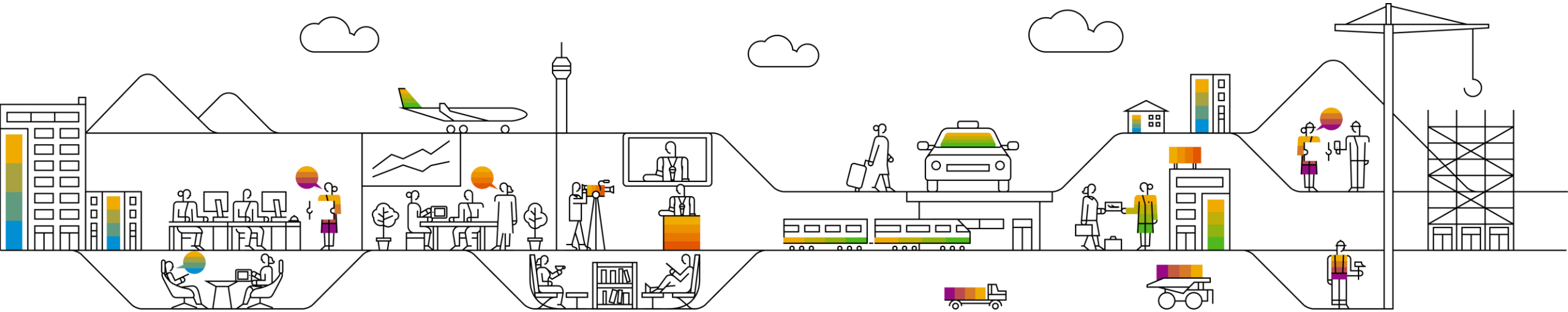
GDPR (General Data Protection Regulation)

Les Smith: 23rd August, 2018

Time: 1325-1405



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.

Agenda

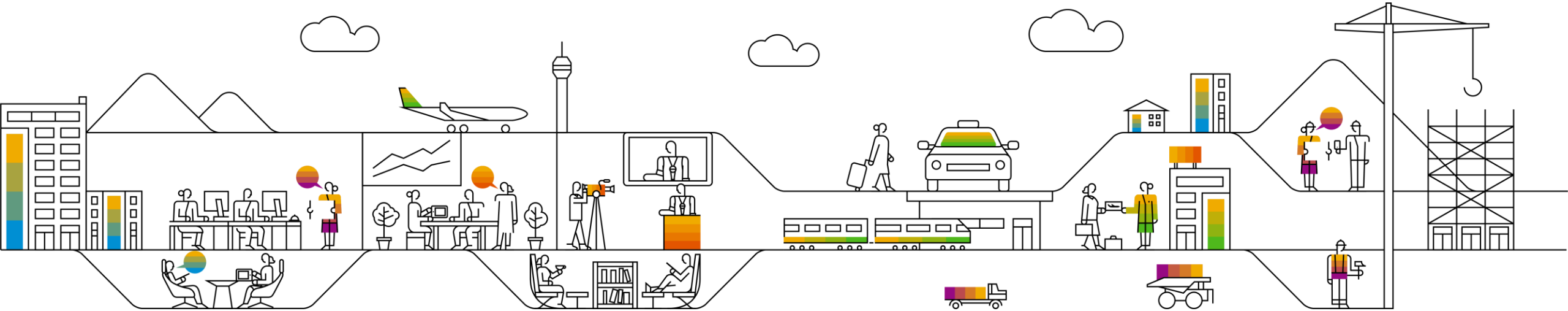
Why is it different and why does it matter?

What's the business impact?

How do we talk about it?

What are our new capabilities, and what's coming?

Where can I get more info?



Why is it different and why does it matter?

One of the most far reaching pieces of regulation, ever

What is the General Data Protection Regulation?

The General Data Protection Regulation (GDPR) (EU Regulation 2016/679), effective May 25, 2018, gives **individuals control** and **protection** of their **personal data**. Data **controllers**, who determine the purpose and means of processing personal data, and **processors**, who process for controllers, are affected.

Penalties up to 4% of annual global revenue or **€20 million** whichever is greater

Who must comply?

Organizations that offer goods or services to, or monitor the behavior of, EU data subjects and those that process or hold the personal data of EU residents

Applies to:

Natural persons, whatever their nationality or place of **residence** in the EU, in relation to the processing of their personal data

What the GDPR adds

Protects fundamental rights related to the processing of personal data

Demonstration of compliance

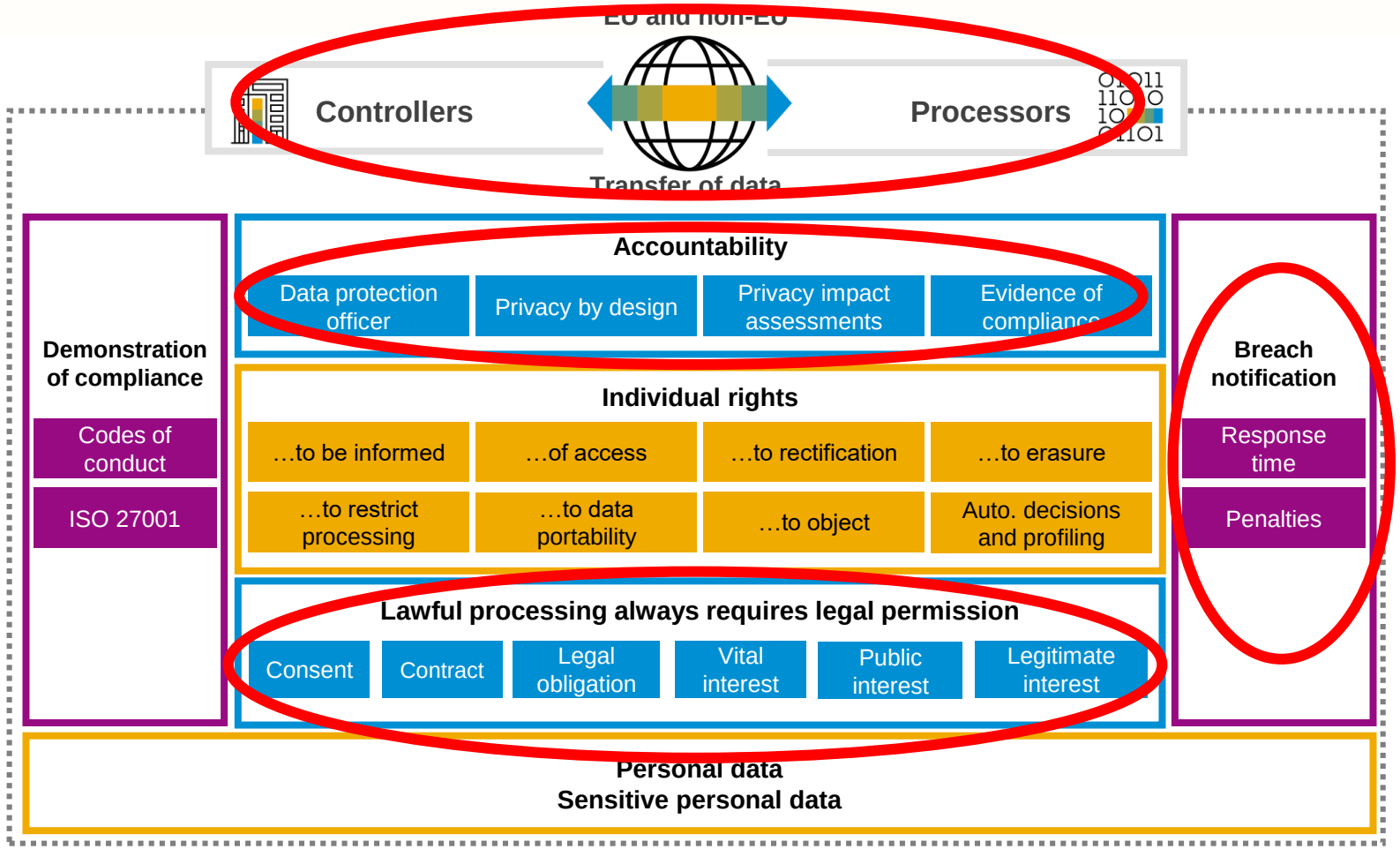
- Compliance and accountability are integral to a data protection program.
- Codes of conduct and policies can help ensure accountability.

Accountability

- Produce and maintain evidence of compliance-supporting actions
- Build data protection into product design and development
- Appoint a data protection officer (DPO) if your company has large-scale processing requirements

Lawful processing

- Requires a legal basis, e.g. a contract, consent, or legitimate interest for the processing of personal data
- Must keep such data accurate and stored only as long as needed



Personal data

- Includes online identifiers, mobile device IDs, IP addresses, and more; may include de-personalized data
- Requires parental consent for children under 16 years

Controllers and processors

- Non-EU data controllers and processors must also comply when processing data of EU individuals.
- Controller is accountable for failures of the data processor; both controller and processor are liable for breaches.

Breach notification

- Mandatory notification to authority within 72 hours of becoming aware of breach
- Communication to affected individuals without undue delay
- Maximum fine can apply

Individual rights

- The GDPR suggests self-service apps for personal data-related information requests
- Rights apply across all systems, including those of third parties.
- Businesses generally cannot charge and must respond in <1 month.

What is GDPR Personal Data?

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;

Examples of Personal Data (this is not a legal definition)

- First Name or Initial, Last Name, Data of Birth
- Social Security number, Drivers License Data, Account numbers
- Email address (private and business)
- Tel/Fax number (private / business)
- Pictures where persons can be identified
- Personnel files, Merchandise and product order history
- GPS data
- Payment history, Income, Financial transaction information
- Military history
- Criminal charges, convictions & court records
- Internet Protocol (IP) addresses, Internet URLs
- CV / Employment history
- Body identifier (for example, tattoos, scars)
- Education records
- Descriptive consumer listings, customer relationships
- Credit reports and credit scores, purchases
- Loan or deposit balances
- Voting history
- Biometrics include fingerprints, iris, voiceprint
- Health include medications, organ donations, health history

Sensitive Personal Data types

- Racial or ethnic origin
- Political opinions
- Religious or philosophical beliefs
- Trade-union membership
- Health or sex life
- Genetic data and biometric data (for identification)

Some Key Definitions: Scope of Processing Personal Data

Data Breach:

"a breach of **security** leading to the accidental or unlawful destruction, loss, alteration, unauthorised disclosure of, or access to, personal data transmitted, stored or otherwise **processed**"

Processed:

"collection, recording, organising, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction"

The controller shall be responsible for, and be able to **demonstrate compliance**

Challenges

High costs of addressing and maintaining compliance

**Gartner predicts that by the end of 2018, more than 50%
of companies affected by the GDPR will not be in full compliance with the regulation.**

(Source: Gartner Says Organizations Are Unprepared for the 2018 EDPR, May 2017)

Increased workload and resources needed to meet and maintain compliance

"Of those noncompliant firms, 50% will intentionally not comply – meaning they have weighed the cost and risk and are taking a path that presents the best position for their firms."

(Source: Forrester Predicts 80% of Companies Will Fail to Comply with GDPR in 2019, Nov. 2017)

Complexity of processes and number of stakeholders involved

Under GDPR, not all data requires the same level of governance, with use cases defining the differentiation. This approach enables greater flexibility and agility in accessing data. It also increases the possibilities for as-yet-unknown uses of data – all while maintaining compliance with GDPR requirements.

(Source: Gartner blog: How GDPR Is an Opportunity to Create Business Value, Jan. 2018)

Business impact of losing customer trust and loyalty for noncompliance

Handled effectively, there is great potential to obtain consent to increase data access, use, and sharing rights – in line with the goals of a wider organizational data and analytics strategy. This can lead to competitive advantage, while helping to achieve compliance in other countries and regions.

(Source: Gartner blog. How GDPR Is an Opportunity to Create Business Value, Jan. 2018)

Some scenarios

A tourist from Auckland logs onto the website of their local Auckland grocery store from their hotel in the EU. They provide personal data such as their Auckland delivery address and NZ credit card details, to order a delivery to their home in Auckland = GDPR is not applicable - *it is not an EU transaction and it does not matter where the data is processed*.

A tourist from the EU logs onto the website of their local EU grocery store from their hotel in Auckland. They provide personal data such as their EU delivery address and EU credit card details to order a delivery to their home = GDPR is applicable - *this is a service being delivered in the EU.*

A tourist from Auckland logs onto the website of a nearby EU pizza restaurant from their EU hotel. They provide personal data such as credit card details and name, to order a pizza delivery to their EU hotel = GDPR is applicable - *this is a product and service being provided in the EU*.

Some scenarios

A tourist from the EU logs onto the website of a nearby Auckland pizza restaurant from their Auckland hotel. They provide personal data such as credit card details and name, to order a pizza delivery to their Auckland hotel = GDPR is not applicable - *this is not a product or service being provided in the EU.*

A person logs onto the website of a car parts store in Auckland, from their home in the EU, to order a car part. They provide personal data such as credit card details and their EU home address for delivery of the car part = GDPR is applicable - *this is related to a product or service to be provided in the EU.*

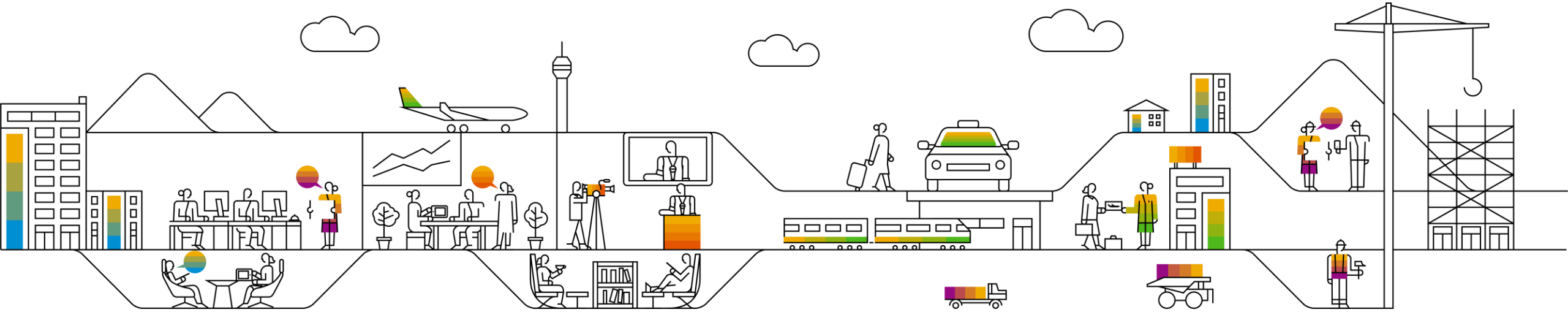
If local banks (in NZ for example) are offering services to citizens of the European Union, have subsidiaries in the EU or use data analytics to understand and predict customer behaviour, they have new obligations under GDPR.

Some scenarios

International Student? College or university. The reason is, no matter where your institution is based, if you are collecting or storing any personal information from European Union (EU) residents, you are subject to this new regulation.

The major banks will all be captured by GDPR as they all trade European currency.

If an non EU bank customer uses their mobile banking app in Europe and the lender using data analytics on transactions, there is the potential for that bank to be captured by GDPR.



What’s the business impact?

Data Subject ‘Letter from Hell’

Dear Sir/Madam:
I am writing to you in your capacity as data protection officer for your company. I am a customer of yours, and in light of recent events, I am making this request for access to personal data pursuant to Article 15 of the General Data Protection Regulation. I am concerned that your company’s information practices may be putting my personal information at undue risk of exposure or in fact has breached its obligation to safeguard my personal information.

Please advise as to the following:

1. Please confirm to me whether or not my personal data is being processed. If it is, please provide me with the categories of personal data you have about me in your files and databases.
   a. In particular, please tell me what you know about me in your information systems, whether or not contained in databases, and including e-mail, documents on your networks, or voice or other media that you may store.
   b. Additionally, please advise me in which countries my personal data is stored, or accessible from. In case you make use of cloud services to store or process my data, please include the countries in which the servers are located where my data are or were (in the past 12 months) stored.
   c. Please provide me with a copy of, or access to, my personal data that you have or are processing.

7. I would like to know whether or not my personal data has been disclosed inadvertently by your company in the past, or as a result of a security or privacy breach.
   a. If so, please advise as to the following details of each and any such breach:
      i. a general description of what occurred;
      ii. the date and time of the breach (or the best possible estimate);
      iii. the date and time the breach was discovered;
      iv. the source of the breach (either your own organization, or a third party to whom you have transferred my personal data);
      v. details of my personal data that was disclosed;
      vi. your company’s assessment of the risk of harm to myself, as a result of the breach;
      vii. a description of the measures taken or that will be taken to prevent further unauthorized access to my personal data;
      viii. contact information so that I can obtain more information and assistance in relation to such a breach, and
      ix. information and advice on what I can do to protect myself against any harms, including identity theft and fraud.
   b. If you are not able to state with any certainty whether such an exposure has taken place, through the use of appropriate technologies, please advise what mitigating steps you have taken, such as
      i. Encryption of my personal data;
      ii. Data minimization strategies; or,
      iii. Anonymization or pseudonymisation;
      iv. Any other means

UBER as a Cyber/InfoSec GDPR Use Case

Bloomberg reported on a breach that exposed details of 57 million customers & drivers.

Uber knew about the breach **over 1 year** before becoming public knowledge. CEO “The incident did not breach our corporate system or infrastructure.”

Bloomberg: Uber **paid** the **hackers** $100,000 to delete the data and keep quiet about it.

- Deputy commissioner James Dipple-Johnson said these actions were unacceptable.
- Uber haven't released detailed figures, can only speculate on the potential data privacy related fine. If this were post May 2018, the fines could be multi-millions.
- The potential bigger ‘cost’ is reputational damage.
- The breach began when attackers accessed Github.com, a website used by software engineers, and obtained login credentials there for information stored on an Amazon Web Services account controlled by Uber, Bloomberg said. In that account they found an archive containing rider and driver data.

TalkTalk as a Use Case

Youngsters, Simple Attack, 'Low' Data Loss, High Business Impact:

Four people arrested and tried: ages 15 to 20 years old

Initial attack was **DDOS** (distributed denial of service)

Around 16,000 bank account numbers and sort codes were stolen, accessed around 160,000 customer personal data (name, address, dob, phone numbers, email addresses)

- TalkTalk shares lost about a **third of their value**
- October 2016 - ICO fine £400,000. Fines will increase with GDPR (tens of £millions) £59m under **GDPR…**

ICO: In spite of its expertise and resources, when it came to the basic principles of cyber-security, TalkTalk was found wanting

University Fundraising Data Breach Allegations - Purpose of Processing

University fundraising is to be examined by the Information Commissioner.

UK universities belonging to the Russell Group sent former students' data to firms for wealth screening before approaching them for donations.

Profiling *individuals for a fundraising campaign is* ***not illegal****, but the law requires that people are* ***informed*** *of how their* ***data is being used***

- Purpose: "Personal data belongs to the individual and that means they have the right to make choices about how it is used. The law requires organisations to tell people what it's going to be used for and who it's going to be shared with - and that's what people expect."

https://www.theguardian.com/education/2017/nov/20/university-fundraising-under-scrutiny-after-data-breach-allegations

Imagine what could have been with GDPR in effect….

	FINES BEFORE GDPR	POTENTIAL FINES IF OCCURRED AFTER GDPR
The UK subsidiary of a major healthcare group	**£200K** Data breach April 2015	**£1.6B** Data breach
A US global financial services group	**$27M+** Data breach May 2017	**$125M+** Data breach
A major internet service provider	**£400K** Security failure Oct 2015	**£59M** Security failure

Based on publicly available data – companies anonymized

Calculated based on maximum fines against annual revenues

Facebook

Facebook refuses to promise GDPR-style privacy protection for US users

Alex H

@alex

Wed 4 Ap

140

FACEBOOK STITCHES UP AUSSIES

AUSTRALIANS will become second-class online citizens in a sneaky move by Facebook designed to rob us of new privacy rights.

The social media giant, which suffered the biggest data scandal in its history this year, will be forced to deliver new privacy tools today, when European Union's General Data Protection Regulation comes into force.

But Facebook will use a loophole to ensure Australians do not receive the same rights as their European counterparts, moving them from Facebook's Irish arm to the United States, where privacy laws are more lax.

The move is likely to affect 1.5 billion Facebook users, including others in Asia, Africa, and Latin America.

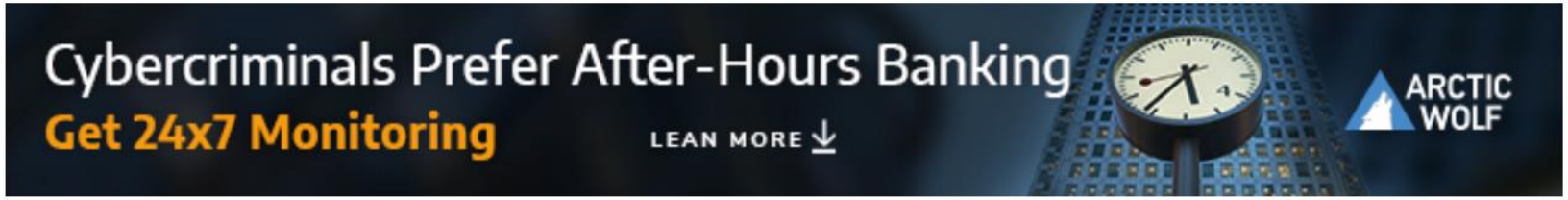
The move would mean Australians couldn't request investigations into how their information was being used.

Report: More than 1,000 personal data breaches reported in Ireland since GDPR deadline

The top GDPR-related complaints are: processing involving the disclosure of personal data without a legal basis; user requests for information on their data; and unfair processing.

Robin Kurzer on August 6, 2018 at 2:55 pm

BANK INFO SECURITY®



Topics News Training Resources Events Jobs

TRENDING: Fraud & Breach Prevention Summit: Toronto - September 11th & 12th >>

Breach Preparedness , Breach Response , Data Breach

Under GDPR, Data Breach Reports in UK Have Quadrupled

Privacy Regulator Sees 1,750 Breach Reports in June, Up From 400 in April

Mathew J. Schwartz (euroinfosec) • July 25, 2018 1 Comment

Twitter Facebook LinkedIn Credit Eligible Get Permission

Butlins data breach hits 34,000 users

SHARE TWITTER LINKEDIN FACEBOOK GOOGLE+ @

WRITTEN BY
Clare Hopping

NEWS

13 Aug, 2018

Butlins thinks the data was stolen via a phishing attack

Up to 34,000 Butlins customers may be affected by the company's data breach, security specialists have warned, with personal details such as postal addresses and holiday arrival dates thought to have been among

Search

Privacy Commissioner
Te Mana Matapono Matatapu

Privacy Act & codes

Introduction

Personal information held by agencies

The Privacy Act controls how 'agencies' collect, use, disclose, store and give access to 'personal information'. The privacy Codes of Practice do the same, but they apply to specific areas - particularly health, telecommunications and credit reporting.

Personal information is information about identifiable, living people.

Almost every person or organisation that holds personal information is an 'agency'. So, for example, the Privacy Act covers government departments, companies of all sizes, religious groups, schools and clubs.

Exemptions from the Act

Only a few organisations and people are not 'agencies'. Other rules exist to govern how they manage personal information, so the Privacy Act does not cover what they do. Organisations that aren't covered by the Privacy Act

Ask us a question

Bills and Laws

Bills (proposed laws)

Supplementary Order Papers

Proposed members' bills

View all

Privacy Bill

This bill repeals and replaces the Privacy Act 1993, as recommended by the Law Commission's 2011 review of the Act. Its key purpose is to promote people's confidence that their personal information is secure and will be treated properly.

Get notifications

MP in charge

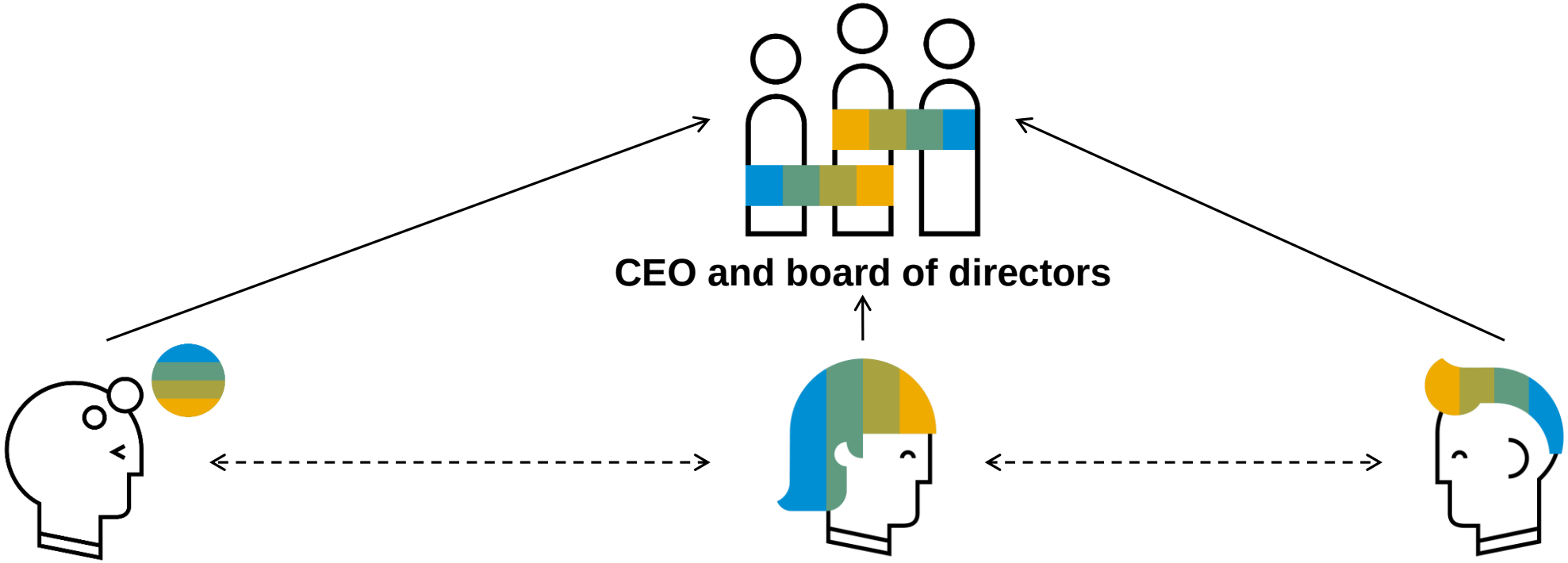
Little, Andrew

Progress of the bill

What do the symbols mean?

In	1	SC	2	CH	3	RA
Bill Introduced 20/03/18	**First Reading** 11/04/18	**Select Committee**	Second Reading	Committee of whole House	Third Reading	Royal Assent

Who is Involved?



Legal

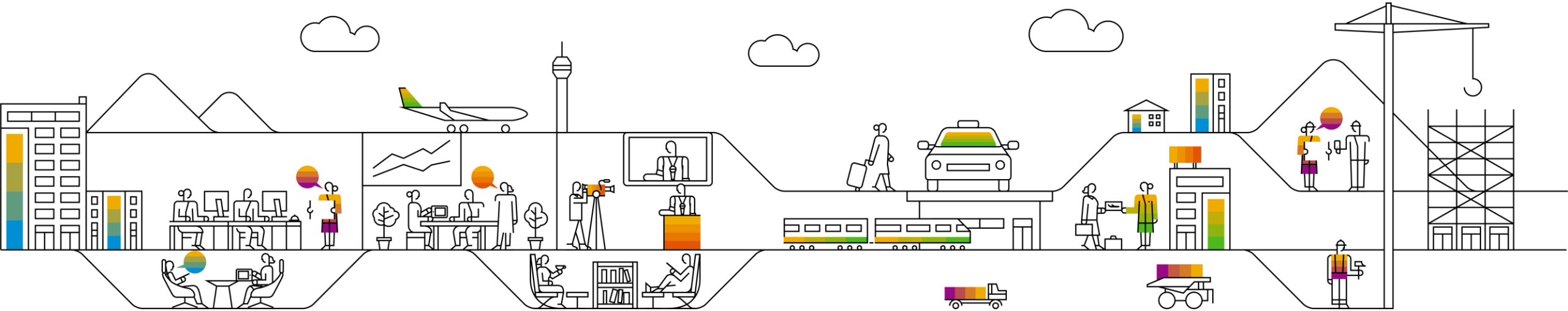
- **Data protection officer**
- Chief compliance officer
- Chief risk officer
- Head of legal
- Chief audit executive

Line of Business

- HR
- O2C
- P2P
- Business process owners

IT Operations

- Chief information officer
- Chief information security officer



How do we talk about it?

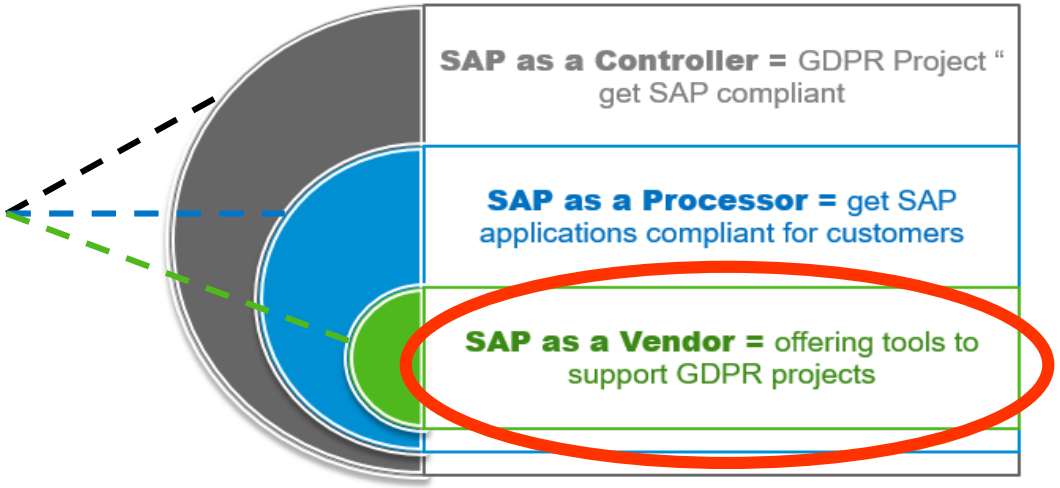
The broader SAP messaging for GDPR is critical

Our three messages:

I. We comply (protect our customers, business partner and employee data)

II. Core SAP business systems provide data privacy management capabilties

III. We help you comply (with DDM / GRC)



Leading with GRC and DDM offerings, with service options available:

- Solutions to help customers get and stay compliant
- Services options available with SAP and Ecosystem

SAP is accelerating our global GDPR message to the market:

- GRC / DDM collaborating with Corp Marketing on our three messages
- Working to communicate a more comprehensive message through the Trust Center on sap.com

Data Protection and Privacy

Data protection and privacy is part of our DNA. SAP protects the rights of our employees, applicants, customers, suppliers, partners, and more. When we process and use data, we protect it, preserve its ownership, and maintain the privacy of the person who it belongs to.

EU General Data Protection Regulation (GDPR)

GDPR harmonizes data protection regulation throughout the EU and gives individuals more control over their data.

Learn more ›

Data Protection and Privacy Agreements

Learn about our rules and standards for the collection, processing and use of personal data, by SAP and our sub-processors.

Learn more ›

Data Protection Management System

Learn how the data protection management system (DPMS) helps us achieve and maintain an effective and appropriate level of data protection and privacy at SAP.

Learn more ›

Cloud Service Status

Keep your business up and running with real-time insights into your cloud system. By providing transparency into availability, downtime, and maintenance, we can help you plan ahead and optimize resources.

Select a product

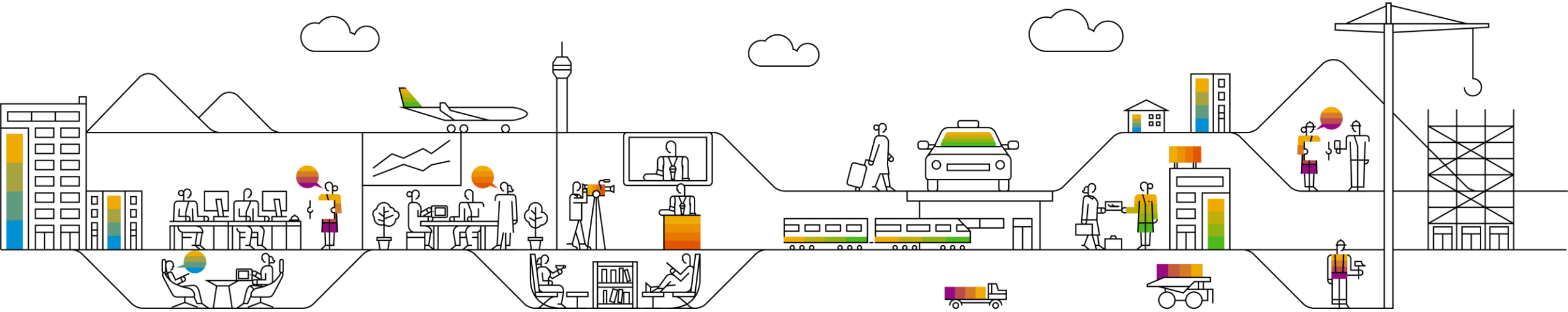
SAP Cloud Platform Integration

Select a time zone

UTC+10 - 11:56 ...

Previous week | Next week

	Current Status	Mon 8/13/18	Tue 8/14/18	Wed 8/15/18	Thu	Fri 8/17/18	Sat 8/18/18	Sun 8/19/18
SAP Cloud Platform Integration	✓	✓	✓	✓	✓	✓	✓	✓ ✕
Australia: Sydney	✓	✓	✓	✓	✓	✓	✓	✓ ✕
Brazil: São Paulo	✓	✓	✓	✓	✓	✓	✓	✓ ✕



What are our capabilities, what's coming?

Opening Questions and some Solution Answers

Operations

Where is your personal data?

- **Locate data in SAP and non-SAP systems – IS & DS**
- **Risk of data (DPIA) & owners - PC**

Retention, block, delete, collect data?

- **Retention, block, delete SAP systems – ILM, OpenText**
- **Collect data – IS & DS, HANA, MDG**

Business processes register?

- **Processes, linked data, risk, owners – PC**
- **Linked purpose, lawful processing – PC**

Business Security?

- **Data Access – AC, DAM, UI tools**
- **Monitoring, investigation – ETD, DAM, UI**
- **Data breaches – PC**

Data protection officer

Who is accountable?

- **Document roles and responsibilities of personal data & processes owners, approvals - PC**
- **Inform and advise organisation, employees, 3rd parties about GDPR - PC**

Duties, transfers of data in/out of the EU?

- **Evidence of organisational compliance with the 6 principles, duties of a processor and controller, data transfer out the EU - PC**

Reports on processing activities

- **Maintain records of processing activities, ready for the supervising authority – PC**
- **Internal breach reporting procedures – ETD, DAM, UI tools, PC**

Governance

GDPR policies and procedures

- Develop and maintain GDPR policy, codes, privacy notices (esp. children) - PC

GDPR rolled out?

- Perform DPIA as appropriate, by design and default – PC
- Regularly test, assess, evaluate effectiveness of technical + organizational measures for processing security - PC
- Data breaches manged and remediates – PC, ETD, DAM,UI tool
- Impact of regulatory changes e.g. WP29, ePrivacy directive (PECR revision) - PC

Third party contracts?

- Governance of binding corporate rules, standard data protection clauses – PC

THIS IS NOT LEGAL ADVICE

SAP's Data Protection & Privacy offerings are clustered in 4 Pillars

Governance

- Record of processing activities
- Data Privacy Impact Assessment
- Controls
- Policies

SAP Process Control

SAP Risk Management

SAP Audit Management

Data Discovery & Mgmt

- Privacy Data mapping, profiling
- Blocking, deletion
- Data flow analysis
- Data transfer, Geo fencing
- Data minimization

SAP Information Lifecycle Management

SAP Information Steward

SAP Process Mining by Celonis

SAP OpenText

SAP SCP Retention & Personal Data Mgmt

SAP Data Custodian

Data Security

- Access governance
- Breach notification and anti breach management
- Customer Identity management
- UI Masking and Logging

SAP Access Control

SAP Enterprise Threat Detection

SAP UI Logging & Masking

SAP Dynamic Authorization Management by NextLabs

SAP IDM &SSO

SAP SCP Identity Access Governance

Interaction Center

- Data subject interaction center
- Customer preference and consent management
- Authority Interactions
- Breach response

SAP Gigya Preference Management

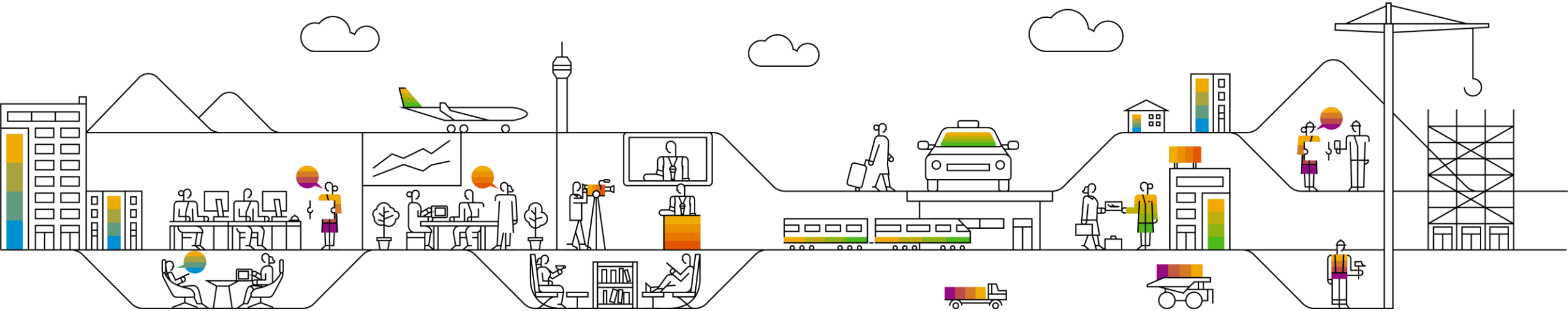
SAP Gigya Business Partner Identity Mgmt

GRC & Security

DDM

Hybris

Cloud Platform



Where can I get more info?

Where to find more: SAP.COM/GDPR

Thank you

Contact information:

Les Smith
Solution Lead – Finance and Risk
Centre of Excellence (ANZ)

Les.Smith@sap.com
+61 407 635 724