

# Countdown to GDPR

Impact on the Security Ecosystem and How to Prepare



**Susan Kohn Ross, Esq.**  
**Mitchell Silberberg & Knupp LLP**



**Jasvir Gill**  
**Alert Enterprise**



**Lora Wilson**  
**Axis Communications**

## Affected Countries

Austria, Belgium, Bulgaria, Croatia, Cyprus, Czech Republic, Denmark, Estonia, Finland, France, Germany, Greece, Hungary, Iceland, Ireland, Italy, Latvia, Lichtenstein, Lithuania, Luxembourg, Malta, Netherlands, Norway, Poland, Portugal, Romania, Slovakia, Slovenia, Spain, Sweden, and United Kingdom.

## GDPR Article 4.1

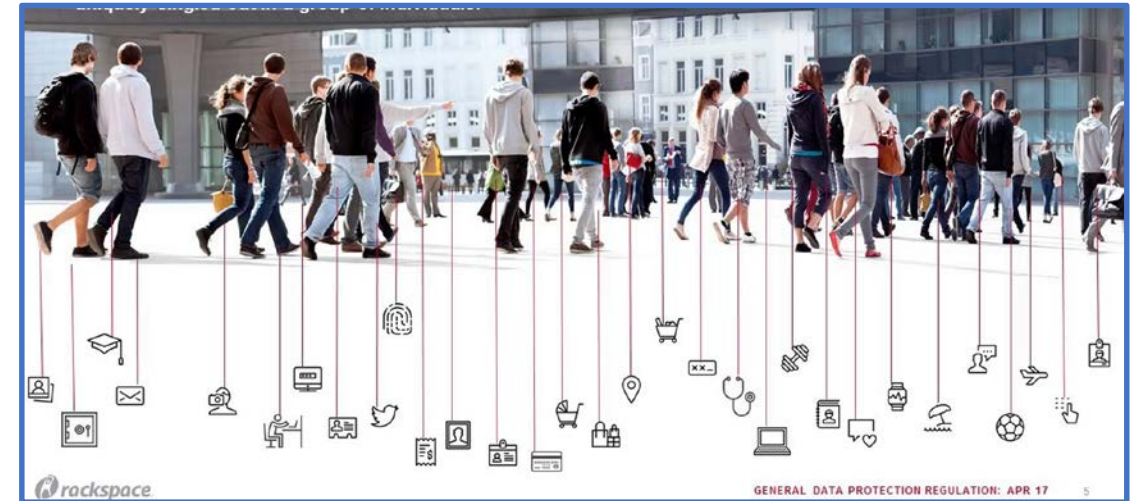
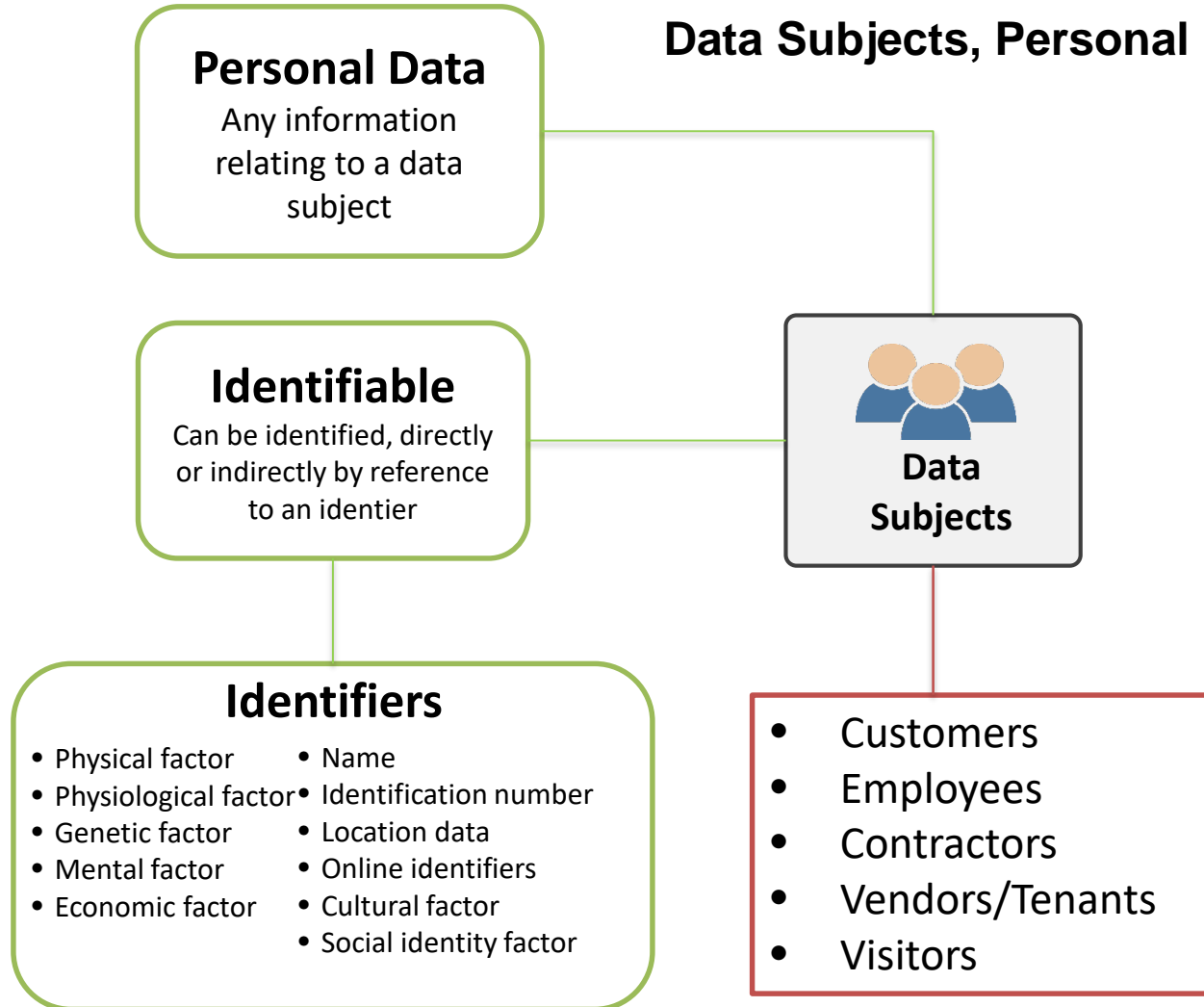
“Personal data” means any information relating to an identified or identifiable natural person (‘data subject’); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person ...

## GDPR Article 3.2

This Regulation applies to the processing of personal data of data subjects who are in the Union by a controller or processor not established in the Union, where the processing activities are related to:

- (a) the offering of goods or services, irrespective of whether a payment of the data subject is required, to such data subjects in the Union; or
- (b) the monitoring of their behavior as far as their behavior takes place within the Union.

## Data Subjects, Personal Identifiable Information (PII) is broad under GDPR



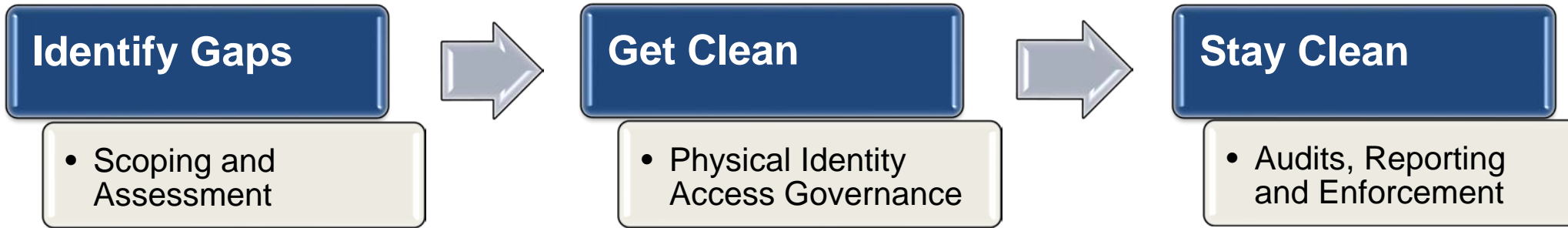
## What Organizations must do to comply with GDPR

- Organizations are responsible for complying with **Data Subjects Rights** for all PII data collection, lawfulness of processing and retention
  - ✓ Privacy by Design (classifications and segregation of PII)
  - ✓ Audits and Reports of PII data management through Personal Data Register
  - ✓ Security (pseudonymisation, encryption, minimization)
  - ✓ Consent & Transparency ( clear, concise, intelligible and easy accessible)
  - ✓ Monitoring and responding to changes in compliance mandates
  - ✓ Managing and governing Data Processors and Third-Party interaction relative to the processing and handling of PII.
  - ✓ Notifying Supervisory Authorities of data breaches within 72 hours of breach discovery





## Most effective approach to GDPR (lessons from past/serious regulations like SOX)



### Identify Gaps

- Scoping and Assessment

- Engage the Organization's GDPR Readiness Committee
- Establish, inventory Identities (employees, contractors, vendors, tenants, visitors, etc.; and their access rights)
- Identify PII data touch points (what, where, why, how long, etc.)
- Understand PII data processing activities and consent management
- Assess the risk with PII data processing and access activities
- Establish consent, record keeping, retention policies and procedures in according to GDPR

### Get Clean

- Physical Identity Access Governance

- Clean up of existing data
- Establish and harmonize consolidated Identity and Data Registry
- Identification and detection of data propagation policies
- Capturing consent for existing data sets
- Documenting reasoning and auditing
- Provide mean for data corrections / removal

### Stay Clean

- Audits, Reporting and Enforcement

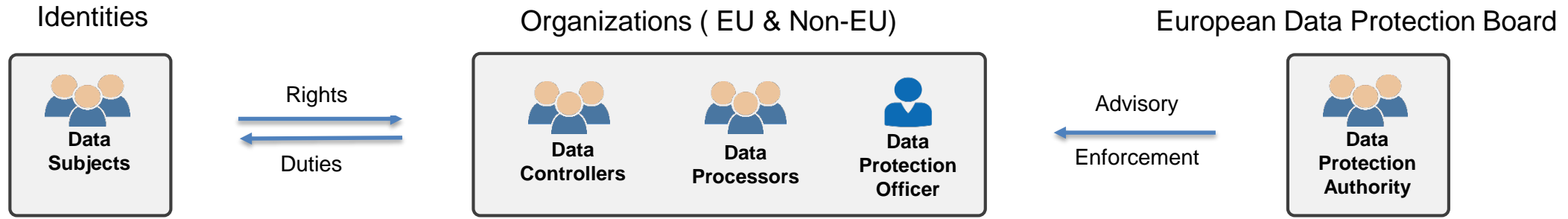
- Capturing Consent from end users up front
- Providing transparency and reasoning to end users
- Means to submit data erasure/correction/portability requests
- Enhanced segregated data views and PII protection protocols
- Periodic and event based access review and re-certification audits
- Dashboard and Reporting to show compliance posture



## GDPR Solution Set (Think Active Policy Enforcement – Continuous Compliance)

- Provide an easy automated way to report EU personnel data storage outside of EU servers,
- Provide a mechanism for Data Protection officer to review and reaffirm current Data state
- Provide mechanism for End users to consent on Data Storage and renew it on regular basis
- Provide features to End users to review their profile information across the servers and update
- Encrypt PII information wherever possible (decrypted information should be readily available during emergencies)
- Due to business reason, even if data is stored for employees/contractors outside EU, provide a strong mechanism so that no one except for EU personnel can view it
- Provide a mechanism for Visitors to sign consent to store PII during the visit, need to delete visitor information once the visit is over

## Leverage NIST validated approach to Converged Security & Compliance to GDPR



- Role Based Access Governance
- Data Subjects Consent Management

- Audits & Reporting
- Data Breach Notification



### Employees

- New Hire
- Transfer
- Termination



### Non-Employees


- New Contract
- Change Contract
- Contract Expiration



## Get Clean, Stay Clean – real life example from Fortune 100 customers

**Review Access Information** Review Access Information Notes (0) Attachments (0)

---





**SID** BRAD.PITT  
**First Name** Pitt  
**Last Name** Brad  
**Manager SID** V480956

---

Modify Enterprise Access

---

Search  [Advanced Search](#)

Access Name	
<input checked="" type="checkbox"/> 	<b>HQ LOBBY_EA</b> ⓘ <b>Valid From:</b> 2018/01/22 13:19:36 <b>Valid To:</b> 2099/12/31 23:59:59
<input checked="" type="checkbox"/> 	<b>LFC MARKETING TEAM_EA</b> ⓘ <b>Valid From:</b> 2018/01/22 13:54:02 <b>Valid To:</b> 2099/12/31 23:59:59

- Ability to review current propagation of identity and access data
- Reasoning for data propagation
- Means to submit removal as needed
- Fully workflow driven to seek approval prior to committing changes

# Leverage core framework + GDPR Content Pack

## EU Users

- Sign the Consent Form
- Review Profile resides outside country and request for deletion
- Review Personal information and request for a change (if necessary)
- End Users can only search Identities within their Region

## Data hiding, encryption

- HR ID is hidden, unique ID is created for each HR ID
- Photos are watermarked
- Other PII Data is encrypted
- Minimum data sent to the downstream system

## Data Protection Officer

- Automated reporting on EU profiles resides outside EU server and no consent signed
- Report/Dashboard of all Consent signed/not signed
- Start a Review Process for Managers/Supervisors to justify profile resides outside EU but no consent signed

## Administration and Reporting

- Segregated Administration – Administrators can see requests/profiles and take actions within their region
- Audit Reports show data within the region of logged in User



## GDPR Compliance is Critical

- Commitment to safeguarding individuals' integrity and privacy
- Ability for individuals to control their own data is in direct alignment with company core values
- GDPR will help ensure we continue to operate with full transparency and respect for individual integrity, holding ourselves accountable to a formalized set of guidelines

## Preparation

- Formal Project Team
- Governance Committee
- Inventory
  - Data we own and process
  - How we gain consent
  - How we store and manage data
- Centralized systems with proper controls in place
  - Right to be forgotten
- ROPA
- DPA
- Become *and remain* compliant!





EU General Data  
Protection Regulation  
**25 May 2018**



## Contact

Susan Kohn Ross, Esq.  
Mitchell Silberberg & Knupp LLP  
Los Angeles, CA  
[skr@msk.com](mailto:skr@msk.com) | [www.msk.com](http://www.msk.com)  
(310) 312-3206

Lora Wilson  
Director of Marketing, North America  
Axis Communications, Inc.  
Chelmsford, MA  
[lora.wilson@axis.com](mailto:lora.wilson@axis.com)  
(978) 614-2073

Jasvir Gill  
CEO  
Alert Enterprise  
Fremont, CA  
[jasvir@alertenterprise.com](mailto:jasvir@alertenterprise.com)  
(510) 440-0840

Jake Parker  
Director of Government Relations  
Security Industry Association  
Silver Spring, MD  
[jparker@securityindustry.org](mailto:jparker@securityindustry.org)  
301-804-4700