

RSA®Conference2016

San Francisco | February 29 – March 4 | Moscone Center

SESSION ID: PRV-T11

Bridging Privacy, Security, IT and Information Governance to prepare for new European General Protection Regulation

MODERATOR: **Dana Louise Simberkoff, JD, CIPP/US**

Chief Compliance and Risk Officer
AvePoint Inc.
@danalouise



Connect **to**
Protect

PANELISTS:

Bojana Bellamy

President
Centre for Information Policy Leadership
@the_cipl

JoAnn Stonier

EVP, Chief Information Governance &
Privacy Officer
Mastercard
@privacydesign

Michelle Dennedy

Chief Privacy Officer
Cisco
@mdennedy



#RSAC

The new EU Data Protection Regulation requires that you rethink privacy, security and information governance strategy.



#RSAC

- Understand and articulate the “new” (and not new) obligations the EU GDPR will create for the CISO, IT and the CIO
 - Privacy and Security by Design and Default
 - Privacy Impact Assessments
 - Inventory and Data Maps for all Systems that hold PII
 - Mandatory Breach Notification
 - Etc....
- Securely Manage and Share Information utilizing a “Risk Based” approach
- Ensure IT, Security and Privacy Work Better Together

EU Data Protection Regulation at a Glance

Harmonisation and some progress	Wider scope	Increased obligations	Strengthened rights of individuals	Increased enforcement, fines, liability
<ul style="list-style-type: none"> • Harmonised rules, but not fully (e.g. employee data, children data) • One Stop Shop: Lead DPA for pan-European matters, in cooperation with other DPAs; Local DPA for local matters and redress for individuals • Risk-based approach • Some reduction of administrative burden (no national registration of processing, or prior authorisation) • BCR, seals and certifications 	<ul style="list-style-type: none"> • Controller and processor • Extraterritorial application to foreign controller and processor • Wider definition of personal data and sensitive data; anonymous data and pseudonymisation • Processing children data under 16 require parental consent 	<ul style="list-style-type: none"> • DP principles tightened (consent, transparency/notices) • Profiling rules • Privacy Impact Assessment • Privacy by Design • Breach notification - to DPAs and individuals • Direct obligations and liability for processor • Accountability - privacy program • Internal record of processing • DP Officer 	<ul style="list-style-type: none"> • Right to erasure • Data portability • Right not to be subject to automated profiling / right to object 	<ul style="list-style-type: none"> • Regulatory fines up to 4% of annual worldwide turnover • Individual action • Class action • Criminal sanctions (in national laws) • Larger role for European Data Protection Board (EDPB)

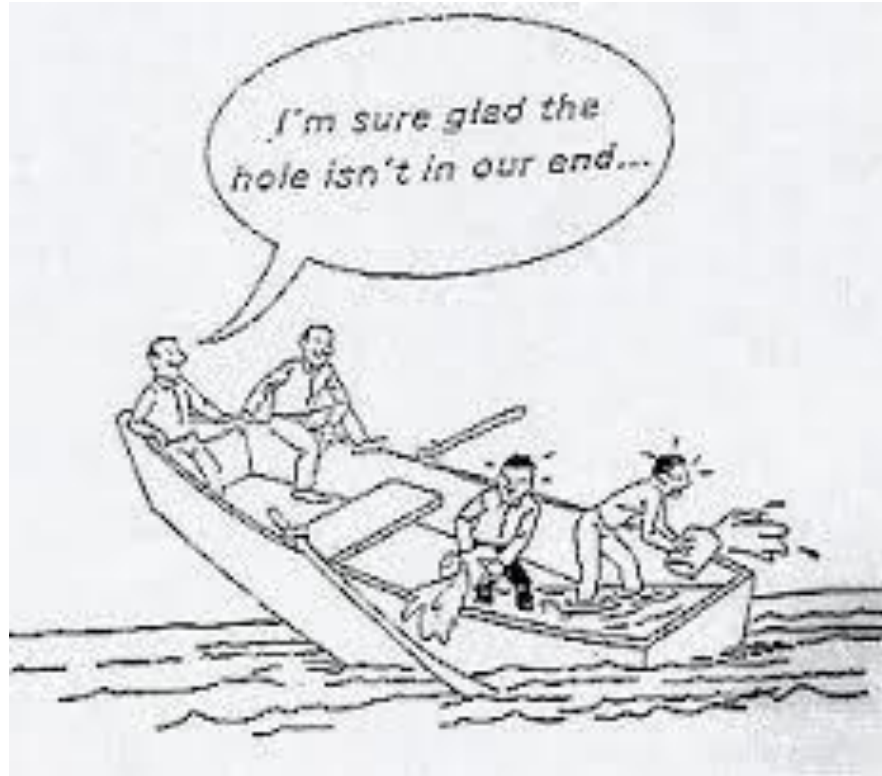
Panel Questions...



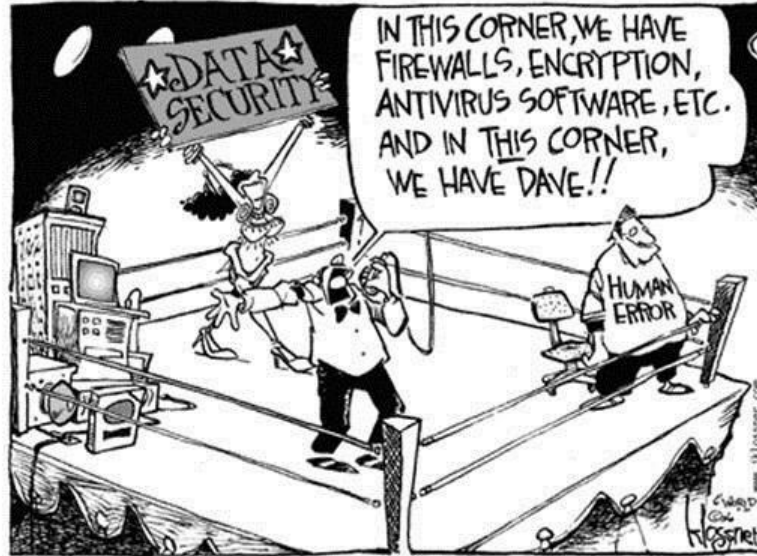
How do we reconcile the idea that “more is better”
when it comes to data or is that even a conflict?



What do the CIO, CISO and “The Business” Need to know about the GDPR?



What do you see as the role of automation?



© DESPAIR.COM




MISTAKES

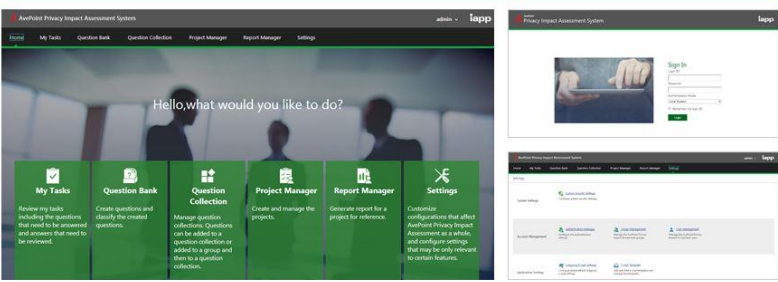
IT COULD BE THAT THE PURPOSE OF YOUR LIFE IS
ONLY TO SERVE AS A WARNING TO OTHERS.

Resources

About APIA

- Developed by AvePoint
- Distributed exclusively by IAPP
- Global Support provided by AvePoint
- Educational Resource ***Cost Free***! (AvePoint Global Research and Development Team)
- Extended by the Privacy Community!
- https://www.privacyassociation.org/resource_center/epoint_privacy_impact_assessment_system

**AvePoint®**
PRIVACY IMPACT ASSESSMENT (APIA) SYSTEM



admin | Inapp

My Tasks Question Bank Question Collection Project Manager Report Manager Settings

Hello, what would you like to do?

My Tasks
Review my tasks including the questions that need to be answered and answers that need to be reviewed.

Question Bank
Create questions and identify the related questions.

Question Collection
Manage questions collections. Questions can be added to a question collection or added to a group and then to a question collection.

Project Manager
Create and manage the projects.

Report Manager
Generate report for a project for reference.

Settings
Customize configurations that affect AvePoint Privacy Impact Assessment as an artifact and configure settings that may be only relevant to certain instances.

Sign In
Email
Password
Sign In

FREE DOWNLOAD

Download the Most Recent Templates
Click here for the full list and to download templates that suit your needs.

APIA Forum
Connect with other privacy experts, get insight and share ideas on the APIA Forum, a community discussion board.

The AvePoint Privacy Impact Assessment (APIA) System can help you automate the process of evaluating, assessing and reporting on the privacy implications of your enterprise IT systems. Exclusively available through the IAPP, the APIA System allows you to select questions from the prepopulated bank of PIA questions or create your own, meaning you can build and save PIA templates to be reused and reported out.

- Comply with Privacy Regulations
- Automate Privacy Impact Assessments
- Report on PIAs for Stakeholder Review
- Extend to Security and Vulnerability Assessments



- IAPP web page:
https://www.privacyassociation.org/resource_center/avepoint_privacy_impact_assessment_system
- APIA website (on avepoint.com):
<http://www.avepoint.com/privacy-impact-assessment/>
- Centre for Information Policy Leadership
<https://www.informationpolicycentre.com/>
- Privacy and Information Security Law Blog
<http://www.huntonprivacyblog.com>
- EU GDPR Readiness Benchmark- CIPL-AvePoint (coming in 2016)

Our Contact Information...



#RSAC

- Dana Simberkoff, JD, CIPP/US , Chief Compliance and Risk Officer, AvePoint Inc., Dana.Simberkoff@avepoint.com @danalouise
- Bojana Bellamy, President, Centre for Information Policy Leadership bbellamy@hunton.com @THE_CIPL
- JoAnn Stonier, EVP, Chief Information Governance & Privacy Officer, Mastercard [JoAnn Stonier@mastercard.com](mailto:JoAnn_Stonier@mastercard.com) @privacydesign
- Michelle Dennedy, Chief Privacy Officer, Cisco @mdennedy

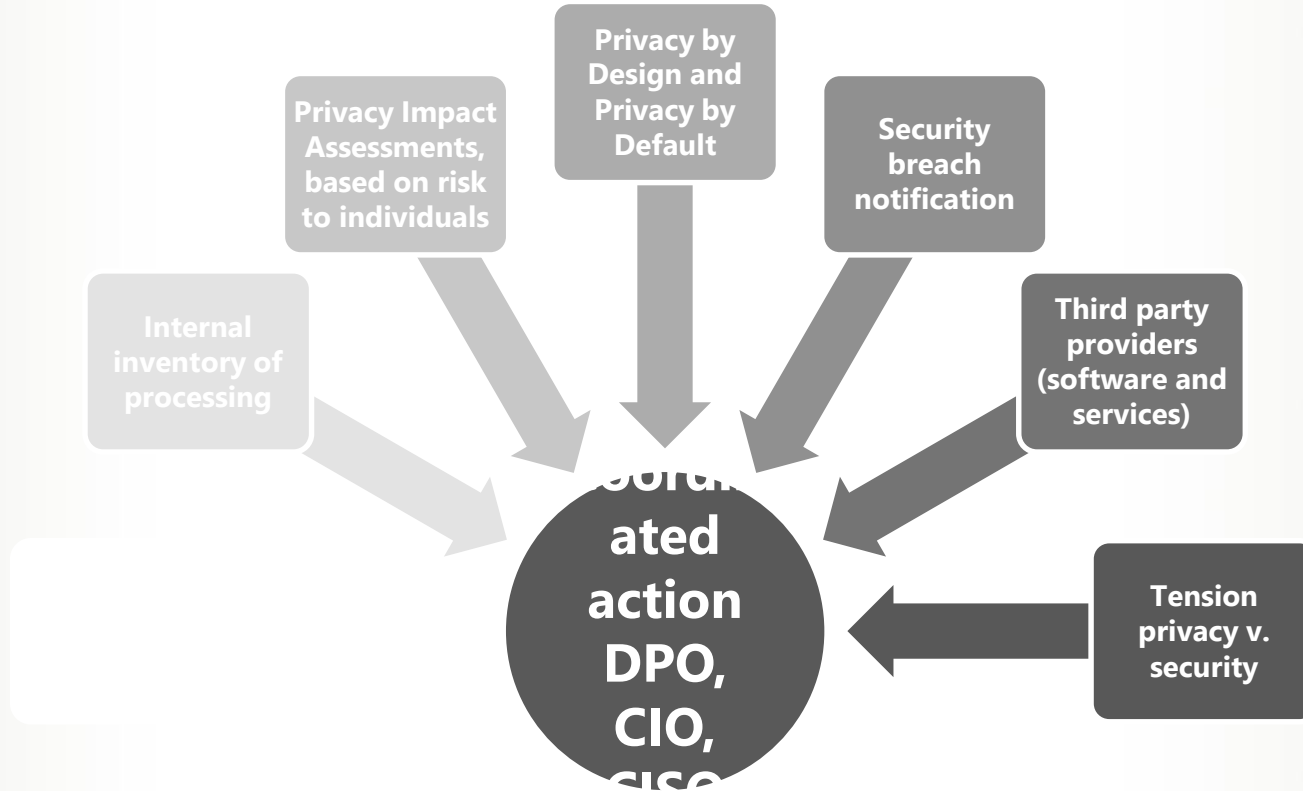
Gracias	ευχαριστώ	Danke	Grazie	Hvala	Obrigado	Kiitos	شكراً	谢谢
Ahsante	Teşekkürler	متشكرم	Salamat Po	Cám ơn	شكريه	Terima Kasih	Dank u Wel	Tack
நன்றி	Köszönöm	ありがとう ございます	ขอบคุณครับ	Mulțumesc	thank you			
תודה	多謝晒	дякую	Ďakujem	спасибо				
благодаря	Tak	감사합니다	Děkuji	Dziękuję				

GDPR Background

EU Data Protection Regulation at a Glance

Harmonisation and some progress	Wider scope	Increased obligations	Strengthened rights of individuals	Increased enforcement, fines, liability
<ul style="list-style-type: none"> • Harmonised rules, but not fully (e.g. employee data, children data) • One Stop Shop: Lead DPA for pan-European matters, in cooperation with other DPAs; Local DPA for local matters and redress for individuals • Risk-based approach • Some reduction of administrative burden (no national registration of processing, or prior authorisation) • BCR, seals and certifications 	<ul style="list-style-type: none"> • Controller and processor • Extraterritorial application to foreign controller and processor • Wider definition of personal data and sensitive data; anonymous data and pseudonymisation • Processing children data under 16 require parental consent 	<ul style="list-style-type: none"> • DP principles tightened (consent, transparency/notices) • Profiling rules • Privacy Impact Assessment • Privacy by Design • Breach notification - to DPAs and individuals • Direct obligations and liability for processor • Accountability - privacy program • Internal record of processing • DP Officer 	<ul style="list-style-type: none"> • Right to erasure • Data portability • Right not to be subject to automated profiling / right to object 	<ul style="list-style-type: none"> • Regulatory fines up to 4% of annual worldwide turnover • Individual action • Class action • Criminal sanctions (in national laws) • Larger role for European Data Protection Board (EDPB)

EU DPR - Key Red Flags for IT, CIO, CISO



Holistic Approach to Privacy and Security

