



◦ The General Data Protection Regulation (GDPR) era: Ten steps for compliance of Data Processors and Data Controllers What about the Users ?

Costas Lambrinoudakis
Professor
Department of Digital Systems– University of Piraeus
Member of the Board of the Hellenic Data Protection Authority
clam@unipi.gr



The Drivers for the GDPR

- **Need for modernization**
- **Need to give to individuals back control over their personal data**
- **Need to simplify the regulatory environment for business**

GDPR Milestones

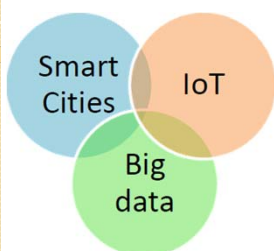
- **In January 2012** EU proposes a reform of data protection rules to increase users' control of their data and to cut costs for businesses
- **In March 2014** the European Parliament approves the proposal for the new regulation (first reading)
- **In April 2016** the GDPR is announced
- **In May 2016** the GDPR enters into force
- **In May 2018** the GDPR applies

6 September 2018

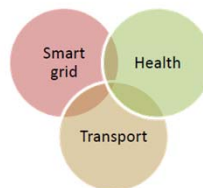
TrustBus2018

3

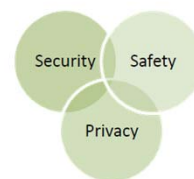
Today.....



Systems



Application Domains



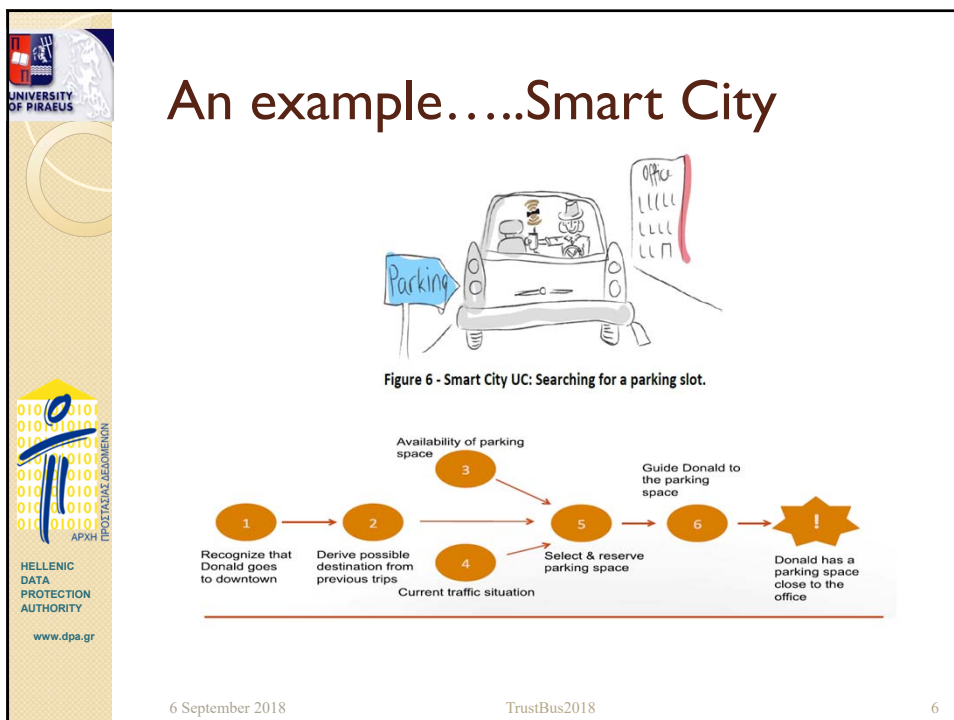
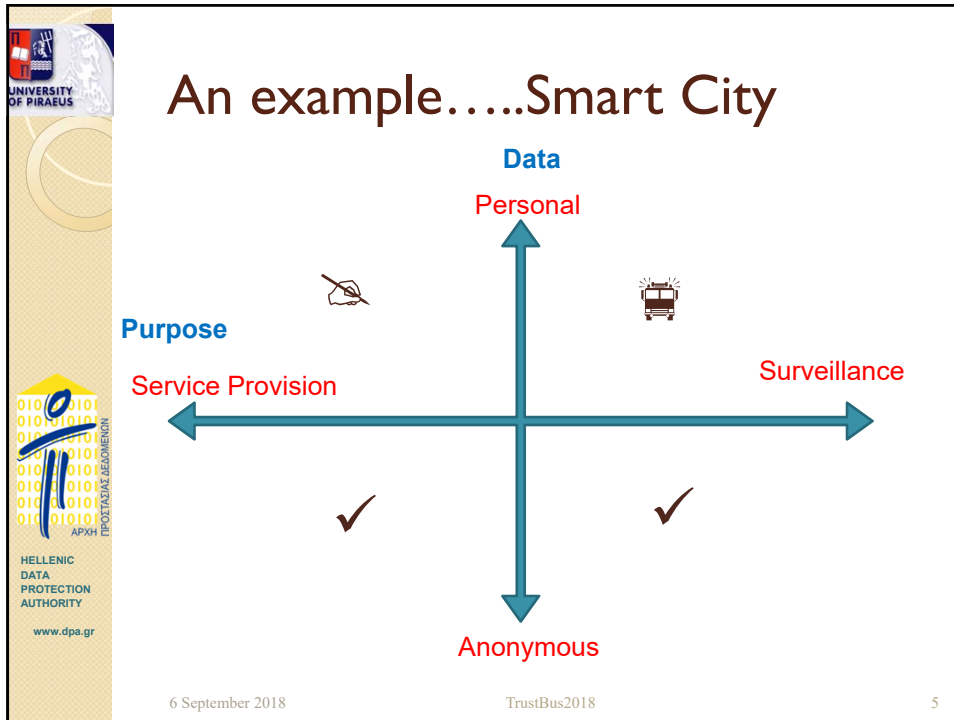
Concerns



6 September 2018

TrustBus2018

4



An example.....Smart City

- **Initial Purpose:**
 - Tracking traffic conditions
 - Problem prediction and warning of drivers => provision of suitable parking spaces
- **Personal Data Processing:**
 - The service provider: Personal data (travel habits, location, speed, etc.)
 - The car insurance company: Driving behaviour
 - The Municipality: Planning the toll policy
 - Targeted advertising providers
- **Responsibility Issues:**
 - Who Manages Personal Data? Who has the right to do it? In what way? Where will my personal data be, and how much can I control their processing? Who has the ownership?

6 September 2018

TrustBus2018

7

GDPR: Main Concept

- It sets the requirements for the protection of individuals with regard to the processing of their personal data and the free movement of such data
- It is mandatory for organizations managing personal data of European citizens

6 September 2018

TrustBus2018

8

GDPR: Key Terms

- **Processing** means...
 - any operation or set of operations performed on personal data, whether or not by automated means (such as collection, storage, alteration, retrieval, use, dissemination, erasure etc)

6 September 2018

TrustBus2018

11

GDPR: Key Terms

- **Controller** means...
 - 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

6 September 2018

TrustBus2018

12

GDPR: Key Terms

- **Processor** means...
 - a natural or legal person, public authority, agency or other body which processes personal data on behalf of the controller

6 September 2018

TrustBus2018

13

GDPR: The 6 Privacy Principles

- **Lawfulness, fairness and transparency**
 - We must have a lawful reason for collecting the personal data and must do it in a fair and transparent way
- **Purpose limitation**
 - We must only use the data for the reason we collected it
- **Data minimisation**
 - We mustn't collect any more data than we need
- **Accuracy**
- **Storage limitation**
 - We can't keep it any longer than we need it for
- **Integrity and confidentiality**
 - We must protect the personal data
- Supported by the **accountability** principle that ensures that the other principles are satisfied

6 September 2018

TrustBus2018

14

GDPR: The Rights of the Data Subject (Users)

- **Right to information**
 - What we collect, purpose etc
- **Right of access**
 - Allowing them to see their data
- **Right to rectification**
 - Correct their data
- **Right to erasure (right to be forgotten)**
 - Remove their data if we have no legal right
- **Right to restriction of processing**
 - Revoke their consent for part of the processing
- **Right to data portability**
 - Move to a different provider
- **Right to object**
 - Consider objection on what we hold and do with their data

6 September 2018

TrustBus2018

15

GDPR vs. Directive 95/46/EC: What is changing ?

Personal Data based on Directive 95/46/EC (Article 2)

- Any information relating to an identified or identifiable natural person ('data subject')
- An identifiable person is one who can be identified, directly or indirectly, in particular by reference to an identification number or to one or more factors specific to his physical, physiological, mental, economic, cultural or social identity

Personal Data based on GDPR (Article 4)

- 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

6 September 2018

TrustBus2018

16

GDPR vs. Directive 95/46/EC: What is changing ?

Special categories of Personal Data based on Directive 95/46/EC (Article 2)

Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, trade-union membership, and the processing of data concerning health or sex life

Special categories of Personal Data based on GDPR

- Personal data revealing racial or ethnic origin, political opinions, religious or philosophical beliefs, or trade union membership, and the processing of **genetic data, biometric data** for the purpose of uniquely identifying a natural person, data concerning health or data concerning a natural person's sex life or sexual orientation

6 September 2018

TrustBus2018

17

GDPR vs. Directive 95/46/EC: What is changing ?

The Data Protection Controller based on 95/46/EC

- Must implement appropriate technical and organizational measures to protect personal data against accidental or unlawful destruction or accidental loss, alteration, unauthorized disclosure or access
- Must, choose a processor, where processing is carried out on his behalf, providing sufficient guarantees in respect of the technical security measures and organizational measures governing the processing to be carried out, and must ensure compliance with those measures

The Data Protection Controller based on GDPR

- Shall be responsible for, and be able to demonstrate compliance with the GDPR requirements
- Shall implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with GDPR, taking into account the **nature, scope, context and purposes of processing as well as the risks of varying likelihood and severity for the rights and freedoms of natural persons**, Those measures shall be reviewed and updated where necessary.
- Implementation of appropriate data protection policies, in relation to processing activities

6 September 2018

TrustBus2018

18

GDPR vs. Directive 95/46/EC: What is changing ?

Scope based on Personal Data based on Directive 95/46/EC (Article 4)

- The processing is carried out in the context of the activities of an establishment of the controller on the territory of the Member State

Scope based on GDPR

- Application 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**
- Application to the processing of personal data of **data subjects who are in the Union** by a controller or processor not established in the Union

6 September 2018

TrustBus2018

19

GDPR vs. Directive 95/46/EC: What is changing ?

Consent Based on Directive 95/46/EC

- The data subject's consent shall mean any freely given specific and informed indication of his wishes by which the data subject signifies his agreement to personal data relating to him being processed

Consent based on the GDPR

- The data subject's consent means any **freely given, specific, informed and unambiguous** indication of the data subject's wishes by which he or she, **by a statement or by a clear affirmative action**, signifies agreement to the processing of personal data relating to him or her

6 September 2018

TrustBus2018

20

GDPR vs. Directive 95/46/EC: What is changing ?

Notification of a personal data breach to the supervisory authority

- Not applicable

Notification of a personal data breach to the supervisory authority and data subjects based on GDPR (Article 33, 34)

- In the case of a personal data breach, the controller shall without undue delay and, where feasible, **not later than 72 hours** after having become aware of it, notify the personal data breach to the **supervisory authority**
- When the personal data breach is likely to result in a high risk to the rights and freedoms of natural persons, the controller **shall communicate the personal data breach to the data subject** without undue delay

GDPR vs. Directive 95/46/EC: What is changing ?



Personal privacy

- Individuals have the right to:
- Access their personal data
 - Correct errors in their personal data
 - Erase their personal data
 - Object to processing of their personal data
 - Export personal data



Controls and notifications

- Organizations will need to:
- Protect personal data using appropriate security
 - Notify authorities of personal data breaches
 - Obtain appropriate consents for processing data
 - Keep records detailing data processing



Transparent policies

- Organizations are required to:
- Provide clear notice of data collection
 - Outline processing purposes and use cases
 - Define data retention and deletion policies



IT and training

- Organizations will need to:
- Train privacy personnel & employee
 - Audit and update data policies
 - Employ a Data Protection Officer (if required)
 - Create & manage compliant vendor contracts

..and what does that mean for the organization?

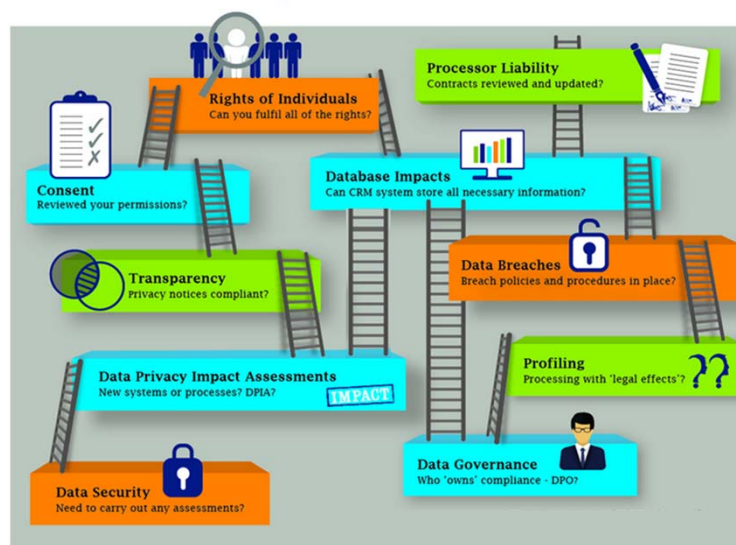


6 September 2018

TrustBus2018

23

GDPR Compliance.....



6 September 2018

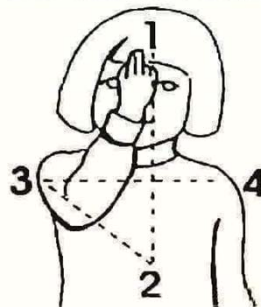
TrustBus2018

24

GDPR Compliance.....

..... Not a straightforward task.....

4 EASY STEPS FOR GDPR COMPLIANCE



6 September 2018

TrustBus2018

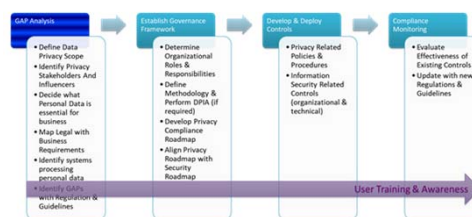
25

GDPR Compliance: Awareness - Readiness

1



- Compliance with the GDPR should be dealt as a systematic action with appropriate planning.
- Human resources should be aware of the new legal framework and understand the consequences it brings.
- Perform a high level gap analysis (maturity assessment – flagging of readiness of the company)



6 September 2018

TrustBus2018

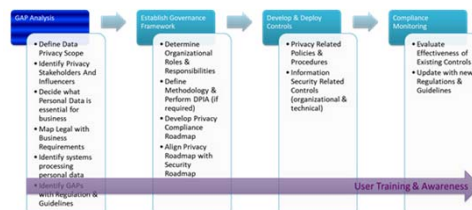
26

GDPR Compliance: Maintain a record of processing activities



2

- The organization should recognize the **processing purposes** that the organization serves and all related **processing activities** per processing purpose
- Who?** (identity of the data controller, persons in charge of processing operations and the data processors)
- What?** (categories of data processed, sensitive data)
- Why?** (purposes of the processing – legal basis)
- Where?** (storage location, data transfers)
- Until when?** (data retention period)
- How?** (security measures in place)



6 September 2018

TrustBus2018

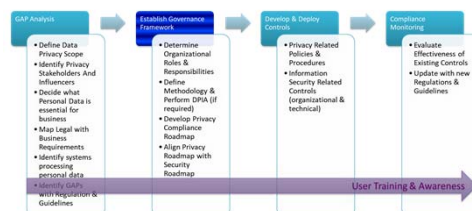
27

GDPR Compliance: Data Protection Officer (DPO)



3

- DPO mandatory** when
 - public bodies
 - large scale systematic monitoring
 - large scale processing of special categories of data or criminal convictions and offences related data
- DPO profile**
 - reports to the highest mgt level
 - independent
 - adequate resources
 - internal or external
 - data protection experience and knowledge
- DPO tasks**
 - advise
 - train staff
 - conduct internal audits
 - monitor compliance
 - point of contact for DPAs and individuals



6 September 2018

TrustBus2018

28

GDPR Compliance: Data Protection Impact Assessment (DPIA)



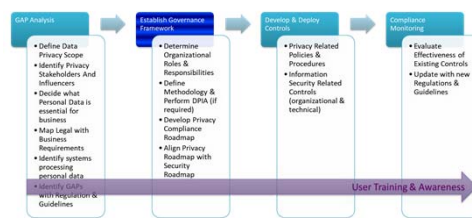
4

DPIA = tool to build & demonstrate GDPR compliance

- Mandatory if processing is “likely to result in a high risk to the rights and freedoms of natural persons”
- DPAs define list of the processing operations that require a DPIA
- If high residual risks => consultation with DPA

DPIA Contents

- Processing operations (purposes)
- Legal basis
- Assessment of risks to individuals
- Measures to address risks



6 September 2018

TrustBus2018

29

GDPR Compliance: Data Protection Impact Assessment (DPIA)



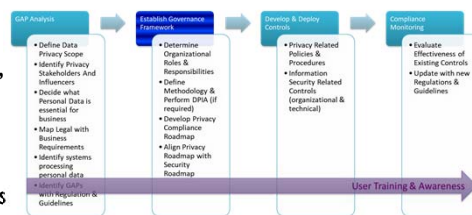
4

Security risk management for personal data processing <> “typical” risk management

- Privacy-specific notion of impact : organization <> individuals’ freedoms and rights
- Scale may not be relevant
- Secondary adverse effects to be considered
- Different risk acceptance criteria
- Different specific technical and organizational measures

Measures depend on:



- nature, scope, context, purposes, risks of varying likelihood and severity for rights and freedoms of individuals



6 September 2018

TrustBus2018

30


HELLENIC
DATA
PROTECTION
AUTHORITY
www.dpa.gr

GDPR Compliance: Data Protection Impact Assessment (DPIA)



4

Example: Levels of impact (Guidelines for SMEs on the security of personal data processing, ENISA, 2016)

LEVEL OF IMPACT	DESCRIPTION
Low	Individuals may encounter a few minor inconveniences, which they will overcome without any problem (time spent re-entering information, annoyances, irritations, etc.).
Medium	Individuals may encounter significant inconveniences, which they will be able to overcome despite a few difficulties (extra costs, denial of access to business services, fear, lack of understanding, stress, minor physical ailments, etc.).
High	Individuals may encounter significant consequences, which they should be able to overcome albeit with serious difficulties (misappropriation of funds, blacklisting by financial institutions, property damage, loss of employment, subpoena, worsening of health, etc.).
Very high	Individuals which may encounter significant, or even irreversible consequences, which they may not overcome (inability to work, long-term psychological or physical ailments, death, etc.).



6 September 2018
TrustBus2018
31

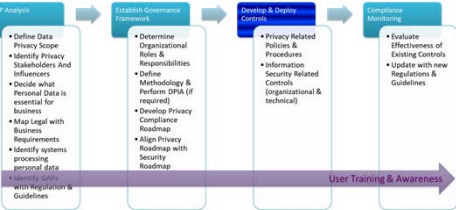
HELLENIC
DATA
PROTECTION
AUTHORITY
www.dpa.gr

GDPR Compliance: Consent

5

I Agree

- The controller must be able to prove that:**
 - he has obtained the consent of the data subjects
 - the consent was **'free'**
 - the consent is specific and explicit for a well-defined processing purpose
 - the consent has been obtained with a **clear positive action** (e.g. filling in a box when visiting a web site, selecting desired technical settings for a service etc). *Silence, pre-filled boxes or inactivity should not be taken as consent*
 - for underage persons the consent is considered to be "valid" when the child is at least 16 years of age. Otherwise consent must be given by the person who has parental responsibility



6 September 2018
TrustBus2018
32

GDPR Compliance: Privacy by Design and by Default



6

Data Protection by Design

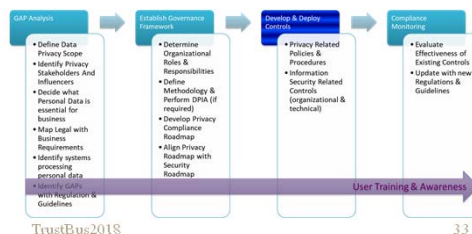
- Each new service or business process must take personal data protection into consideration. Protection of users' privacy must be a basic parameter in the early stages of each project and then throughout its life cycle.

- Issues that should be considered are:

- Data minimization
- Pseudonymization

Data Protection by Default

- Protection of personal data as a default property of systems and services



6 September 2018

33

GDPR Compliance: Protection / Security of Processing



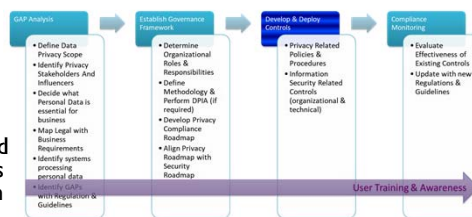
7

- According to the DPIA's results **it is necessary for the organization to employ the appropriate/suitable technical measures for the security of processing**. Indicatively:

- Pseudo-anonymization and encryption
- Ensuring Integrity, Availability and Reliability
- Restoration of availability and access in the event of an incident
- Testing, assessing and continually evaluating the effectiveness of the protection measures

Certifications, Seals, Codes of Conduct

- Codes of conducts and certification mechanisms help specify the measures required
- Certification will be issued by supervisory authorities or accredited certification bodies.



6 September 2018

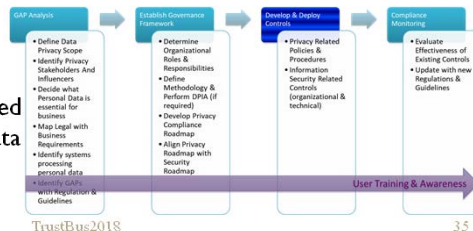
34

GDPR Compliance: Data Protection Policy



8

- The organizations need to update/enhance their data protection policies in relation to the existing legal framework, and thus provide information on:
 - the legal basis for the processing (which "complicates" the information as it requires legal analysis)
 - the time frame that the processing / storage will take place
 - the existence of any automated decision making process, including profiling, with information on possible consequences
 - data collected from other sources
 - the Data Protection Officer's data
 - the procedures employed in order to satisfy all data subjects' rights



6 September 2018

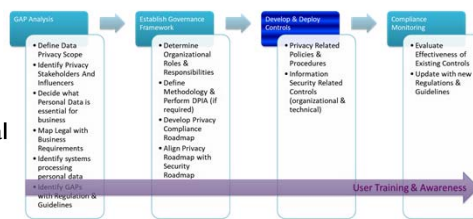
TrustBus2018

35

GDPR Compliance: Data Breaches

9

- **Personal data breach definition**
 - breach of security that causes destruction, loss, alteration, unauthorised disclosure of, or access to, personal data
 - *more than just losing personal data*
- **Breach notification**
 - To DPA within 72 hours (failure to notify breach raises fine up to 10 million Euros or 2 % of global turnover)
 - To Individuals if their rights and freedoms are at high risk
- **Notification Contents**
 - Nature of the breach
 - categories and number of individuals
 - categories and number of personal data records
 - DPO contact details
 - consequences of the personal data breach
 - measures to, mitigate any possible adverse effects



6 September 2018

TrustBus2018

36

GDPR Compliance: Acting in several EU countries / Transferring Data to non EU countries

10

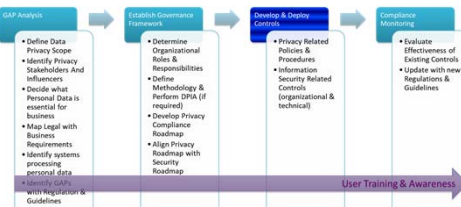
It is important for the organization to clearly address the following questions

- Which is the place / country of the main establishment (headquarters)?
- Are the basic decisions for processing taken in the headquarters or not?
- Are there any joint data controllers?



Transferring data to non-EU countries

- Ensure that it is legal to do so (Binding Corporate Rules – BCRs, Standard Contract Clauses SCCs etc).
- Explore whether there is an obligation to inform the persons whose data will be transferred.



6 September 2018

TrustBus2018

37

GDPR Compliance: Compliance Monitoring

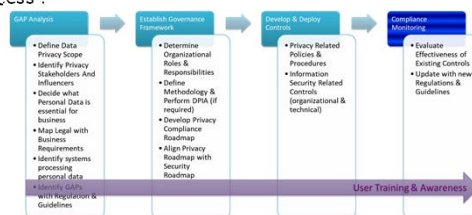


For each purpose of processing:

- Is the purpose clear?
- Is the processing serving only this purpose?
- How have the data been collected?
- Are the collected data absolutely necessary for this purpose?
- For how long should the data been maintained?
- In case of a processor, is the processing solely on the basis of the orders of the controller?

How secure is the maintenance / further processing of data?

- Are they encrypted / pseudo-anonymised ?
- Who has been granted access ?
-



6 September 2018

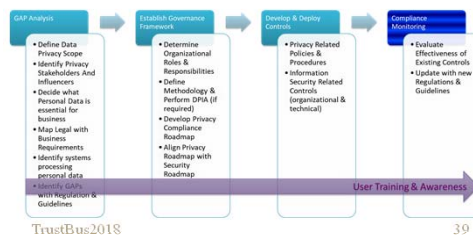
TrustBus2018

38

GDPR Compliance: Compliance Monitoring



- Do the processors provide guarantees for compliance with the GDPR?
 - Is there permission of the controller for the processing?
- Verification of compliance with the principles governing the lawful processing of data and respect for the rights of individuals must be **continuous**



6 September 2018

TrustBus2018

39

We forgot the Users ...

6 September 2018

TrustBus2018

40

Implications for User's Consent

- Based on the GDPR the controller shall be able to demonstrate that the data subject has consented to the processing of his or her personal data
- The request for consent shall be presented in an intelligible and easily accessible form, using clear and plain language

Privacy Statements/Policies are the primary mechanism used to obtain user's consent

Do they Work?

6 September 2018

TrustBus2018

41

What Happens in Reality?

- Users do not seem aware of the amount of personally identifiable information that they provide and who can access them
- They disclose considerable amounts of personal information in online settings having misconceptions of the privacy risks
- They have misperceptions of privacy policies and terms
- They tend to adopt a relaxed attitude towards personal privacy
- They are not aware of the privacy features of each online application and how to configure them
- They lack understanding of the big picture: how the different pieces of personal information are combined into producing a personal profile

6 September 2018

TrustBus2018

42

...and if the User Reads the Policy, will (s)he be Privacy Aware?

- Privacy Awareness:
 - understanding of the respective privacy settings and policies
 - stimulation of privacy concerns due to the appreciation of the importance of privacy
 - Association of data with threats against privacy
- Knowing about privacy threats from the news, reviews and friends notifications
- Separation of risk elements

Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 33, No. 4, pp. 434-457

...Being Privacy Aware... Giving Informed Consent

- ✓ Understand consenting
- ✓ System benefits and functions
- ✓ Sense of control over location data sharing
- ✓ Resources consumption
- ✓ Changes in the policy and application to already collected data

Tsohou, A. and Kosta, E. (2017), Enabling valid informed consent for location tracking through privacy awareness of users: A process theory, Computer Law & Security Review: The International Journal of Technology Law and Practice, Vol. 33, No. 4, pp. 434-457

