GDPR – what we "really" did

Urban Karlström
Stockholm, 2018-10-01
Forefront Consulting guidar företag och organisationer genom det digitala landskapet

380+
Medarbetare

Från starten 2008 har vi vuxit organiskt. En del av tillväxten sker genom vårt traineeprogram som nu är inne på sjunde generationen.

Huvudsponsor

9
Kontor

2
Världsdelar

Strategi & Verksamhet
Design
Teknik
Agenda

- What is GDPR?
- Which areas affected SAS?
- Our environment
- What was implemented step by step
- Decisions taken under ways
EU General Data Protection Regulation (GDPR)

- Intends to strengthen and unify data protection for individuals within EU
- Enforcement began on 25 May 2018
- Directive (recommendation) vs Regulation (law)

The regulation affects any organization (commercial or governmental) globally who collects, stores or processes data on EU individuals.
Changed the way we are allowed to handle personal data!

All kind of information, processed by automated means, which directly or indirectly (including pseudonymized data) can be related to a customer who is alive.

Aggregated or anonymized data that can no longer be connected to a specific customer is not considered personal data.
Three concepts

1. Personal data
2. Personal identifying data
3. Pseudo anonymization

- Name
- Address
- Email
- Birthdate
- Social security number
- Phone number
- IP-address
# 5 Main areas applicable for SAS

<table>
<thead>
<tr>
<th>Area</th>
<th>Tasks</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiling and Consent Management</td>
<td>Verify that customer data will be processed according to given consents and GDPR principles.</td>
</tr>
</tbody>
</table>
| Data minimization                            | Verify that we don’t collect and store data that is not being used and that every roll has access to data on a “need-to-know basis”.  
(Is there data that we don’t need to store? Is it possible to “hide” the customer when not needed?) |
| Customer Cleansing                           | Verify that customer data will be cleansed/anonymized if the customer withdraw the consent, the expire date of the consent is reached or the customer dies. Also includes the right for the customer to correct data and block data from being erased. |
| Right to access and portability              | Verify that the customer can get a data extract, in digital format if required.                                                                 |
| Access right revision                        | Verify that personal data will be handled in a safe way and that data access is limited to the right roles.                                |
Our environment

- SAS DI-Server
- 60 TB data
- 10 yrs + of historical data
- Data from central DWH, operational systems and external files
- Sales and customer details data
- Data for customer analysis, modelling, campaigns and reporting
- Ca 50 analysts and 300 report consumers
- EG and SAS Studio as user tools (reporting in Tableau)
What was implemented?
Implementation

- A company wide system for anonymization and cleansing of customers
- CRM system master for deleted/anonymized customers
- Signals to and from other systems
Decision – Pseudo-anonymized data is ok to be used company wide unless retention time has passed.
Decision – KISS!
Implementation – Step 0

- A data dictionary was created
  - Identify PI data
  - Used for documentation
Decision – PI data not in historical data, refreshed on a daily basis. Only to be used for address labeling and send outs.
SAS Architecture

- Separate PI-data into special storage (dedicated libnames).
- Drop PI-data columns from primary layer and historical tables.
- ETL-flows updated for dropped columns
- Secure ETL-flows so PI data is refreshed in staging libnames.
- Create datasets with flags for PI-data existence.
- Central DWH table with anonymized/cleansed customer numbers and collected consents imported.
Other development
Macro for copying and encrypting test data.
  • Creates bogus ids.
  • Encrypts PI columns.
Anonymization of data older than 10 years

Macros and DI-transformations with control tables for creating bogus id variables. Process run twice a year. Removes connection to any customer.
The “darn” email address!!

Email address primary key in some integrations.
Macro and DI-transformation to encrypt email address.

\[\text{EmailKey} = \text{put(md5(cats(“Salt”,email)),hex32.)}\]
Restrict access with use of ACTs
Cleansing of logs and external files

– Delete them all !! –

Macros and jobs with control tables to configure and perform deletion of files in the environment.
(Back-ups were reviewed).
All data stored and created in SAS was either distributed from other systems or deemed out of scope for A&P.
## Summary for SAS

<table>
<thead>
<tr>
<th>Area</th>
<th>Measures taken</th>
</tr>
</thead>
<tbody>
<tr>
<td>Profiling and Consent Management</td>
<td>Campaigns and send outs honoring consents and anonymization from DWH.</td>
</tr>
<tr>
<td>Data minimization</td>
<td>Data totally anonymized after 10 years. Data collected according to “balance of interests”.</td>
</tr>
<tr>
<td>Customer Cleansing</td>
<td>PI data separated into special storage honoring anonymization from DWH. Logs and external files deleted.</td>
</tr>
<tr>
<td>Right to access and portability</td>
<td>Out of scope for SAS.</td>
</tr>
<tr>
<td>Access right revision</td>
<td>ACTs for restricting access implemented.</td>
</tr>
</tbody>
</table>