KPMG

All Systems Go For GDPR?

2018 June 21 Cayman Chamber of Commerce

Today's Agenda

Welcome and Introductions

About Privacy

GDPR

How to comply

What do I Need to Do Right Now?

Q&A

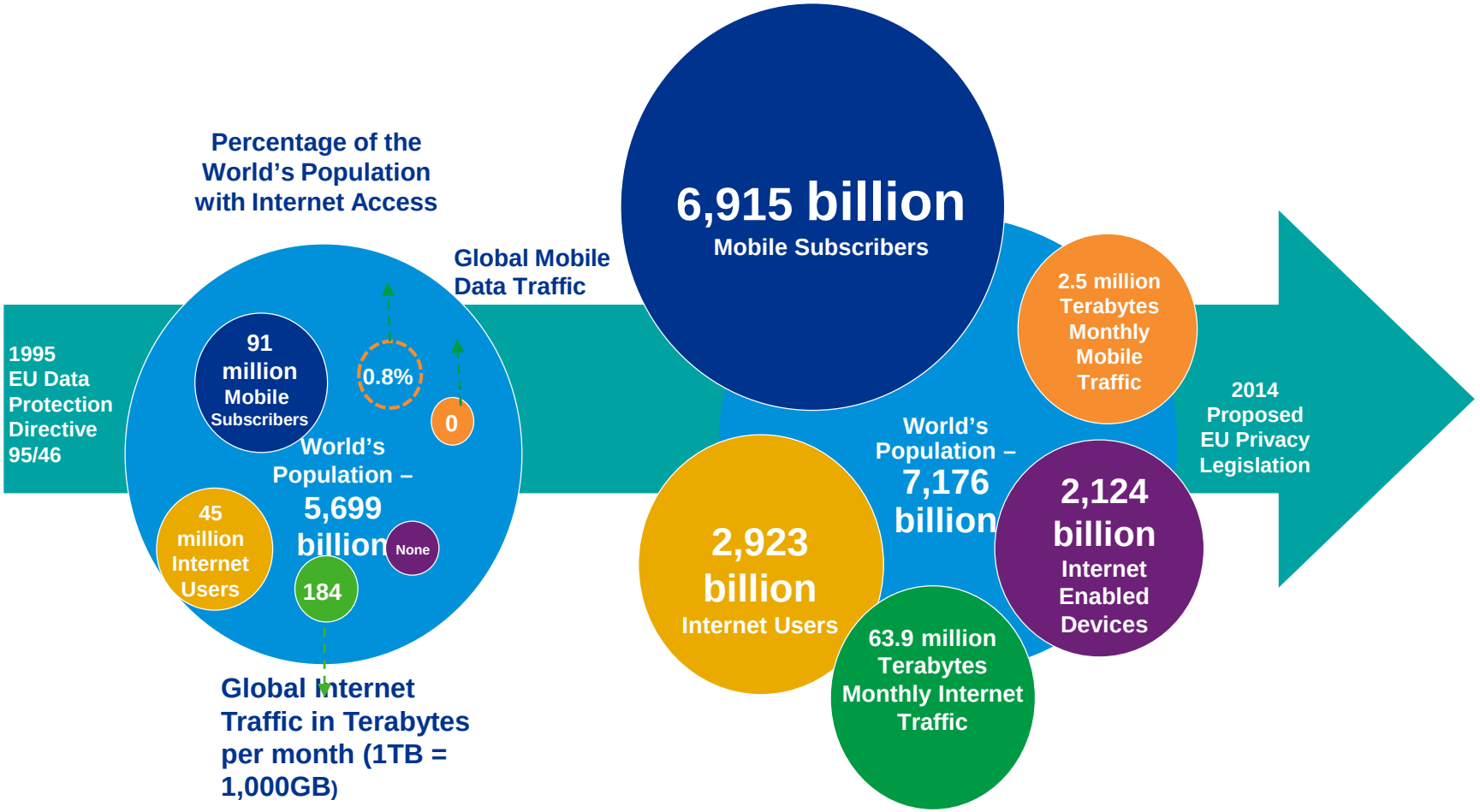
© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

About Privacy

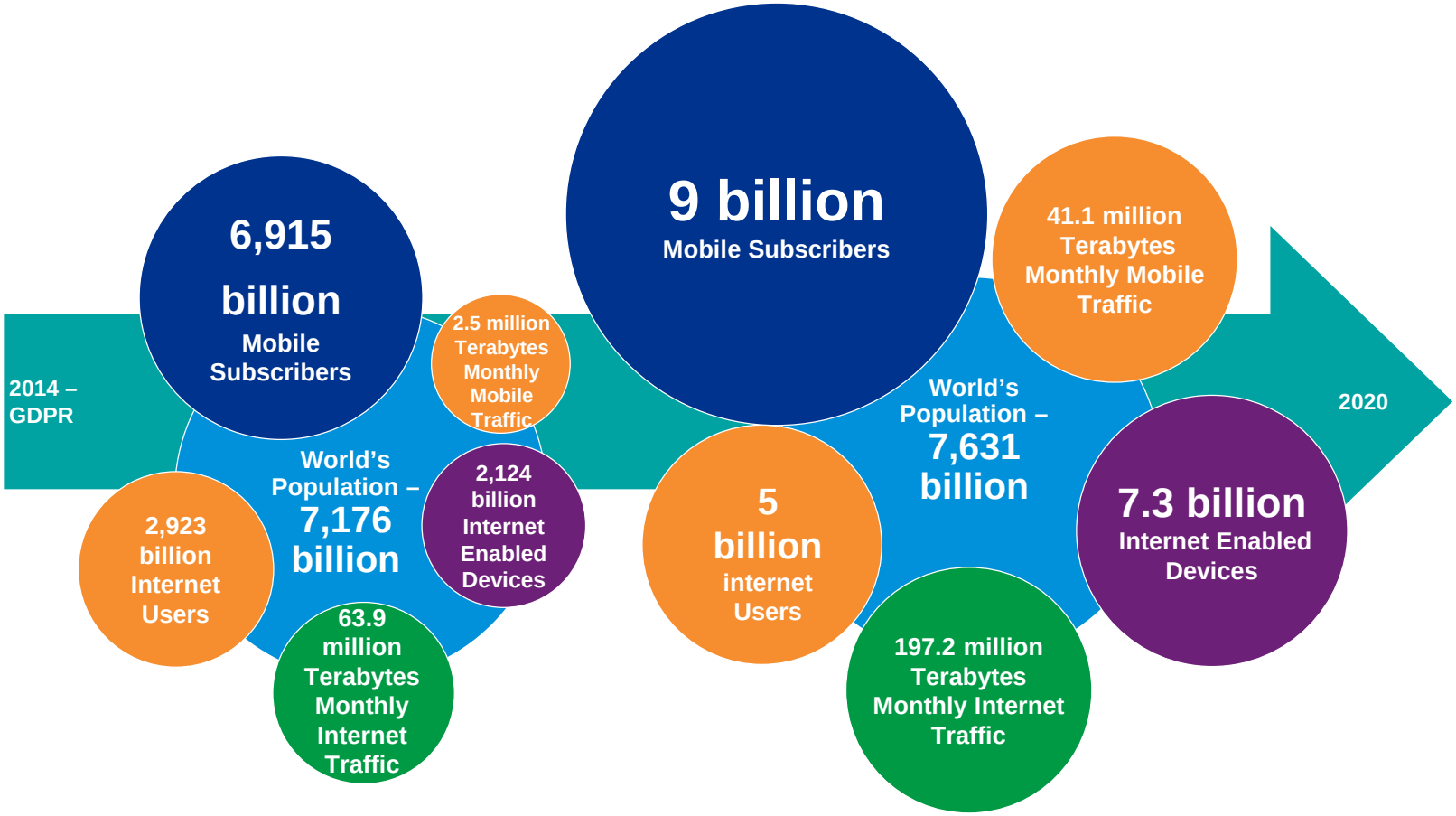
The world has changed



© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

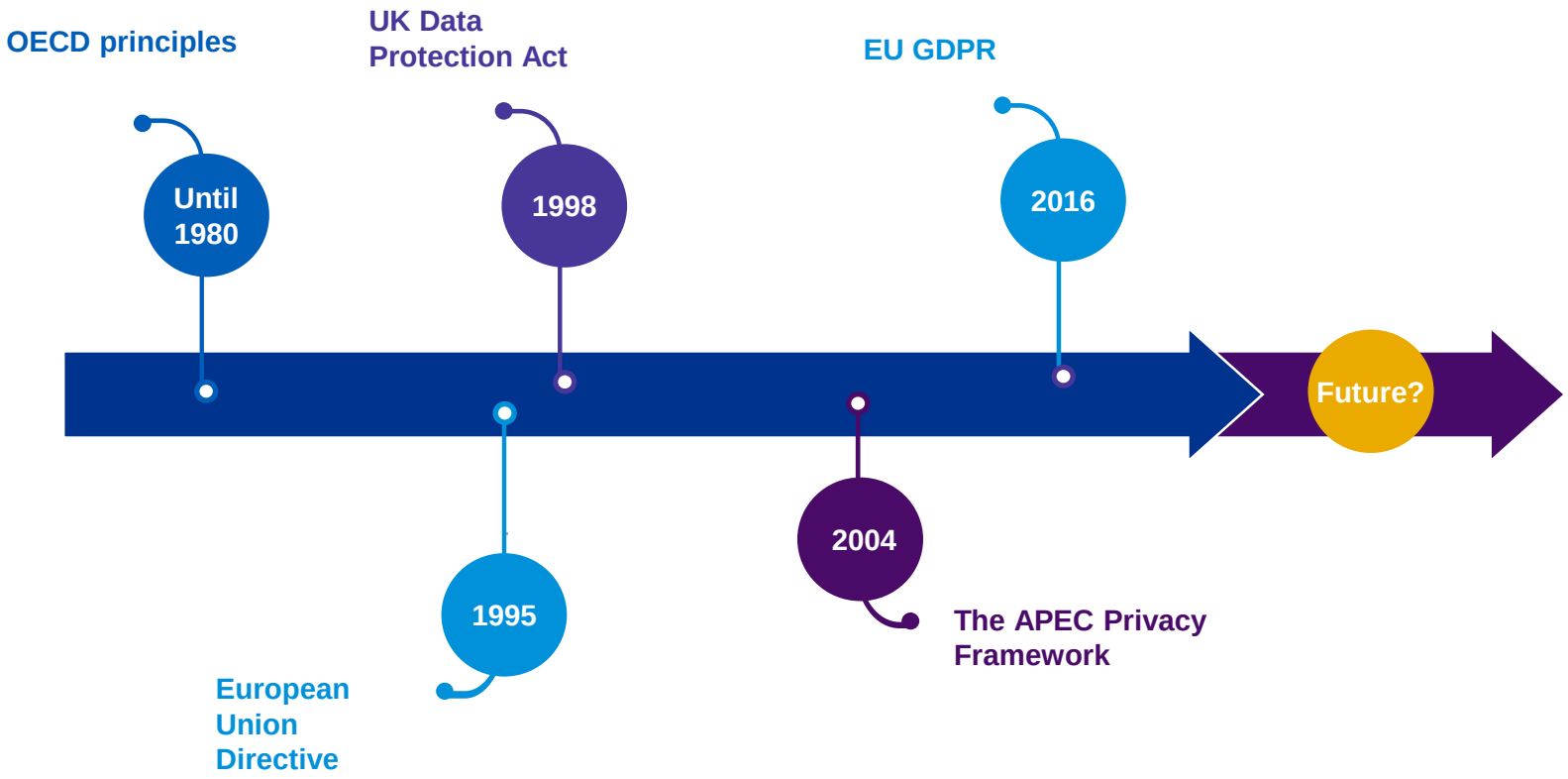
The world has changed (cont.)



© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

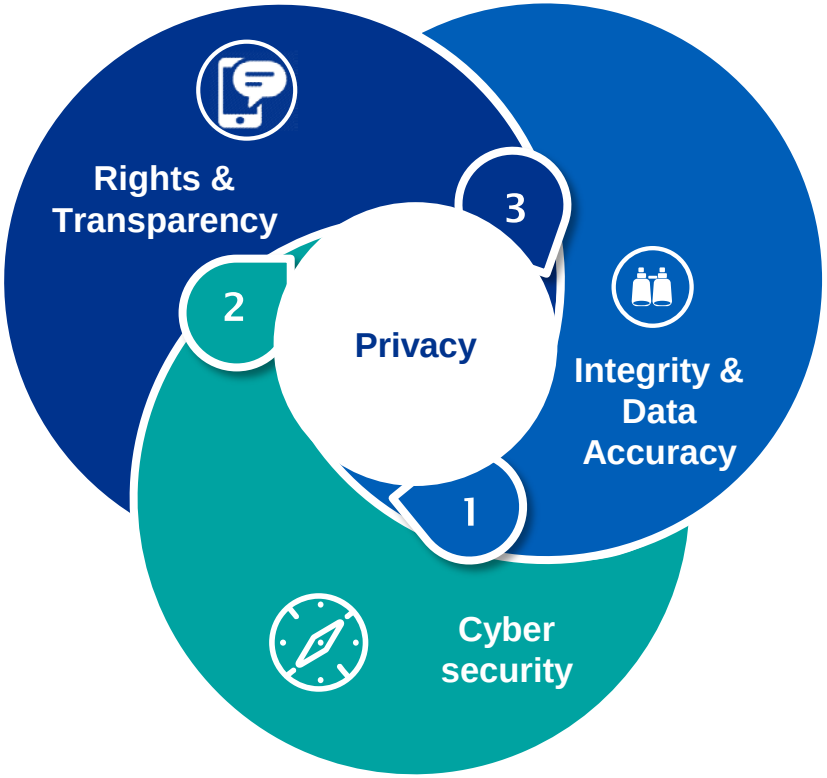
Background of privacy regulation



© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

What is privacy?

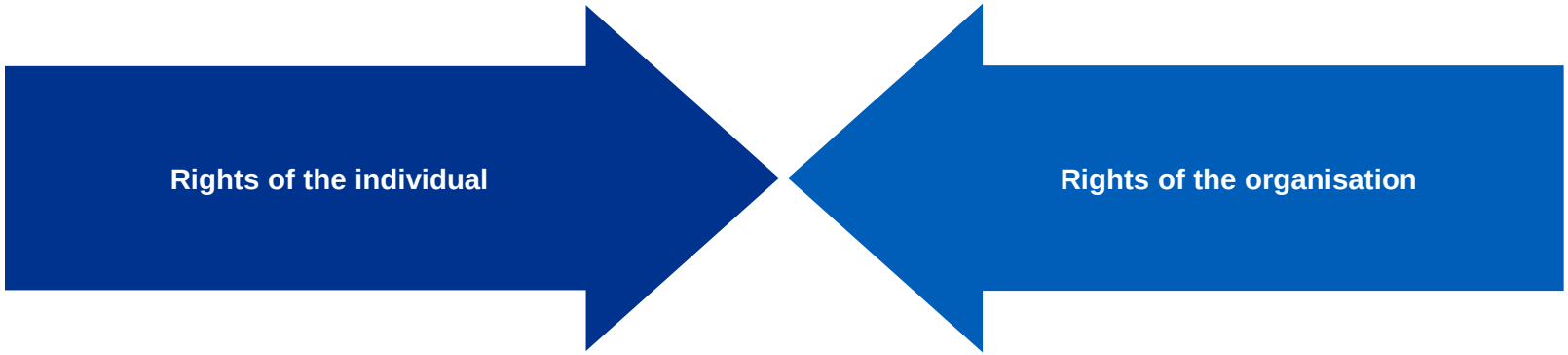


> Privacy encompasses the rights and obligations of **individuals** and **organisations** with respect to the collection, use, retention, disclosure, and disposal of personal information.

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Privacy rights: For whom?



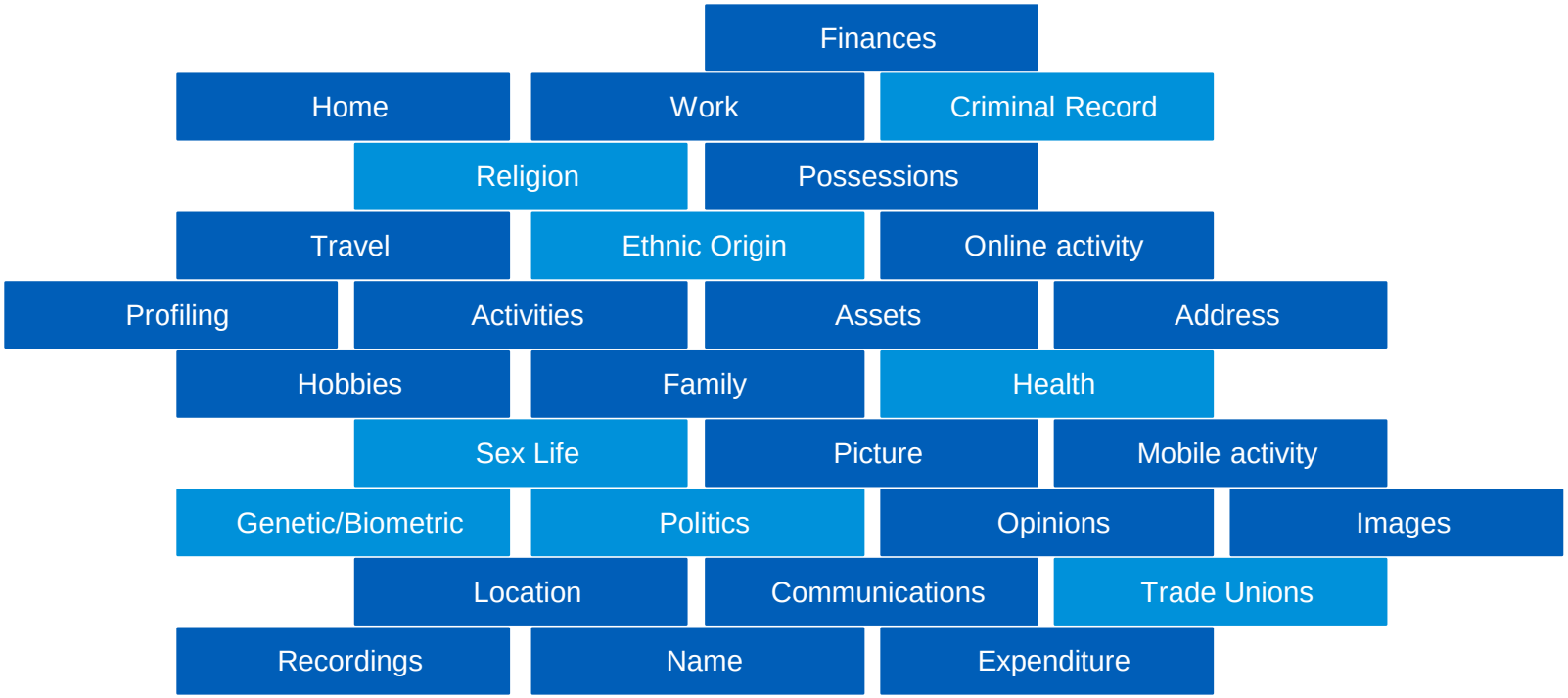
© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

What is Personal Information?

Personal Information – GDPR

'Personal information means any information relating to an identified or identifiable natural person.'



© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

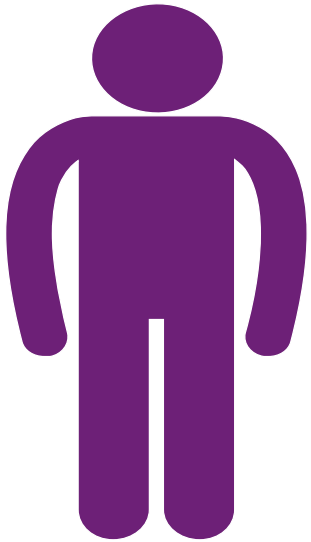
Document Classification: KPMG Confidential

What is a data subject?

'Identified or identifiable natural person'

EU DPAs treat information as Personal Information if it can be linked to a unique individual

Data Subject



Typical links/identifiers:

- Name
- Passport no.
- Driving Licence no.
- NINO/SSN
- Mobile device ID (e.g. IMEI)
- SIM
- IP address
- MAC address
- PC Machine ID
- Genetic/Biometric data

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

The new digital world - our traces everywhere

- Your digital footprint is a collective profile created from all of your online activity
- Some data is voluntarily given such as social media posts, blogging, product reviews, or online shopping
- Some data comes from browser cookies, silent data collections, and installing new apps or software

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Clicking away privacy – the "I Agree" waiver

Illustrative Privacy 'click-wrap' contract:

"We use the information that we receive for the services that we offer to you, and to other users such as your friends, our partners, advertisers who purchase publicity on the site, and developers of games, applications and web sites."

So <u>you</u> are the product that they sell

*Google, Inc., Annual Report (Form 10-K)

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

GDPR Overview

The EU general data protection regulation (GDPR)

Passed in May 2016, the GDPR came into force on **May 25, 2018**.

Harmonise Privacy law across Europe

Reflect the Digital Age

Give individuals greater control of their own information

Increased accountability for organisations

‘Our current data protection rules [were] adopted in 1995 when only 1% of the EU population was using the internet... and the founder of Facebook was only 11 years old’
Vivian Reding, European Commissioner for Justice, 18 June 2012

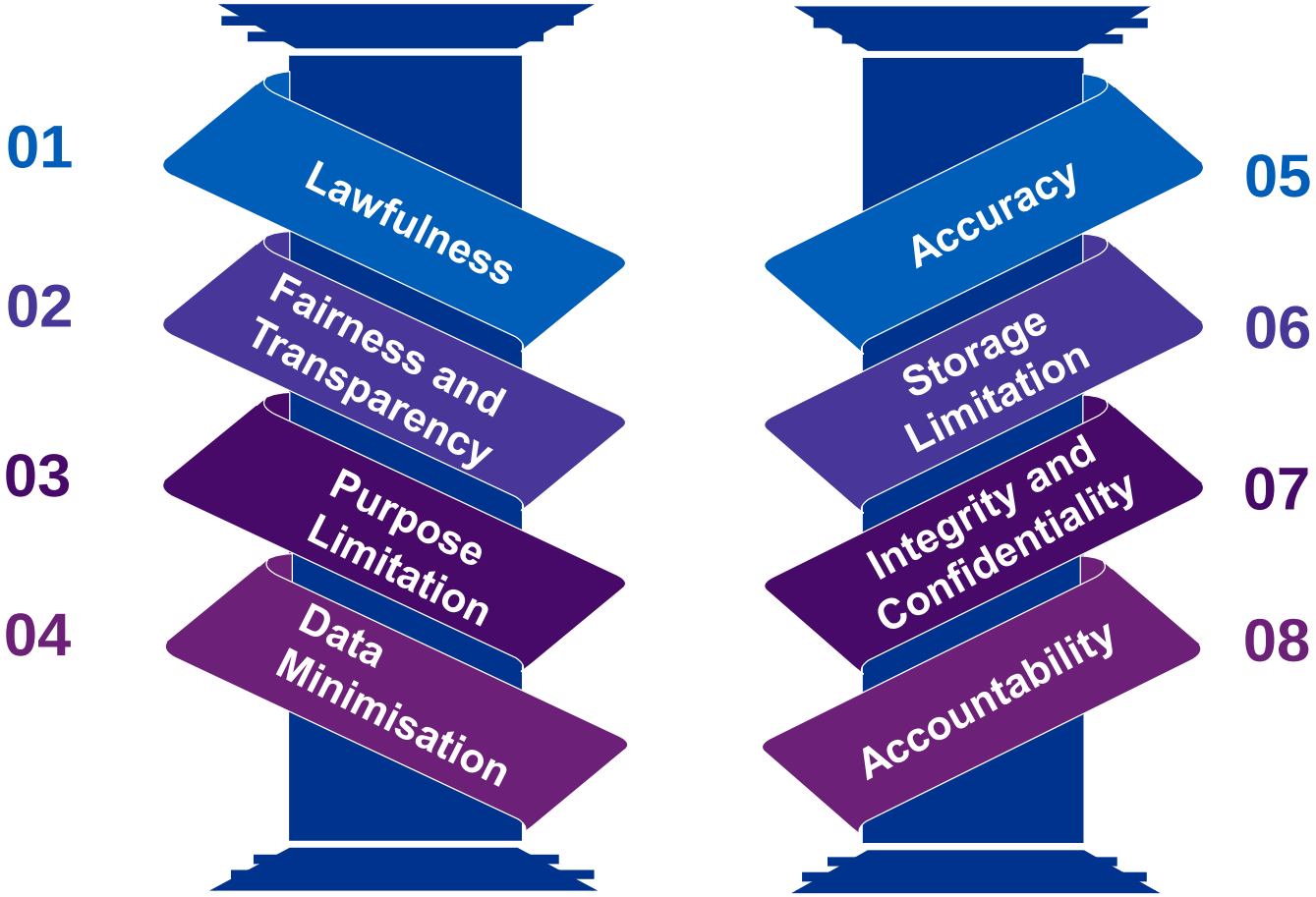
EU Data Protection Directive 95/46/EC → **EU GDPR**

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

The EU general data protection regulation (GDPR)



© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Privacy regulation
What has changed?

	Data Protection Directive 95/46/EC	GDPR
	**Fines** Fines vary by jurisdiction (e.g. **UK £500,000)**	**Fines** A fine of up to €10 million or **2% of global annual turnover** Maximum fine of up to €20 million or **4% of global annual turnover**
	**Data Protection Officer (DPO)** Generally no requirement to appoint a DPO	**Data Protection Officer (DPO)** DPO **required** for 'government bodies' and organisations conducting **mass surveillance** or **mass** processing of **Special Categories** of data
	**Privacy Seals** Generally not recognised	**Privacy Seals** Privacy seals introduced

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Privacy regulation
What has changed? (cont.)

	Data Protection Directive 95/46/EC	GDPR
	**Supervisory Authorities (SA) Enforcement Powers** SA have limited powers under national law	**SA Enforcement Powers** SAs will be given wide-ranging powers to enforce compliance
	**Inventory** No requirement to maintain a personal information inventory	**Inventory** Generally organisations will need a personal information inventory
	**Breach Notification** Generally there are no obligations to report breaches	**Breach Notification** Requirement to report Privacy breaches to the regulator within 72 hours and potentially to the Data Subject

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Privacy regulation
What has changed? (cont.)

	Data Protection Directive 95/46/EC	GDPR
	**Security** Vague requirements around security (i.e. 'adequate level')	**Security** Requirements around monitoring, encryption and anonymisation
	**Privacy Impact Assessments (PIAs)** There is no mandated requirement to perform PIAs	**Privacy Impact Assessments (PIAs)** Companies must perform PIAs if the activity is considered 'high-risk'
	**Data Subject's Rights** Various rights, including right of access	**Data Subject's Rights** Rights extended to include Data Portability and the Right to Erasure

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Privacy regulation
What has changed? (cont.)

	Data Protection Directive 95/46/EC	GDPR
	**Sensitive Personal Data** This includes religious beliefs, physical/mental health and ethnic origin amongst others	**Sensitive Personal Data** Similar but extended to include biometric and genetic data
	**Consent** Potential to rely on 'implicit' consent depending on jurisdiction	**Consent** Requirement to gain unambiguous consent (i.e. explicit)
	**Data Processors (DP)** Processors have limited regulator exposure for processing activities	**Data Processors (DP)** Processors are also covered. Controllers must conduct due diligence into processors' suitability

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

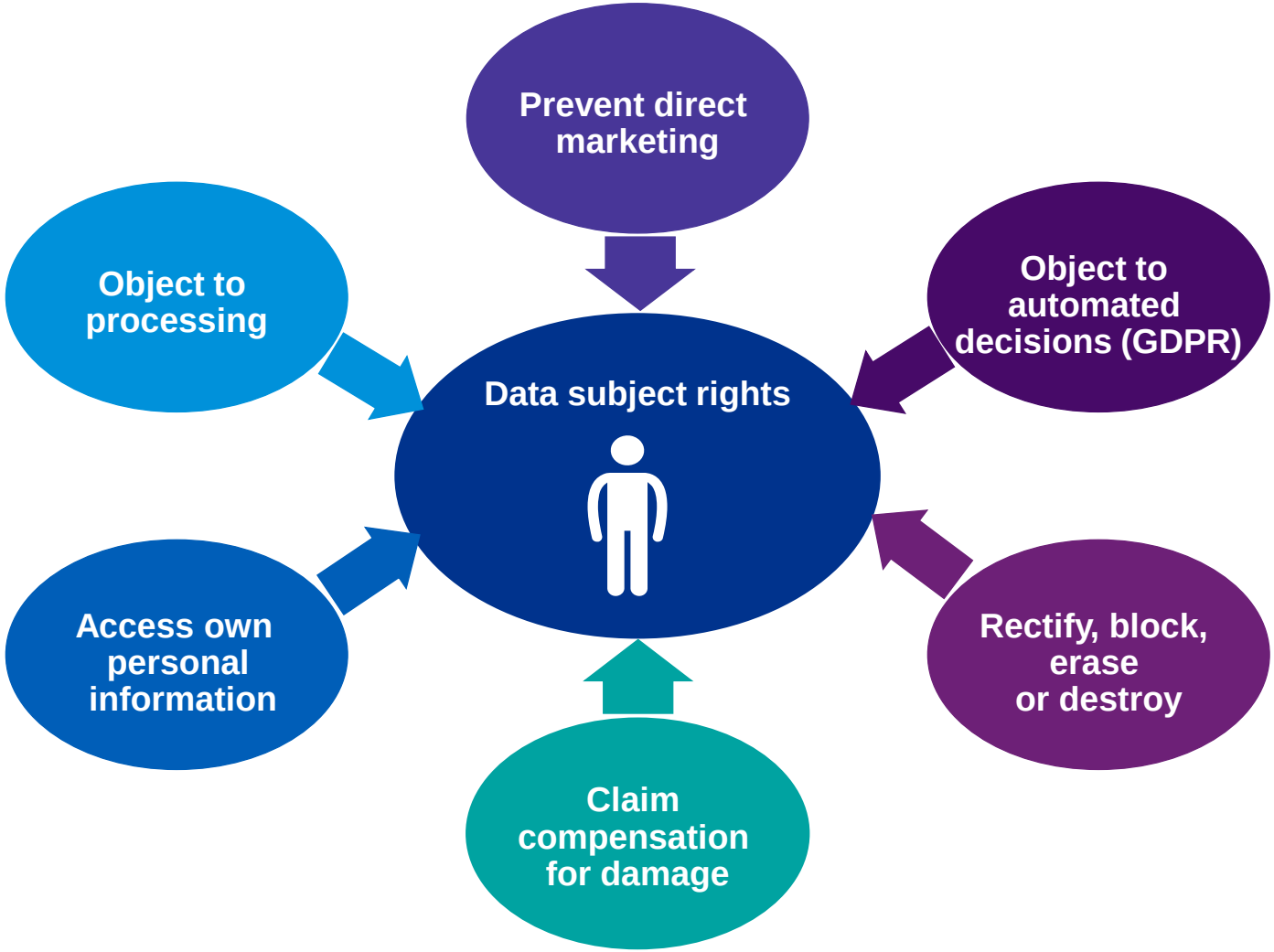
Privacy regulation
What has changed? (cont.)

	Data Protection Directive 95/46/EC	GDPR
	**Control Environment** No general requirement to maintain ‘documentation’	**Control Environment** General requirement to maintain certain ‘documentation’
	**International Transfers** Personal Information cannot be transferred outside the EU unless appropriately legitimised	**International Transfers** Adequacy arrangements i.e. ‘Privacy Shield’ – Binding Corporate Rules – Standard Contract Clauses.

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative (“KPMG International”), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

Data subject rights - Rights of individuals



KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

GDPR
How to Comply

12 Key Steps to GDPR compliance

1. Appoint Privacy Officer / consider need for DPO
2. Consider impact and applicability of GDPR
3. Prepare a record of processing activities – data inventories and mapping
4. Establish lawful basis of processing / conditions for using personal data
5. Consider presence and management of sensitive and children's data
6. Review and update privacy notices and management of consent

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

12 Key Steps to GDPR compliance

7	Update / formalize your data breach notification procedures
8	Review third party / data processor transfers (overseas transfers and appropriate terms)
9	Update systems and procedures to cater for rights of individuals, including Subject Access Requests
10	Review policies for privacy by design and privacy impact assessment
11	Undertake a risk assessment of security safeguards protecting personal information
12	Determine lead data protection supervisory authority (if applicable)

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#1 - Appoint a privacy officer and consider whether required to appoint a data protection officer (DPO)

The Data Protection Officer (GDPR) has *inter alia* the following tasks:

- Inform and advice data controller or processor as well as employees;
- monitor compliance with data protection laws;
- cooperate with and act as contact person for supervisory authorities;
- not always required, must be appropriately qualified and independent

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#2 - Consider impact and applicability of GDPR

GDPR Reach, Art 5(2) – "the controller shall be responsible for and be able to demonstrate, compliance with the principles"

- Any organization – with very few exceptions – that processes personal data within the European Union will fall under the scope of the GDPR
- Non-EU data controllers and processors must comply with the European Data Protection obligations when they process data from individuals in the EU for specific goals:
  - Offering goods or services to individuals in the EU. Targeting EU citizens
  - Monitor behaviour of individuals inside the Union

GDPR 'Controllers' and 'Processors'

- A controller determines the purposes and means of processing personal data
- A controller has obligations to ensure their contracts with processors comply with the GDPR.
- A processor is responsible for processing personal data on behalf of a controller
- A processors has specific legal obligations, including a requirement to maintain records of personal data and processing activities. They have legal liability if responsible for a breach.

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#3 - Prepare a record of processing activities

GDPR - Obligation to maintain records of processing activities

- Name and contact details of the controller(s) / representative / processor / DPO
- Purposes of the processing
- Description of the categories of data subject and of the data processed
- Categories of recipients
- Transfers to third parties / overseas documenting suitable safeguards
- Time limits for erasure
- General description of technical and organisational security measures

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#3 - Prepare a record of processing activities (cont.)

GDPR Art 30 – prepare and maintain a record of processing activities

GDPR requires a central register processing data inventory ('data register'). Consider creating a full data inventory to ensure completeness:

- The nature of the data holding (e.g. Human resources data)
- The owner of the data holding
- Location of the data holding
- The volume of information in the data holding
- The format of the information (Paper or electronic? Structured or unstructured?)
- The use of the information
- The data elements (e.g. name, physical address, email address, government identifier, health information, salary information)
- Where the data is stored (in which country/countries)
- Where the data is accessed (from which country/countries)
- International transfers (data flows – country by country)

KPMG

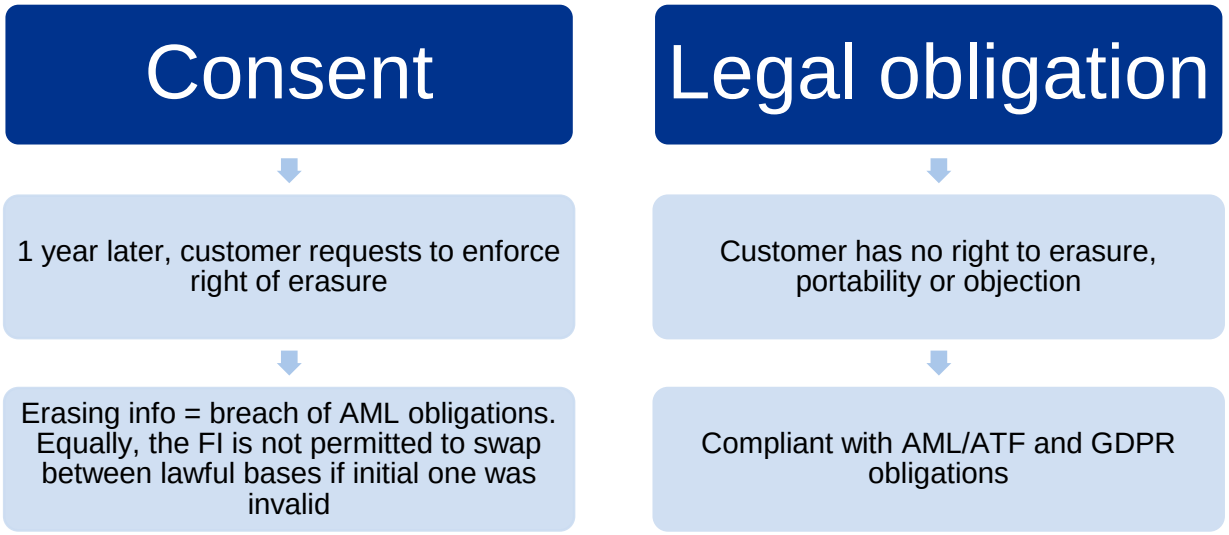
© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#4 Establish a lawful basis for processing

Example

A financial institution asks its potential customers for personal identification required for AML/ATF purposes. The financial institution must contain on its notice to customers the basis for processing.



Consent is only appropriate if you can offer customers real choice and control over how you use their data.

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#5 - Managing sensitive and children's data

GDPR
"special categories of personal data"

You must have a lawful basis for processing AND also satisfy one of ten specific conditions:

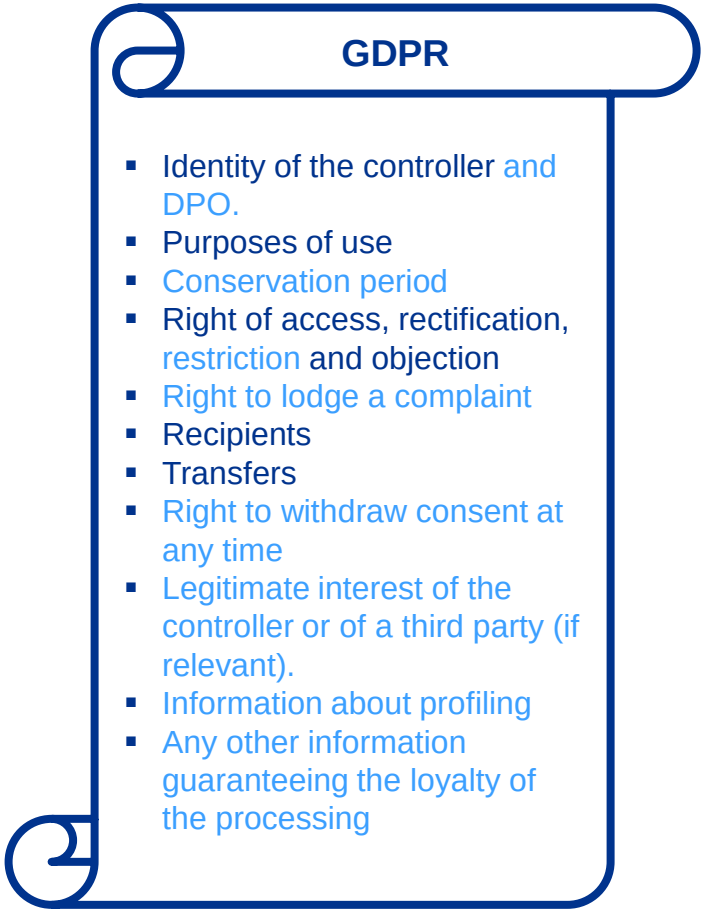
- Explicit consent
- Employment/social security obligations
- Necessary to protect vital interests of individual
- Not-for-profit activities
- Personal data made public by individual
- Necessary for defense/exercise of legal claims
- Substantial public interest
- Medical reasons
- Public health reasons
- Public interest, scientific, historical research purposes

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

6- Review and update privacy notices and management of consent



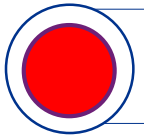
© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#7 - Breach notification procedures

Personal data breach

GDPR - "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"



any incident impacting CIA (Confidentiality, Integrity, Availability)

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#7 - Breach notification procedures (cont.)

Supervisory Authority / Commissioner Notification

- Nature of the breach
- Within 72 hours of becoming aware of the breach (GDPR)
- DPO identification (GDPR)
- Consequences of the breach
- Measures taken to remedy the breach
- Can be done in steps (GDPR)

Data Subject / Individual Notification

- Under GDPR - notification without undue delay in case of high risk to the rights and freedom of individuals
- Under GDPR - no notification if data is encrypted, if technical measures have been taken or if notification involves disproportionate efforts

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#8 - International transfers - GDPR

Adequate country

Countries declared as 'adequate' by EC Decisions include Switzerland, Canada, Argentina, Israel and Uruguay.

US Privacy Shield

A framework of Privacy Principles that guarantees an adequate level of protection by US Companies that sign up and adhere to it.

Binding Corporate Rules

A set of data protection policies, processes and standards, together with contractual provisions that bind the entities and employees of an international organisation to adhere to them.

EU Model Clauses

Contractual clauses published by the European Commission that bind a non-EEA entity to provide an adequate level of protection.

Consent

A specific, informed and freely-given indication of the individual's wishes.

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#8 - Review data processor transfers (terms)

GDPR - Controller must establish a contract that covers:

- Description of subject-matter and duration of the processing
- Description of nature and purpose of the processing
- Types of personal data and categories of data subjects
- Obligations and rights for Controller (responsibilities and audit rights)

GDPR - Direct obligations on data processors include:

- Commit personnel to data secrecy
- Assist Controller to respond to data subject's rights
- Comply with security measures
- Assist Controller with security breach and DPIAs
- Cooperate in case of audits, including inspections

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#9 - Update systems and procedures to cater for rights of individuals

Rights of individuals

- Right to be informed
- Right of access
- Right to rectification
- Right to erasure
- Right to restrict processing
- Right to data portability
- Right to object
- Right not to be subject to automated decision making including profiling

Response to these rights

- Policies and procedures document
- Method of locating, accessing, deleting, correcting an individual's data
- Method of providing this information to an individual
- 1 month (GDPR) to comply with a data request, unable to charge for this and you can only refuse requests which are "manifestly unfounded or excessive"

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#10 - Introduce policies for privacy-by-design

Privacy by design

- Processing activities have to be planned, designed and performed with data security and, more generally, compliance with the privacy regulation in mind

Privacy by default

- By default, only personal data which are necessary for each specific purpose of the processing shall be processed
- By default personal data are not made accessible without the individual's intervention to an indefinite number of individuals

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#10 - Introduce policies for privacy by design

Elements of privacy by design and privacy by default

	No personal data are collected beyond the minimum necessary for each specific purpose of the processing	✓
	No personal data are retained beyond the minimum necessary for each specific purpose of the processing	✓
	No personal data are processed for purposes other than the purposes for which they were collected	✓

	No personal data are disseminated to non-public third parties for purposes other than the purposes for which they were collected	✓
	No personal data are sold	✓
	No personal data are retained in unencrypted form	✗

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#10 - Evaluate use of privacy impact assessments

Under the GDPR (Art35) a Privacy Impact Assessment (PIA) is mandatory when the processing is likely to result in a **high risk** for the rights and freedom of individuals. It should include:

- A description of the processing
- An assessment of the necessity and proportionality of the processing operations in relation to the purposes
- Involvement of the Data protection officer (DPO) where one is designated
- Requires consultation with the Supervisory Authority (SA) if controller does not mitigate the high risk

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#11 - Undertake a risk assessment of security safeguards protecting personal information

GDPR Art.32
"Security of processing"

"Taking into account the state of the art, the costs of implementation and the nature, scope, context and purposes of processing as well as the risk of varying likelihood and severity for the rights and freedoms of natural persons, the controller and the processor shall implement appropriate technical and organisational measures to ensure a level of security appropriate to the risk, including inter alia as appropriate"

- Pseudonymisation and encryption
- Ongoing CIA and resilience
- Timely restoration
- A process for regularly testing, assessing and evaluating the effectiveness of measures

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

#12 - Determine lead data protection supervisory authority under GDPR (if applicable)

1. Identify your main establishment
2. Monitor your Lead SA closely for guidance and enforcement priorities
3. Build good relations with your Lead SA
4. Identify likely Concerned SA that your Lead SA will liaise with
5. Monitor communications from the EDPB and SAs on how the 'One Stop Shop' with be interpreted and applied in practice

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

What do I Need to do Right Now?

What do I need to do right now?

We are recommending the following stages of action in priority order to our clients who find themselves still working towards the GDPR implementation Deadline of May 25.

1. Appoint an individual to assume the Data Privacy responsibilities (you will likely not be required to officially appoint and register a DPO as you do not meet the requirements of being (a) public authorities, (b) organizations that engage in large scale systematic monitoring, or (c) organizations that engage in large scale processing of sensitive personal data per (Art. 37));

2. Review and revise your external privacy notices to ensure they are GDPR compliant including, but not limited to your lawful basis for collection and processing. This will likely require the assistance of legal counsel. Additional Information - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/individual-rights/right-to-be-informed/

   Notice should include:

   1. Controller's identity
   2. Purpose(s) of processing
   3. Details of disclosures
   4. Other information necessary to ensure fair processing
   5. How to exercise Data Subject Rights:
      - Access,
      - Rectification
      - Deletion

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

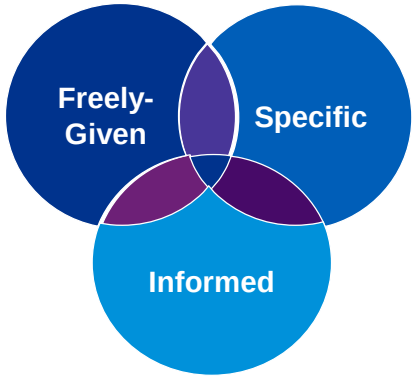
Document Classification: KPMG Confidential

What do I need to do right now?

3. Obtain consent from your EU resident clients for the collection and processing of their personal data. This is very time sensitive as a failure to obtain consent is a clear external indicator of non-compliance visible to all of your clients and with the exception of a data breach, will likely be the most significant risk of a complaint to the regulator. Additional Guidance- https://ico.org.uk/media/about-the-ico/consultations/2013551/draft-gdpr-consent-guidance-for-consultation-201703.pdf

Consent must include:

1. An indication of consent must be unambiguous and involve a clear affirmative action.
2. Consent should be separate from other terms and conditions. It should not generally be a precondition of signing up to a service.
3. The GDPR specifically bans pre-ticked opt-in boxes.
4. It requires granular consent for distinct processing operations.
5. You must keep clear records to demonstrate consent.
6. The GDPR gives a specific right to withdraw consent. You need to tell people about their right to withdraw, and offer them easy ways to withdraw consent at any time.



KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

What do I need to do right now?

4. Conduct a data audit to identify what personal data you hold, what format it is in, where it came from and who you share it with as well as an assessment of the lawful need to collect and retain. This review will also include assessing data retention policies and procedures;

5. Update your policy and procedures to ensure they are compliant and outline the rights of individuals including:
    1. the right to be informed;
    2. the right of access;
    3. the right to rectification;
    4. the right to erasure;
    5. the right to restrict processing;
    6. the right to data portability;

Consider conducting a Privacy maturity assessment to measure your current Privacy program against the requirements of the GDPR. This will then provide you with explicit areas of focus to address as part of your ongoing compliance program.

https://www.reuters.com/article/us-europe-privacy-analysis/european-regulators-were-not-ready-for-new-privacy-law-idUSKBN1I915X

KPMG

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

Document Classification: KPMG Confidential

KPMG

Q&A

kpmg.bm

The information contained herein is of a general nature and is not intended to address the circumstances of any particular individual or entity. Although we endeavor to provide accurate and timely information, there can be no guarantee that such information is accurate as of the date it is received or that it will continue to be accurate in the future. No one should BTC on such information without appropriate professional advice after a thorough examination of the particular situation.

© 2018 KPMG, a group of Bermuda limited liability companies which were member firms of the KPMG network of independent member firms affiliated with KPMG International Cooperative ("KPMG International"), a Swiss entity. All rights reserved.

The KPMG name, logo and are registered trademarks or trademarks of KPMG International.

Document Classification: KPMG Confidential