GDPR AND GRC: GOVERNANCE, RISK MANAGEMENT AND COMPLIANCE FOR DATA PROTECTION

Andrea LEONARDI - Stefano MICHELOTTI
LEONARDI, Andrea (CONSULTANT, TRAINER, AUDITOR – MINERVA GROUP SERVICE)

Graduating from Bocconi University with over 20 years experience in several industries, functions and projects, Andrea LEONARDI is Co-Founder and Vice President of Minerva Group Service s.c.c.p.a, a company focused in providing advisory, training and audit services. He is advisor, trainer and auditor for GDPR and related ISO standards (e.g. ISO27001 Information Security Management System, ISO 20000-1 IT Service Management System, ISO 22301 Business Continuity Management System).

http://www.linkedin.com/pub/andrea-leonardi/18/2a3/442  @AndreaLeonardix

MICHELOTTI, Stefano (CHAIRMAN– MINERVA GROUP SERVICE)

Stefano MICHELOTTI is Co-Founder and Chairman of Minerva Group Service s.c.c.p.a, a cooperative joint stock consortium company that is the hub of a network of companies (consortium companies). Minerva Group Service is strongly committed to providing professional and business services (e.g. GRC, GDPR, ISO Management System, Cybersecurity, Project Management, etc.). He is advisor, trainer and auditor for GDPR, Risk Management (ISO 31000) and Compliance Management (ISO 19600).

https://www.linkedin.com/in/stefano-michelotti-49a30418/  @StefanoArchisto
GDPR IS LANDING ON YOUR PLANET ...ARE YOU READY?

What and When?

REGULATION (EU) 2016/679 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL of 27 April 2016 on the protection of natural persons with regard to the processing of personal data and on the free movement of such data, and repealing Directive 95/46/EC (General Data Protection Regulation)

Who and Where?

“information relating to an identified or identifiable natural person (‘data subject’)”

Why?

No GDPR (compliance) ?! No (Business ) Party ....and huge administrative fines !

How?

A GRC road map to GDPR...

...following ISO Management Systems!
CHAPTER IV Controller and processor

Section 1 General obligations

Section 2 Security of personal data

Section 3 Data protection impact assessment and prior consultation

Section 4 Data protection officer

Section 5 Codes of conduct and certification
CHAPTER V Transfers of personal data to third countries or international organisations

CHAPTER VI Independent supervisory authorities
  Section 1 Independent status
  Section 2 Competence, tasks and powers

CHAPTER VII Cooperation and consistency
CHAPTER VIII Remedies, liability and penalties
CHAPTER IX Provisions relating to specific processing situations
CHAPTER X Delegated acts and implementing acts
“This Regulation applies to the processing of personal data wholly or partly by automated means and to the processing other than by automated means of personal data which form part of a filing system or are intended to form part of a filing system”
“any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person;”
### CHAPTER I General provisions

**PERSONAL DATA**

**PROCESSING**

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction.

**profiling**

Any form of automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects relating to a natural person, in particular to analyse or predict aspects concerning that natural person's performance at work, economic situation, health, personal preferences, interests, reliability, behaviour, location or movements.

**pseudonymisation**

The processing of personal data in such a manner that the personal data can no longer be attributed to a specific data subject without the use of additional information, provided that such additional information is kept separately and is subject to technical and organisational measures to ensure that the personal data are not attributed to an identified or identifiable natural person.

---

**Who?**

GDPR

MINERVA GROUP SERVICE
“This Regulation applies to the processing of personal data in the context of the activities of an establishment of a controller or a processor in the Union, regardless of whether the processing takes place in the Union or not. 4.5.2016 L 119/32 Official Journal of the European Union EN “

“....This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to: (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or (b) the monitoring of their behaviour as far as their behaviour takes place within the Union. “
SUPERVISORY AUTHORITY

imposition

administrative fines

effective, proportionate and dissuasive.

CHAPTER VIII Remedies, liability and penalties

e.g. for Italy

GARANTE PER LA PROTEZIONE DEI DATI PERSONALI
administrative fines = € up to 10 000 000 EUR

Infringements of the following provisions

- obligations of the controller and the processor
- obligations of the controller and the processor

CHAPTER II Principles
- Art. 8
- Art. 11

CHAPTER IV Controller and processor
- Art. 25 → 39
- Art. 42 → 43

up to 2% of the total worldwide annual turnover of the preceding financial year

Why?

GDPR
Infringements of the following provisions

CHAPTER II Principles
- Art. 5
- Art. 6
- Art. 7
- Art. 9

Infringements of the following provisions

CHAPTER III Rights of the data subject
- Art. 12 ➔ 22

Why?

administrative fines

€ up to 20 000 000 EUR

up to 4 % of the total worldwide annual turnover of the preceding financial year

COMPANY
Governance, Risk Management, Compliance for Data Protection

How?

ISO 29100
ISO 19011
ISO 29134
ISO 31000
GDPR
GRC
MINERVA GROUP SERVICE

GOVERNANCE
PRIVACY
RISK MANAGEMENT
COMPLIANCE


ISO/IEC 29134 Information technology — Security techniques — Guidelines for privacy impact assessment

GDPR

CONTROLLER

“...the natural or legal person, public authority, agency or other body which, alone or jointly with others, determines the purposes and means of the processing of personal data...”

PROCESSOR

“...natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller;..”

PII PROCESSING CONTROLS GDPR

“...appropriate technical and organisational measures”

“...records of processing activities”

Principles Policies GDPR

COMPLIANCE

Roles, responsibilities and interactions
“..to inform and advise the controller or the processor and the employees who carry out processing of their obligations pursuant to this Regulation and to other Union or Member State data protection provisions; ..”

“...to monitor compliance with this Regulation, with other Union or Member State data protection provisions and with the policies of the controller or processor in relation to the protection of personal data, including the assignment of responsibilities, awareness-raising and training of staff involved in processing operations, and the related audits; ...”

“...to cooperate with the supervisory authority..”

“...to act as the contact point for the supervisory authority on issues relating to processing, including the prior consultation referred to in Article 36, and to consult, where appropriate, with regard to any other matter. “
Establishing the internal context

Risk assessment

Risk identification

Risk analysis

Risk evaluation

Risk treatment

“…Taking into account the nature, scope, context and purposes of processing…”

“…the risks of varying likelihood and severity for the rights and freedoms of natural persons…”

“…appropriate technical and organisational measures”
Preparing the grounds for PIA

process for conducting a PIA

PIA Report

Annex A (informative)
Scale criteria on the level of impact and on the likelihood

Preparation of the PIA
Perform the PIA
Follow the PIA

General
Determine whether a PIA is necessary (threshold analysis)

General
Report structure

Scope of PIA
Risk Assessment
Risk Treatment Plan
Conclusions and Decisions
PIA Public Summary
How?

ISO 19600

COMPLIANCE MANAGEMENT FRAMEWORK

Legal, contractual, regulatory, technical Requirements

GDPR

SUPERVISORY AUTHORITY

Privacy Shield

Standards

Compliance

Code of Conduct

Certification
“...appropriate technical and organisational measures”
How?


Standard ISO 22301:2012 “Societal security — Business continuity management systems — Requirements”
How?

SMS ISO 20000-1 and relationships with ISMS ISO 27001 and BCMS ISO 22301

ISO 20000-1

ISO 27001, Annex A

A.17

SMS ISO 20000-1 PROCESS

Design and transition of new or changed services

Service delivery processes

- Capacity management
- Service continuity & availability management
- Information security Management
- Budgeting & accounting for services
- Service level management
- Service reporting

Control processes

- Configuration management
- Change management
- Release and deployment management

Resolution processes

- Incident and service request management
- Problem management

Relationship processes

- Business relationship management
- Supplier management
How?

SMS ISO 20000-1 and main relationships with GDPR

SMS ISO 20000-1 PROCESS

Design and transition of new or changed services

Service delivery processes

Capacity management
Service continuity & availability management
Information security Management
Budgeting & accounting for services
Service level management
Service reporting

Control processes

Configuration management
Change management
Release and deployment management

Resolution processes

Incident and service request management
Problem management

Relationship processes

Business relationship management
Supplier management

Privacy by design
Privacy by default
Privacy Impact assessment
Rights of the data subject
Privacy breach
External processors and third parties

Privacy Impact assessment
Rights of the data subject
Privacy breach
External processors and third parties
How?


How?

GDPR

Data Integrity, Availability, Confidentiality

Information Security Objectives

Integrity, Availability, Confidentiality

ISO 27001

Threat

Vulnerability

Incident

Organization and HR security perimeter

assetts

IT

SW

Physical and Environmental security perimeter

Processing

Physical and Environmental security perimeter

IT security perimeter ("cybersecurity")
...appropriate technical and organisational measures
A.18 Compliance

A.18.1 compliance with legal and contractual requirements

A.18.1.4 privacy and protection of personal identifiable information (PII)
How?

GDPR

ISO 22301

GDPR

Privacy breach

Incident

DISRUPTION

PROCESSING

DATA

Impact

Loss of Availability

DATA SUBJECT

GDPR

RESILIENCE

RISK ASSESSMENT

ISO 31000

GDPR

(PIA) Privacy Impact Assessment

GDPR

Privacy by design

Privacy by default

ISO 29134

(PIA) Privacy Impact Assessment

GDPR

Privacy by design

Privacy by default

GDPR

BUSINESS CONTINUITY STRATEGY

GDPR

BUSINESS CONTINUITY PLANS

GDPR

BUSINESS CONTINUITY PLANS

GDPR

BUSINESS CONTINUITY PLANS

GDPR

TESTING AND EXERCISING

GDPR

TESTING AND EXERCISING