

General Data Protection Regulation

Michal Koščík

← → ↻ fortune.com/2016/04/14/eu-parliament-gdpr/

FORTUNE


NEWS POPULAR VIDEOS FORTUNE 500 🔍

TECH DATA PROTECTION

Here Come the World's Toughest Privacy Laws APRIL 14, 2016

by David Meyer APRIL 14, 2016, 9:58 AM EDT

✉️ 🐦 📺 📧




Here's what you need to know about the EU's General Data Protection Regulation.

EU justice commissioner Věra Jourová

Finally, after four years of negotiations and formalities, the European Union will have its tough new privacy rules, replacing two-decades-old legislation that was much more open to interpretation by individual countries.

RECOMMENDED FOR YOU



Tourists Flocking to a Weak British Pound Drives Up Burberry's UK Sales 9:35 AM EDT

As Clinton Expands Into Red States, Trump Again Claims Fraud 9:31 AM EDT

Chinese State Firms Pledge \$1.8 Billion to Fight Poverty 9:12 AM EDT

Deutsche Bank to Pay \$38 Million in U.S. Silver Price-Fixing Case 9:08 AM EDT

Dick's Sporting Goods Reportedly Planning to Bid for Golemsmith's U.S. Stores 4:50 AM EDT

Tesco Grows Its Market Share For the First Time in 5 Years 4:48 AM EDT

United Says Low Airfares and Wage Hikes Will Squeeze Profits 4:36 AM EDT

Danone's Sales Growth Is Hurt By Challenges in China 4:35 AM EDT

Here's Where Wall Street Republicans Are Making Their Political Donations 4:22 AM EDT

This Family Trio Is Set to Be Charged in a Giant Corruption Probe 4:21 AM EDT

China's Richest Man Begins Courting Hollywood Filmmakers 3:28 AM EDT

Fortune's Most Powerful Women Give Gen Z Girls a Standing Ovation 2:42 AM EDT

This Texas Unicorn Is Ready for a Rare Oil IPO 1:38 AM EDT

IBM Shares Fall Despite Higher-Than-Expected Sales 1:17 AM EDT

Apple Retail Chief Angela Ahrendts on Turning Stores Into Town Squares 1:10 AM EDT

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)

(Text with EEA relevance)

THE EUROPEAN PARLIAMENT AND THE COUNCIL OF THE EUROPEAN UNION,

Having regard to the Treaty on the Functioning of the European Union, and in particular Article 16 thereof,

Having regard to the proposal from the European Commission,

After transmission of the draft legislative act to the national parliaments,

Having regard to the opinion of the European Economic and Social Committee ⁽¹⁾,

Having regard to the opinion of the Committee of the Regions ⁽²⁾,

Acting in accordance with the ordinary legislative procedure ⁽³⁾,

Whereas:

- (1) The protection of natural persons in relation to the processing of personal data is a fundamental right. Article 8(1) of the Charter of Fundamental Rights of the European Union (the 'Charter') and Article 16(1) of the Treaty on the Functioning of the European Union (TFEU) provide that everyone has the right to the protection of personal data concerning him or her.
- (2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended to contribute to the accomplishment of an area of freedom, security and justice and of an economic union, to economic and social progress, to the strengthening and the convergence of the economies within the internal market, and to the well-being of natural persons.
- (3) Directive 95/46/EC of the European Parliament and of the Council ⁽⁴⁾ seeks to harmonise the protection of fundamental rights and freedoms of natural persons in respect of processing activities and to ensure the free flow of personal data between Member States.

Basic pillars of regulation

„Old“ (current) directive

Broad definition of PD

Title to process PD

Consent

Legal entitlement

Triangle of

Data subject

Controller

Processor

„New“ GDPR

Even broader definition of PD

Title to process PD

Consent

Legal entitlement

Triangle of

Data subject

Controller

Processor

Comparison

„Old“ (current) directive

32 Articles

Needs to be adopted by member states

„New“ GDPR

99 Articles

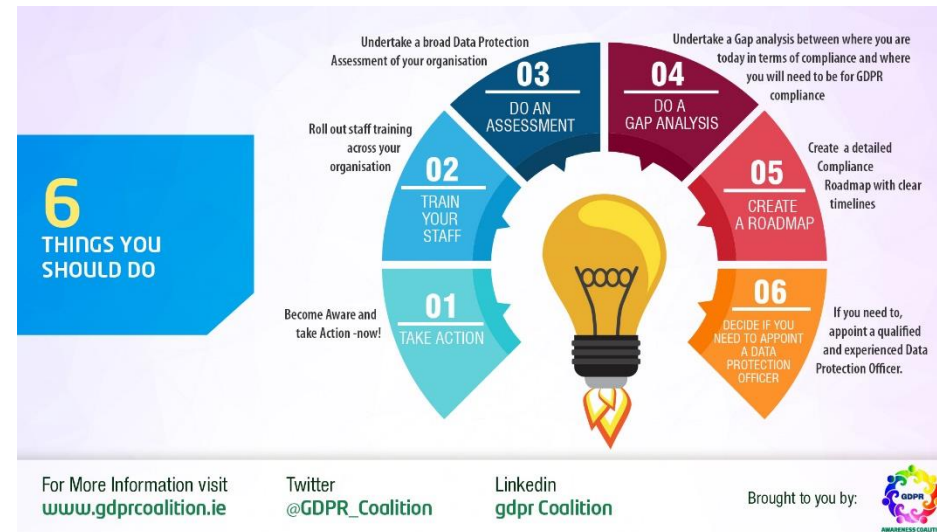
Direct effect



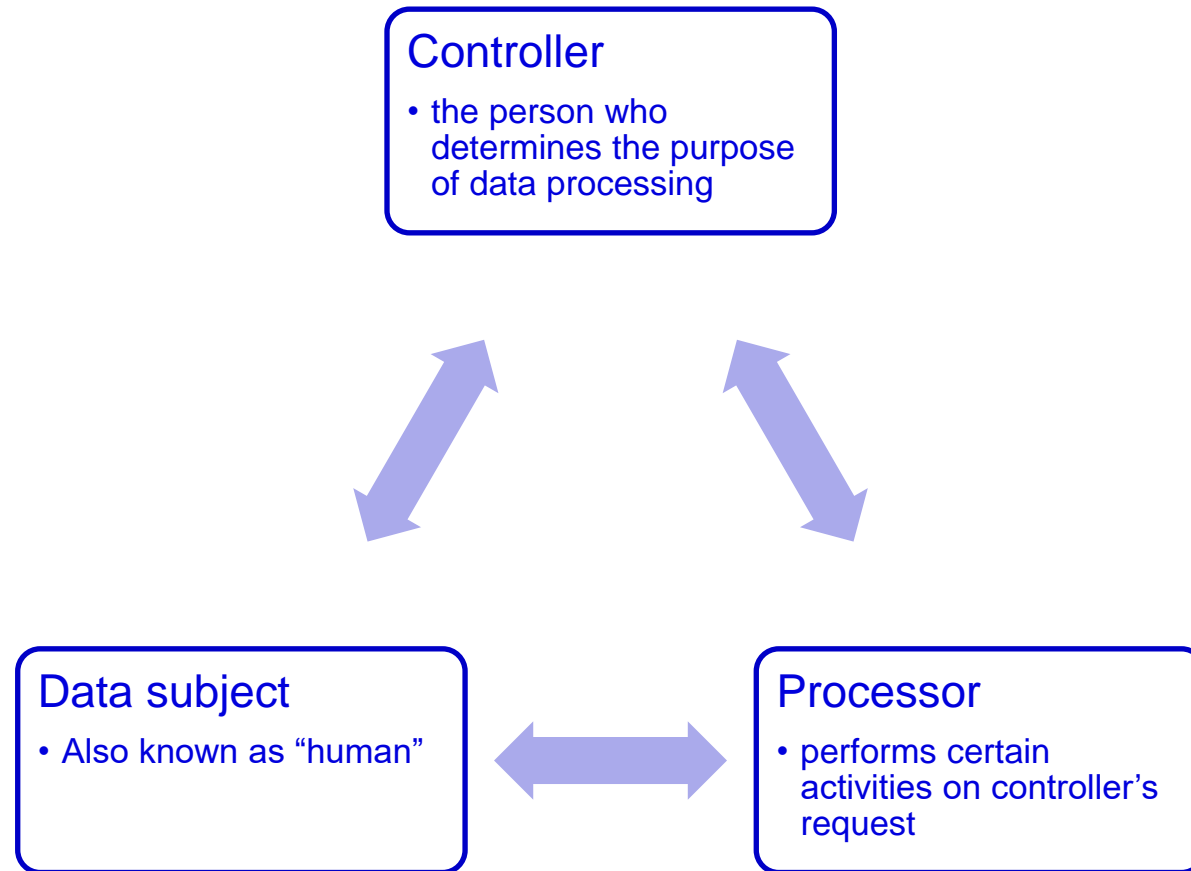


From 1995 to 2016 Data protection needed some
FACELIFTS but did not change that much

Fire safety analogy?



Principles



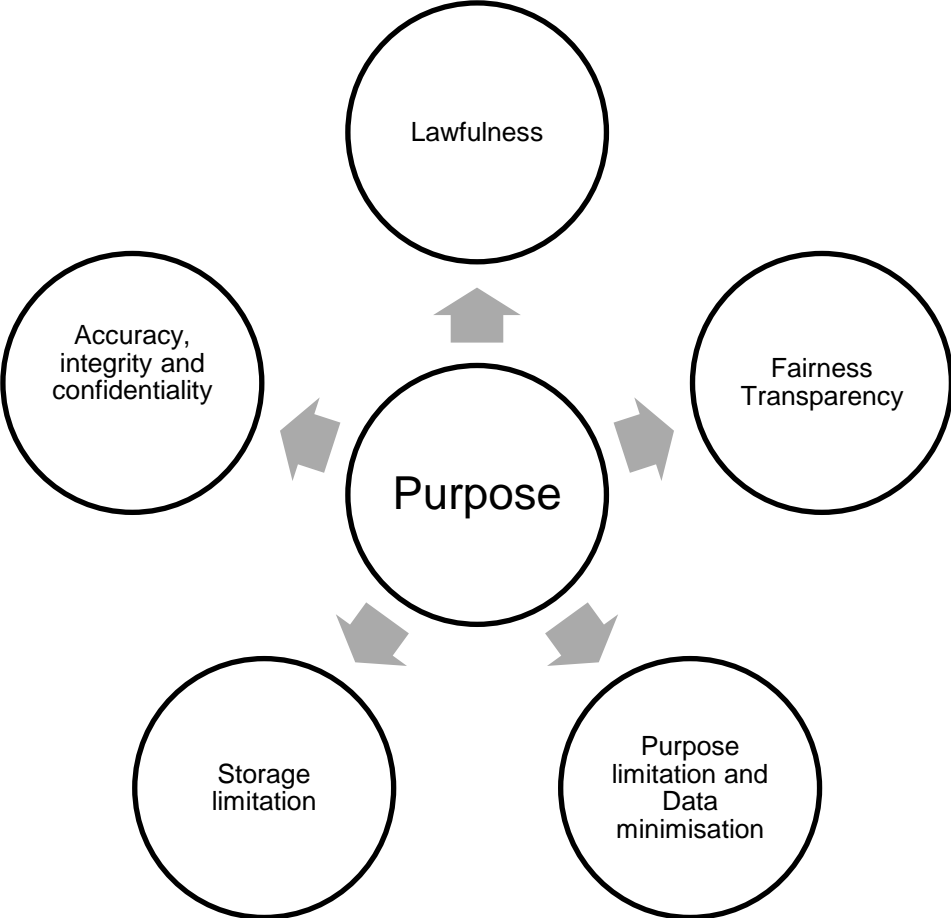
Data processor VS data controller

determines the purpose of data processing

- One information can be processed by various processors

performs certain activities

- Provides services
- Performs only what controller orders



Processing data without consent

performance of a contract to which the data subject is party

compliance with a legal obligation of a controller

in order to protect the vital interests of the data subject or of another natural person

for the performance of a task carried out in the public interest

the exercise of official authority vested in the controller

legitimate interests pursued by the controller

The principle of storage limitation and exception for archiving in public interest

that personal data must not be kept in a form which permits identification of data subjects for no longer than is necessary for the purposes for which the personal data are processed

Exception

- long term processing “solely for archiving purposes in the public interest, scientific or historical research purposes or statistical purposes
- public repositories are in general entitled to collect, process, store and make available certain personal information, even if that information was not originally created or collected for the purposes of archiving in a repository

Proportionality!

RIGHT TO OBJECT AND RIGHT TO ERASURE

Right to object and right to erasure (right to be forgotten)

- the controller shall have the obligation to erase personal data on request, if there are no overriding legitimate grounds for the processing, such as
 - exercising the right of freedom of expression and information
 - compliance with a legal obligation
 - reasons of public interest in the area of public health
 - archiving purposes in the public interest, scientific or historical research purposes

Data protection by design

Old concept, newly defined

The liability starts even before processing takes place

form of good practice of the data controller to design its processes and systems in order to minimize the risks of data protection breaches

The GDPR introduces obligation of the controller to implement appropriate technical and organisational measures to ensure and to be able to demonstrate that processing is performed in accordance with this Regulation

The controller is explicitly required to assess the risks, make plans for the security of the data both at the time of the determination of the means for processing and at the time of the processing itself

Anonymisation, pseudonymisation and profiling

Anonymized

- The key to pseudonyms does not exist

Pseudonymized

- can be de-cyphered and the individual can be tracked and identified
- pseudonymized data is personal data and fall within the scope of the regulation.

Profiling

- automated processing of personal data consisting of the use of personal data to evaluate certain personal aspects



Liability for personal data in software (?)





The Bessemer Cloudscape

Top 300 Cloud Computing Companies

Software as-a-Service

END USERS

<p>Enterprise Social Media</p> <p>hootsuite, heardlysocial, vitrue, SOCIALCAST, Yammer, gigya, chatter, Lithium, WILDFIRE, radian6, Zuberance, BUDDYMEDIA, ELOQUA</p>	<p>Marketing Demand Generation</p> <p>KENSHOO, VerticalResponse, ELOQUA, unbounce, Constant Contact, Marketo, ExactTarget, iContact, Bronto, vocus, bizo, Silverpop, CampaignMonitor, Infusionsoft, XYDO, contact@21, responsys, MailChimp, Marin</p>	<p>Human Resources</p> <p>workday, Cornerstone, LinkedIn, bambooHR, BULLHORN, saba, upmo, EPICOR, HALOGEN, echospan, Ultimate Software, selectmech, Taleo, SuccessFactors, SAP Business ByDesign, REPLICON, Lumesse</p>	
<p>Marketing Analytics</p> <p>Google Analytics, GinzaMetrics, Simply Measured, CLICOTALE, HubSpot, SIMULMEDIA, COVARIO, convertro, SEO MOZ, VOCUS, Keybroker, Adobe, BRIGHT EDGE, WordStream</p>	<p>CRM</p> <p>NETSUITE, salesforce.com, insideView, satisfaction, liveops, SurveyMonkey, MEDALLIA, nimbly, clearslide, RightNow, xactly, Steelwedge, PARALINE, zendesk, uservoice, LIVEPERSON, MarketTools, Microsoft</p>	<p>Vertical</p> <p>MINDBODY, SERVICE MAX, PointClickCare, CoreCloud, active47, REALPAGE, OP@WER, YARDI, golista, navicure, superderivatives, RPX, KINUSER, DealerTrack, ppptools, WebPT, Averkie, ooxtime, MicroAnalytics, Vevo, clo, DEALER.COM</p>	<p>Document Management</p> <p>box, Dropbox, Scribd, SugarSync, EchoSign, sendthisfile, REALPAGE, youenoit, WordPress, Drupal, DocuSign, CloudApp, CARBONITE, mozy, Allresco, watchdox, bitcasa, ShareFile, backupify, slideshare</p>
<p>Finance & Accounting</p> <p>Intacct, statpro, NETSUITE, aria, kyriba, Bill.com, FRESHBOOKS, SOSO, Expensify, ARDA, coupa, uora, Adaptive Planning, Chargify, ncur, QAD ERP, WQVE, truaxis, Avalara, expensecloud, RECURLY, FINANCIAL FORCE.COM</p>	<p>Business Intelligence</p> <p>mixpanel, Rosslyn Analytics, SUMIALL, SpatialKey, 1010 data, birst, visier, INSIGHT SQUARED, Cloud IQ, EdgeSpring, GoodData, JASPERSIGHT, Kontagent, SAP Business Objects, BI OnDemand, pivotlink, LATTICE ENGINES, RPX, kognitio, pentaho, Datasphere, bime</p>	<p>Collaboration</p> <p>box, 37signals, TeamViewer, Atlassian, skype, jive, moxie, FORTA, Google Apps, PODIO, Teambox, COLLABNET, RingCentral, GFI, clarizen, liquid, Zimbra, anyto, thinking phone networks, asana, Webex, LogMeIn, Office365, GoToMeeting, huddle</p>	<p>Retail & E-Commerce</p> <p>SRPLY, shopify, BIG Commerce, RSI, DELIVERYAGENT, PowerReviews, QONESTOP, Magento, volusion, Bazaarvoice, VeriSign, yodle</p>

Platform as-a-Service

heroku, SendGrid, Madlogic, JETPCLOUD, CLOUDFLARE, actionio, acquia, CLOUD FOUNDRY, BOOM, janrain, X APPRIO, CloudBees, cloudkick, Parse, Expect Labs, github, AppAssure, cloudshare, DIGASPACE, ppenda, dotcloud, CMCsoft, twilio, CLIGR, aster data, RALLY, SOASTA, splunk, JULY, MarkLogic, SUNSPYPROCESS, Simply Measured, force.com, Orimp, CloudPassage, snoplogic, New Relic, xeround, CloudLock, Cloud IDE, infochimps, loglogic, enan, buncy, Simplified, okta, AppDynamics, Zerto, appfog, ALERTLOGIC, RAPID7, Skytap, standingcloud, Acronis, silver, abicavo, SCALESXTRME, apptio, DynamicOps, kapow, veeam, MuleSoft, service now, stripe

Infrastructure as-a-Service

amazon.com, rackspace, redhat, piston, nebula, SOFTLAYER, CITRIX, CloudPassage, actifio, hp, ORACLE, EUCALYPTUS, nimbus, vmware, Joyent, Parallels, terremark, nicira

DEVELOPERS & IT

Download a digital copy or nominate your company: bvp.com/cloud

©Bessemer Venture Partners 2012 v3.3

The most significant question:

Your role

- Are you data controller
- Are you data processor
- Are you ISP provider?

Other questions

Sharing data

Imported data

Subcontractors

Foreign subjects



**PRÁVNICKÁ
FAKULTA**

Masarykova univerzita

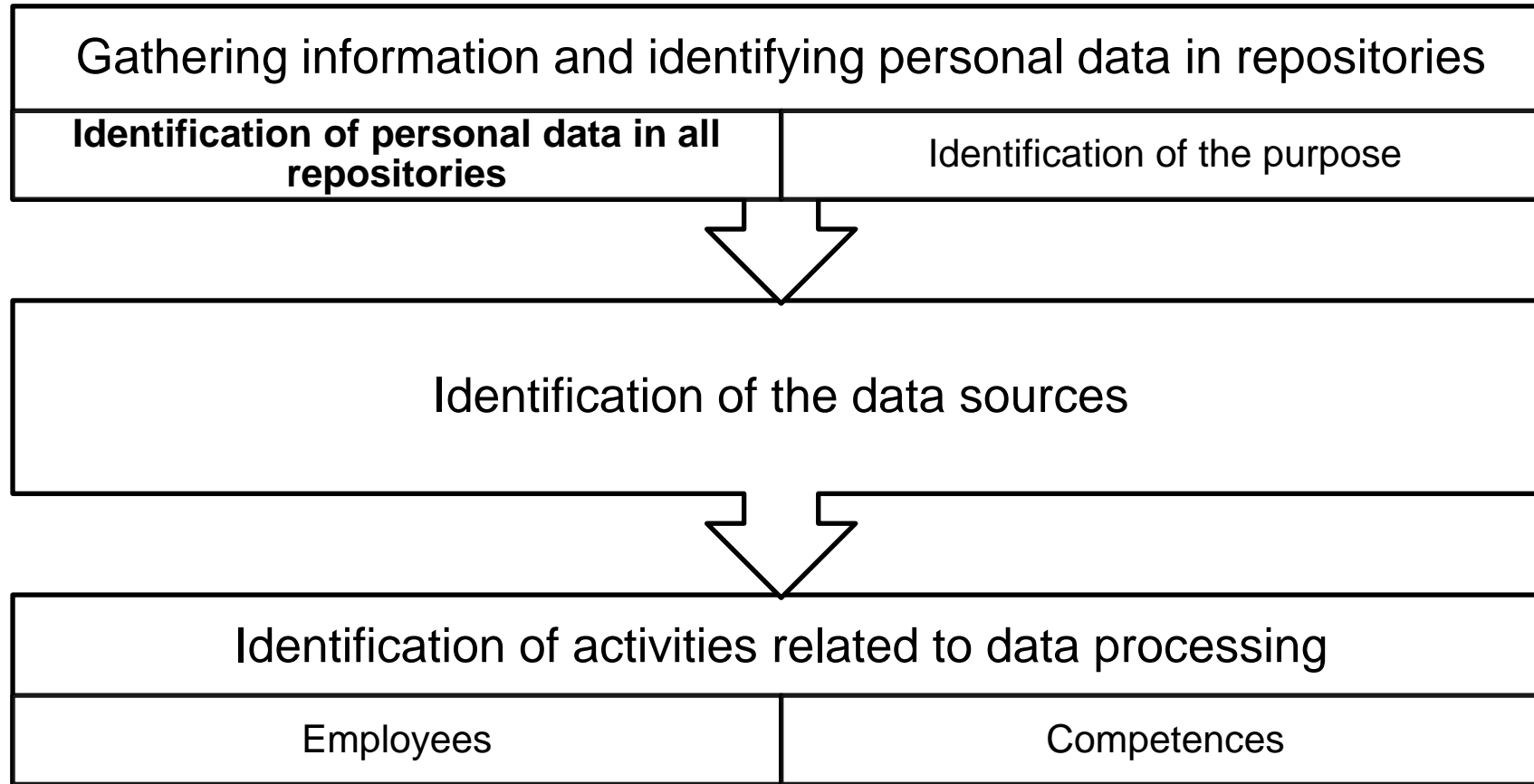
INSTITUTIONAL RULES AND POLICIES FOR SHARING AND STORING DATA



General Data Protection Regulation



Step 1 - Monitoring



Step 2 Adopting policies and internal rules

- General data protection policy
- Privacy (transparency) policy
- ... ?

IDENTIFICATION OF PERSONAL DATA IN ALL ARCHIVES/REPOSITORIES

Identification of personal data

- definition of “personal data” is very extensive and covers any information that can be directly or indirectly related to an individual
- data do not have to be structured, in order to be qualified as personal data
- Any information in any media format including photographs, audio and visual records may meet the definition of personal data
- even pseudonymized information is to be considered a personal information.

Identification of the purpose of processing

- Defined purpose for each set of data is necessary to determine whether the institution does require a consent of a data subject or not.
- The general regulatory principles of purpose limitation, data minimisation or storage limitation are directly related to the purpose of data processing.
- Personal data shall be adequate, relevant and limited to what is necessary in relation to the purposes for which they are processed

Identification of the purpose of processing

- The purpose of data processing is also crucial in:
 - dealing with the requests for erasure of data or
 - right to restriction of processing.
 - that the purpose needs to be determined at the time of the collection of the personal data
 - changing purpose of the data processing after the data have been collected is limited by GDPR and restricted to several exactly defined cases.

Identification of Activities

- Processing of personal data is a daily activity in every public institution or business
- governance of personal data has to be based on the purpose the processed data serve
 - i.e. their value to the organization
- After the personal data have been identified, it is necessary to be attribute each set of records to a certain purpose (or purposes) for which they have been collected and processed.

Identification of the data sources

- Anonymous or pseudonymous?
 - Is anonymity absolute or relative?
 - Case C-582/14: Patrick Breyer v Bundesrepublik Deutschland where CJEU ruled that the possibility to combine the data with this additional data must constitute a means likely reasonably to be used to identify the individual

Adopting policies and internal rules

- General data protection policy addressing privacy by design and default
- Privacy (transparency) policy

Data protection by design and default

- Identify major risks
- Keep records
- Identify organizational units that are required to take measures to protect these rights.

Records

- the name and contact details of the controller
- categories of data subjects and of the categories of personal data;
- the categories of recipients to whom the personal data have been or will be disclosed;
- transfers of personal data to a third country or an international organisation, the envisaged time limits for erasure of the different categories of data;
- description of the technical and organisational security measures

Privacy (transparency) policy

- the contact details of the controller and controller's representative;
- the contact details of the data protection officer
- the purposes of the processing;
- the legitimate interests pursued by the controller or by a third party;
- the period for which the personal data will be stored, or criteria used to determine that period;
- the existence of the right to request from the controller access
- information regarding the existence of the right to withdraw

Self governance

- Codes of conducts (40)
- Certifications (42)
- Binding corporate rules (47)



**PRÁVNICKÁ
FAKULTA**

Masarykova univerzita

Thank you for your attention



Definujte zápatí - název prezentace / pracoviště