

THESSALONIKI
digital analytics
MEETUP

Getting practical on GDPR

Thessaloniki Meetup #4

20 Dec 2017



“Information is power”

Power resolves to income...

Maximizing info assets

- Gathering data **is what we have been up to** all these years.
- So now... almost all organizations keep personal data one way or another.
- Worse... for:
 - core activities
 - supporting activities
 - no activities
- Even worse... in many:
 - places
 - subcontractors
 - systems
 - forms

Information is risk

Risk resolves to expenses...

State of play

- EU Regulation. No national law is required. Effective 26/5/2018.
- Regulation = harmonization across EU. No workarounds...
- Notorious fines. Main drive for most organizations.
- Unofficially some “consensus” has been implied in Greece for 6 additional months (2018 Q3-Q4)
- Risk driven supervision. For 2018 Q3-Q4, HDPA (www.dpa.gr) shall focus on critical sectors and formal complaints
- HDPA has increased its auditing staff
- Several complaints may be submitted on Day 1

Threat or Opportunity?

Yes, a cliché... but, still, we've seen the opportunity approach working in many orgs!

Objectives

Compliance (threat driven)

Hard requirements

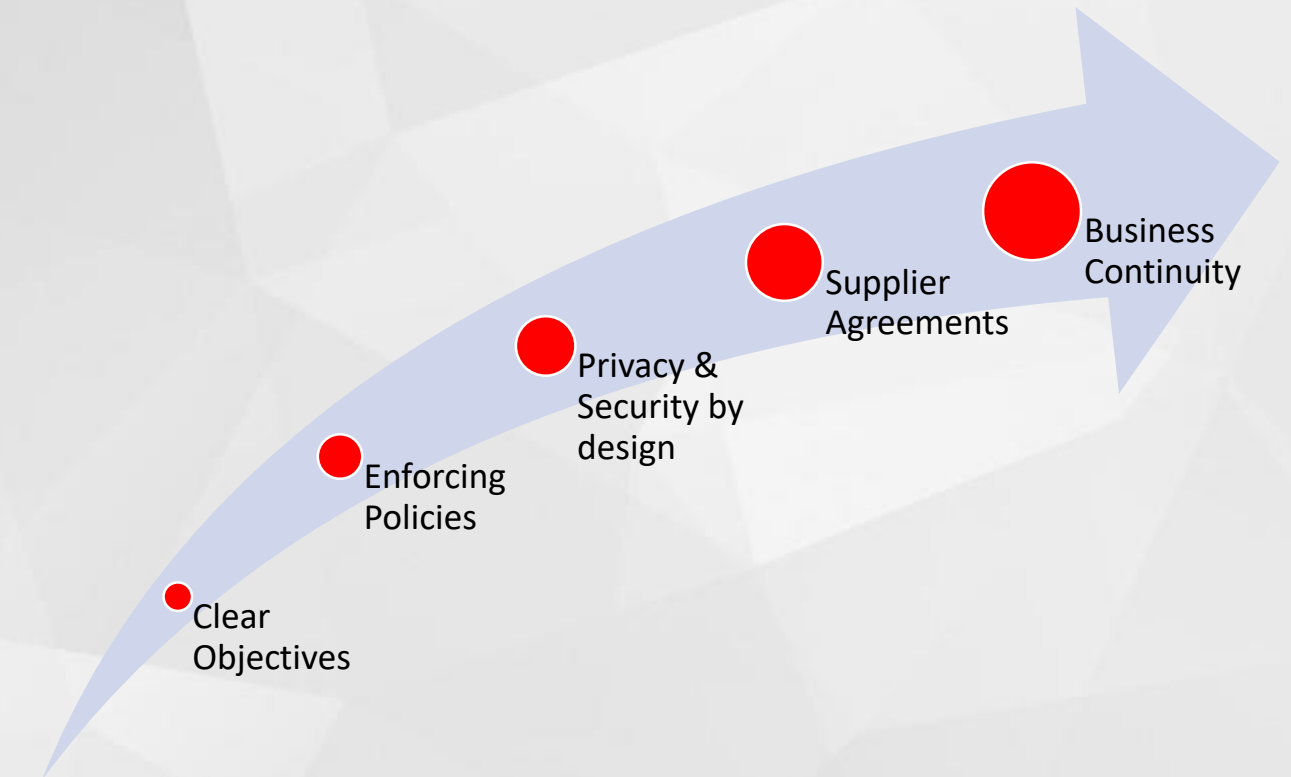
- Implementation

Soft requirements

- Risk driven
(don't forget subjects!)

✓ Budget: Calculated risks in balance sheets

Development (opp. driven)



✓ Budget: Calculated risks + Productivity improvements + Market share increase (med/long term)

A fair assessment

Through the eyes of an auditor...

ISO/IEC 27001 vs. GDPR (Security vs. Privacy)

- 27001 certification is not required & **does not** ensure GDPR compliance
- It serves a different objective: Security Management
- Information Security vs. Data Privacy
 - Google: Probably **highly secure, but highly intrusive** in terms of PD collection
- 27001 is voluntary, GDPR compliance is mandatory
- Organizations may **benefit from 27001** framework and good practices
- It is probably a good approach / cost effective solution to combine these

GDPR certification

- Not required. Recommended.
- No certification scheme yet available
- Non-accredited certification is available

- ✓ Can be used as a compliance evidence
- ✓ Can verify compliance program results

What would an auditor expect?

Evidence of:

- ✓ explicit implementation for hard requirements
- ✓ due care and diligence for soft requirements
 - * based on risk assessment

What would an auditor review?

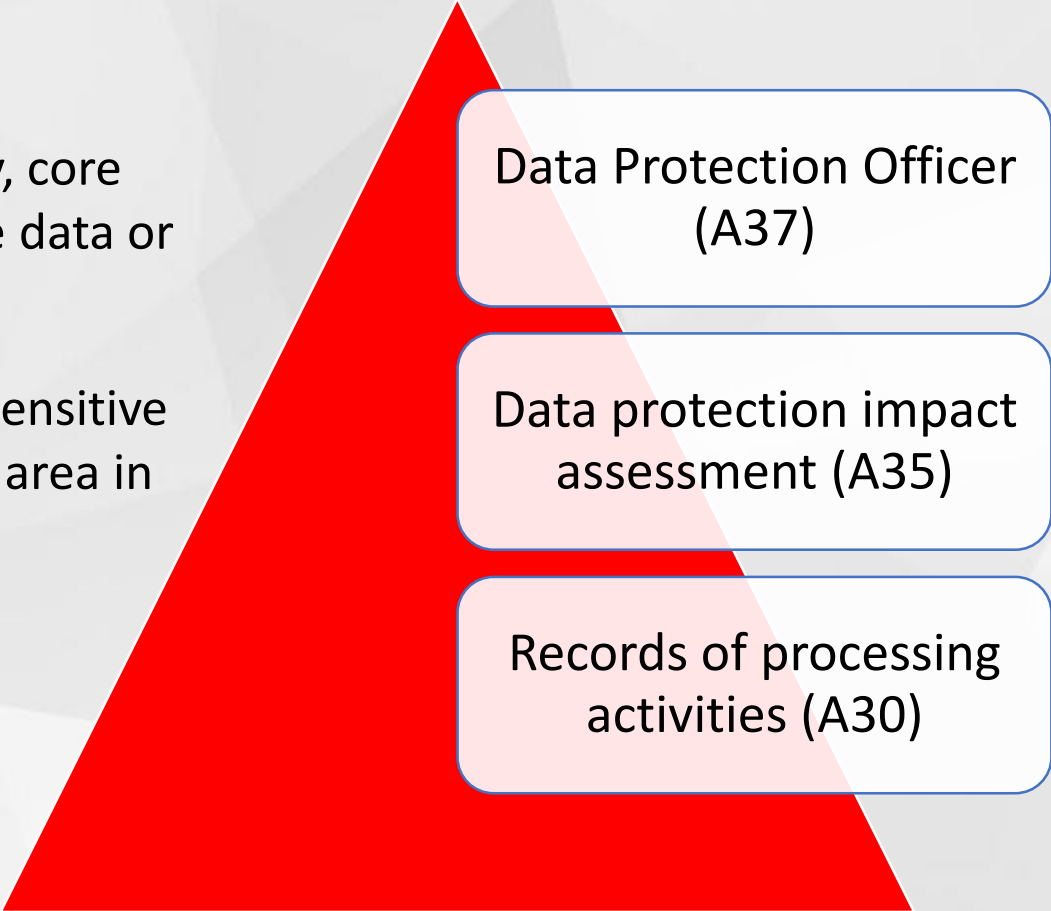
- Complete organization profile (size, activities, locations, personnel, information systems, subcontractors)
- Minimum common requirements
 - Documents: Policies, procedures, etc.
 - Records: Processing registry, legal basis evidence, personnel NDAs, subcontracting agreements, etc.
- Additional requirements (e.g. DPIA, DPO)
- Audit trails:
 - Core/production activities (products, projects, services)
 - Supporting activities (personnel, cameras, web apps, hosting, profiling, marketing, ...)
 - Subcontracted activities (either core or supporting)
 - Do, Plan, Check, Act records (planning, monitoring, assessing, improving evidence)
 - Incident Reports, Complaint Reports, Non-Conformancy Reports
 - Technical Assessments (vulnerabilities, penetration tests)

Examples of requirements to be audited

High risk (public authority, core activities include sensitive data or monitoring in large scale)

Low/med risk (profiling, sensitive data or monitoring public area in large scale)

Everyone (baseline)



Data Protection Officer
(A37)

Data protection impact
assessment (A35)

Records of processing
activities (A30)

Record of Processing Activities

- This is normally where the GDPR compliance project begins
- Exhaustive list of information processed by the organization
- Information per information item:
 - Controller info
 - Purpose of processing
 - Description of data subjects
 - Personal data categorization
 - Recipients
 - Transfers to third countries
 - Retention period
 - Technical + Organizational Measures
 - Legal basis
- In case of processor, an activities file per controller
- Evaluate your current exposure (enables Gap Analysis)

Data protection impact analysis (DPIA)

- Builds on data inventory / processing activities file
- Mainly a risk management process

```
for each activity in processing_file {  
    activity.evaluateRisk();  
}
```
- Purpose: evaluate and document actual risks
- Purpose: identify “red” or “orange” processing activities
- For those activities, propose mitigation actions
- Outcome: acceptable risks (“risk appetite”)
- References:
 - GDPR Article 35
 - [WP-248 “Guidelines on DPIAs”](#) (by Working Party 29)

DPO designation

- Dual role: consultant + supervision
- A small Supervisory Authority in the company itself
- Strongly protected against employer's misconduct (for its DPO role)
- Liability remains on the organization
- Should be easily reachable
- Competency in terms of
 - education/training; legal and technical overview
 - experience, overall view of the company (e.g. junior empl. hardly eligible)
- In any case lack of conflict of interest must be ensured (not to participate in the means and purposes of information processing)
- Combining the later 2 -> main obstacle for appointing an internal DPO

DPO certification

- No certification is required by the Regulation, though recommended
- Written exams, usually after 3-5 days of training on GDPR
- One may take exams without training
- Skills required (degree, infosec profile, law profile)
- Personnel certification (ISO 17024)

References for DPO role:

- GDPR Articles 37, 38, 39
- [WP-243 “Guidelines on DPOs”](#) (by Working Party 29)

Some examples

Let's get our hands dirty...

Simple OOTB web analytics

- ACME Toys (www.acme-toys.gr) has deployed Google Analytics in its corporate website
- Potential Personal Data:
 - IP, Page, Page URL, Page Title, Referrer, Device Details, Internet Provider of the client
 - Page URL when personal data is used in it (e.g. email address)
 - Internal search terms (e.g. search with my name in a site)
 - Fields accepting user input (e.g. contact forms)
- Concerns:
 - Processing of the above PD without legal basis
 - Breaching processor DPA (Google requires that no sensitive PD are stored)
- Recommendations:
 - Enable Google Analytics IP obfuscation (anonymization)
 - Implement PD masking (anonymization)
 - Pass it to a privacy consent, in case of no conflict with DPA

Cookies / Local Storage

- ACME Toys is using cookie identifiers (own or third-party) to track customers (e.g. returning customers, functionality, etc)
- Potential Personal Data:
 - SessionID: Pseudonymized ID, except if combined with PD
 - VisitorID (sticky ID, stored in cookie): Usually for tracking, normally considered PD, unless cannot be used to identify person
- Concerns:
 - Converting pseudonymized IDs to PD and processing (e.g. profiling) without legal basis
- Recommendations:
 - Cookie consent form with clear positive consent acquisition
 - Privacy policy with clear terms and plain language

Excess data or processing purpose

- ACME Toys asks for visitor's gender when subscribing for the newsletter
- Potential excess data:
 - The newsletter is similar for both male and female recipients
- Concerns:
 - Processing of irrelevant data without legal basis
- Recommendations:
 - Remove the male/female data input, or...
 - Draft a forward-looking consent form (hint to escape from future consent updates)

Remarketing

- ACME Toys is using a remarketing platform to target visitors via email based on past behavior
- Potential personal data:
 - Cookie Identifier
 - Personal traits/habits
 - Email address
- Concerns:
 - Profiling visitors based on actions
 - Customer has not given consent
 - Profiling process is not editable by humans
- Recommendations:
 - Get clear consent, publish privacy/cookie policy
 - Establish manual process
 - Allow clients to be excluded
 - DPIA required, DPO possibly

Personnel records

- ACME Security Services (www.acme-security.gr) maintains a personnel file for employment, insurance, payment purposes
- Potential Personal Data:
 - Contact details, family information, identification IDs (Tax number, Social security number, ID)
 - CV related information and records (degrees, trainings, etc)
 - Criminal records (special category)
 - Health records (sensitive data)
- Concerns:
 - Data breach, physical records security
 - Protection of sensitive information from unauthorized access (internal or external) or use
 - Sub-contracting of payroll
- Recommendations:
 - Security controls (see ISO 27001/2)
 - Organizational and technical controls to enforce usage only for the intended purpose
 - Strict terms and agreement with a compliant payroll processor (monitoring, obligations)
 - DPIA + DPO designation required.

Case study

Just a minute...

Santa Claus Ltd.

Receives kids' letters every year... so several concerns arise:

- Are these data considered **personal**?
- What is the **legal basis** for processing this personal data?
- Are these considered **sensitive**?
- Does he have a **retention** policy?
- Finland is a member since 1995, but does he use any **non-EU locations or processors**?
- Are there any special issues since subjects are **kids**?
- Is figuring out whether a kid behaved throughout the year considered **profiling**?
- Is there a designated **DPO** and where can I find contact details?
- Is the data center **secure** and personnel (elves) **certified**?
- Does he have a legal basis to perform further actions, e.g. use address to enter through the **chimney**?



Santa Claus Ltd.

Receives kids' letters every year... so several concerns arise:

- Are these data considered **personal**?
- What is the **legal basis** for processing this personal data?
- Are these considered **sensitive**?
- Does he have a **retention** policy?
- Finland is a member since 1995, but does he use any **non-EU locations or processors**?
- Are there any special issues since subjects are **kids**?
- Is figuring out whether a kid behaved throughout the year considered **profiling**?
- Is there a designated **DPO** and where can I find contact details?
- Is the data center **secure** and personnel (elves) **certified**?
- Does he have a legal basis to perform further actions, e.g. use address to enter through the **chimney**?



Things do not look so good...



Have fun!

And beers...