



# TUV USA, INC. MEMBER OF TUV NORD GROUP

General Data Protection Regulation Overview  
Webinar

# WELCOME GENERAL DATA PROTECTION REGULATION



**TUV USA Team**

Host

TUV USA Academy

**Email:** [academy-us@tuv-nord.com](mailto:academy-us@tuv-nord.com)

**Phone:** 844-488-8872



**Scott Wilson**

Presenter

Chief Security & Privacy Officer

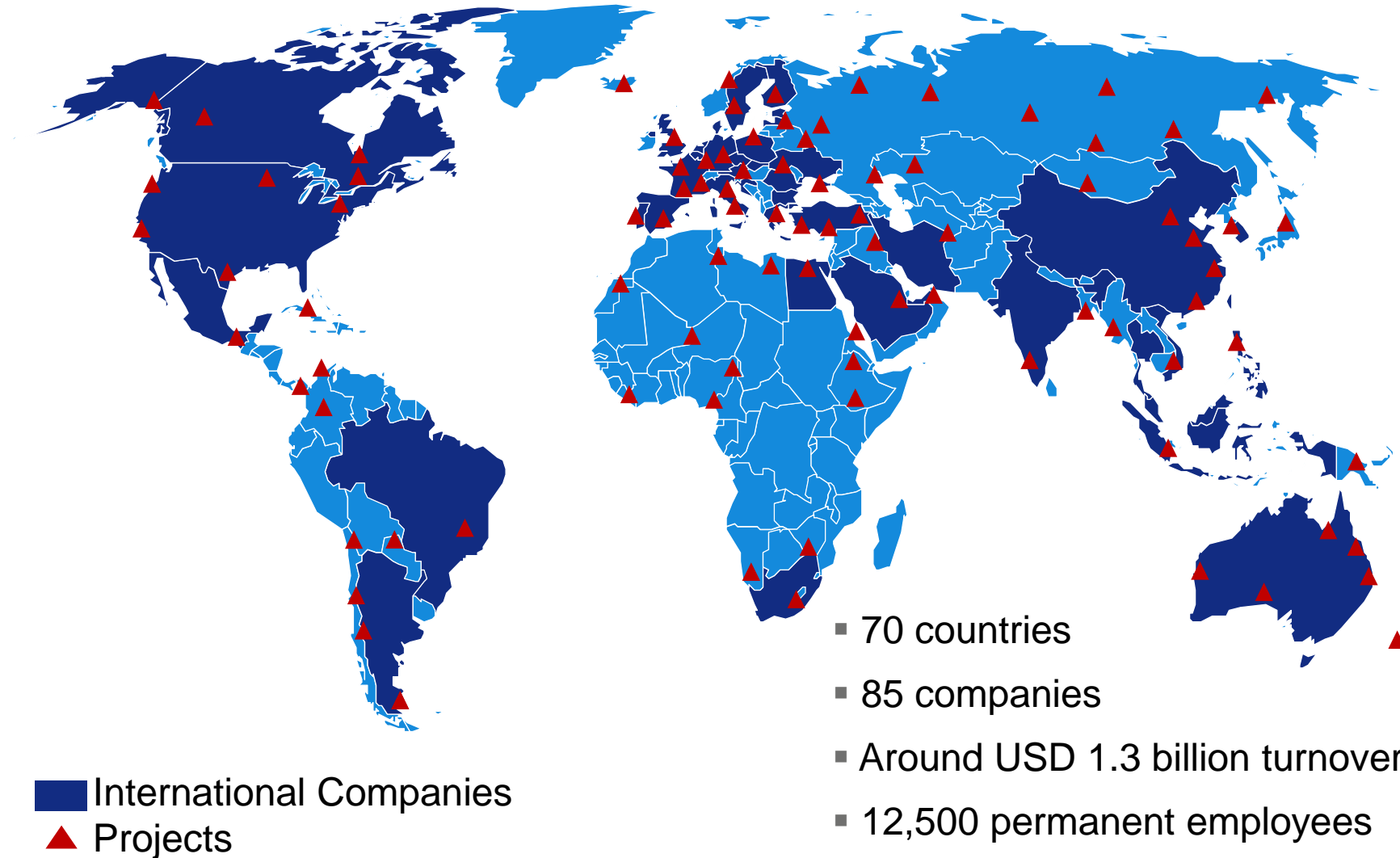
Ventiv Technology Inc.

**Email:** [scott.Wilson@ventivtech.com](mailto:scott.Wilson@ventivtech.com)

**Phone:** +1.770.308.5499

# TÜV NORD GROUP AT A GLANCE

## WORLDWIDE ACTIVITIES





# GLOBAL PRESENCE:

## TÜV NORD GROUP



# QUALITY SYSTEM DIVISION

- DakkS Accreditation for ISO 9001, 14001 and 18001
  - Expert for automotive and IT systems
  - ANAB accreditation for ISO 9001 and AS9100 series
  - Access to a global network of auditors approved under DakkS and ANAB
  - Short turn around times
  - Web-based system to manage system certification
- 
- **Benefits of certification**
    - Increase in economic efficiency
    - Time and cost savings
    - Image enhancement and increased trust on the part of customers and staff
    - Increase in customer satisfaction
    - Clear quality status
  - **Certification of Quality Management Systems**
    - ISO 9001:2015
    - ISO 14001:2015
    - OHSAS 18001 (ISO 45001)
    - AS 9100 series
    - TS16494, IT27001, ISO50001
    - Security 4 Safety
    - Information Technology
    - BS10012





# GENERAL DATA PROTECTION REGULATION (GDPR) T – 78 DAYS AND COUNTING

TUEV Nord Webinar – March 8, 2018



**Scott Wilson**, Chief Security & Privacy Officer for Ventiv Technology.

Scott has been with Ventiv for over 8 years and is a member of the executive team. He currently oversees the security, privacy, & compliance functions globally for the company. This includes operations in the U.S, Europe, Middle East, and APEC.



Scott possesses 20+ years IT Operations, Service delivery, & Security and Privacy experience. Prior to joining Ventiv, Scott served in several Director level roles (Systems Engineering, Service Desk & Data Center Operations, Network Operations) at EarthLink running both internal MIS systems and all customer facing systems/services. Scott has also held various Technology Leadership roles at Bridge Information Systems (Thompson Reuters) and at Savvis.

CIPP/E, CIPP/US, CIPP/C, CIPM, FIP

Email: [Scott.Wilson@ventivtech.com](mailto:Scott.Wilson@ventivtech.com)

Ph: 770.308.5499

Linkedin: <https://www.linkedin.com/in/scottrichardwilson/>

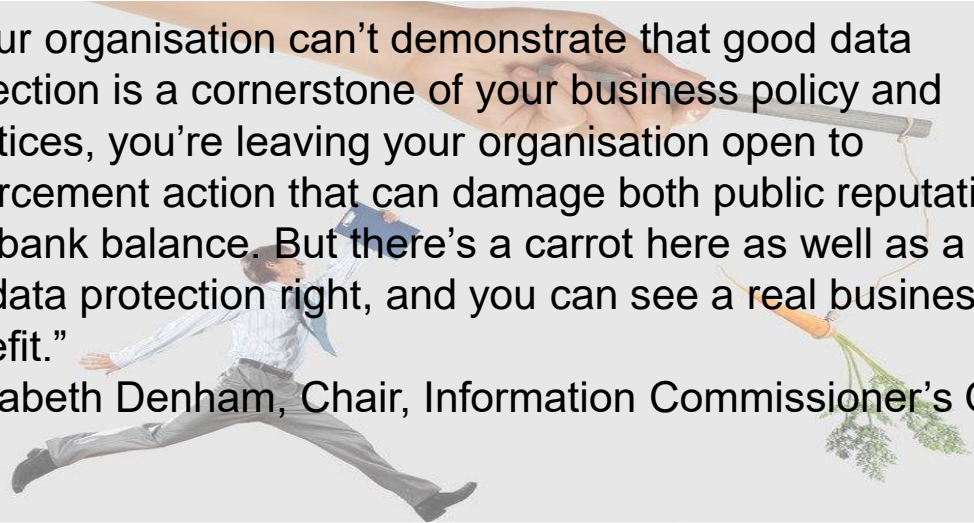




# KEEP CALM AND prepare for GDPR

If your organisation can't demonstrate that good data protection is a cornerstone of your business policy and practices, you're leaving your organisation open to enforcement action that can damage both public reputation and bank balance. But there's a carrot here as well as a stick: get data protection right, and you can see a real business benefit."

Elizabeth Denham, Chair, Information Commissioner's Office





## INTRODUCTION

With less than 3 months to go before the GDPR goes into effect, companies need to have a plan in place to navigate the operational and legal implications of the regulation (the law is still somewhat dynamic and guidance is coming out from both WP29 and EU member states.) This webinar will highlight some of the key areas that companies need to focus on.

# Agenda

- About Ventiv Technology & setting the stage
- Overview of the Regulation
- Record Keeping
- Data Subject Rights
- Data Breach Reporting Requirements
- Supervisory Authorities – Enforcement Actions
- Certifications & Codes of Conduct
- Resources

# ABOUT VENTIV TECHNOLOGY

## Setting the stage

- Ventiv is the largest independent risk, safety, and insurance technology provider (software and SaaS) in the insurtech market
- Our solutions serve some of the most innovative and complex companies and empower them to reduce costs, streamline processes and improve overall performance
- Operations in the U.S, Europe, & Asia
- 500+ global customers
  - Several fortune 50 companies
- 1 Billion+ records hosted across 4 global data centers
- 12 Billion+ transactions a year



# GENERAL DATA PROTECTION REGULATION (GDPR)

## WHAT IS the GDPR?

- GDPR is a complete overhaul/replacement of the EU Data protection directive
  - This is the most wide-reaching privacy regulation in the world (more geographies will be following suit)
- It is binding on all EU member states and becomes enforceable on May 25, 2018
  - GDPR is law and binding to all EU member states (does not require member state ratification)
  - Harmonizes data privacy laws across the EU member states (\*allows for customization by member state)
- Material & territorial scope increase
  - Applies to all organizations (based inside or outside the EU) that handle, store or process EU personal data (regardless of where the data is processed)
  - Broadens the definition of personal data: (online identifiers, biometrics, geolocation, email addresses, etc...)
  - Increase in data subject rights: access requests, objection to processing, erasure, rectification, etc...)
  - Raises the bar for establishing legal basis of processing (consent, fulfillment of a contract, legitimate interest, etc...)
  - Cross-border
- Allows for both administrative sanctions and financial penalties
  - You do not have to have a data breach to be fined. Simply being non-compliant with the regulation opens an organization up to fines)
  - Compel to meet regulation, cease processing, etc...

# GDPR HAS EXTENSIVE REQUIREMENTS FOR COMPLIANCE

[HTTP://EC.EUROPA.EU/JUSTICE/DATA-PROTECTION/REFORM/FILES/REGULATION\\_OJ\\_EN.PDF](http://ec.europa.eu/justice/data-protection/reform/files/regulation_oj_en.pdf)

- 99 Articles
- 173 Recitals
- Chapter 1 – General Provisions
- Chapter II – Principles
- Chapter III – Rights of the data subject
- Chapter IV – Controller and processor
- Chapter V – Transfers of personal data to 3<sup>rd</sup> countries (or international organizations)
- Chapter VI – Independent supervisory authorities
- Chapter VII – Cooperation and consistency
- Chapter VIII – Remedies, liabilities, & penalties
- Chapter IX – Specific processing situations
- Chapter X – Delegated Acts and implementing acts
- Chapter XI – Final provisions

\*

# Highlights of some GDPR ‘Game changers’

While the GDPR strengthens existing data protection laws, it also introduces a number of new requirements which will have significant legal, process, and technology implications for organizations.

## Data Processors

For the first time, GDPR places direct statutory obligations on data processors. (Ventiv is both a data controller & a processor).

## Record Keeping

Extensive record keeping required detailing: processing activities, transfers, data mapping, legal basis for consent.

## Breach notifications

GDPR now mandates that data controllers notify the supervisory authority without undue delay and, where feasible, not later than 72 hours after having become aware of a data breach.

## Right to erasure

Data subjects (employees and customers) now have the power to request the deletion or removal of their personal data, including from backups, archived data and from third parties (e.g., cloud storage).

## Accountability Principle

**ACCOUNTABILITY** : The GDPR introduces an accountability principle which requires organizations to demonstrate compliance.

## Data Retention

Organizations can no longer hold onto personal data indefinitely. Once the initial purpose of processing has been completed, organizations will need to come up with a new legal basis for holding the data or delete it.

## Penalties

The GDPR allows for both administrative sanctions & financial penalties for non-compliance.

Two tiers of penalties:

- \$10M Euros or 2% of global gross turnover (prior year) whichever is greater
- \$20M Euros or 4% of global gross turnover (prior year) whichever is greater

## Privacy by design/Default

Privacy-by-design/default means organizations need to incorporate GDPR requirements in data collection/processing processes (considerations include data minimization, encryption, pseudonymisation) and new tech e.g., IoT, digital platforms etc. “State of the art”.

## Data Protection Officer

Appointment of a DPO in certain circumstances:

- Public authorities
- Large scale processing/profiling of EU subjects
- Processing of special categories/sensitive data.



# KEY CHANGES BETWEEN DPD AND GDPR

- Material and Territorial Scope Increase
  - Definition of Personal Data (emerging data types (IoT, Biometrics, genetics, geo-location)
  - Applies to entities outside of the EU as well
  - Consent – higher threshold for establishing as a legal basis
- Organizations outside of the EU will have to designate a “local” representative in writing
  - What happens to Ventiv when the UK leaves the union??
- Transborder data flows outside of the EU will have to have a legal basis in place for protecting the data
  - Adequacy decision in place
    - U.S under Data Privacy Shield
  - Binding Corporate rules
- Appointment of a Data Protection Officer (DPO)
  - Large Scale systematic processing/profiling of EU subjects
  - Processing of special categories of data (health, genetics, race, sexual orientation, ethnicity, trade union membership)
  - Must be independent and report to the “highest level of mgmt.”
    - Access to the board
- Companies can no longer keep data “forever”
  - When the initial purpose is fulfilled...
  - State retention periods up front
- Data Privacy by Design and Default
  - Encryption
  - Pseudonymisation
  - Anonymization
- State of the Art
- Increased Data Subject Rights
  - Access, Data Portability, Rectification, objection to processing, Right to be forgotten/Erasure
  - Eligible for both material and non-material damages
  - Joint and several liability to ensure effective compensation
- Data Breach Notification
  - 72 hrs. to notify Supervisory Authority
- Enforcement
  - One stop shop
  - Fines for serious violations
  - Article 29 Working Party, EDPB
- Accountability Principle
  - Explicit obligations on controller & processor to demonstrate compliance with GDPR
    - DPO
    - PIA
    - Record Keeping

# KEY DEFINITIONS

- **Personal Data:** 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.
- **Data Controller:** the natural or legal person, public authority, agency or any other body which alone or jointly with others determines the purposes and means of the processing of personal data; where the purposes and means of processing are determined by EU or Member State laws, the controller may be designated by those laws
- **Data Breach:** a breach of security leading to the accidental or unlawful destruction, loss (loss of access to), alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- **Data Processor:** A natural or legal person, public authority, agency or any other body which processes personal data on behalf of the controller
- **Supervisory Authority (Data Protection Authority):** Independent public authority which is established by each member state (Art. 51)
- **Consent:** "The data subject's consent" means 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.
- **Special Category Consent:** Explicit consent
- **Supervisory Authority (DPA):** Monitors, administers, consults, and enforces GDPR



# PERSONAL DATA (ARTICLE 4)

Broad definition – allows for future-proofing the regulation as technology evolves

- "Personal data" means 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 identifier such as a name, an identification number, location data, online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that person.



# RECORD KEEPING – DEMONSTRATING COMPLIANCE (ARTICLE 30)

52 out of the 99 articles require evidence to demonstrate compliance with the GDPR

- The name and contact details of the controller and where applicable, the data protection officer
- The purposes of the processing
- A description of the 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 including recipients in third countries or international organizations
- The transfers of personal data to a third country or an international organization, including the documentation of suitable safeguards
- Consent
- Data Mapping
- The envisaged time limits for erasure of the different categories of data
- A general description of the applied technical and organizational security measures
- Data Retention periods
- Data Subject Requests (SARs, rectification, objections, transfer)
  - Privacy/Fairness statement acknowledgement
  - Opt-in/out
- Legal basis for processing
- Privacy Notices
- Consent tracking
- DPIA(s)
- RISK Assessment
- Data Breach
- Vendor Assessments

# DATA MAPPING

## Scoping

- "staging the map" – prepare a project plan and the necessary tools and materials bespoke to your needs
- questionnaires/templates/guidance documents

## Information Collection

- via questionnaires/interviews collect all required information in order to generate a record of processing
- Consider internal and external resource required for this phase

## Information Analysis & Mapping

- based on the information collected and your specific needs, produce data flow maps and analysis to best record and visualise your organization's data processing activities
- \* we mapped employee data to over 49 different systems (CRM, expense, email, etc...)

# DATA MAPPING & INVENTORY

Application	Hosted	Ventiv	Type of Data	Administrator	Business Owner
Concur	X		E		
American Express	X		E		
Radius	X		E		
ADP	X		E		
Aetna	X		E		
Merrill Lynch	X		E		
WageWorks	X		E		
Office365	X		EC		
Skype/Teams	X		EC		
Employee Mailboxes		X	EC		
Microsoft Docs		X	EC		
Webex	X		EC		
Zoho	X		EC		
Avalara	X				
Slack	X		E		
Ventiv University	X		EC		
VoIP (Nextive)	X		E		
RFPIO	X		EC		
Netsuite	X		EC		
GreenHouse	X		E		
Careerbuilder Employment Background					
Site24X7	X		E		
Fileshares		X	EC		
Engage		X	EC		
Jira		X	EC		
Lexis Nexis	X		C		
HubSpot	X		EC		
BedRock	X		C		
MoveIT		X	EC		
RiskConsole		X	EC		
IVOS		X	EC		
Good		X	E		
Runbook		X	E		
Infrastructure					
Domain Controllers		X	E		
AWS Domain Controllers	X		E		
Firewall logs		X	EC		
System Logs		X	EC		
Splunk		X	EC		
Facebook			EC		
LinkedIn			EC		
Confluence		X	EC		
SmartSheet	X		EC		
Vineo	X		E		
Mitchell	X		EC		
qTest	X		E		
SauceLabs	X		N/A		

Application	Vendor	Hosted	Ventiv	Type of Data	GDPR Compliant contract in place	Business Owner	ISO27001	SOC	other	Data Stored	Data Access locations	DPO	Contact Info
Concur		X		E									
American Express		X		E									
Radius		X		E									
ADP		X		E									
Aetna		X		E									
Merrill Lynch		X		E									
WageWorks		X		E									
Office365		X		EC									
Skype/Teams		X		EC									
Webex		X		EC									
Zoho		X		EC									
Avalara		X											
Slack		X		E									
Ventiv University		X		EC									
VoIP (Nextive)		X		E									
RFPIO		X		EC									
Netsuite		X		EC									
GreenHouse		X		E									
Careerbuilder Employment Background		X											
Site24X7		X		E									
Lexis Nexis		X		C									
HubSpot		X		EC									
BedRock		X		C									
Facebook		X		EC									
LinkedIn		X		EC									
SmartSheet		X		EC									
Vineo		X		E									
Mitchell		X		EC									
qTest		X		E									
SauceLabs		X		N/A									



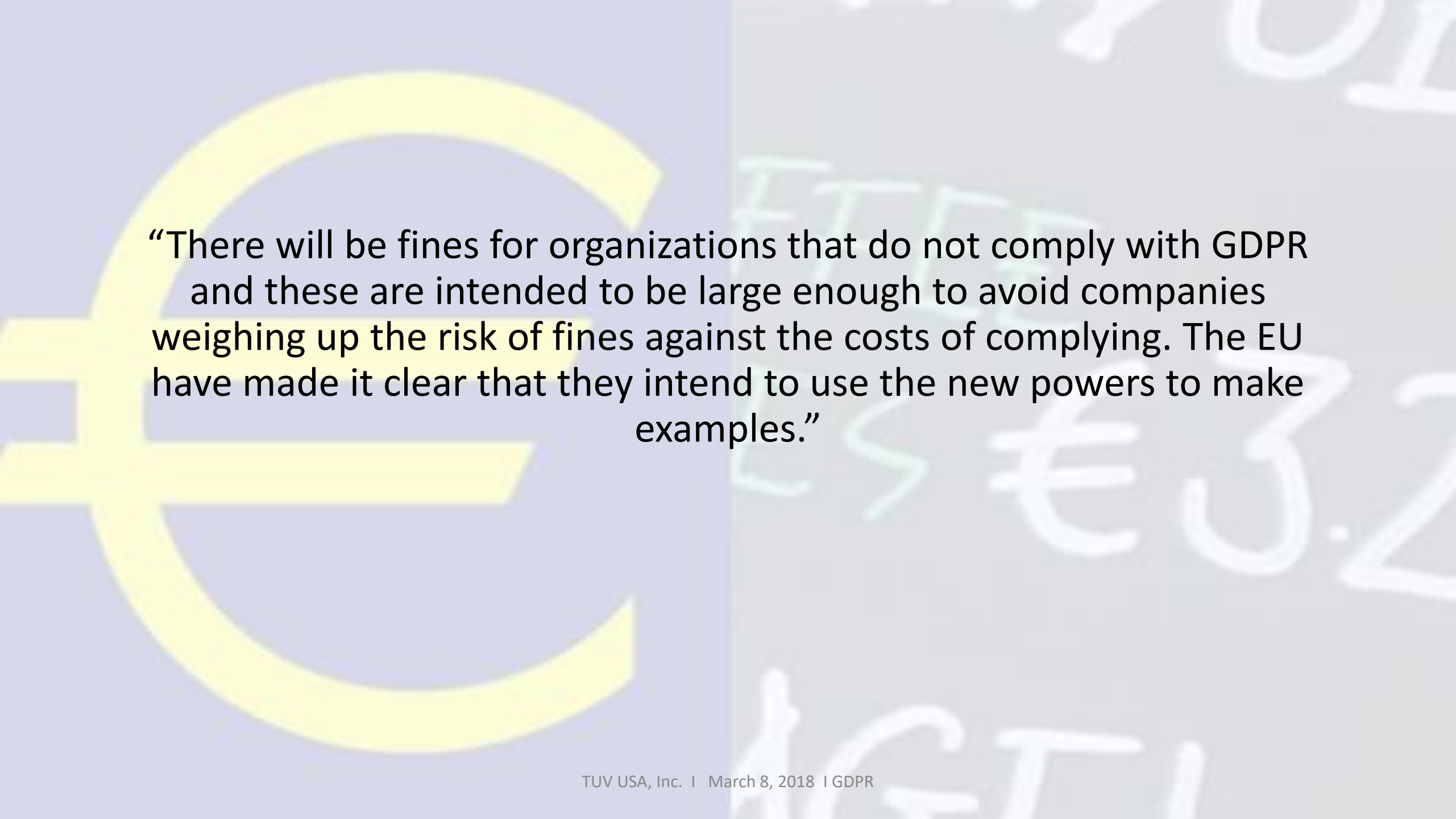
# DATA BREACH REQUIREMENTS – ART. 33

- Data Breach: a breach of security leading to the accidental or unlawful destruction, loss (loss of access to), alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise processed
- Supervisory authority must be notified without undue delay or within 72 hours of becoming aware of the breach:
  - Where this cannot be achieved within 72 hours, an explanation of the reasons for the delay should accompany the notification and information may be provided in phases without undue further delay
- The notification:
  - Describe the nature of the breach
    - Scope of the breach
    - Mitigating factors
  - Communicate the name and contact details of the Data Protection Officer or designated contact
  - Data subjects must be notified “without undue delay,”
- Unless there is controller can demonstrate that the risk is low
- \*Updated guidance released Feb 2018 – WP250rev.01
  - Review what a breach is! Breaches could include:
    - Availability impacts
    - Sending an email to the wrong person
    - Unauthorized access

# DATA PROTECTION AUTHORITIES

Overall, DPAs are very active and enforcement actions are on the increase

- Microsoft's Windows 10 breaches data protection law, say Dutch regulator - <http://www.zdnet.com/article/microsofts-windows-10-breaches-data-protection-law-say-dutch-regulator/>
- ICO fines and enforcement actions increase as GDPR approaches: fines up over 100% and enforcement actions up 155%
- ICO fines would be 79 times higher under GDPR



“There will be fines for organizations that do not comply with GDPR and these are intended to be large enough to avoid companies weighing up the risk of fines against the costs of complying. The EU have made it clear that they intend to use the new powers to make examples.”

# Enforcement

## Administrative Fines

- You don't have to have a data breach to be subject to administrative action & fines
- Fines will be **effective, proportionate, and dissuasive**
- Supervisory authorities will have the power to impose these sanctions from where the data subject habitually resides **or** in the territory that the breach occurs. These changes will significantly increase the risk associated with privacy non-compliance
- Controllers and Processors are liable for statutory fines
- Two Tiers Administrative Fines
  - \$10M or 2% of total worldwide turnover of the preceding financial year
  - \$20M or 4% of total worldwide turnover of the preceding financial year
- Fines administered will take into account technical and organizational measures implemented
  - Technical: Encryption, Anonymization, how they have been applied
  - Organizational: Data Protection Governance, Structure, Training & Awareness, Segregation of Duties





# CERTIFICATIONS AND CODES OF CONDUCT

- Privacy Framework
  - Establish a framework that allows us to meet the requirements of the GDPR but is also “flexible” enough to meet other regulatory requirements as they come out
- Certifications: Establishes a documented baseline of security practices & controls
  - ISO27001:2013
  - ISO27018
  - SOC1 Type2

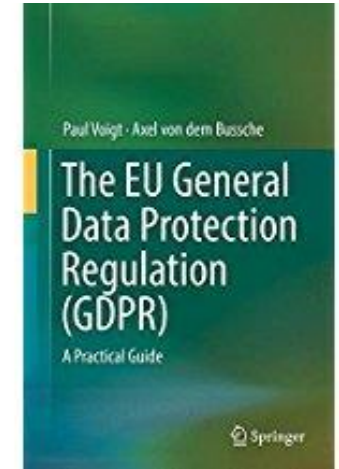
# PRIVACY LAWS

Additional considerations businesses need to keep in mind

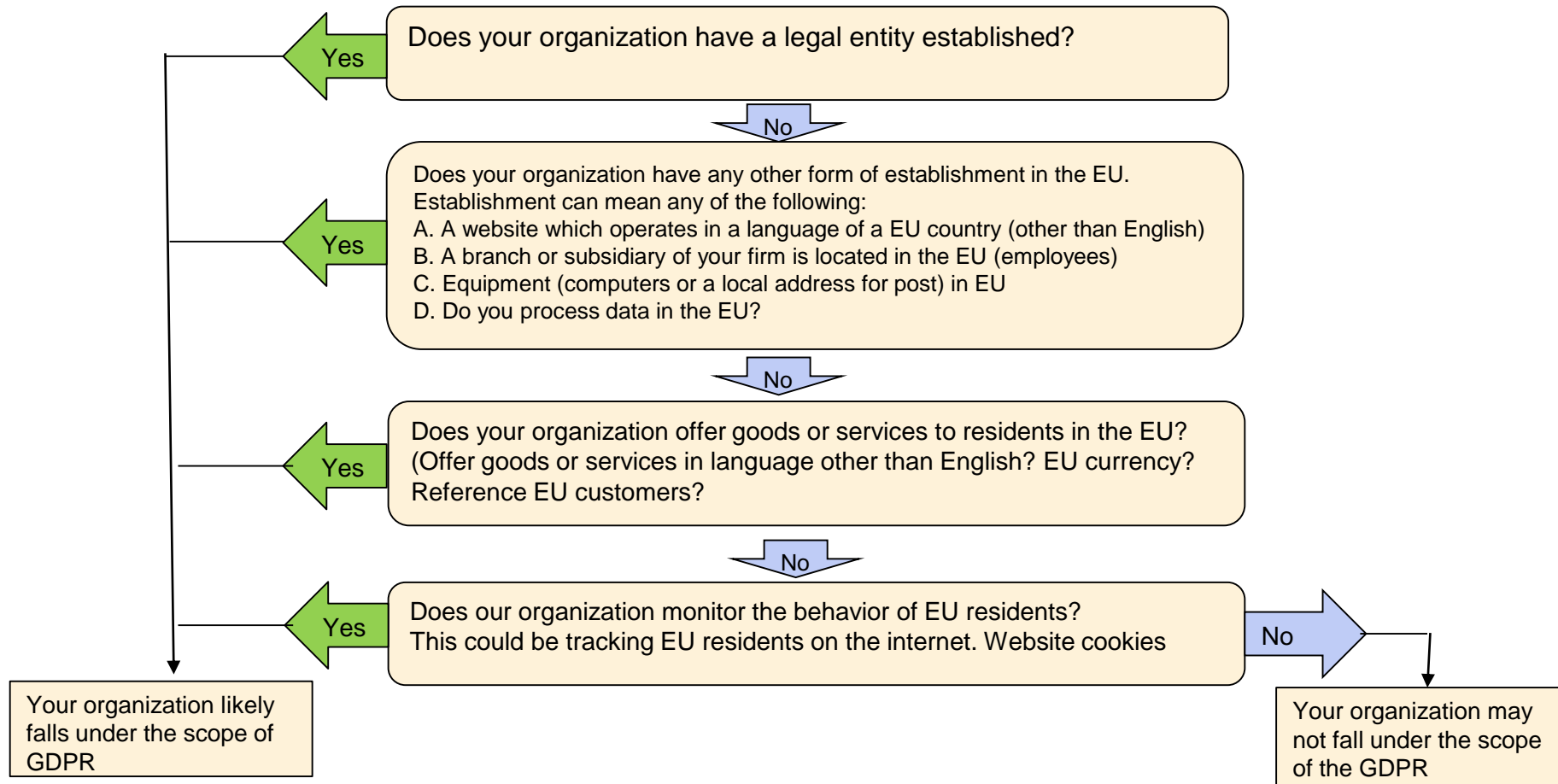
- While GDPR “harmonized” privacy regulations across Europe, companies still need to monitor individual member state law
  - German DPAs, France CNIL, U.K ICO)
- E.U ePrivacy law
- Schremms SCC challenge
- Other Geographies will be implementing GDPR-like regulations
  - Asia (APEC, South Africa, India, Canada, Jamaica)
- Russia, China...
- U.S state & FTC enforcement of “privacy” laws
  - FTC consent decrees

# RESOURCES

- [https://ec.europa.eu/commission/index\\_en](https://ec.europa.eu/commission/index_en)
- [http://ec.europa.eu/newsroom/article29/news.cfm?item\\_type=1308](http://ec.europa.eu/newsroom/article29/news.cfm?item_type=1308) (WP29)
- [http://ec.europa.eu/newsroom/article29/item-detail.cfm?item\\_id=612080](http://ec.europa.eu/newsroom/article29/item-detail.cfm?item_id=612080) (list of European data protection authorities)
  - ICO, CNIL, Germany
- [www.iapp.org](http://www.iapp.org)
- <https://www.dpnetwork.org.uk/>
- The EU General Data Protection Regulation (GDPR): A Practical Guide 1st ed. 2017 Edition
- European Data Protection (Print Copy) – IAPP website



# Does the GDPR apply to us?



# THANK YOU CONTACT US



## **TUV USA Team**

TUV USA Academy

[www.tuv-usa.com](http://www.tuv-usa.com)

**Email:** [academy-us@tuv-nord.com](mailto:academy-us@tuv-nord.com)

**Phone:** 844-488-8872

**Twitter:** @TUV\_USA

**LinkedIn:** TUV USA, Inc.

[www.linkedin.com/company-beta/3812830](http://www.linkedin.com/company-beta/3812830)



## **Scott Wilson**

Chief Security & Privacy Officer **Ventiv Technology Inc.**

**Email:** [scott.Wilson@ventivtech.com](mailto:scott.Wilson@ventivtech.com)

**Phone:** +1.770.308.5499

**LinkedIn:** Scott Wilson

[www.linkedin.com/in/scottRichardwilson](http://www.linkedin.com/in/scottRichardwilson)