GDPR

MAGDALINI SELANIKLI

JULY 5TH, BUDAPEST

GDPR

- Regulation 679/ 2016
- Background Directive 95/46EC
- Recommendations of working party 29
- Recommendations by ENISA (European Union Agency for Network and Information Security)
- ISO27001 is a compliance framework but not 100%
- Activated on May 25th 2018
- Industry had more than 2 years to comply
- National examples of compliance vary with the Scandinavian scoring the highest

GDPR

Definition:

Personal data are any data which can alone or in combination provide unique information for a living person

GDPR

Usually the name along with other 2 information is enough for identification

GDPR

- Processing is as little as receiving in an email or storing in a database, and as big as transmission and dissemination

GDPR BASICS

- DATA that contain personal information **can** be collected but
  - **There needs to be a reason**
  - **Collect only those data needed and not collecting data for the sake of collecting data**
  - **Examine lawfulness of processing**
  - **Processing needs to be proportionate**
  - **You need to foresee the right to access and erase**
  - **NEED TO BE PROTECTED against internal & external threats**

GDPR BASICS

- The following personal data CANNOT be processed (except if for public interest)
  - Political & Religious beliefs
  - Sexual orientation
  - Racial characteristics
  - Biometric and Genetic data

GDPR EXCEPTIONS

- National security
- Defense
- Public security
- Judicial independence
- etc

GDPR

- Elements introduced by the new regulation
  - Data controller
  - Processor
  - Data protection officer
  - Processing should be law full and fair
  - Breach incidents: notify competent authorities within 72 hours after having become aware of it (nature of the breach, actions to mitigate effect)
  - Lead supervisory authority for controlling breach events

GDPR BASICS

- Elements introduced by the new regulation
  - Self regulation in compliance
  - Security by default
  - Anonimization/ Pseudonymisation
  - High level of penalties similar to competition law violation penalties (2%/4% of turmover up to 10,000,000- 20,000,000)

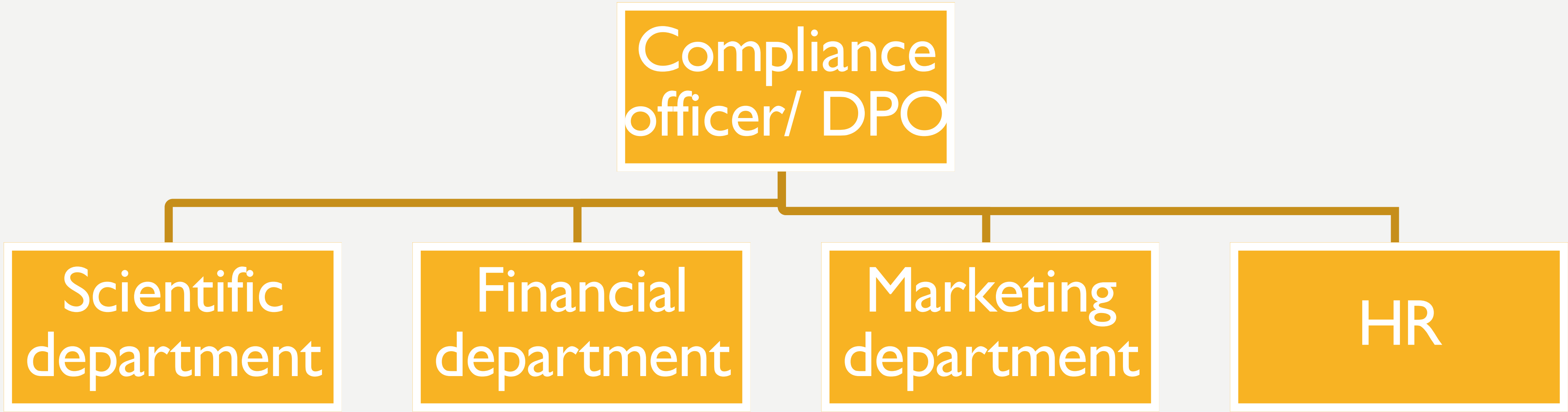
GDPR RIGHTS

- Right of access by the data subject
- Right to rectification
- Right to be forgotten
- Right to restriction of processing
- Right to data portability
- Right to object automated individual decision making

GDPR

- Lawfulness of processing
  - Consent
  - Necessary to fullfil contractual obligations
  - Necessary to comply with legal obligations
  - Public interest
  - Legitimate interest except if this interest is overridden by the fundamental rights and freedoms of the subject

COMPLIANCE CASE STUDY



Compliance officer/ DPO

Scientific department

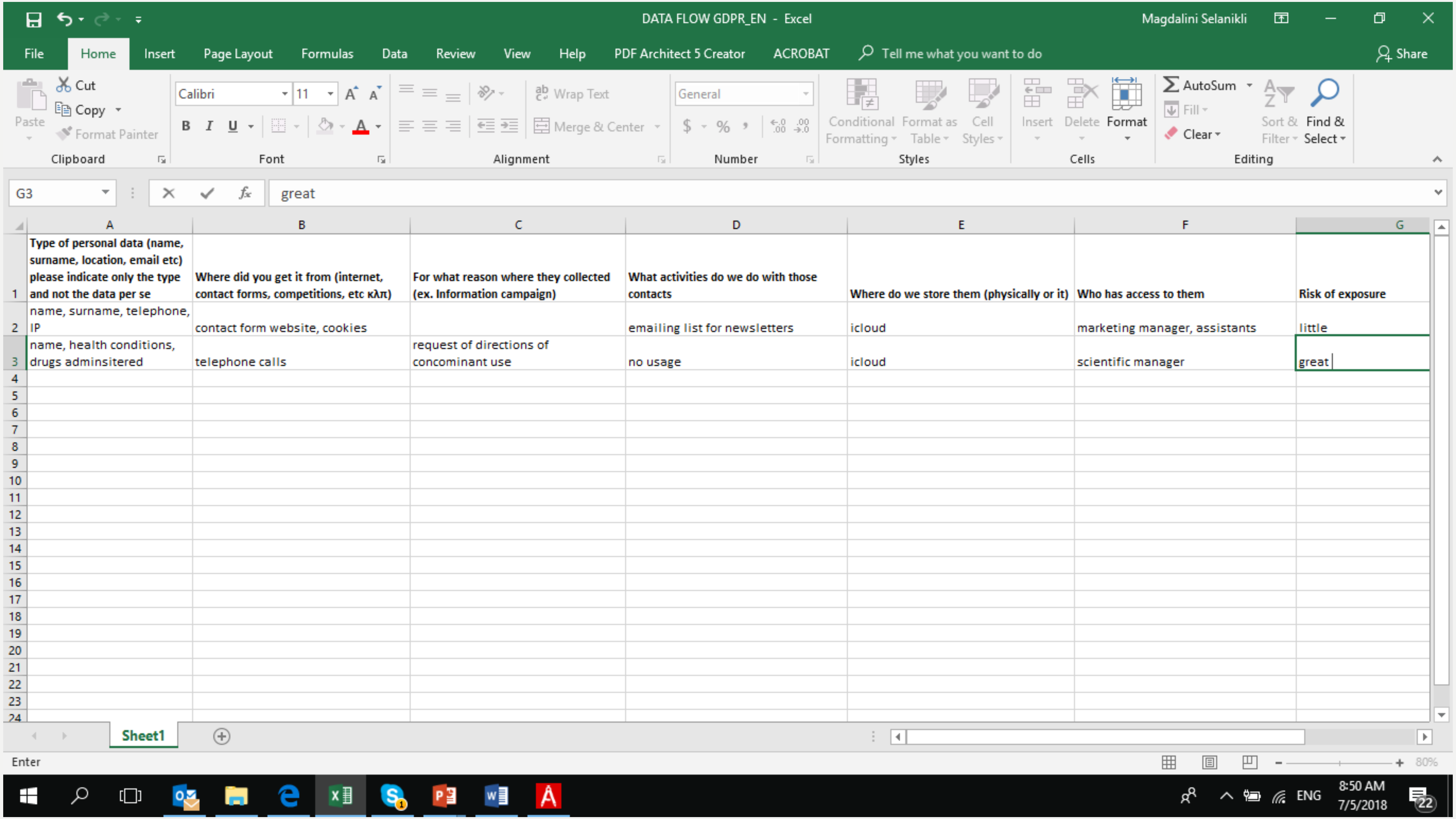
Financial department

Marketing department

HR

GDPR COMPLIANCE

- Inspect, locate where data is and what kind of data is
- How important is that data to your business
- Evaluate severity/ define sensitivity (DPIA- Data Protection Impact Assessment)
- Define processing and roles (data controller or processor)
- Change internal rules – adopt policies
- Redesign security (security by default)
- Assign roles (DPO)
- Adopt breach incident policies



	A	B	C	D	E	F	G
1	Type of personal data (name, surname, location, email etc) please indicate only the type and not the data per se	Where did you get it from (internet, contact forms, competitions, etc κλπ)	For what reason where they collected (ex. Information campaign)	What activities do we do with those contacts	Where do we store them (physically or it)	Who has access to them	Risk of exposure
2	name, surname, telephone, IP	contact form website, cookies		emailing list for newsletters	icloud	marketing manager, assistants	little
3	name, health conditions, drugs adminsitered	telephone calls	request of directions of concominant use	no usage	icloud	scientific manager	great

GDPR- FINANCIAL DEPARTMENT

- Audit revealed three kind of data:
  - Personal data of employees
  - Personal data of clients
  - Personal data of prospective clients/ suppliers

GDPR- FINANCIAL DEPARTMENT

- Employees signed new consent forms
- Clients received new policy rules
- Changed internal rules for:
    - Money & Debt collection
    - Payments
    - Request handling (containing sensitive financial information)
    - Expense reports
    - Prospective clients evaluation

GDPR- HR

- Audit showed three categories of data:
  - Personal information of current – active employees
  - Personal information of past employees
  - Personal information of interviewees
- Taking into account no service discrimination or exclusion HR Selection processes may vary more

GDPR- HR

- Actions required
  - Renew consents
  - Revise way of taking consents (website)
  - Physical data safety
  - Medical information data safety
  - Erase data >1 year

GDPR- SCIENTIFIC

- Audit showed that there are three categories of data and sensitive data
  - Define reasons why taking them
  - Proportionality of the extend of usage
  - Define duration of keeping them
  - Secure consent for obtaining them
  - Set a process for the storage of the info (pseudonymization after a period of time)

GDPR- MARKETING

- Audit revealed two types of data
- Consumer data
    - Security by default over the website
    - Opt in consents
    - Management of information in our databases
    - Right to deny automated profiling, processing that can analyse personal shopping preferences (google analytics)
    - Consents for newsletters
    - Scenario for data-breach

GDPR DPO

- Change internal rules
  - DPO
    - Ensure that processes are applied
    - Ensure that Internet Security tools are activated
    - Make a data registry for the company (voluntary)
    - Make a DPIA (voluntary)
    - Make a breach action plan
    - Request Insurance for IT Breaches
    - Include DPO directly reporting to the CEO in the organogram

GDPR LEGAL

- Written policies
  - Written consents
  - Disclaimers (website)
  - Terms of use
  - Addendums to already existing agreements especially IT ones

GDPR IT

- Redesign security
- Close security gaps
- Address cookies questions
- Address storage issues and back up

GDPR IT

- Data in SAP CRM/ ERP systems
- Data encryption (active and backup systems)
- Establish stricter policies about access rights
- SAP Encryption
- Define email policies (what data are transmitted via email)

GDPR IT

- What kind of data are there in portable storage devices and which of them are encrypted
    - Policy
    - Laptop
    - IPad
    - Smart phones
    - Icloud

CONSEQUENCES OF BREACHES

- Trade faith issues
- Suspension day-to-day business
- Financial losses
- Fines/ Penalties
- Breach of agreements with clients, unfair use of data (unfair competition)
- Insurance package to cover losses and lawsuits damages

CONCLUSION

- It is here so you cannot avoid or overlook it
- 1 individual is enough to cause damage
- Get expert advise, don’t follow blindly what other companies did
- Appoint a voluntary DPO as a coordinator of compliance on the area
- Identify risk areas and deal with them first