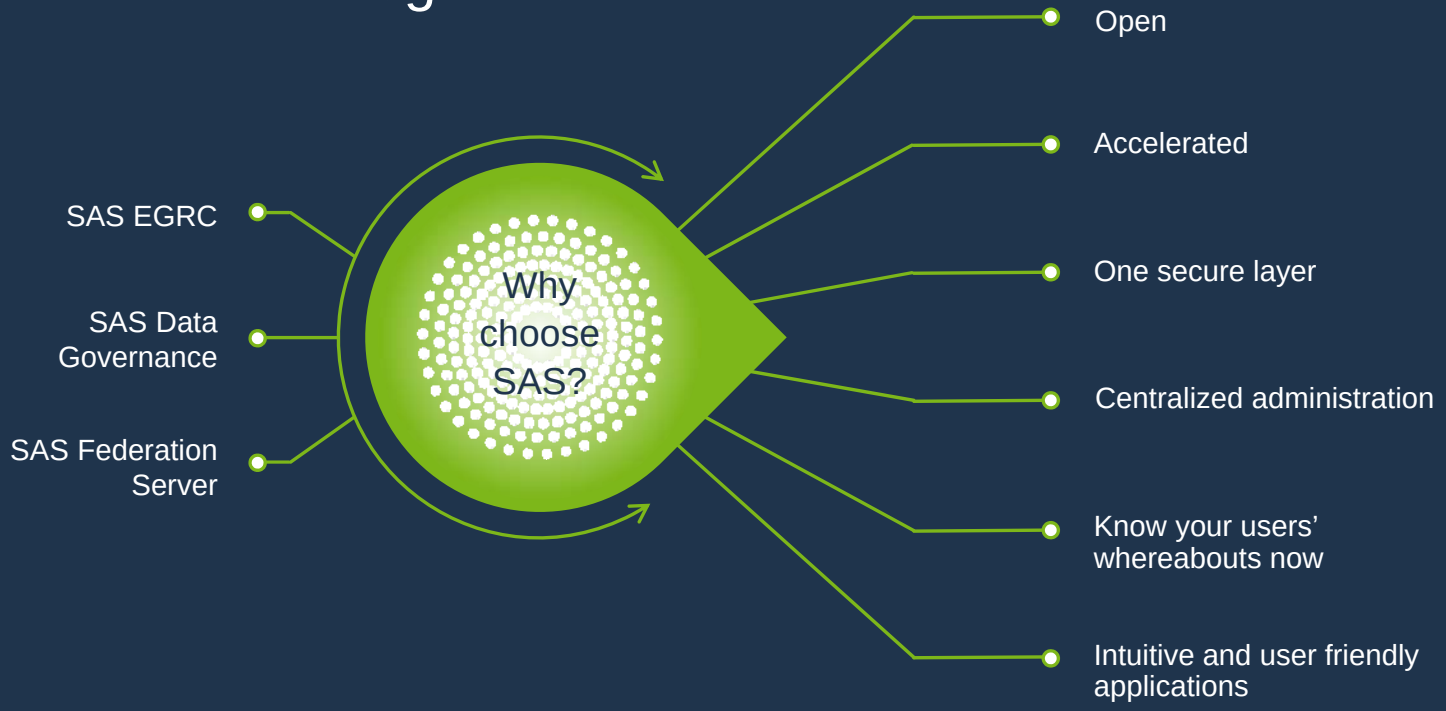
- Get a clear overview on roles & responsibility.
- Define Business Terms in order to align Business & IT
- Link Systems, Processes and Business Owners in data flows

- Anonymization (removing PD)
- Pseudonymization (replacing PD)
- Encryption (encoding PD)
- Secure SAS data sets

- Report
- Visualize
- Centralized administration
- See your users' whereabouts
- Show user log activity for all relevant data store?

sas

EU General Data Protection Regulation



Thank you for your time..

Presented by:

Casper Pedersen
Thought Leader & Certified DPO
SAS Global Data Management