General Data Protection Regulation (GDPR)

CSC4008
8th November 2018

Objectives

The purpose of this session is:

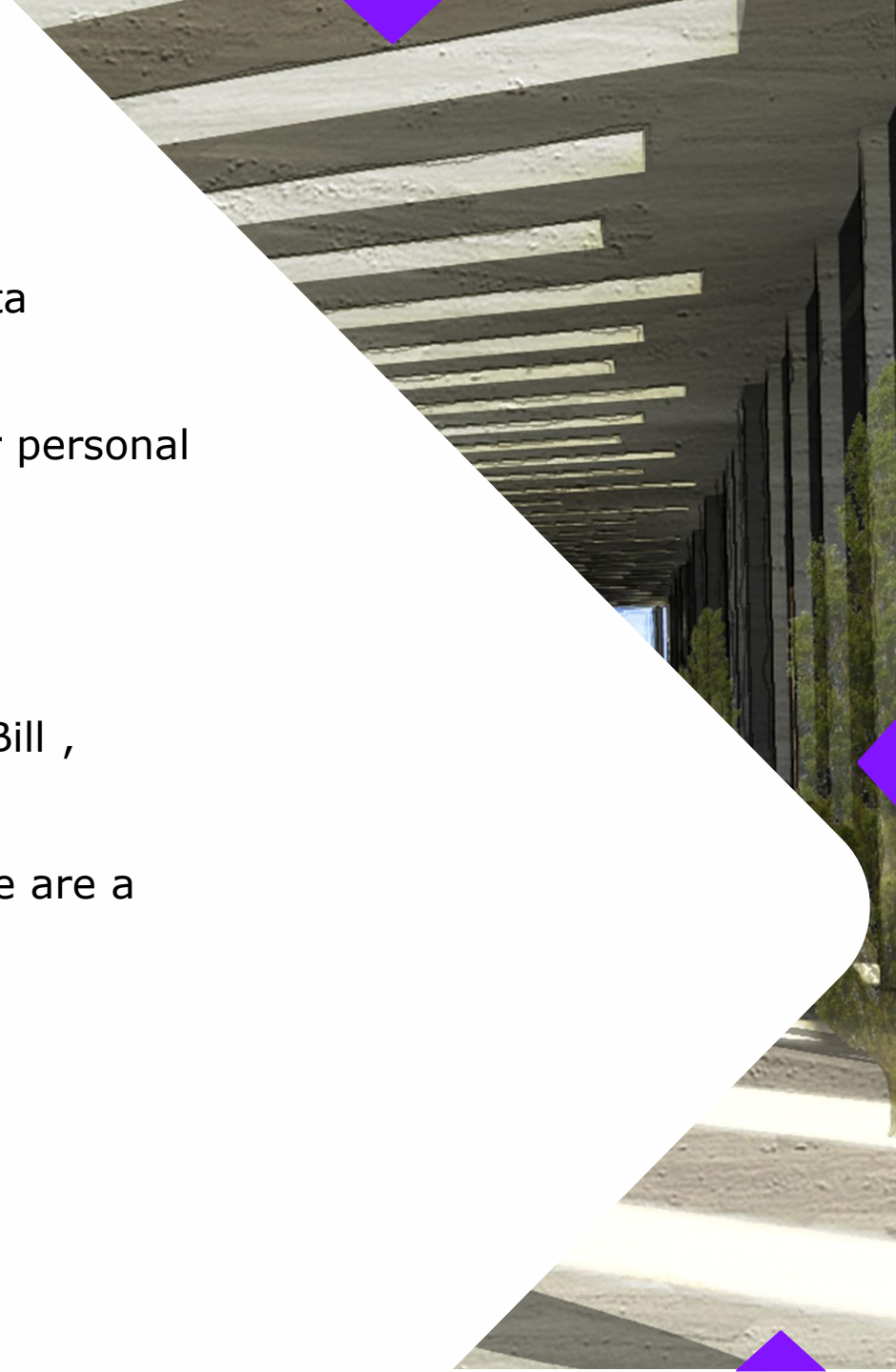
- Provide context on Data Protection in the UK
- to help you understand the key elements of the EU General Data Protection Regulation (GDPR)
- Outline the changes from the Data Protection Act to the GDPR
- Outline what the stages are for implementation of the UK's new Data Protection Act (2017)

EVENTMAP®

Don’t we already have Data Protection Laws

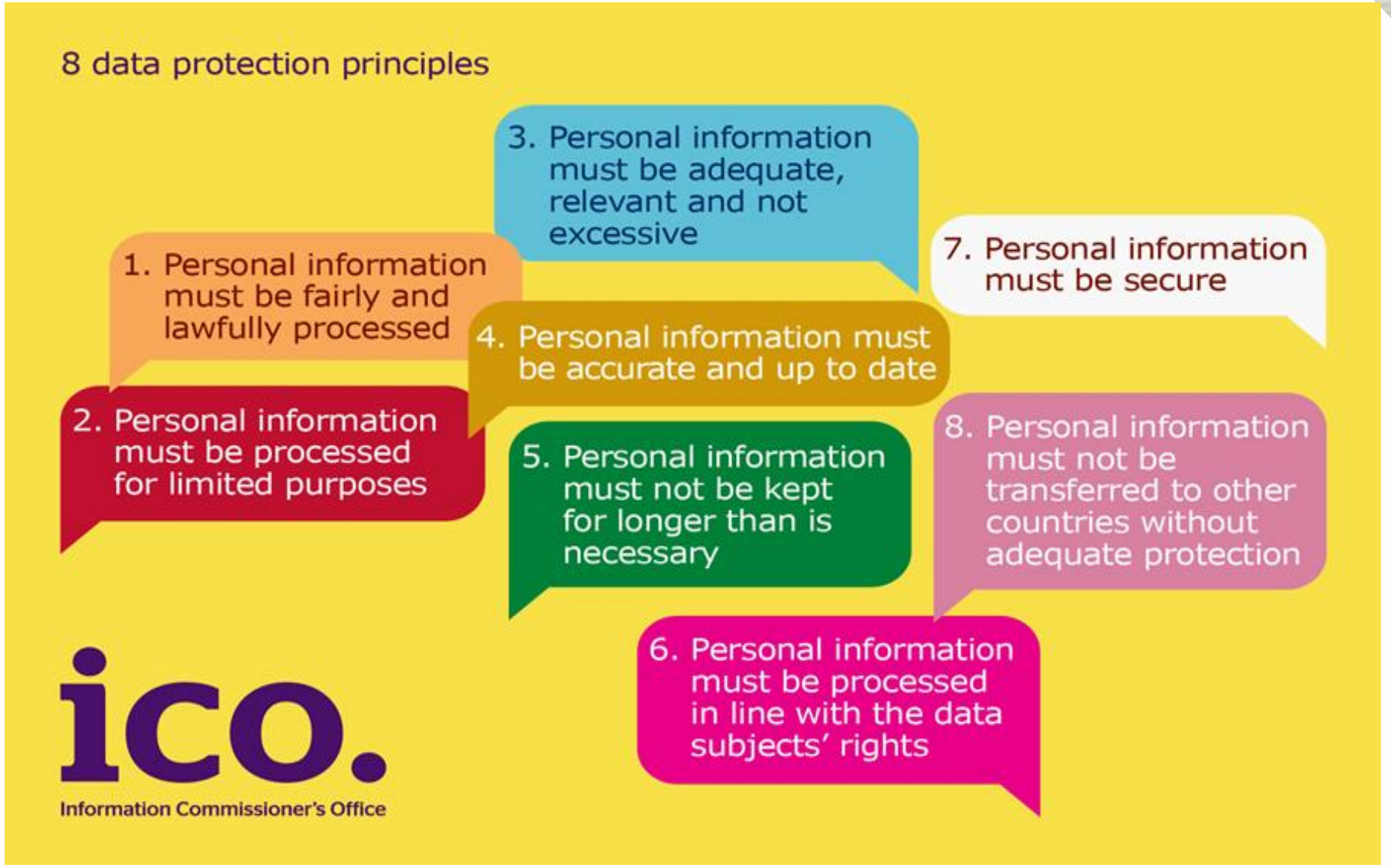
- Each member state in the EU operates under the current 1995 data protection regulation and has its own national laws.
- In the UK, the current Data Protection Act 1998 sets out how your personal information can be used by companies, government and other organisations.
- GDPR changes how personal data can be used.
- Its provisions in the UK will be covered by a new Data Protection Bill , which has now been published by the government.
- New UK Plans include everything within the GDPR – although there are a number of exemptions, specifically added protections for :
  - journalists,
  - scientific and historical researchers,
  - anti-doping agencies

  who handle people's personal information



EVENTMAP®

The Data Protection Act 1998



EVENTMAP®

What? Why? When?

- The GDPR is Europe's new framework for data protection laws
- It replaces the previous 1995 data protection directive, which current UK law is based.
- The Regulation is directly applicable and does not require any domestic law to be written, it must be implemented ‘as is’.
- Current DPA not fit for digital age
- Brexit does not affect the implementation of this regulation
- GDPR comes into force on 25th May 2018

What has been said about it

"A new law will ensure that the United Kingdom retains its world-class regime protecting personal data"

The Queen's Speech
21 June 2017

" … one way or another, GDPR is going to be an important part of the global data protection landscape over the years ahead, with great relevance to UK organisations, the public and their data."

Rob Luke
Deputy Commissioner, ICO
May 2017

"It's a horrific piece of legislation. It was designed for online retailers like Amazon, but it captures us. We have a lot of work to do to become compliant"

Chief Data Officer
Global Investment Bank

EVENTMAP®

GDPR - In Summary

Fines of up to 4% of annual global turnover

€'000 → **€'000,000**

Previously fines were limited in size and impact. GDPR fines will apply to both controllers and processors.

Increased territorial scope

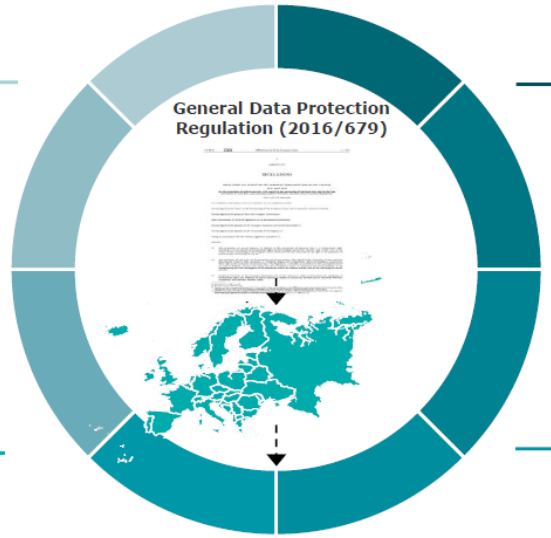
GDPR will apply to all companies processing the personal data of data subjects residing in the EU, regardless of the company's location.

Explicit and retractable consent

Must be provided in an intelligible and easily accessible form, using clear and plain language. It must be as easy to withdraw consent as it is to give it.

Right to access and portability

Data subjects can request confirmation as to whether or not personal data concerning them is being processed, where and for what purpose. Further, the controller shall provide a copy of the personal data, free of charge, in an electronic format.



Breach notification within 72 hours

Now mandatory that breaches, which are likely to "result in a risk for the rights and freedoms of individuals", are reported within 72 hours of first having become aware of the breach.

Privacy By Design

Now a legal requirement for the inclusion of data protection from the onset of the designing of systems, rather than a retrospective addition.

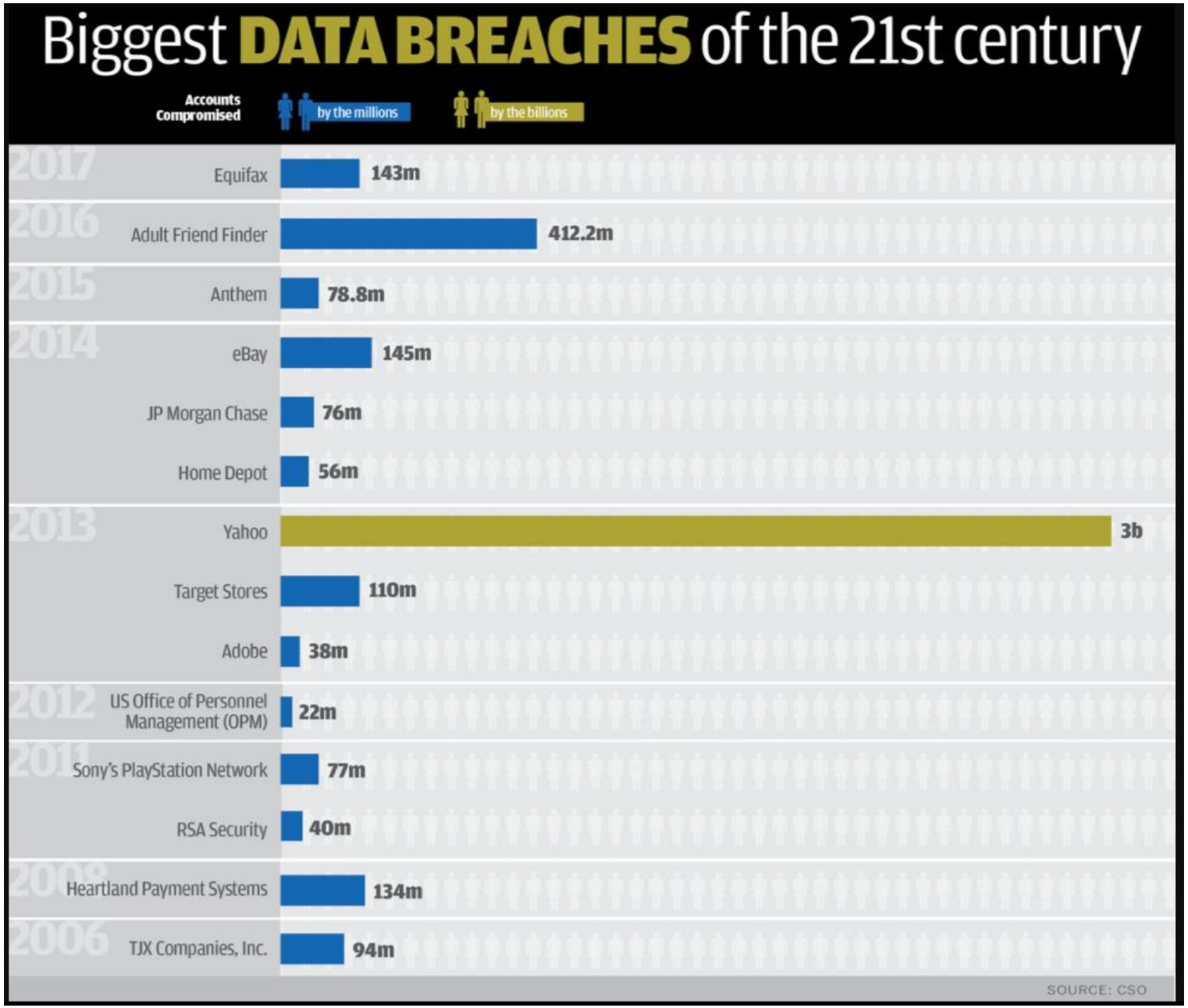
Right to be forgotten

Entitles the data subject to have the data controller erase his/ her personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

Mandatory Data Protection Officers

Appointed in certain cases (public authorities, when monitoring of data subjects on a large scale and when processing special categories of data). To facilitate the need for a company to demonstrate their compliance to the GDPR and compensate for GDPR no longer requiring the bureaucratic submission of notifications/ registrations of data processing activities or transfers based on Model Contract Clauses.

EVENTMAP®



CSO from IDG Publishing

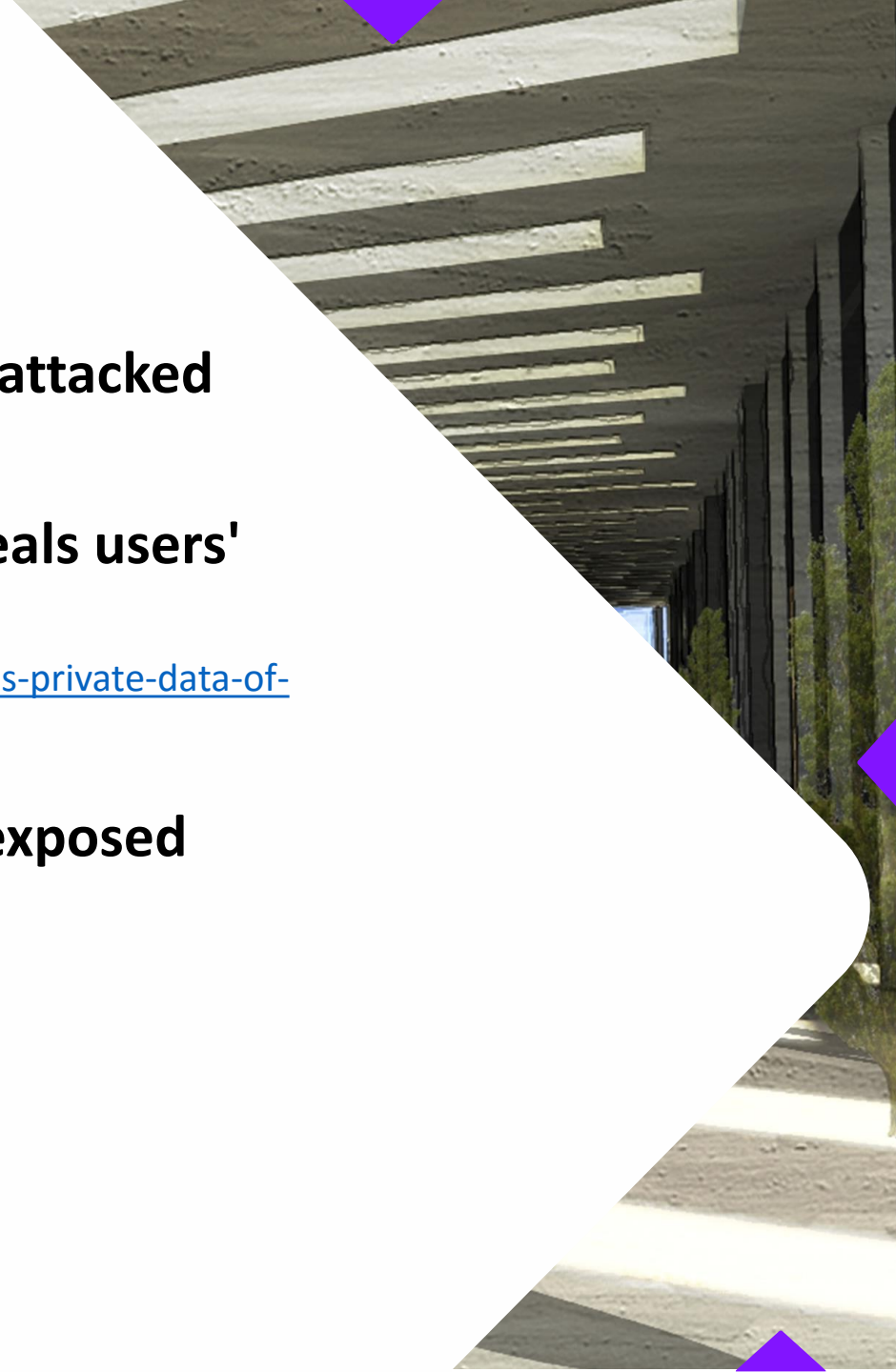
EVENTMAP®

31 of the most infamous data breaches

- Ai.Type
- Clarksons
- Uber
- Pizza Hut
- Yahoo
- Deloitte
- Equifax
- CEX
- 'Onliner' spambot
- Bupa (2017)
- Zomato
- 'Eddie' reveals over 560 million passwords
- Wonga
- Three
- Sports Direct
- Three Mobile
- Tesco Bank
- Sage
- Kiddicare
- TalkTalk
- Moonpig
- Think W3 Limited
- Mumsnet
- Staffordshire University
- Morrison's supermarket
- Yahoo
- Sony PlayStation Network
- Brighton and Sussex University Hospitals NHS Trust
- T-Mobile
- HM Revenue & Customs
- Nationwide Building Society

EVENTMAP®

Resent Data Breaches



29 Sept: Facebook security breach: Up to 50m accounts attacked

https://www.bbc.co.uk/news/technology-45686890

30 Sept: Major security flaw in Tory conference app reveals users' data

https://www.theguardian.com/politics/2018/sep/29/tory-conference-app-flaw-reveals-private-data-of-senior-mps

8 October: Google is killing Google+ after security flaw exposed user information

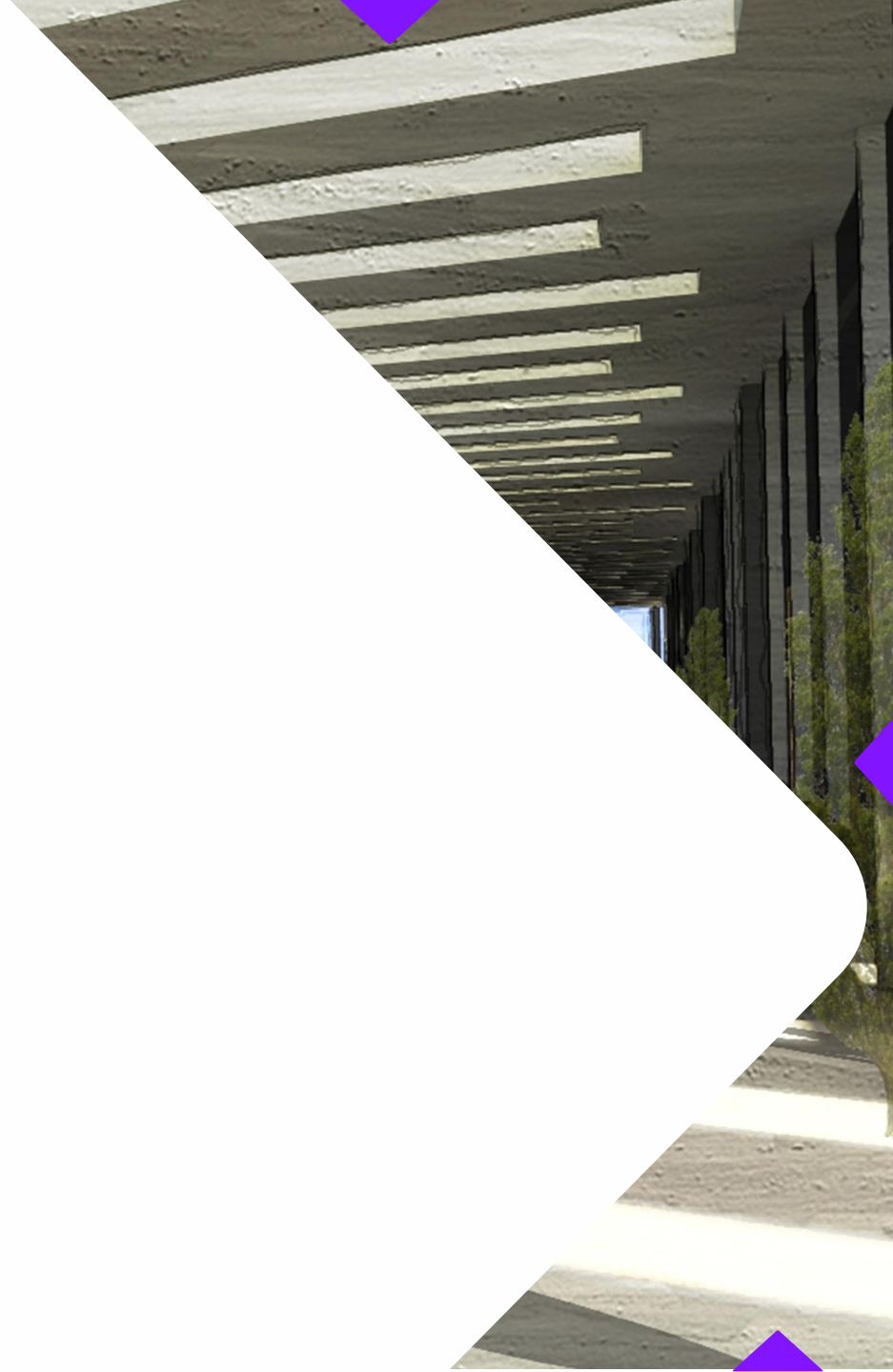
https://bgr.com/2018/10/08/google-plus-data-breach-profile-information/

EVENTMAP®

Seven Principles

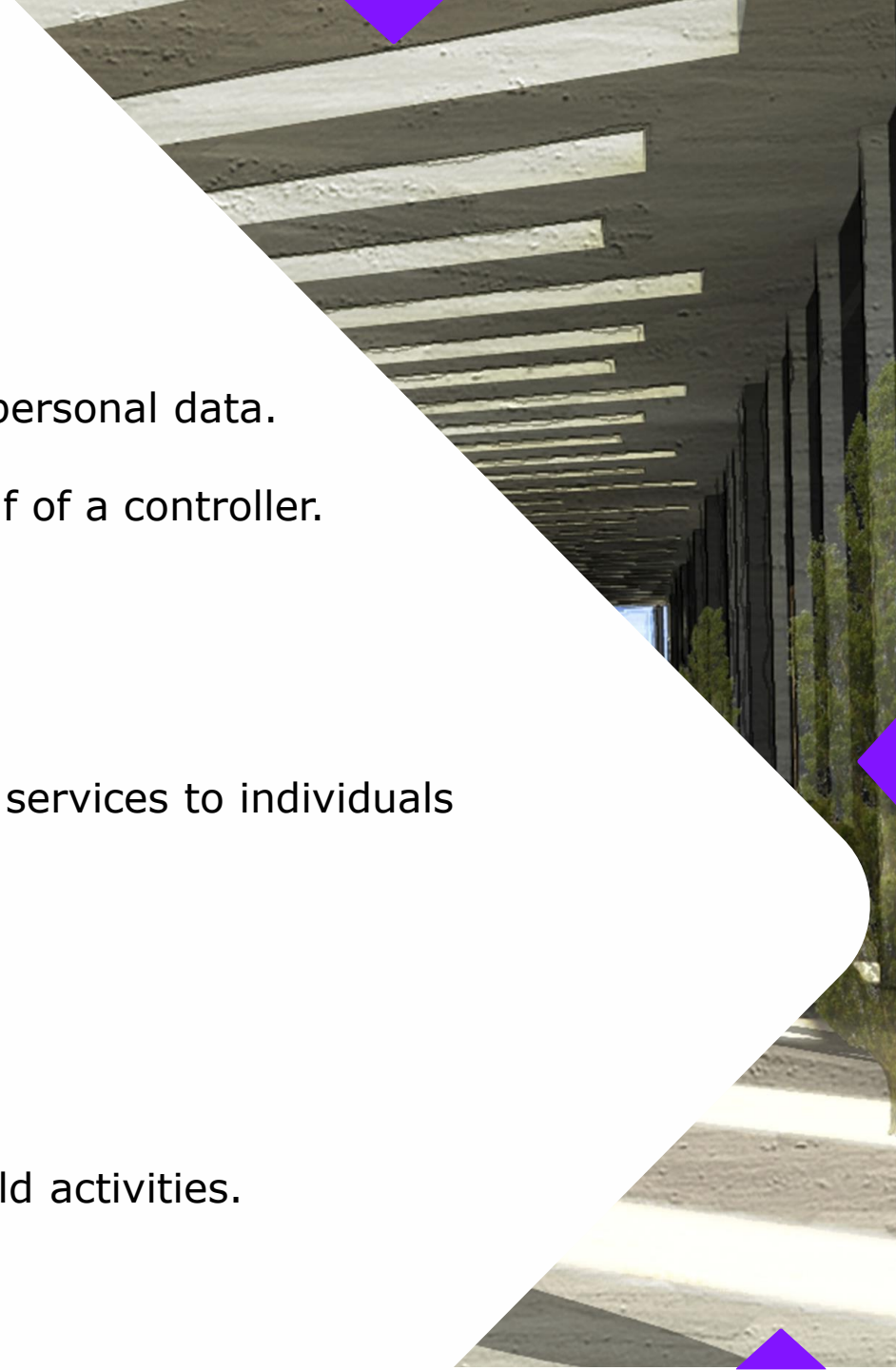
Article 5 of the GDPR requires that personal data shall be:

1. **Lawfulness, fairness and transparency**
2. **Purpose limitation**
3. **Data minimisation**
4. **Accuracy**
5. **Storage limitation**
6. **Integrity and confidentiality**
7. **Accountability**



EVENTMAP®

Who Does it Apply To



The GDPR applies to 'controllers' **and** 'processors'.

- A **controller** determines the purposes and means of processing personal data.
- A **processor** is responsible for processing personal data on behalf of a controller.

The GDPR applies to processing carried out:

- by organisations operating within the EU.
- it also applies to organisations outside the EU that offer goods or services to individuals in the EU.

The GDPR ***does not*** apply to certain activities including:

- processing covered by the Law Enforcement Directive,
- processing for national security purposes
- processing carried out by individuals purely for personal/household activities.

EVENTMAP®

What information does the GDPR apply to

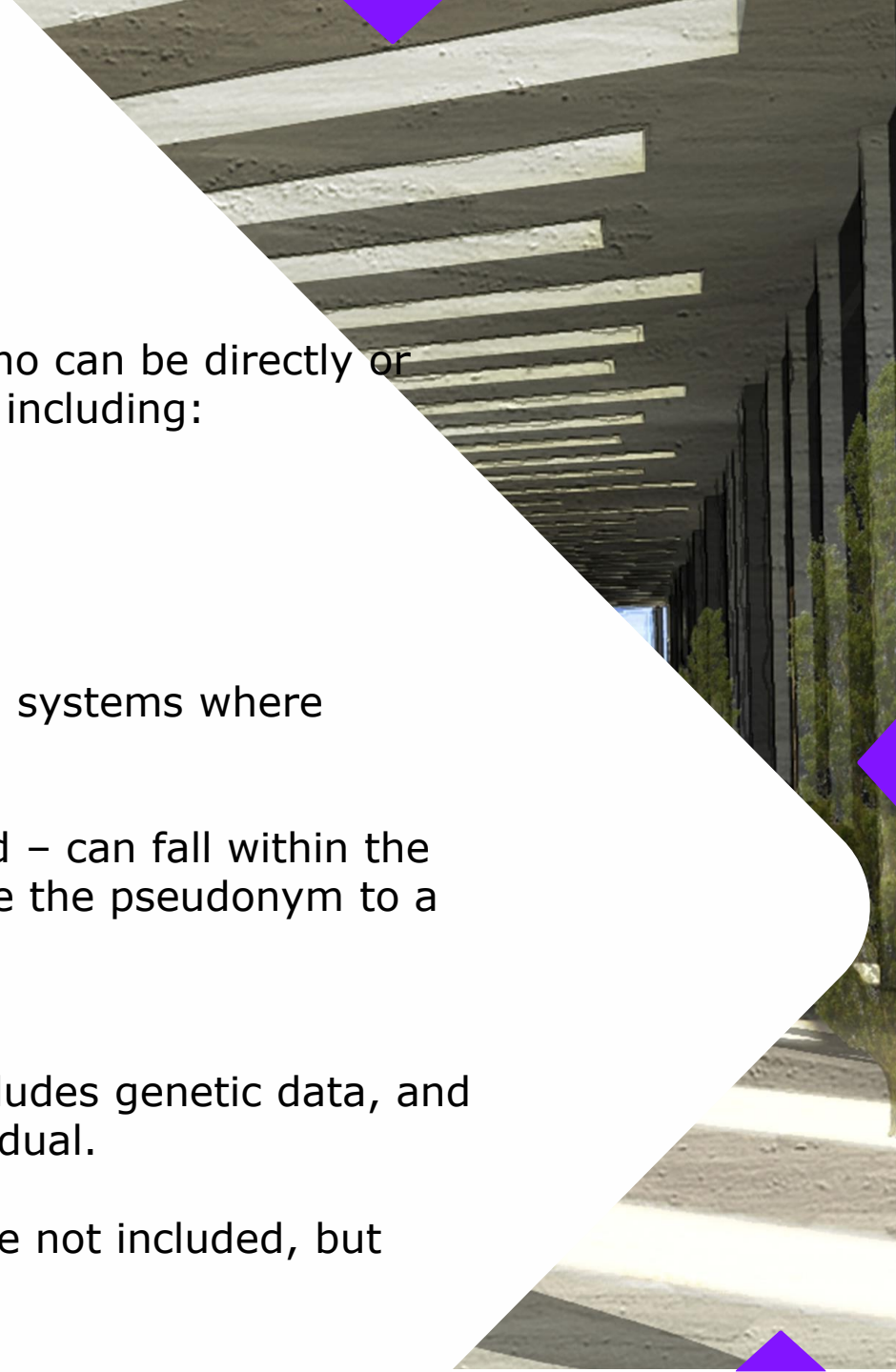
- **Personal data**
  - meaning any information relating to an identifiable person who can be directly or indirectly identified in particular by reference to an identifier, including:
    - Name
    - identification number
    - location data
    - online identifier

  - applies to both automated personal data and to manual filing systems where personal data are accessible according to specific criteria.

  - Personal data that has been pseudonymised – e.g. key-coded – can fall within the scope of the GDPR depending on how difficult it is to attribute the pseudonym to a particular individual.

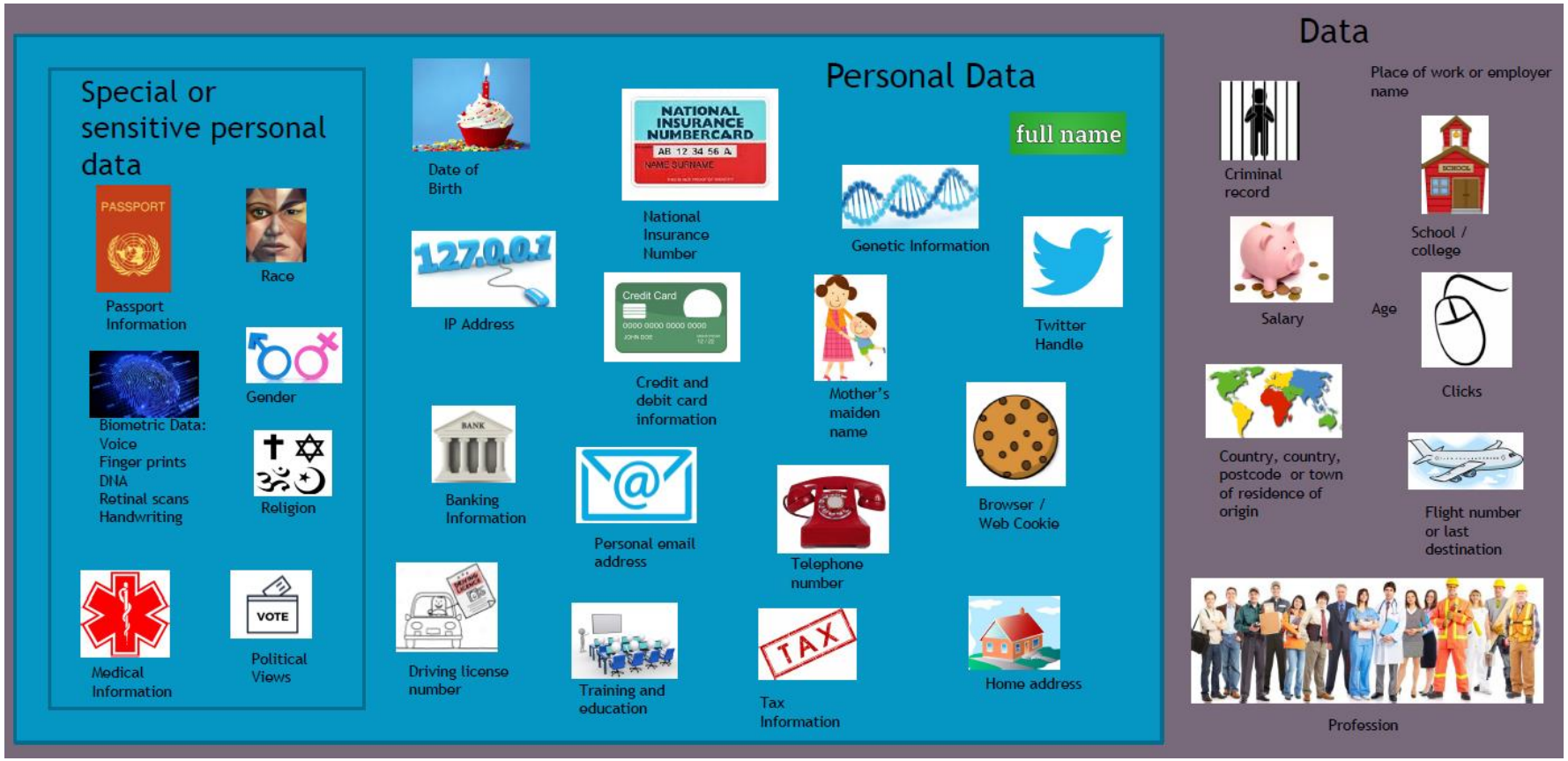
- **Sensitive personal data**
  - meaning "special categories of personal data" specifically includes genetic data, and biometric data where processed to uniquely identify an individual.

  - Personal data relating to criminal convictions and offences are not included, but similar extra safeguards apply to its processing



EVENTMAP®

Yes – pretty much everything



EVENTMAP®

Lawful Basis For Processing

- six available lawful bases for processing
  - **Consent** - requires a positive opt-in
  - **Contract** - to fulfil your contractual obligations to them; - because they have asked you to do something before entering into a contract
  - **Legal Obligation** - if you need to process the personal data to comply with a common law or statutory obligation
  - **Vital Interests** - if you need to process the personal data to protect someone's life
  - **Public Task** - in the exercise of official authority or public interest and law
  - **Legitimate Interests** - where you use people's data in ways they would reasonably expect and which have a minimal privacy impact, or where there is a compelling justification for the processing

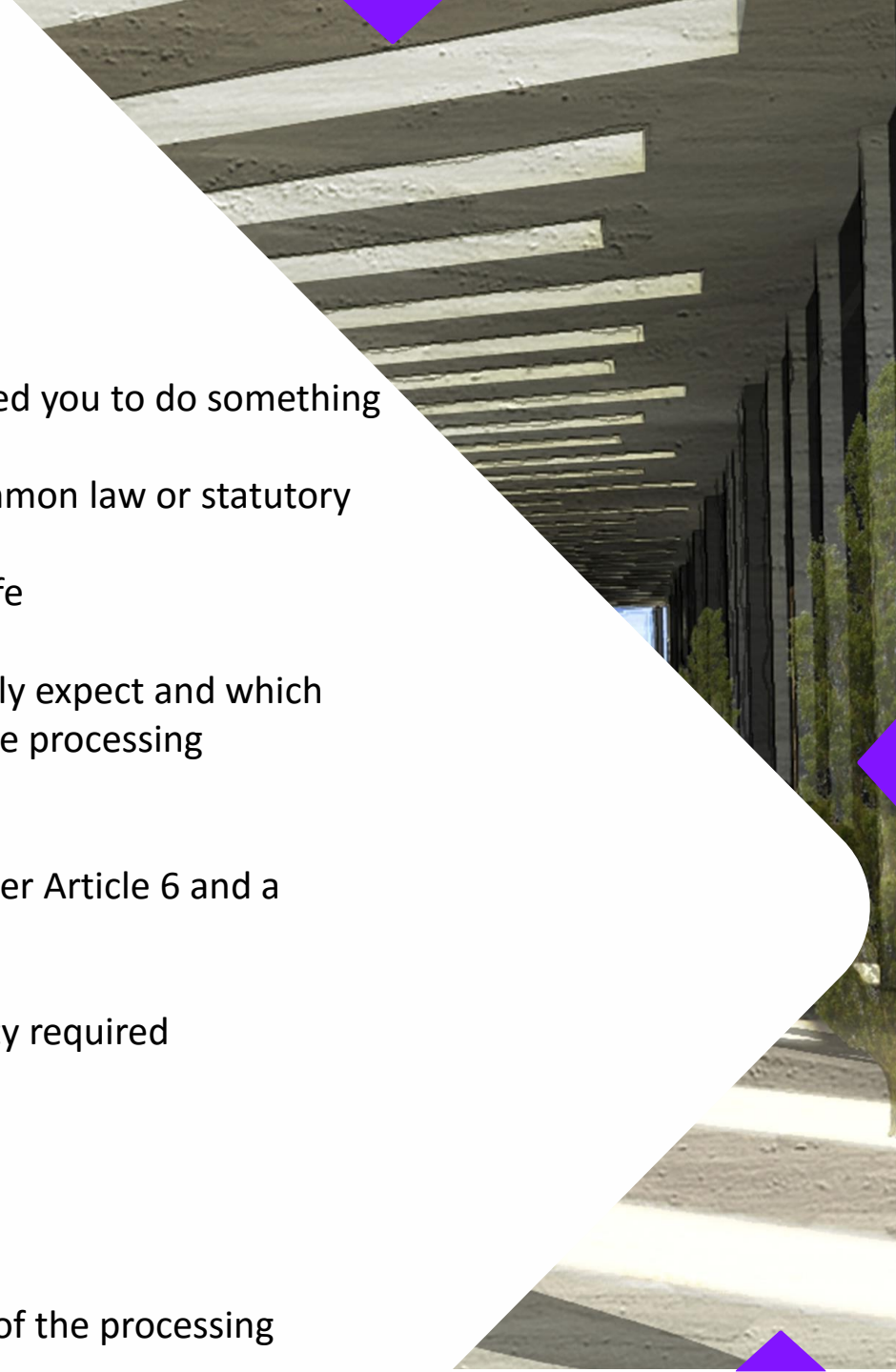
- For data which falls under
  - Special Category Data (10 conditions) - you must identify both a lawful basis under Article 6 and a separate condition for processing special category data under Article 9

  - Criminal Offence Data- as for special category data but additional lawful authority required

- no single basis is 'better' or more important than the others

- determine your lawful basis before you begin processing, and document it

- privacy notice should include your lawful basis for processing as well as the purposes of the processing

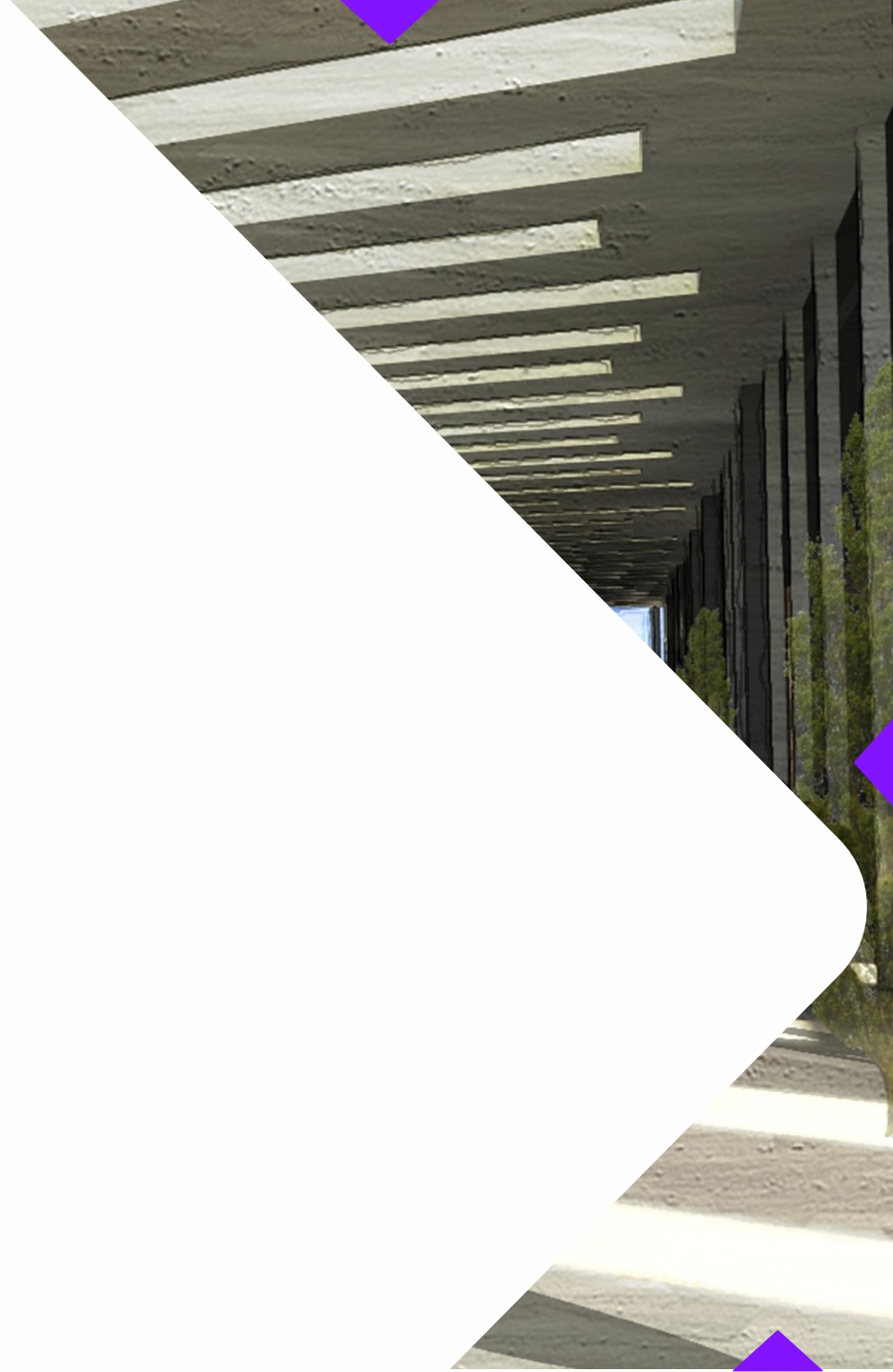


EVENTMAP®

Individual Rights

The GDPR provides the following rights for individuals:

- The right to be informed
- The right of access
- The right to rectification
- The right to erasure
- The right to restrict processing
- The right to data portability
- The right to object
- Rights in relation to automated decision making and profiling.

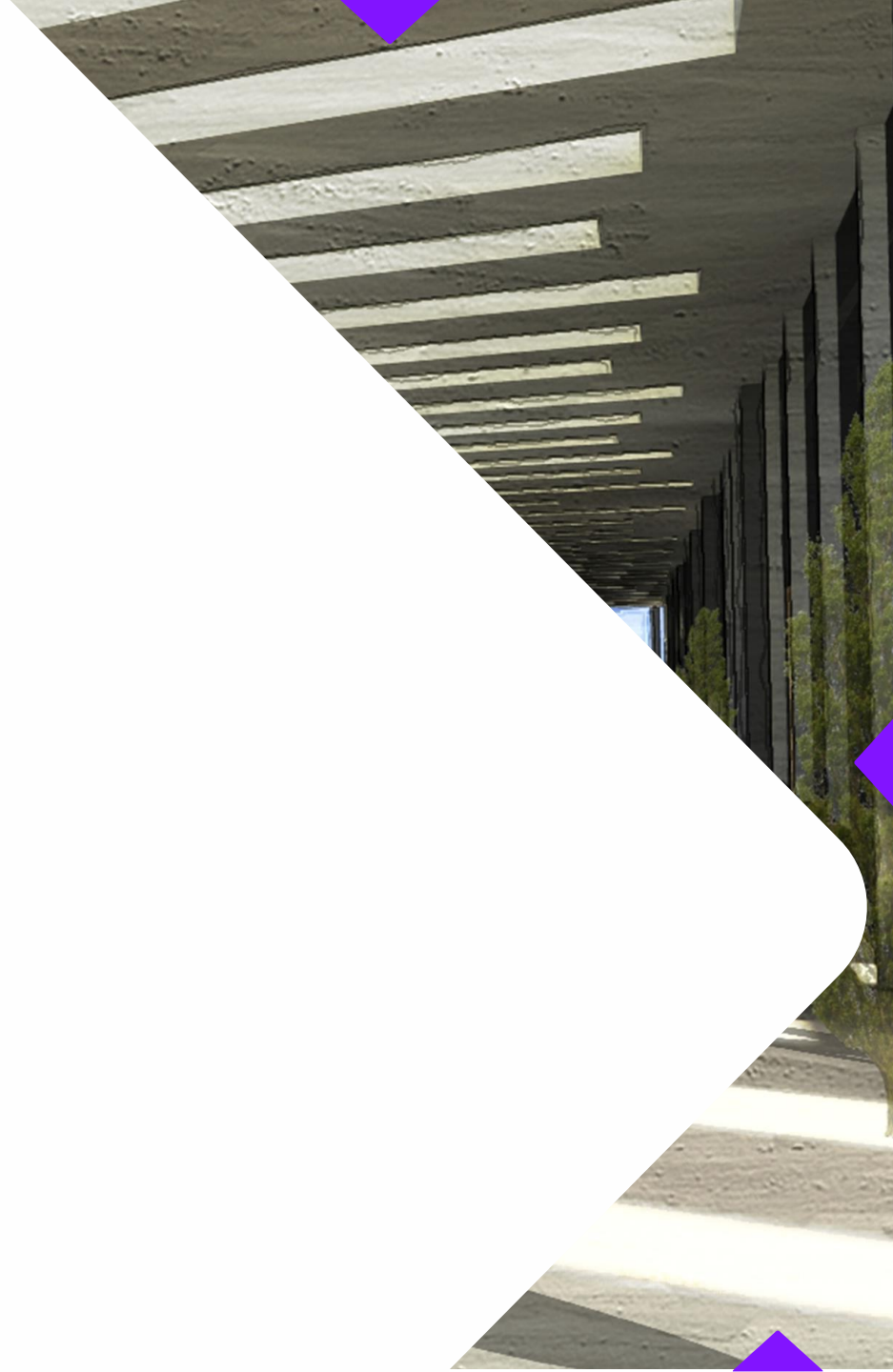


EVENTMAP®

Accountability and Governance

The GDPR promotes the need for:

- Contracts
- Documentation
- Data protection by design and default
- Data protection impact assessment
- Data Protection Officers
- Codes of Conduct and certification



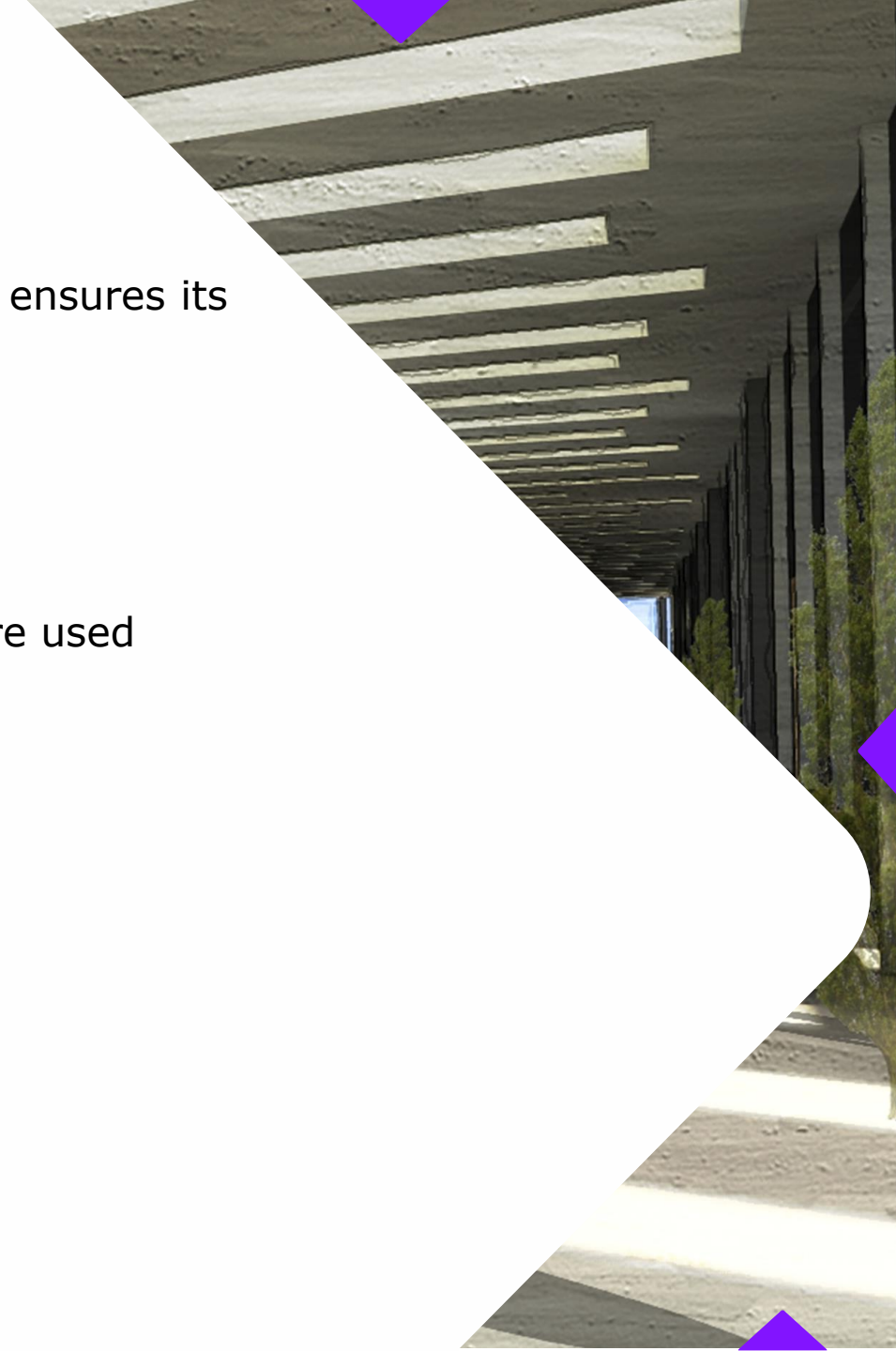
EVENTMAP®

Security

The GDPR requires personal data to be processed in a manner that ensures its security, including:

- protection against unauthorised or unlawful processing
- against accidental loss, destruction or damage

It requires that appropriate technical or organisational measures are used

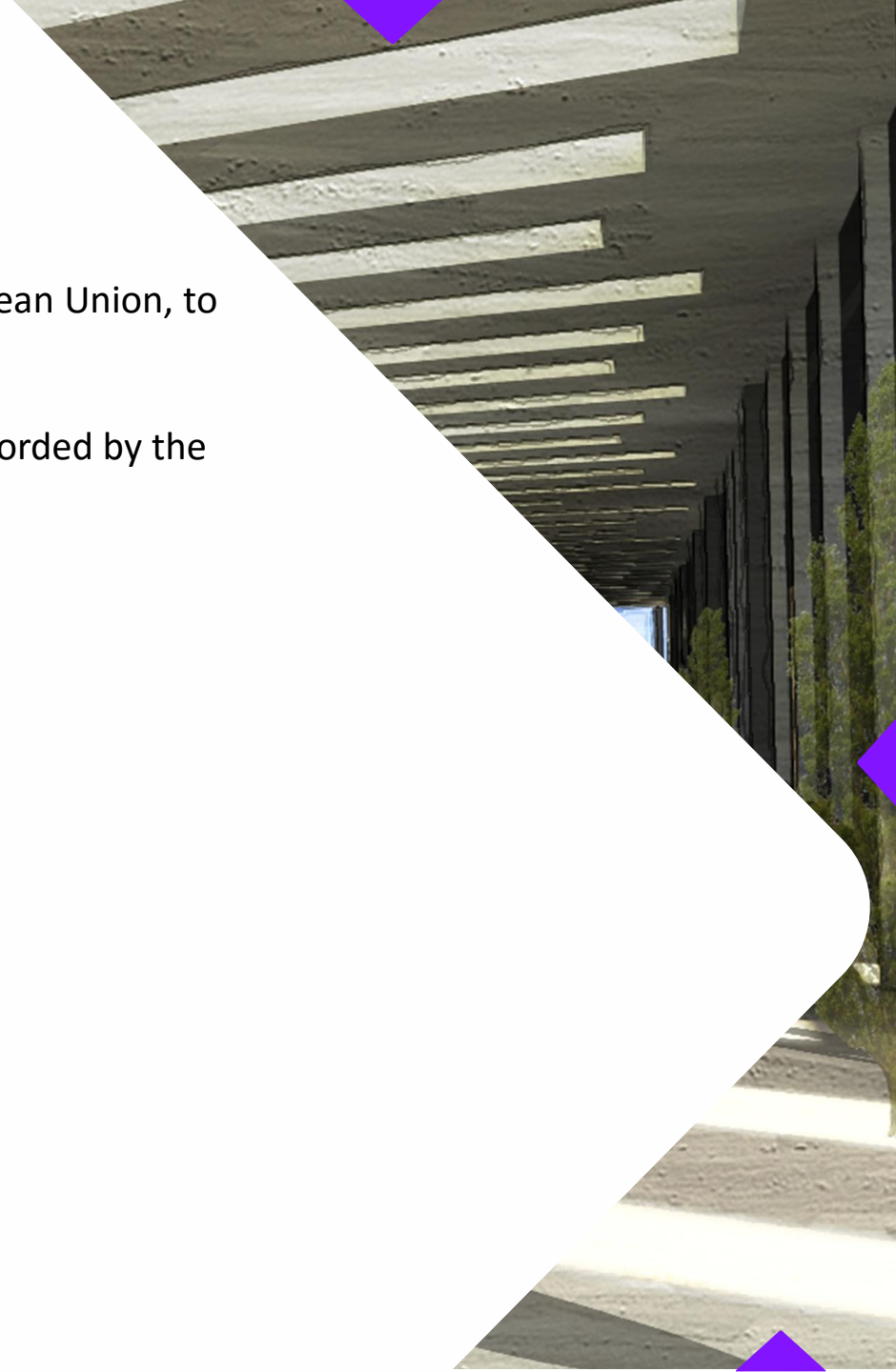


EVENTMAP®

International Transfers

The GDPR imposes restrictions on the transfer of personal data outside the European Union, to third countries or international organisations.

These restrictions are in place to ensure that the level of protection of individuals afforded by the GDPR is not undermined.

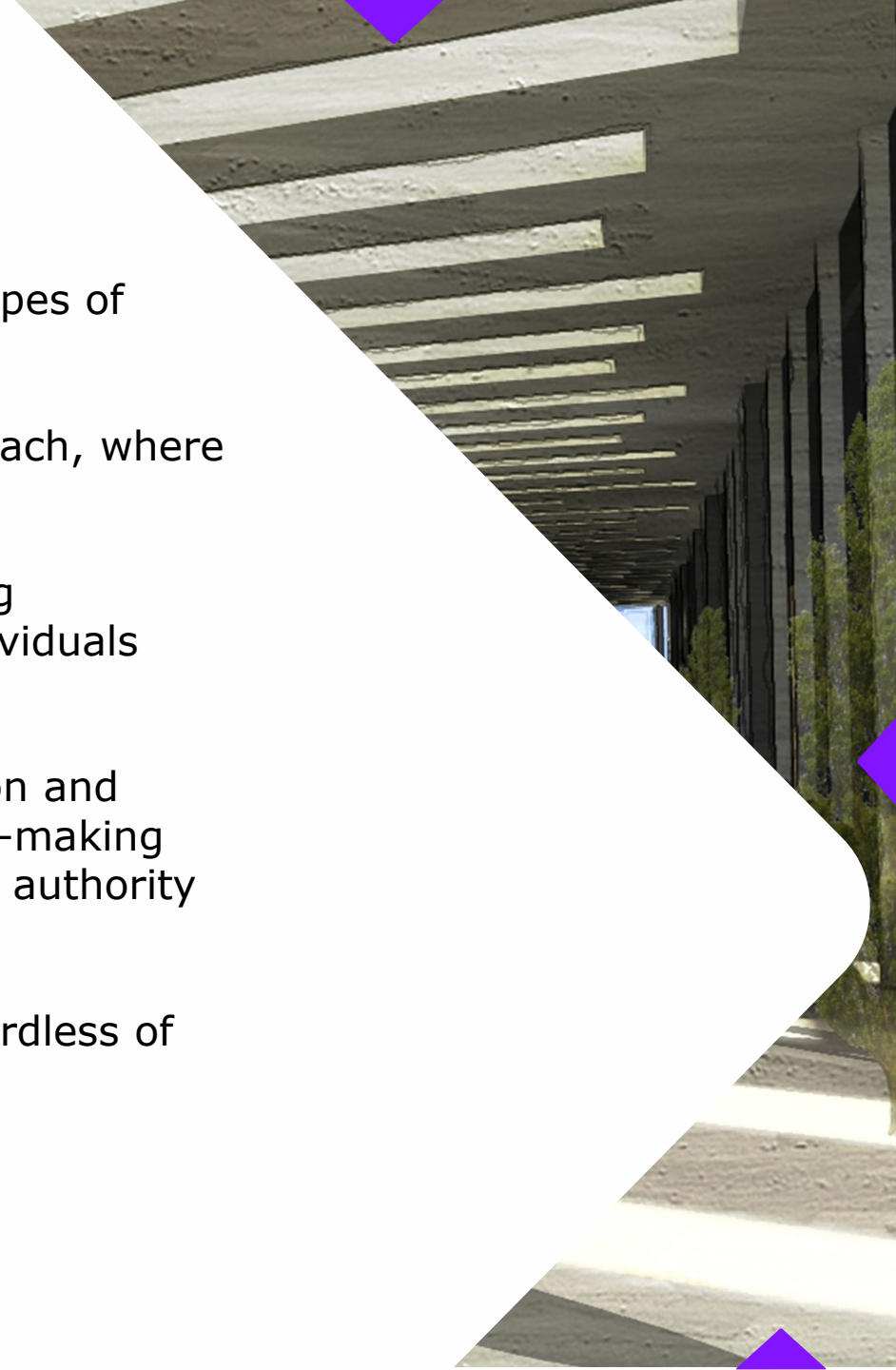


EVENTMAP®

Personal Data Breaches

The GDPR introduces a duty on all organisations to report certain types of personal data breach to the relevant supervisory authority.

- You must do this ***within 72 hours*** of becoming aware of the breach, where feasible.
- If the breach is likely to result in a high risk of adversely affecting individuals' rights and freedoms, you must also inform those individuals without undue delay.
- You should ensure you have robust breach detection, investigation and internal reporting procedures in place. This will facilitate decision-making about whether or not you need to notify the relevant supervisory authority and the affected individuals.
- You must also keep a record of any personal data breaches, regardless of whether you are required to notify



EVENTMAP®

Variations and Exemptions

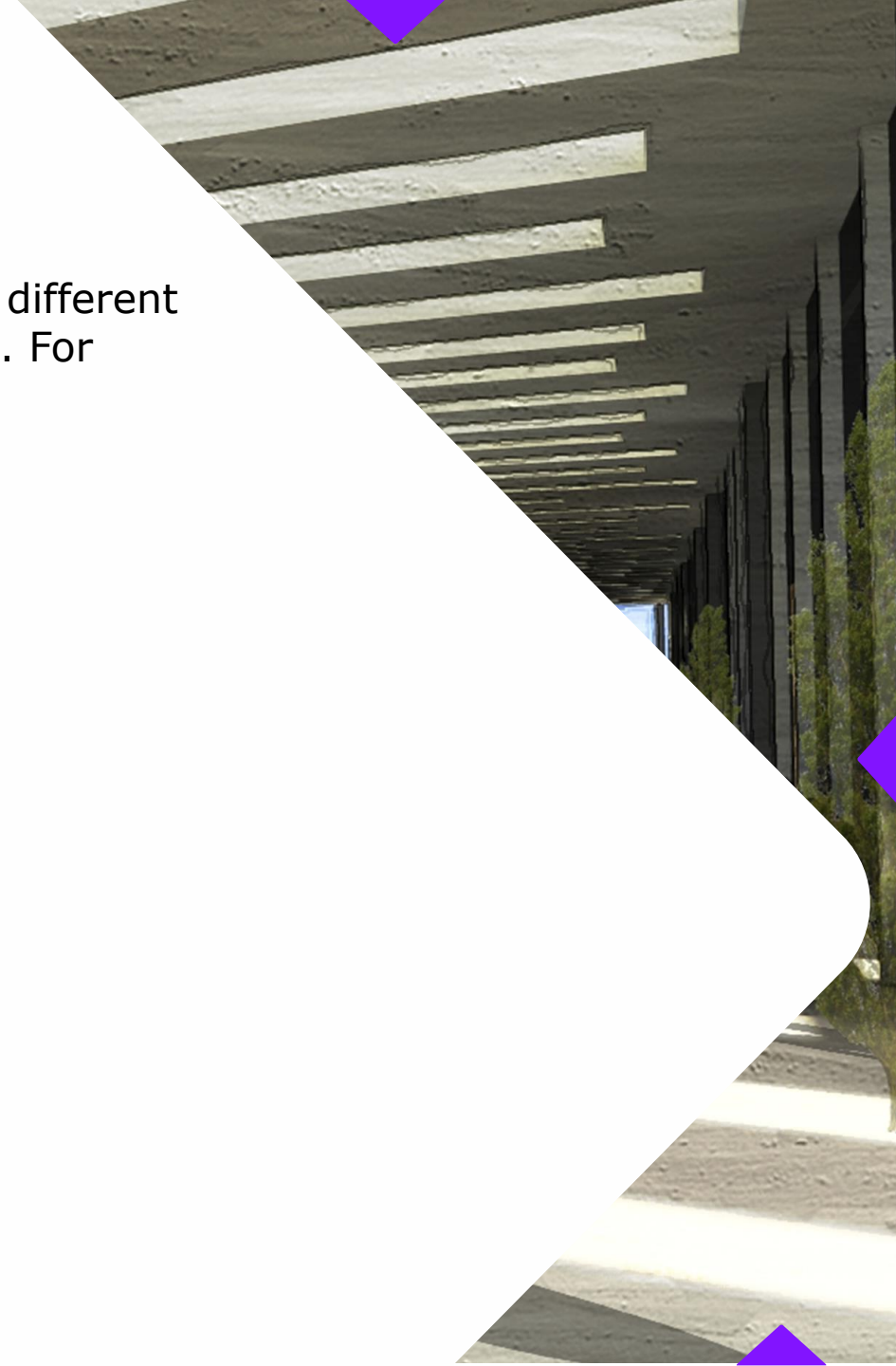
Member states are allowed to introduce variations and exemptions from the GDPR's transparency obligations and individual rights, but only where:

- ***the restriction respects the essence of the individual's fundamental rights and freedoms*** and
- **is a necessary and proportionate measure in a democratic society to safeguard**:
  - national security;
  - defence;
  - public security;
  - prevention, investigation, detection or prosecution of criminal offences;
  - other important public interests, in particular economic or financial interests, including budgetary and taxation matters, public health and security;
  - the protection of judicial independence and proceedings;
  - breaches of ethics in regulated professions;
  - monitoring, inspection or regulatory functions connected to the exercise of official authority regarding security, defence, other important public interests or crime/ethics prevention;
  - the protection of the individual, or the rights and freedoms of others; or
  - the enforcement of civil law matters..

EVENTMAP®

Guidance

To assist organisations in applying the requirements of the GDPR in different contexts, we are working to produce guidance in a number of areas. For example, children’s data, CCTV, big data, etc

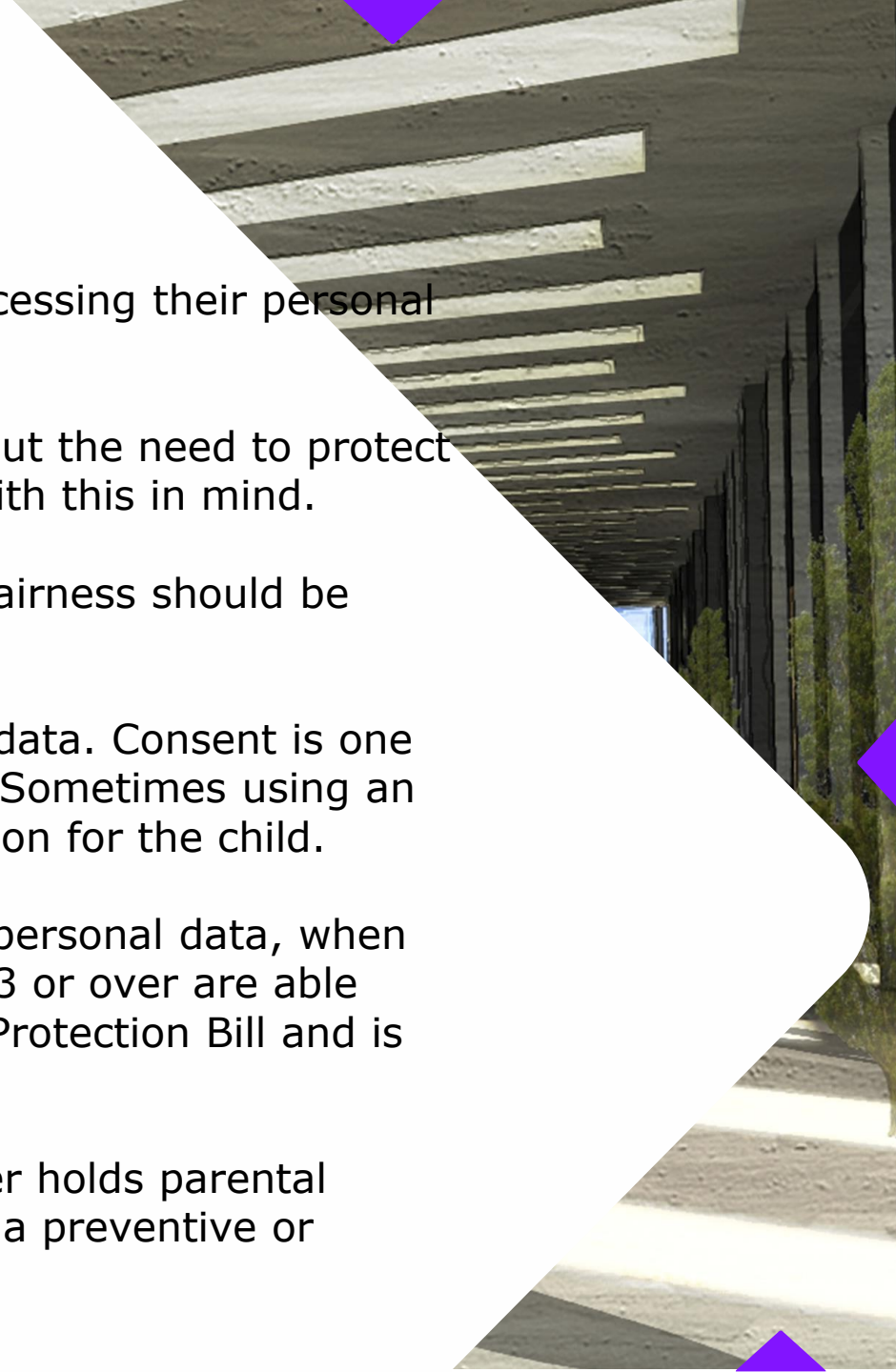


EVENTMAP®

Children

Children need particular protection when you are collecting and processing their personal data because they may be less aware of the risks involved.

- If you process children's personal data then you should think about the need to protect them from the outset, and design your systems and processes with this in mind.
- Compliance with the data protection principles and in particular fairness should be central to all your processing of children's personal data.
- You need to have a lawful basis for processing a child's personal data. Consent is one possible lawful basis for processing, but it is not the only option. Sometimes using an alternative basis is more appropriate and provides better protection for the child.
- If you are relying on consent as your lawful basis for processing personal data, when offering an online service directly to a child, only children aged 13 or over are able provide their own consent.(This is the age proposed in the Data Protection Bill and is subject to Parliamentary approval).
- For children under this age you need to get consent from whoever holds parental responsibility for the child - unless the online service you offer is a preventive or counselling service.



EVENTMAP®

Sources and Further Reading

Information Commissioners Office on GDPR - https://ico.org.uk/for-organisations/guide-to-the-general-data-protection-regulation-gdpr/

ICO on Privacy By Design - https://ico.org.uk/for-organisations/guide-to-data-protection/privacy-by-design/

EU Directive - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0089.01.ENG&toc=OJ:L:2016:119:TOC

EU Regulation - http://eur-lex.europa.eu/legal-content/EN/TXT/?uri=uriserv:OJ.L_.2016.119.01.0001.01.ENG&toc=OJ:L:2016:119:TOC

UK Data Protection Act 1998 - http://www.legislation.gov.uk/ukpga/1998/29/contents

UK Data Protection Bill 2017 - https://www.gov.uk/government/collections/data-protection-bill-2017

EU Data Breaches- https://www.techworld.com/security/uks-most-infamous-data-breaches-3604586/