storebrand

A Circle of Trust:
GDPR and Infosec as business enablers

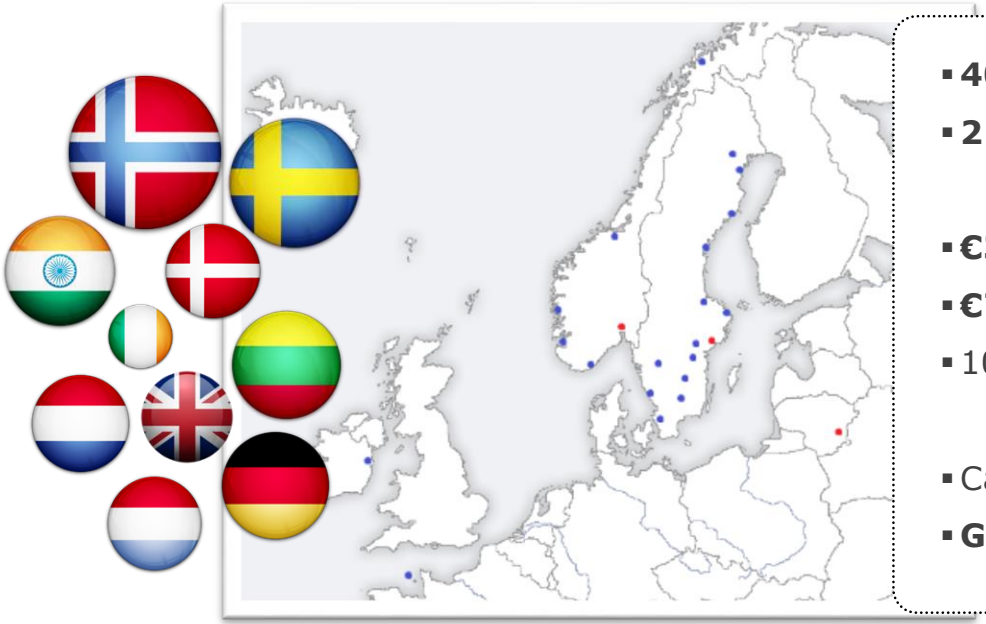
ISACA Netherlands Chapter
11.04.2019

Magnus Solberg, CISSP, CISM
Principal Security Manager
Storebrand Group

storebrand

(just some quick facts)

Nordic leader in occupational pension – asset mgmt – insurance - banking



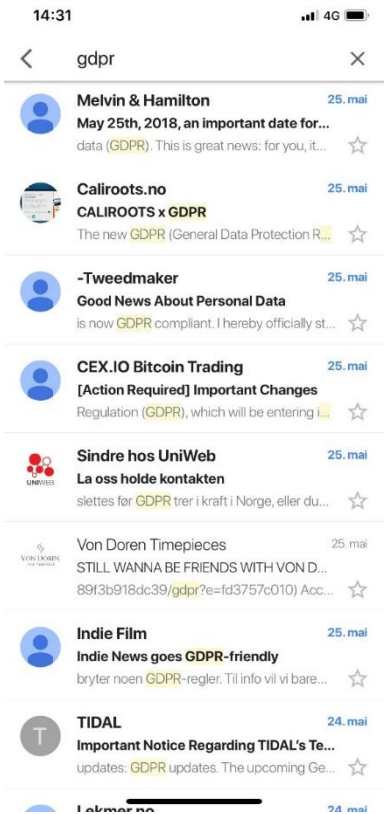
- **40.000** corporate customers
- **2 million** individual customers

- **€34 billion** Group profit
- **€73 billion** in assets under management
- 100% of assets mngd by **sustainable criteria**

- Ca. **1 800 employees** in Norway/Sweden
- **Global sourcing** of business & IT services

Trustworthy – Straightforward – Forward-thinking - Sustainable

GDPR – a flashback



storebrand

What do they know about you?

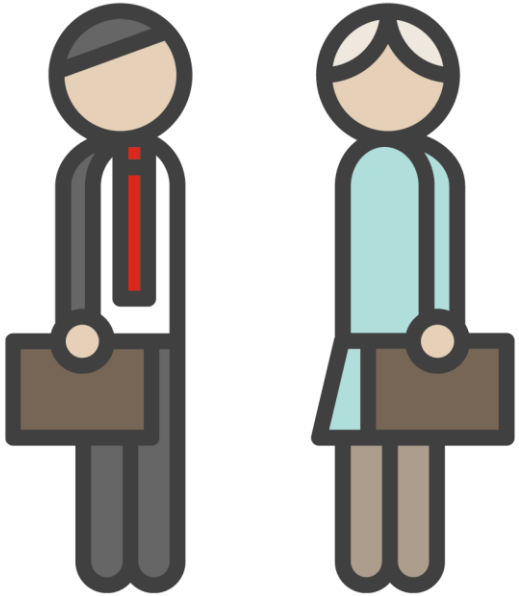
storebrand

A "random" use case: Let's make it fair (and profitable)

Sven, 43

From: Oslo
Income: 765.000
Wealth: 1.4m
Children: 3

Married
Higher education
Low debt



Marte, 41

From: Bergen
Income: 800.000
Wealth: 1.2m
Children: 2

Married
Higher education
Low debt

Use, abuse, and lack of transparency

- Companies have shared and NOT cared for too long…
  - Just like you and me…
- Legal or illegal – does it really matter?
- Sloppy security leads to messy breaches!
- Consumers gonna consume…but who will they choose?

storebrand

Are we seeing a shift?

- Storebrand customer survey points to an **increased awareness** and concern among consumers
- …**but customers were positive** to sharing more information - *if they saw the value and if we were 100% transparent*
- **Partners and corporate clients** are increasing their supplier audit efforts – as are we!
- **Sustainability index** is more and more based on infosec
- **Government agencies** (Finance Inspection, Data Inspection) are on the offensive

"It is critical that our brands remain not only in a safe environment, but a suitable one. Fake news, racism, sexism, terrorists spreading messages of hate, toxic content directed at children…it is in the digital media industry's interest to listen and act on this. Before viewers stop viewing, advertisers stop advertising and publishers stop publishing."

- K. Weed, CMO Unilever

Who's responsible?

Industry

Creates basis for goods and services

Government

Regulates goods and services

Business

Sells/provides goods and services

Individuals

Consumes goods and services

Who's responsible?

Industry

Privacy & security by default not by choice/target market

Government

Strong, relevant, and future-oriented regulations

Business

Corporate responsibility, transparency and accountability

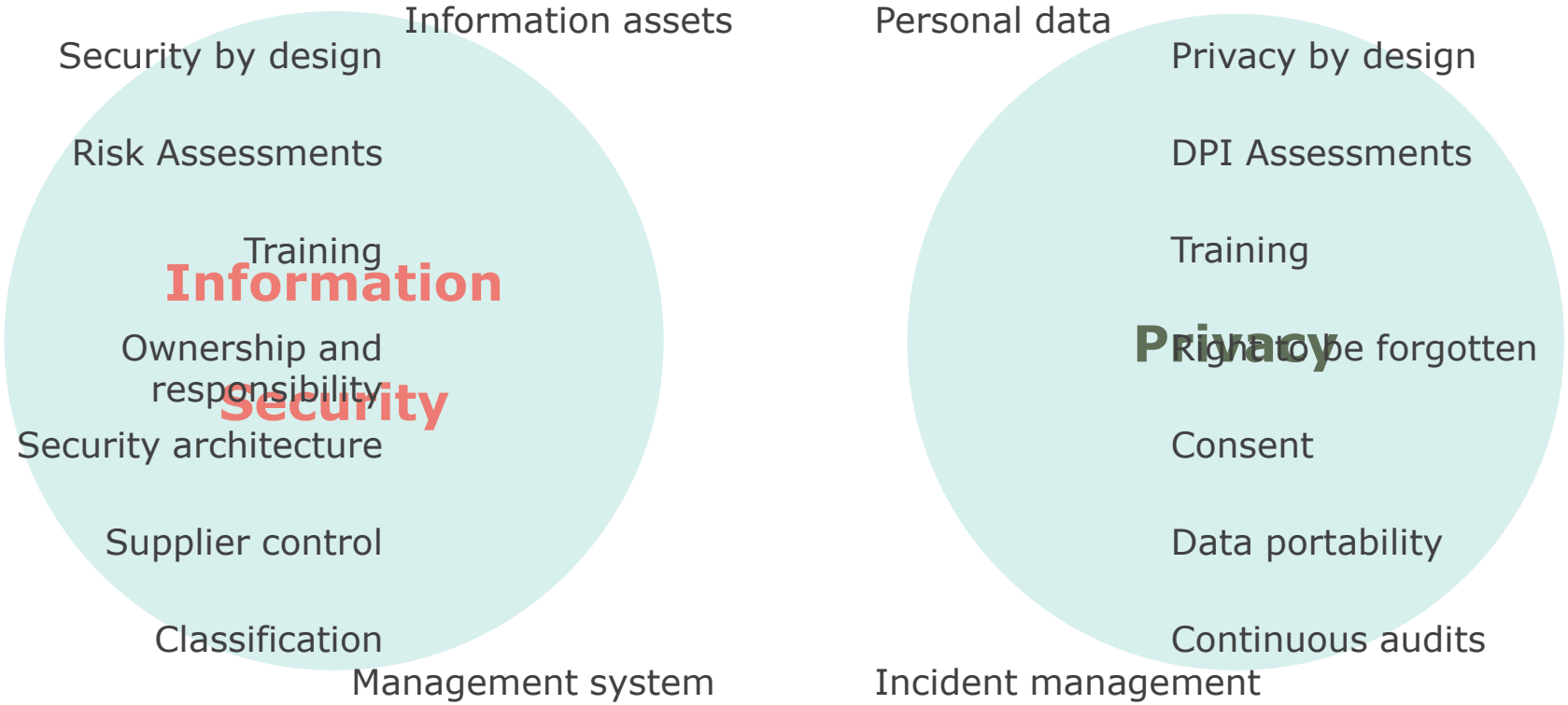
Individuals

Informed, conscious choices and strict demands to business


I'VE DESTROYED ALL OF OUR OLD CREW LISTS...
I BURNED THE LOT AND THREW THEM OVERBOARD...
WHY ON EARTH WOULD YOU WANT TO...
GDP ARRRRRRRR!
imgflip.com

storebrand

Digital trust: Prerequisites



storebrand

The Program "Privacy 2018 – Digital Trust"

GDPR-program
Privacy 2018 – Digital Trust
16 Group-wide "work streams"

01. Employee data and HR
02. External data processors
03. IT changes
04. Building blocks for good privacy
05. Overview of Storebrands processing
06. Internal guidelines & policies
07. Training
08. Assessments of privacy impact/DPIAs
09. "My privacy page" and consents
10. Incident/breach handling
11. Information and agreements with corp. clients
12. Information and agreements with private clients
13. Organizational concsequences
14. Data warehouse
15. Secure customer communication
16. Unstructured data

Supported by the ISMS project

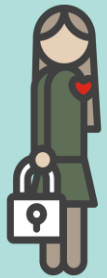
DEFENDABLE POSITION

DIGITAL TRUST

storebrand

Checklist for good privacy

1. **Managers and employees have the required expertise on privacy and security**
2. Purposes have been defined, and mapping of which personal data that's being processed has been established
3. Legal grounds for all processing can be documented
4. **Overview and requirements of external data processing has been established**
5. Clients and employees have been informed of our processing
6. **Policies, procedures, and tools that protects the rights of clients and employees have been established**
7. Consents are compliant with GDPR requirements
8. Processing of minors' personal data is especially ensured
9. Procedures for incident reporting and handling are established
10. Processing that involves high risk is identified and managed
11. **IT systems and development satisfies requirements for "privacy and security by design"**
12. Responsibility for privacy has been clearly placed
13. Requirements for processing across regional/international borders are ensured
14. **Sufficient information security for personal data is achieved**



storebrand

The ISMS project

The following main activities needs to be carried out on regular basis as part of the ISMS:

- Implement and follow up corrective action based on risks identified in the risk assessment
- Close identified gaps from the gap analysis
- *If the risk is too high, mitigating controls must be implemented."*

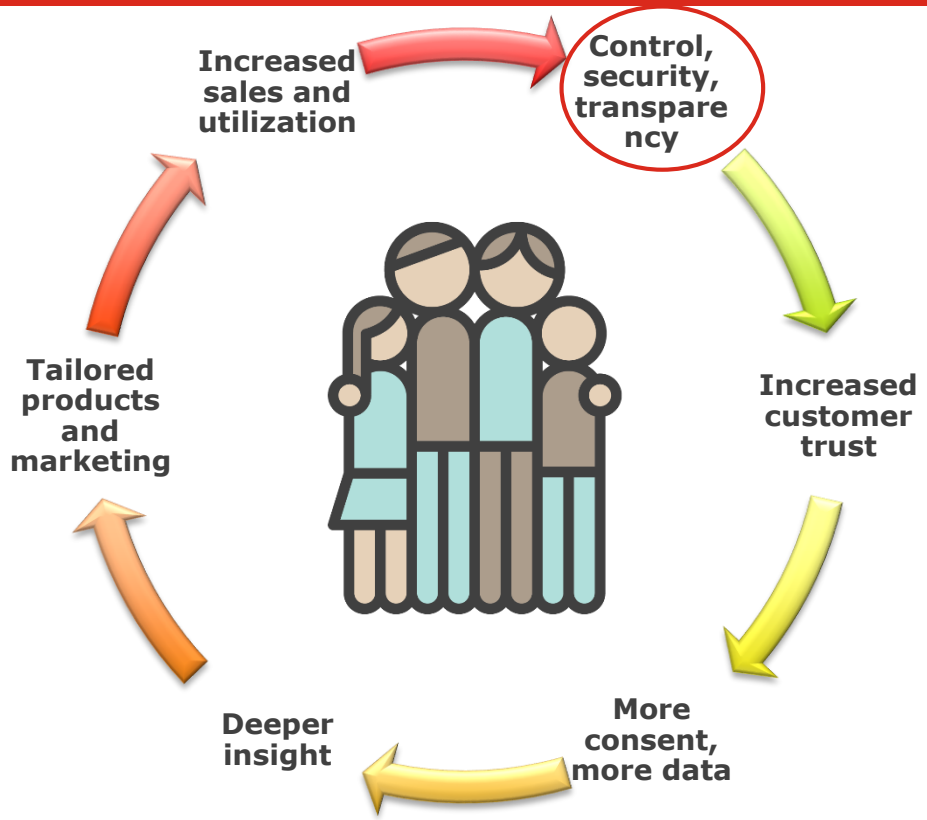
- Identify and classify information element, and document in the Business Impact Assessment *(BIA)*
- *"We must know what to protect and the value of our information in order to be able to protect our assets"*

- Identify and evaluate information security risk. Management of information security risks is integrated to the ordinary and existing risk management process for operational risks in the group
- *"We must understand the risk of potential information security incidents."*

- Review compliance to the information security controls. In total, 114 information security controls will be implemented and followed up in Storebrand as a part of the ISMS
- Please visit ISMS Controls (in menu on the left) for guidance and mapping between policies, controls and relevant tools
- *"We must know how we protect our information assets"*

storebrand

The Circle of Digital Trust!



storebrand

Summary

- **Personal data is the new currency** in the digital economy
- It's been "the Wild West" for too long – but **the individual is now in the driver's seat!**
- **Companies and organizations** need to take responsibility
  - Transparency
  - Compliance
  - Information Security
- Don't let all that time and money spent on getting GDPR compliant **go to waste!**
- **GDPR + information security = <u>Business enablers</u>**
  - It WILL pay off
  - MARKET you efforts!

Digital trust is the ultimate differentiator - make sure you survive in the new economy!

storebrand

Thanks! Questions?