knowledge17

http://clabs.link/lab132020

WORK at LIGHTSPEED

How ServiceNow Can Help Your Compliance Journey to GDPR

Manoj Patel
Security & Risk Global Practice EMEA
ServiceNow

Eric Le Martret
Security & Risk Global Practice EMEA
ServiceNow

© 2017 ServiceNow All Rights Reserved

servicenow

Speaker Introduction



Name: Eric Le Martret

Title: Sr. Advisory Solution Consultant

Function: Security & Risk Global Practice EMEA

Company: ServiceNow

Eric Le Martret serves as a Senior Advisory Solution Consultant of ServiceNow's Global Security and Risk Practice. This business unit is focused on solving Enterprise Risk & Security challenges. He joined ServiceNow in Summer 2015 in charge of ServiceNow's GRC offering across EMEA, rapidly growing the pipeline and closing key deals. He added Security Operations to his scope as Geneva was released. He contributed to most of the GRC and SecOps deals in the UK, France, Benelux and Nordic countries in 2016. Eric brings a total of 30+ years of experience in Risk, Compliance, Audit and Security Management, mostly as a practitioner. He is based out of London. Prior to joining ServiceNow, he worked in different positions for KPMG, BG Group, T-Systems or Capgemini , as CRO, CISO or head of GRC, and RM Partners or ADIS as CEO.

He is a former member of the Institute of Risk Management and is certified in ISO 31000. He holds an MBA (Finance) from AUDENCIA (France).

© 2017 ServiceNow All Rights Reserved

Speaker Introduction



Name: Manoj Patel

Title: Advisory Solution Consultant

Function: Security & Risk Global Practice EMEA

Company: ServiceNow

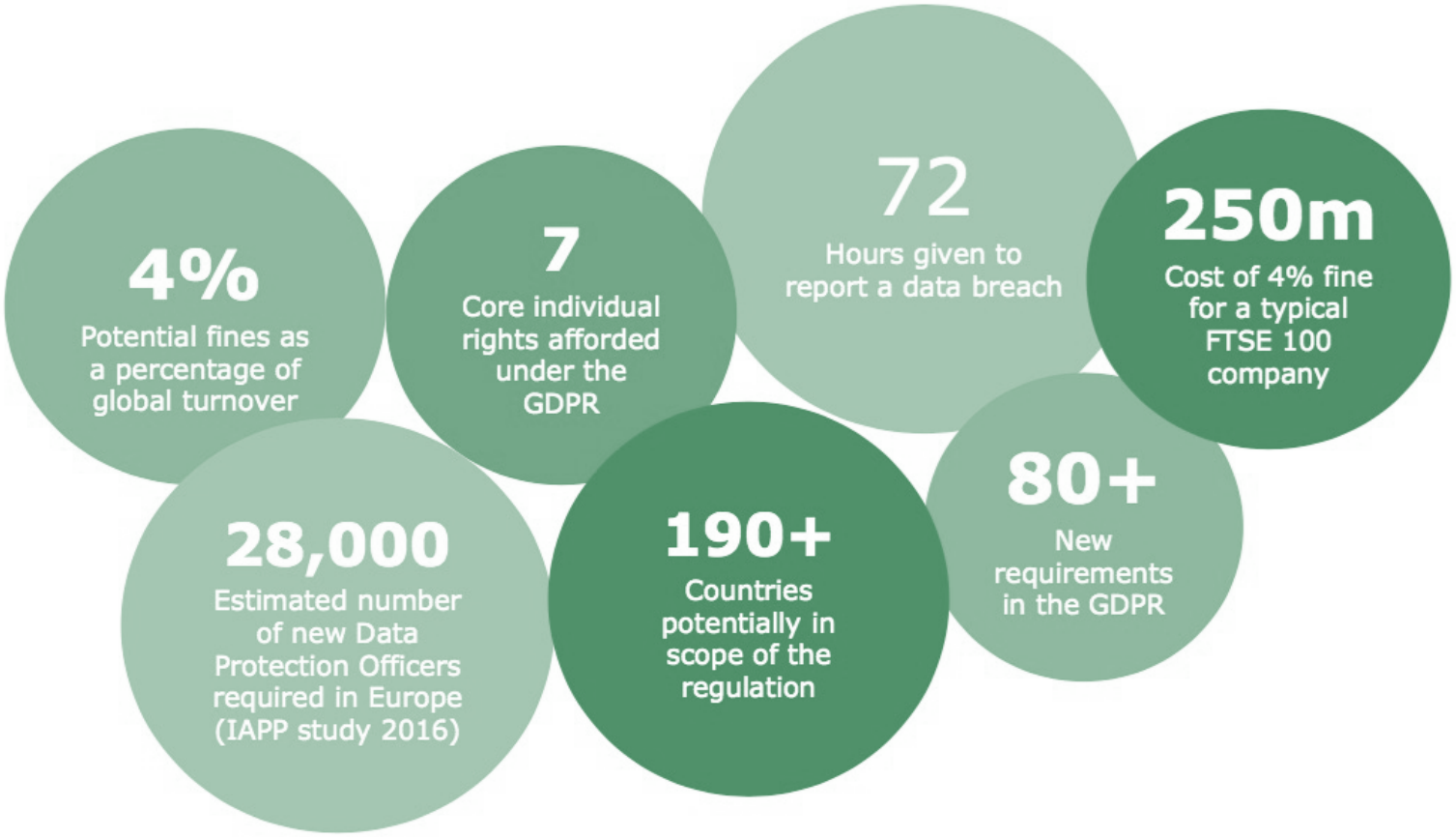
Manoj Patel serves as an Advisory Solution Consultant of ServiceNow's Global Security and Risk Practice. This business unit is focused on solving Enterprise Risk & Security challenges. He joined ServiceNow in Summer 2014 and positioned ServiceNow, especially in non-IT Space – including GRC, Security and Financial Management and successfully contributed building pipeline and closing key deals in EMEA. He was awarded Top-SC EMEA Central in 2015. Manoj brings a total of 20+ years of experience in Enterprise Service Management and Legal, Security & Defense space. He is based out of Munich. Prior to joining ServiceNow, he worked in different positions for DaimlerChrysler, BMC software, FrontRange, and CA Nimsoft, as well as for a Enterprise Legal, Risk & Defense Management subsidiary of Wolters Kluwer, leading teams in EMEA, APAC and LatAm.

He is certified GRCP (OCEG) and CSX CyberSecurity (ISACA). He holds an MBA (Finance) from UK, M.S. (Computer Science) from Germany, and B.Sc. (Physics) from India.

© 2017 ServiceNow All Rights Reserved

GDPR: At a glance

SecOps & GRC

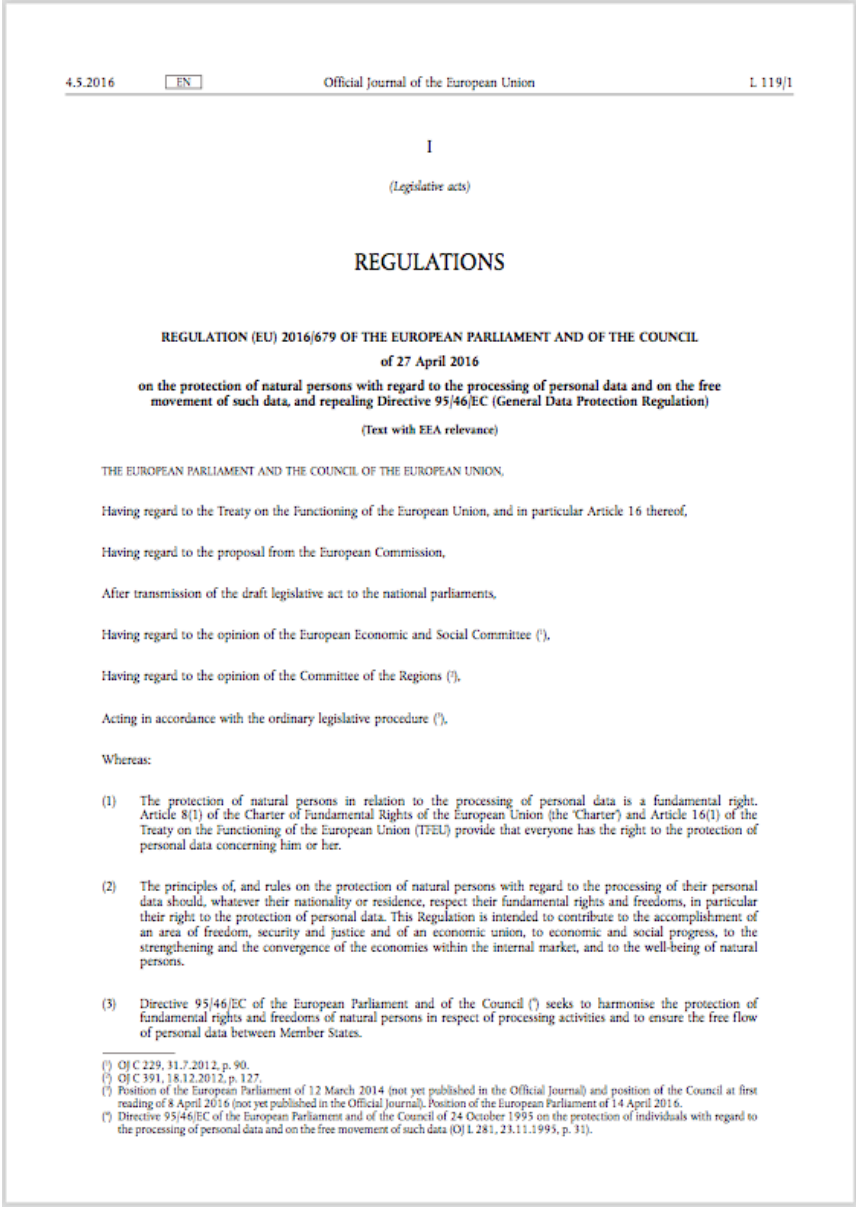


© 2017 ServiceNow All Rights Reserved

GDPR – What is it?

- The General Data Protection Regulation (GDPR) (Regulation (EU) 2016/679) is a Regulation by which the European Commission intends to strengthen and unify data protection for individuals within the European Union (EU).

- Major goals of the General Data Protection Regulation (GDPR) (2016/679/EU) are:
  - protection of EU citizens' personal data
  - define the rules for a free movement of personal data in the EU



4.5.2016 EN Official Journal of the European Union L 119/1

I

(Legislative acts)

REGULATIONS

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.

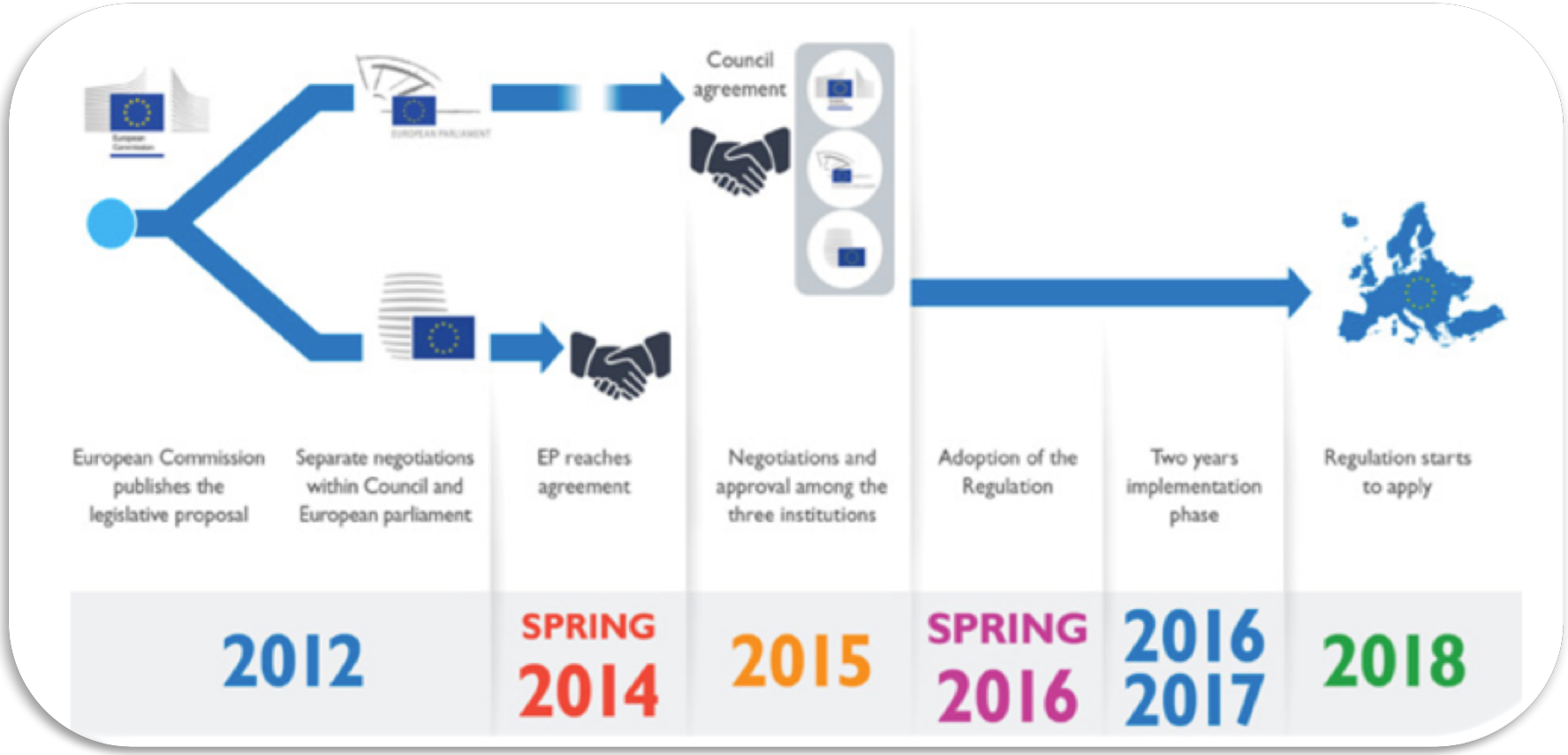
(2) The principles of, and rules on the protection of natural persons with regard to the processing of their personal data should, whatever their nationality or residence, respect their fundamental rights and freedoms, in particular their right to the protection of personal data. This Regulation is intended 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.

(1) OJ C 229, 31.7.2012, p. 90.
(2) OJ C 391, 18.12.2012, p. 127.
(3) Position of the European Parliament of 12 March 2014 (not yet published in the Official Journal) and position of the Council at first reading of 8 April 2016 (not yet published in the Official Journal). Position of the European Parliament of 14 April 2016.
(4) Directive 95/46/EC of the European Parliament and of the Council of 24 October 1995 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (OJ L 281, 23.11.1995, p. 31).

© 2017 ServiceNow All Rights Reserved

GDPR – Roadmap



Enforcement date: 25 May 2018 - at which time those organisations in non-compliance will face heavy fines

© 2017 ServiceNow All Rights Reserved

EU GDPR Personal Data - Definition

“Personal data is any information relating to an individual, whether it relates to his or her private, professional or public life. It can be anything from a name, a photo, an email address, bank details, posts on social networking websites, medical information, or a computer’s IP address."

© 2017 ServiceNow All Rights Reserved

GDPR – Scope & Assessment

- A single set of rules will apply to all EU member states. Applies to all organisations operating in EU or processing EU citizen's personal data.



Citations | New | Reference | Art. 35

Authority Document = 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 (Gener > Reference >= Art. 35

Reference ▲	Name	Description
Art. 35	Art. 35	Data protection impact assessment
Art. 35.1.	Art. 35.1.	Where a type of processing in particular using new technologies, and taking into account the nature, scope, context and purposes of the processing, is likely to result in a high risk to the rights and freedoms of natural persons, the controller shall, prior to the processing, carry out an assessment of the impact of the envisaged processing operations on the protection of personal data. A single assessment may address a set of similar processing operations that present similar high risks.
Art. 35.10.	Art. 35.10.	Where processing pursuant to point (c) or (e) of Article 6(1) has a legal basis in Union law or in the law of the Member State to which the controller is subject, that law regulates the specific processing operation or set of operations in question, and a data protection impact assessment has already been carried out as part of a general impact assessment in the context of the adoption of that legal basis, paragraphs 1 to 7 shall not apply unless Member States deem it to be necessary to carry out such an assessment prior to processing activities.
Art. 35.11.	Art. 35.11.	Where necessary, the controller shall carry out a review to assess if processing is performed in accordance with the data protection impact assessment at least when there is a change of the risk represented by processing operations.
Art. 35.2.	Art. 35.2.	The controller shall seek the advice of the data protection officer, where designated, when carrying out a data protection impact assessment.
Art. 35.3.	Art. 35.3.	A data protection impact assessment referred to in paragraph 1 shall in particular be required in the case of:
Art. 35.3.(a)	Art. 35.3.(a)	a systematic and extensive evaluation of personal aspects relating to natural persons which is based on automated processing, including profiling, and on which decisions are based that produce legal effects concerning the natural person or similarly significantly affect the natural person;

- **Data Protection Impact Assessments (Article 35) have to be conducted when specific risks occur to the rights and freedoms of data subjects.**
- Risk assessment and mitigation is required and a prior approval of the DPA for high risks.

© 2017 ServiceNow All Rights Reserved



Data protection officer

© 2017 ServiceNow All Rights Reserved



Opt-in for data collection

© 2017 ServiceNow All Rights Reserved



Right to be “forgotten”

© 2017 ServiceNow All Rights Reserved



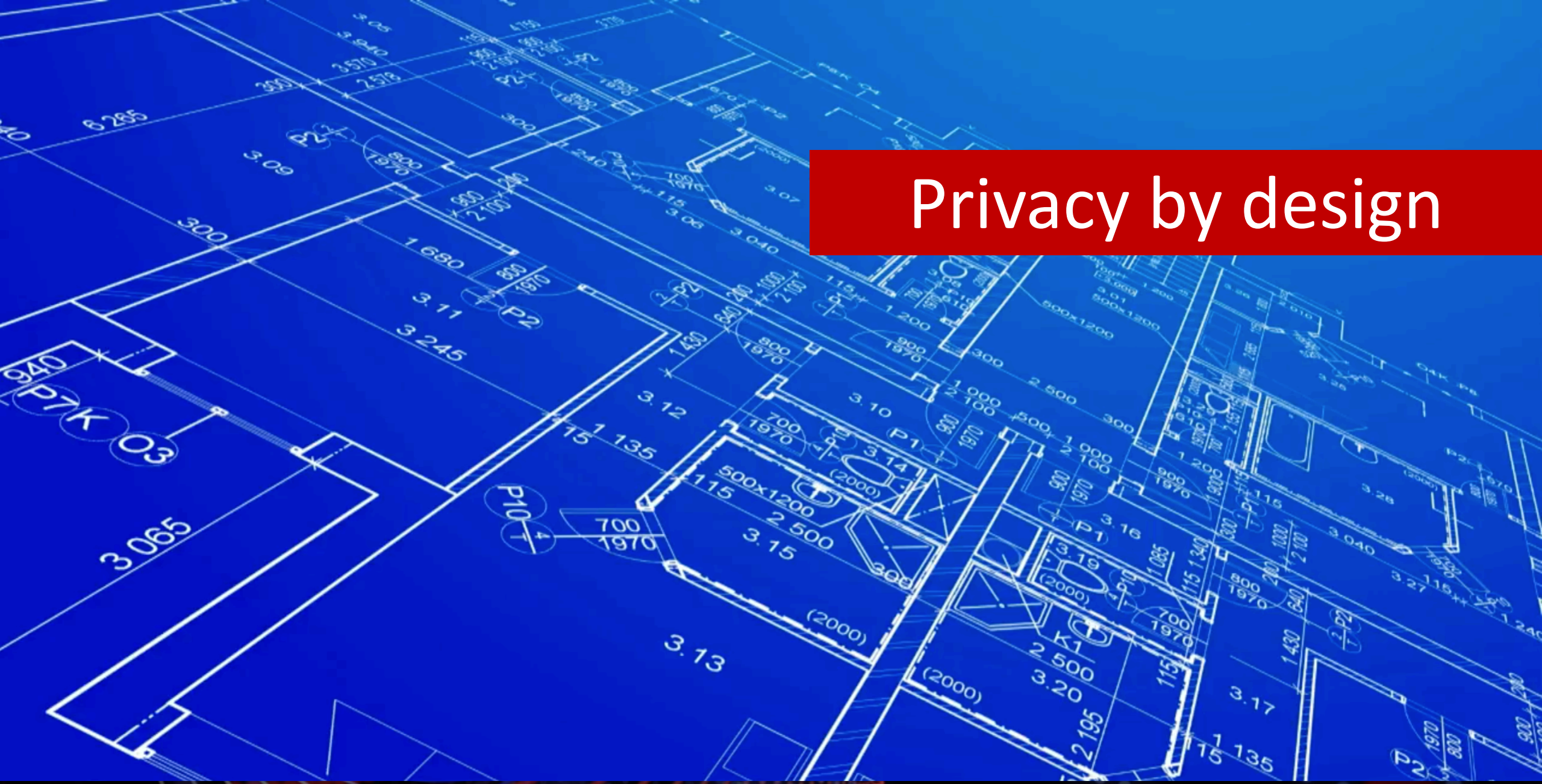
Breach notification

© 2017 ServiceNow All Rights Reserved



€ 20.000.000 / 4% global turnover

© 2017 ServiceNow All Rights Reserved



Privacy by design

© 2017 ServiceNow All Rights Reserved



One-stop shop

© 2017 ServiceNow All Rights Reserved

Top Takeaways

1

- GDPR is a fact.
- You have to align your data & processes with GDPR and there is not much time left to do so!

2

- Familiarize with GDPR challenges & requirements while collecting and utilising EU citizen personal data.
- Map those to your organizational policies & procedures.

3

- Get professional guidance.
- Implement GRC Best Practices.
- **If not started yet, you are already late**

© 2017 ServiceNow All Rights Reserved

Note:

- Lab guide updates:
  - Page 15, #1: The GDPR Compliance gauge should be empty. Not yellow. It will be yellow at a later stage.
  - Page 23, #6: Go to Compliance overview DB. The gauge should be yellow now.
  - Page 25, #13. Wait for all attestations to be completed.

© 2017 ServiceNow All Rights Reserved

Note:

- Lab guide updates:
  - Page 15, #1: The GDPR Compliance gauge should be empty. Not yellow. It will be yellow at a later stage.
  - Page 23, #6: Go to Compliance overview DB. The gauge should be yellow now.

Student Instance admin password: 132020W311#K17
Student Instance Reservation URL: http://clabs.link/lab132020

© 2017 ServiceNow All Rights Reserved

Thank You

Lab Sponsored by Microsoft Azure



Manoj Patel
Security & Risk Global Practice EMEA
ServiceNow

Eric Le Martret
Security & Risk Global Practice EMEA
ServiceNow

@Man0jPatel| @EricLeMartret | #Know17 | http://clabs.link/lab132020

© 2017 ServiceNow All Rights Reserved

Q & A

Manoj Patel
Security & Risk Global Practice EMEA
ServiceNow

Eric Le Martret
Security & Risk Global Practice EMEA
ServiceNow

@Man0jPatel| @EricLeMartret | #Know17 | http://clabs.link/lab132020

© 2017 ServiceNow All Rights Reserved