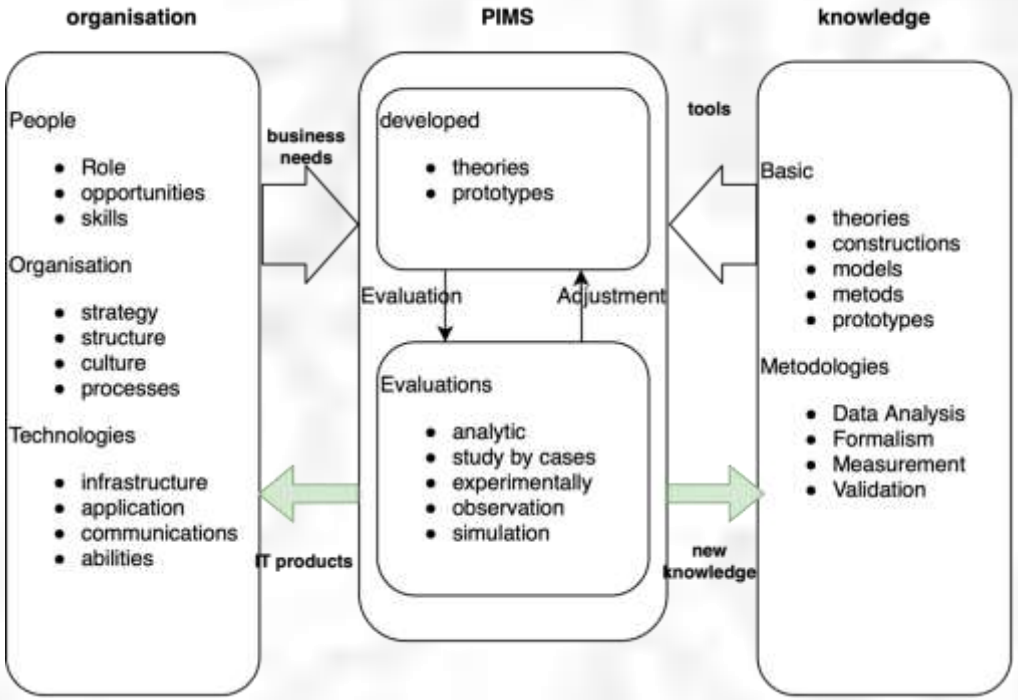
The Science of Design as a methodology for building Personal Information Management System

Tzanko Valkov Tzolov

PERSONAL INFORMATION MANAGEMENT SYSTEM (PIMS)

- Ecosystem whose goal is to empower individuals to control the sharing of their personal data;
- New understanding and transformation of the current, supplier-oriented and the way a business system is made to a human - centered system;
- Individuals are protected from illegal processing of their data;
- New approaches in data protection, allowing increased control and a proactive position of the data subject;

THE SCIENCE OF DESIGN



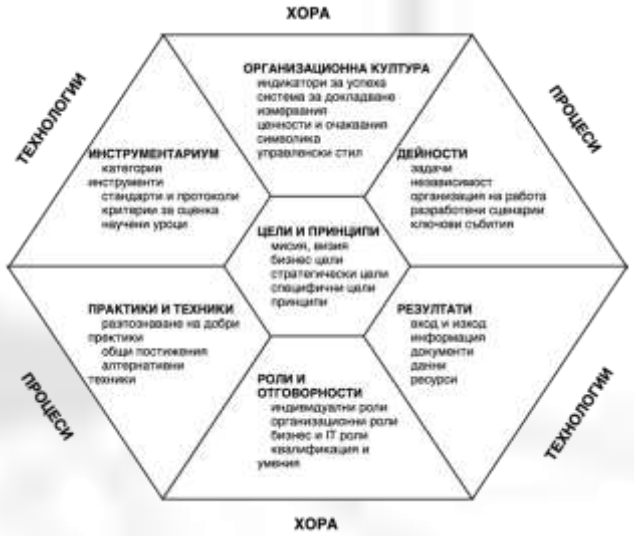
SCIENCE OF DEGIGN

- dual in nature - practical aspect it is a design activity, and as a science - a set of constructions relevant to the problem area;
- products and their incorporation into our physical, psychological, economic, social and virtual environment;
- methodology includes content analysis, methods and principles related to the study of information technology in the construction of information systems
- 2 processes - construction and evaluation, 4 elements constructors, models, methods and prototypes of systems;

CONSTRUCTOTS

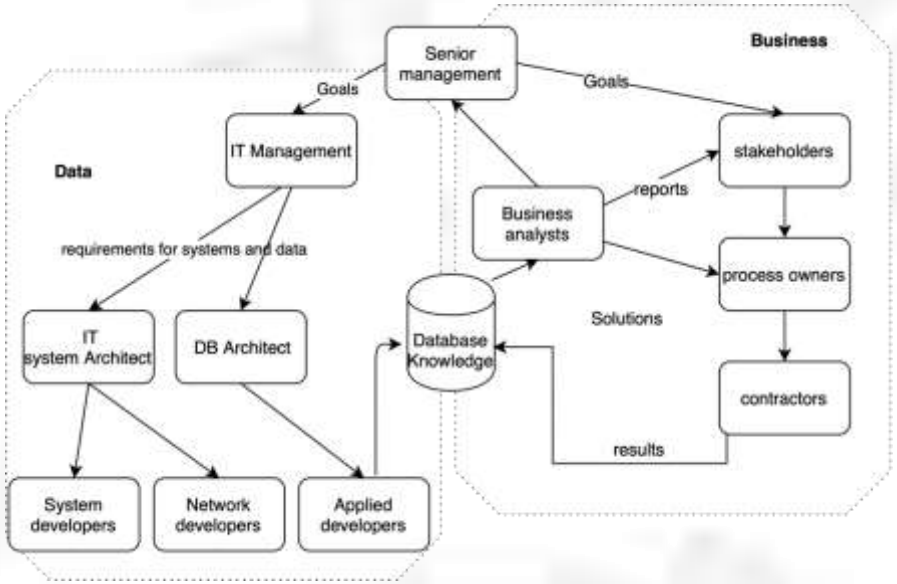
aspect	constructor	aspect	constructor
organization	purpose	people	role
	principle		responsibility
	mission		skills
	vision		qualification
	value		preparation
	organizational culture		
	management style	GDPR	role
	success indicator		data classification
technologies	information		processing operations
	documents		data transfer
	data		processing principles
	resources		rights of the subjects
	input parameters		consent
	output parameters		information systems
	standards / protocols		data security
	evaluation criteria		risk assessment
	tools		impact analysis
	lessons learned		code of conduct
processes	tasks		data protection officer
	scope		supervision
	process organization		integrity in design
	scripts		default privacy
	key events		technical and organizational measures
	good practices		security breach
	alternative techniques		certification
	results		

- influenced by the model introduced by DAMA;
- GDPR

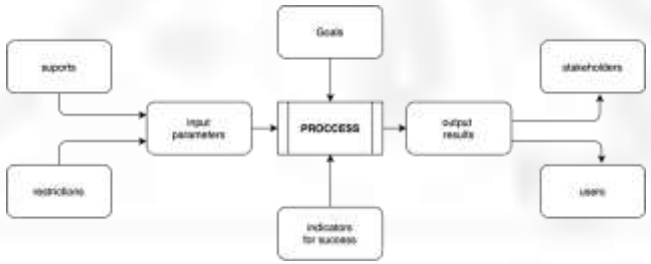


MODELS

Model of the organization



Process description

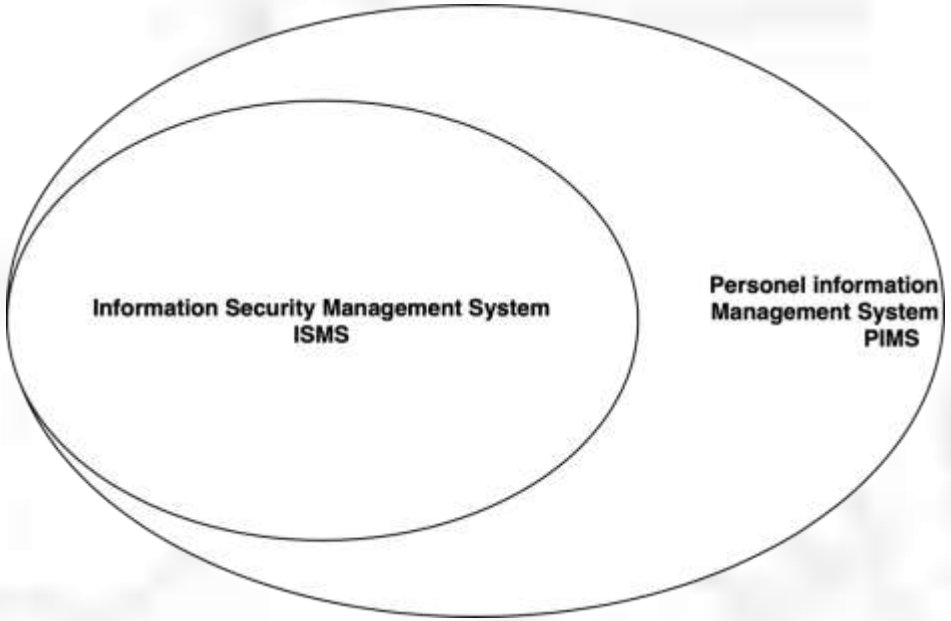


Model of the DATA (metadata)

Type	Definition	area GDPR
administrative	Metadata used to manage and administer collections and information resources	Acquisition information - data sources Property and playback - data subject, ALD, processor Legal requirements for processing - principles of processing Location information - where the data IS, warehouses are located Criteria for personal data recognition - discovery of personal data.
descriptive	Metadata used to identify and describe collections and information resources	Data cataloguing - (1) data types that are processed; (2) states that change the type of data Categorization of data by aids - data processing for categories of subjects, encrypted and anonymized data Differentiation between versions - historical data meanings Specialized indices - automated data access (which systems or applications Curatorial information - change management "golden record Derivative data and new collections - results of business analyses and references Annotations from creators and users - additional data requirements from users
storage	Metadata related to the management of the preservation of collections and information resources	Documenting the physical state of resources - availability, confidentiality, accessibility Documentation of processing operations and the actions taken - reporting Documenting changes that occurred during processing - change the meaning (value) of the data.
technically	Metadata related to how a system works or the behaviour of metadata	Hardware and software documentation - system status, database, hardware Technical information for digitalization, -, compression coefficients, zooming, combinations - data formats Monitoring the response times of the system - access time, failure recovery Certification and protection data - encryption keys, passwords.
use	Metadata related to the level and type of use of collections and information resources	Circulation records - who used what data Physical and logical access to the data - actions of privileged users User use and tracking - actions performed by users Information on reuse and multi-version of the content - use for a purpose other than that for which they were collected Log processing - event recognition Usage rights - who has what rights to access the data

MODELS

Security Model



- Security layers:
  1. Physical security - physical protection of devices or areas from unauthorized access and abuse
  2. Personal security - protection of a natural person or group of persons who are authorized to access the organization and its assets
  3. Security of operations - protection of certain operations or series of activities
  4. Communication security - protection of communication channels, technologies and content
  5. Network security - protection of network components, connections and content
- ISMS model - the model adopted by the National Security Systems Committee, described by John Mc Cumber in 1991;
- PIMS model:
  1. demonstration lawful processing
  2. compliance subjects rights

METHODS

- Modelling business processes in the organization (**Business Process Modelling**);
- Analysis of discrepancies between the existing information security system and the personal information management system (**Gap Analysis**);
- Assessment of the impact of the actions taken in the construction of the personal information management system (**Impact Assessment**)
- Verification of a built system (**Verification**)
- Optimization (improvement) of the established system for personal information management (**Evaluation**)

PROTOTYPES

BUSINESS ANALISYS	DATA FLOWS	GAP ANALISYS	IMPACT ACCESSMENT	VALIDATION
DAMA model of the organization Model of the organization in the digital age Business flow model	Technological model of the organization Data model in the organization	Model of the ISO 27001 information security system Model of the personal data management system ISO 27701	ISO 31001 risk assessment model Impact assessment model	Consultation Certification Code of conduct
Goal, Principles of Processing, Mission Vision, Values, Indicators of Success Transfers, Consent Accountability Roles, responsibilities, skills, qualifications, training Processes, tasks Scope How the data is collected, physical categories. persons whose data is being processed	Carrier type Information system Physical place Storage period Expected volume Data categories • Personal data • Special • Public	ISMS • physical • personal • documentary • of operations • AIS and networks • communication PIMS • demonstration of compliance • rights of entities • awareness	Active (source Vulnerability Threat Recognition criteria Risk, risk weighting, level of risk treatment measures Security level residual risk	Opinion of the supervision Certificate Brand Printing Code of conduct

- The construction of the prototype is based on the application of a sequence of methods based on selected models and reaching the design of constructors.
- The process sequence will generate a Personal Data Management System that complies with the requirements of the General Data Protection Regulation.

CONCLUSION

- Building a PIMS for most organizations requires significant changes in understanding the nature of business as part of the digital economy;
- Many small and medium-sized organizations do not have the resources or knowledge to do so themselves;
- The framework for building a PIMS, potentially applicable to each organization without being influenced by its size and compliance with the requirements of.
- The framework has been tested in Bulgaria but the nature of the GDPR as a Regulation and the wide application of standards will allow application in a wider range in all countries applying the General Regulation.
- One later stage, its impact on the specifics of the various national laws needs to be assessed, but expectations are largely universal.

Thank you

Tzanko Valkov Tzolov

Member of the Commission for Personal Data Protection,

2, prof. Cvetan lazarov Blvd, 1592 Sofia, Bulgaria

tzolov@cpdp.bg