Opportunities and Challenges from the Implementation of the GDPR
Procedures, Procedures and Policies

Dr. Neil Patrick. Director COE GRC & Security, EMEA South
7th February 2018

CUSTOMER

SAP Run Simple

Legal Disclaimer

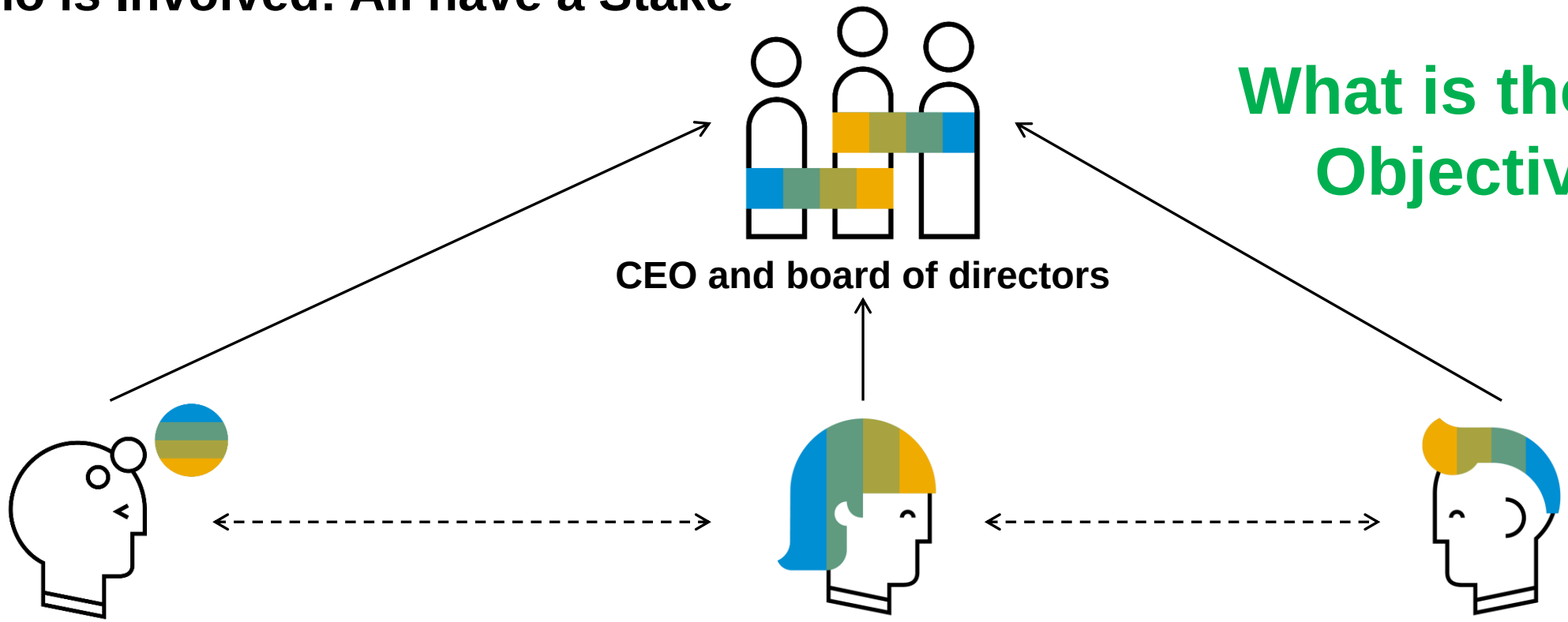
The information in this presentation is confidential and proprietary to SAP and may not be disclosed without the permission of SAP. This presentation is not subject to your license agreement or any other service or subscription agreement with SAP. SAP has no obligation to pursue any course of business outlined in this document or any related presentation, or to develop or release any functionality mentioned therein. This document, or any related presentation and SAP's strategy and possible future developments, products and/or platforms directions and functionality are all subject to change and may be changed by SAP at any time for any reason without notice. The information on this document is not a commitment, promise or legal obligation to deliver any material, code or functionality. This document is provided without a warranty of any kind, either express or implied, including but not limited to, the implied warranties of merchantability, fitness for a particular purpose, or noninfringement. This document is for informational purposes and may not be incorporated into a contract. SAP assumes no responsibility for errors or omissions in this document, and shall have no liability for damages of any kind including without limitation direct, special, indirect, or consequential damages that may result from the use of this document. This limitation shall not apply in cases of intent or gross negligence.

All forward-looking statements are subject to various risks and uncertainties that could cause actual results to differ materially from expectations. Readers are cautioned not to place undue reliance on these forward-looking statements, which speak only as of their dates, and they should not be relied upon in making purchasing decisions.

NOTE: The information contained in this presentation is for general guidance only and provided on the understanding that SAP is not herein engaged in rendering legal advice. As such, it should not be used as a substitute for legal consultation. SAP SE accepts no liability for any actions taken as response hereto.
It is the customer's responsibility to adopt measures that the customer deems appropriate to achieve Data Privacy compliance.

What I’m Hearing

Who is Involved: All have a Stake



What is the end Objective?

Legal

- **Data protection officer**
- Chief compliance officer
- Chief risk officer
- Head of legal
- Chief audit executive

Line of Business

- HR
- O2C
- P2P
- Business process owners

IT Operations

- Chief information officer
- Chief information security officer

GDPR Accountability – Fundamental to GDPR and 'New' Requirement

Article 5 lists the 6 principles for processing of personal data:

a. lawful, fairness & transparency
b. purpose limitation
c. data minimisation
d. accuracy
e. storage limitation
f. integrity & confidentiality

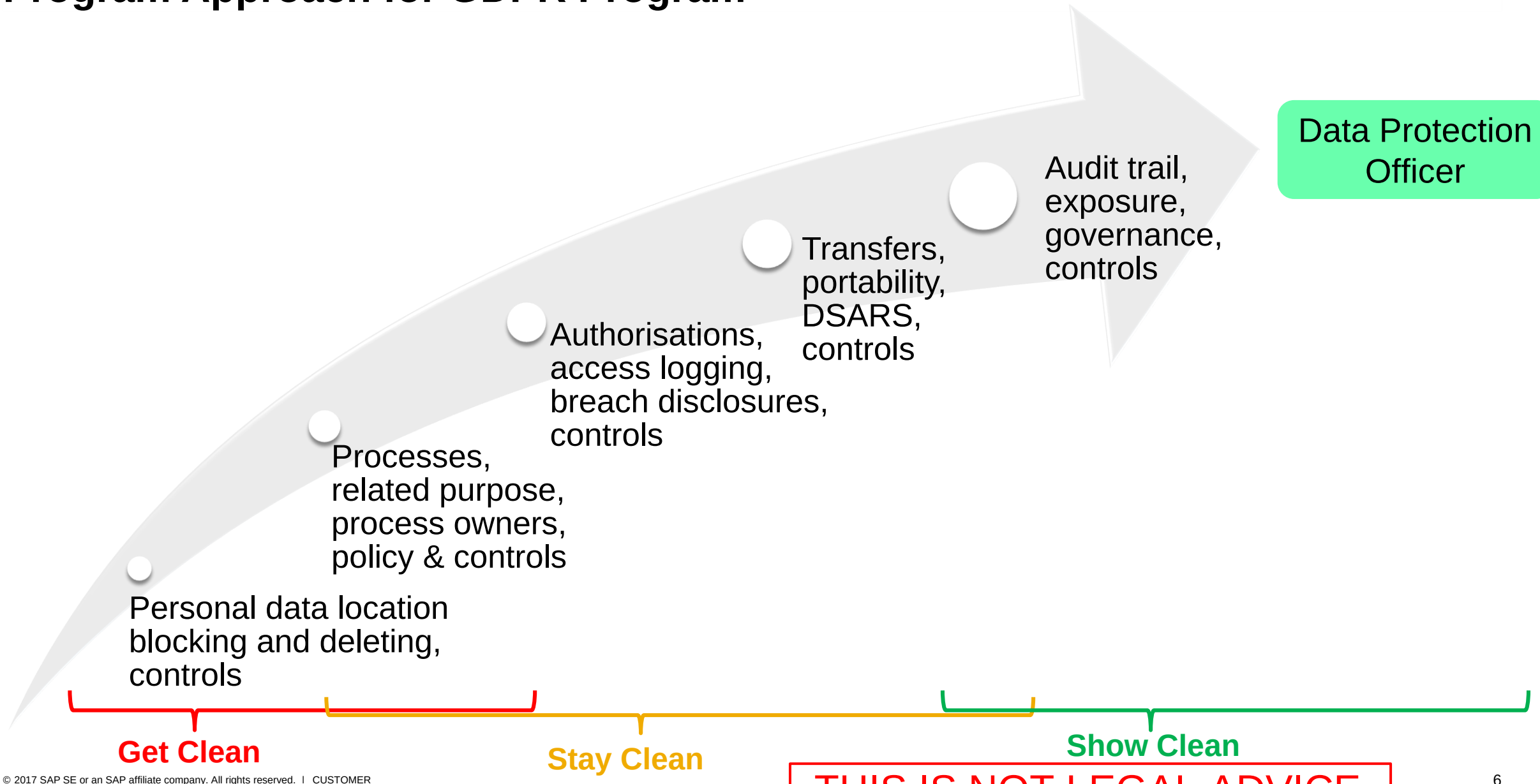
The controller shall be responsible for, and be able to demonstrate compliance with, paragraph 1 ('accountability')

ICO comment on addition of GDPR from DPA:

The most significant addition is the accountability principle. The GDPR requires you to show ***how*** you comply with the principles – for example ***documenting the decisions*** you take about ***processing*** activity.

THIS IS NOT LEGAL ADVICE

Program Approach for GDPR Program

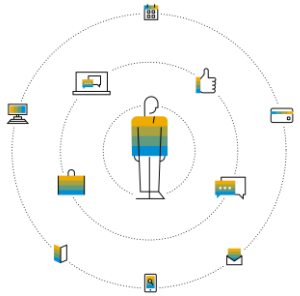


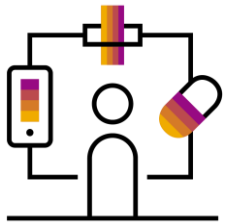
THIS IS NOT LEGAL ADVICE

3-Tier Requirements – Enables a Risk-based Approach

DPO, Board

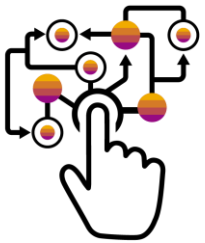
1. lawful, fairness & transparency
2. purpose limitation
3. data minimisation
4. accuracy
5. storage limitation
6. integrity & confidentiality



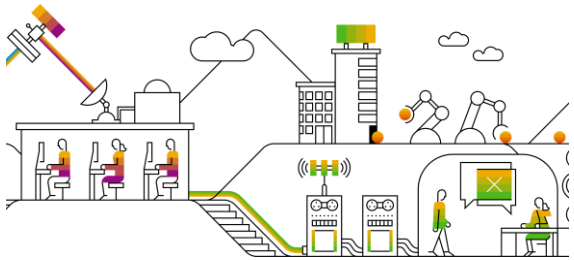


Demonstrate compliance with paragraph 1 ('accountability')

Audit, Governance



Security & availability of processing activities



Documented records of processing activities

IT, Operations

On-prem, all instances

Hybrid & Cloud, all instances

Paper, file stores, all instances

Legal Compliance: Show Clean

- Accountability
- Governance objectives vs actuals, manage by exception
- By design and by default linked to Process Governance

Process Governance: Stay Clean

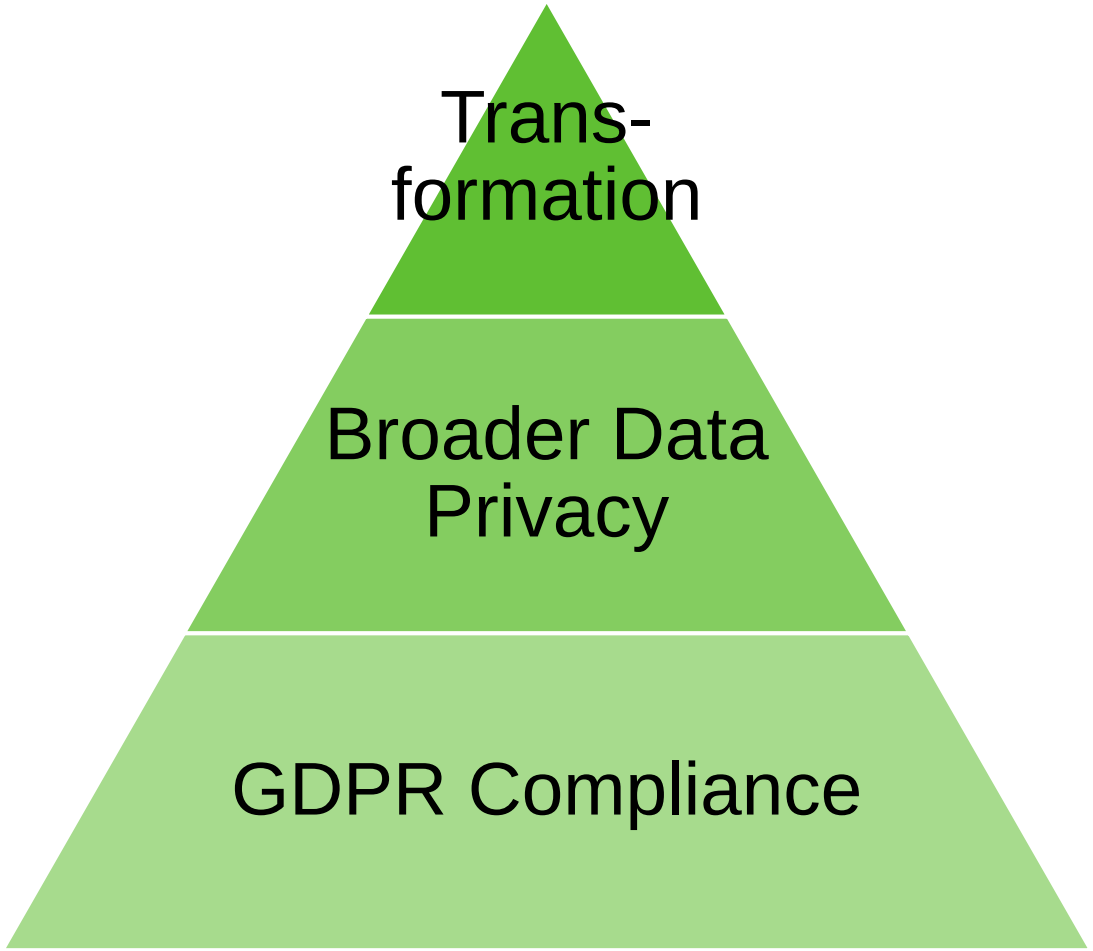
- Process & purpose register, DPIA's
- Policies and procedures, controls
- LOB process owners & approvals
- Breach handling (for example)
- Linked to Technical Tools

Technical Tools: Get Clean

- Personal data location, type
- Consent & Retention
- Blocking, Deletion
- Encryption, Pseudonymisation
- User authorisations, access alerts

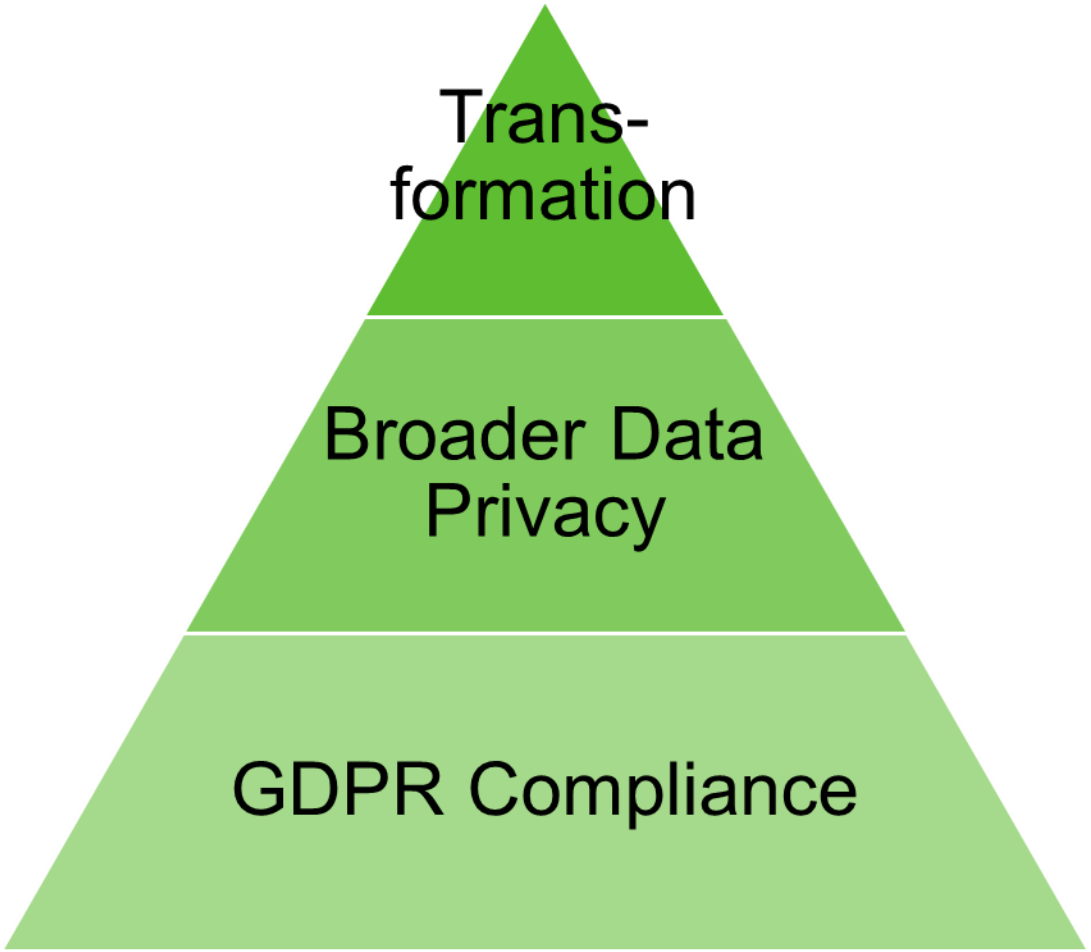
THIS IS NOT LEGAL ADVICE

What is the End Objective?



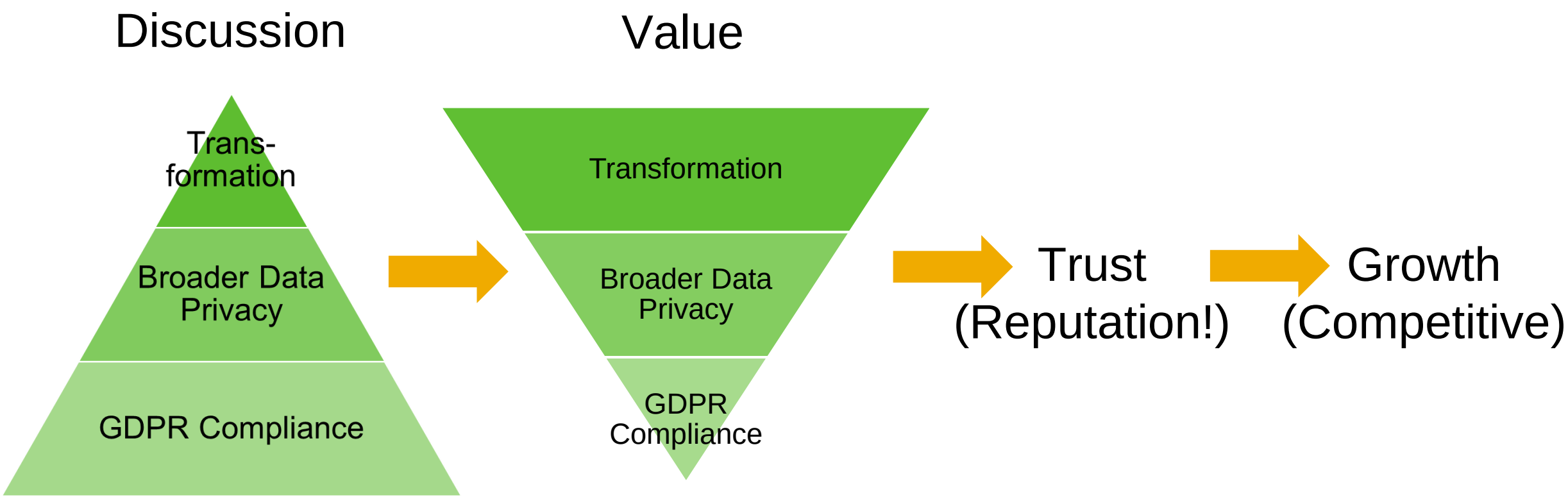
THIS IS NOT LEGAL ADVICE

What is the End Objective?



THIS IS NOT LEGAL ADVICE

What is the End Objective?



THIS IS NOT LEGAL ADVICE

Thank you.

Contact information:

Dr. Neil Patrick
Director GRC & Security, Centre of Excellence, EMEA South
neil.patrick@sap.com
+44 7833 480 248