



**TwoBlackLabs**

Working together to manage privacy risk

# GDPR and New Zealand



# What is the GDPR and who is covered?



# GDPR Introduction and Aim

- GDPR stands for '**General Data Protection Regulation**'.
- It was enacted in 2016 and came into full effect on 25 May 2018.
- The aim of the GDPR is to give individuals (known as '*data subjects*') better control over their personal information held by organisations.
- The regulation focuses on keeping businesses more transparent and expanding the privacy rights of data subjects.
- Organisations are required to '*implement appropriate technical and organisations measures*' in relation to the nature, scope, context and purposes of their handling and processing of personal information.
- Fines for non compliance can be up to 4% of annual turnover or 20 million Euros which ever is the larger amount.

# Which individuals are covered by the GDPR?

4

Firstly some key characteristics of the individual:

- Living natural individuals
- Nationality is not a factor as to if the person is covered by the GDPR.

The individual is then covered by the GDPR if:

- They are in the European Union when their information is processed.
- They are interacting with an organisation who is established in the European Union.



BIOMETRICS

DATA  
REGULATIONPERSONAL  
FILE STORAGE

PRIVACY POLICY

GLOBAL  
COMPLIANCETECHNICAL  
SECURITY

PROTECTION

# Which organisations does GDPR apply to?

# Are you a controller, processor or both?

6



**Controller**

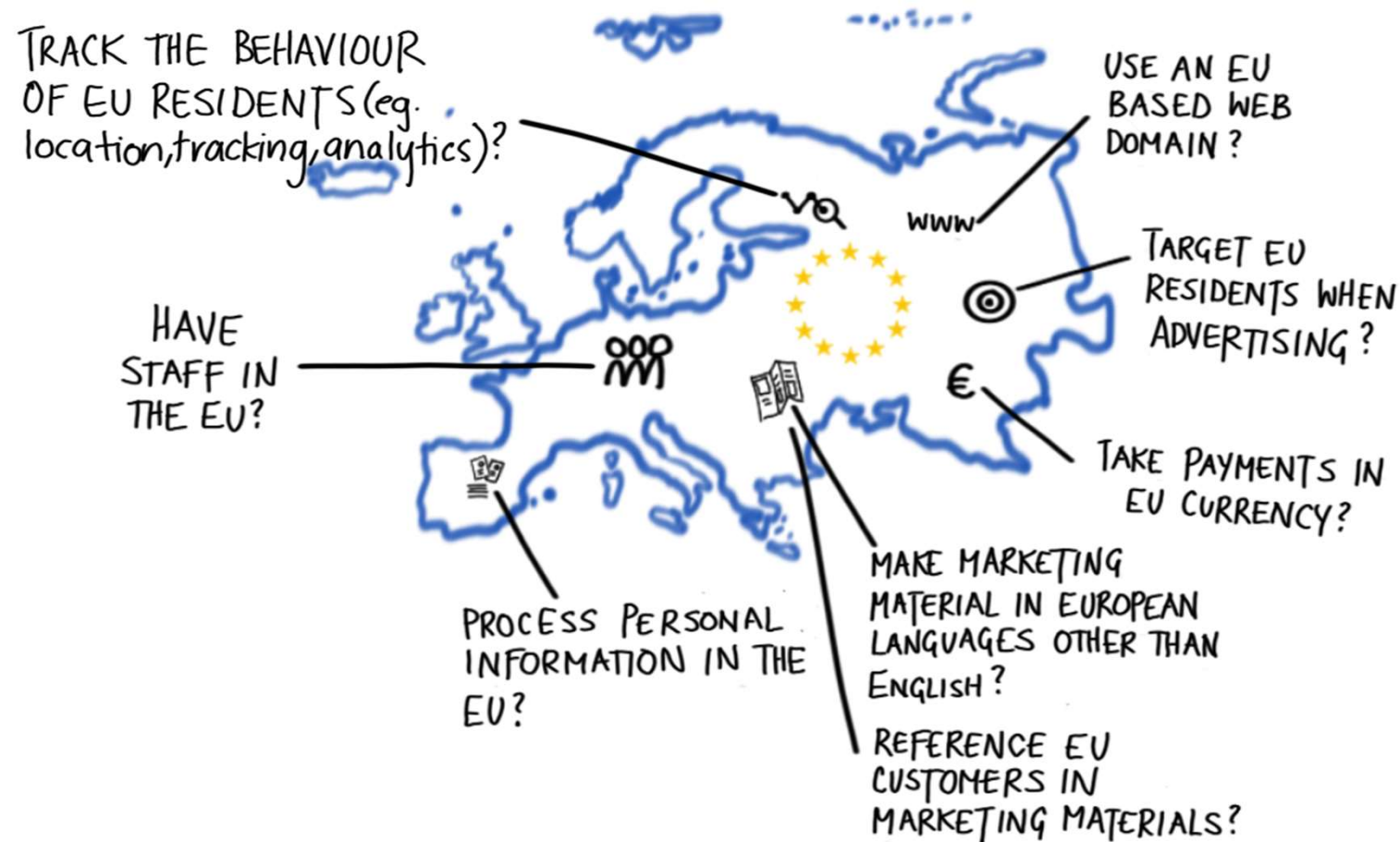


**Processor**



# Which controllers are in scope?

7



BIOMETRICS

DATA  
REGULATIONPERSONAL  
FILE STORAGE

PRIVACY POLICY

GLOBAL  
COMPLIANCETECHNICAL  
SECURITY

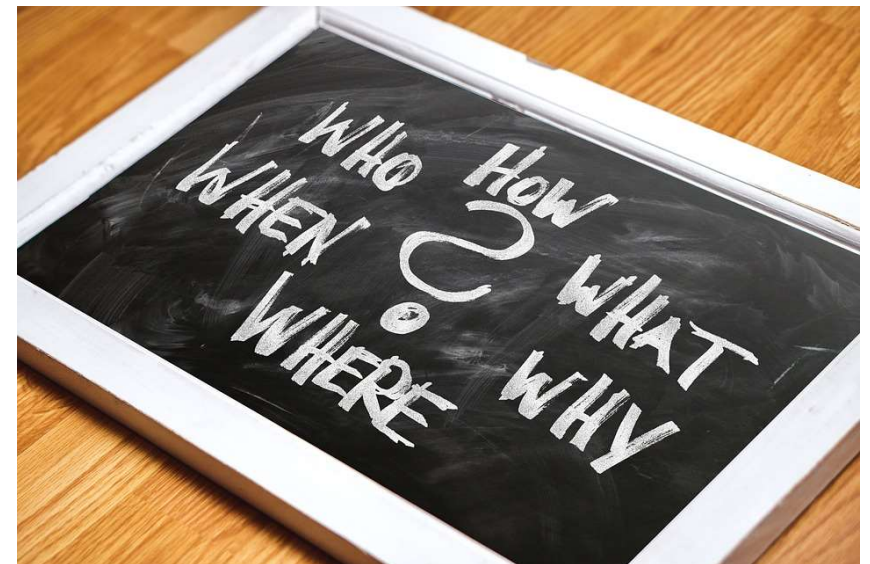
PROTECTION

# What is required for GDPR compliance?



# What are the principles?

- Lawfulness, fairness and transparency
- Purpose limitation
- Data minimisation
- Accuracy
- Storage limitation
- Integrity and confidentiality



# What are the key differences?



The GDPR widens the definition of personal data.



The GDPR tightens the rules for obtaining valid consent to using personal information.



The GDPR makes the appointment of a DPO mandatory for certain organisations.



The GDPR introduces mandatory PIAs.

# What are the key differences?



The GDPR introduces a common data breach notification requirement.



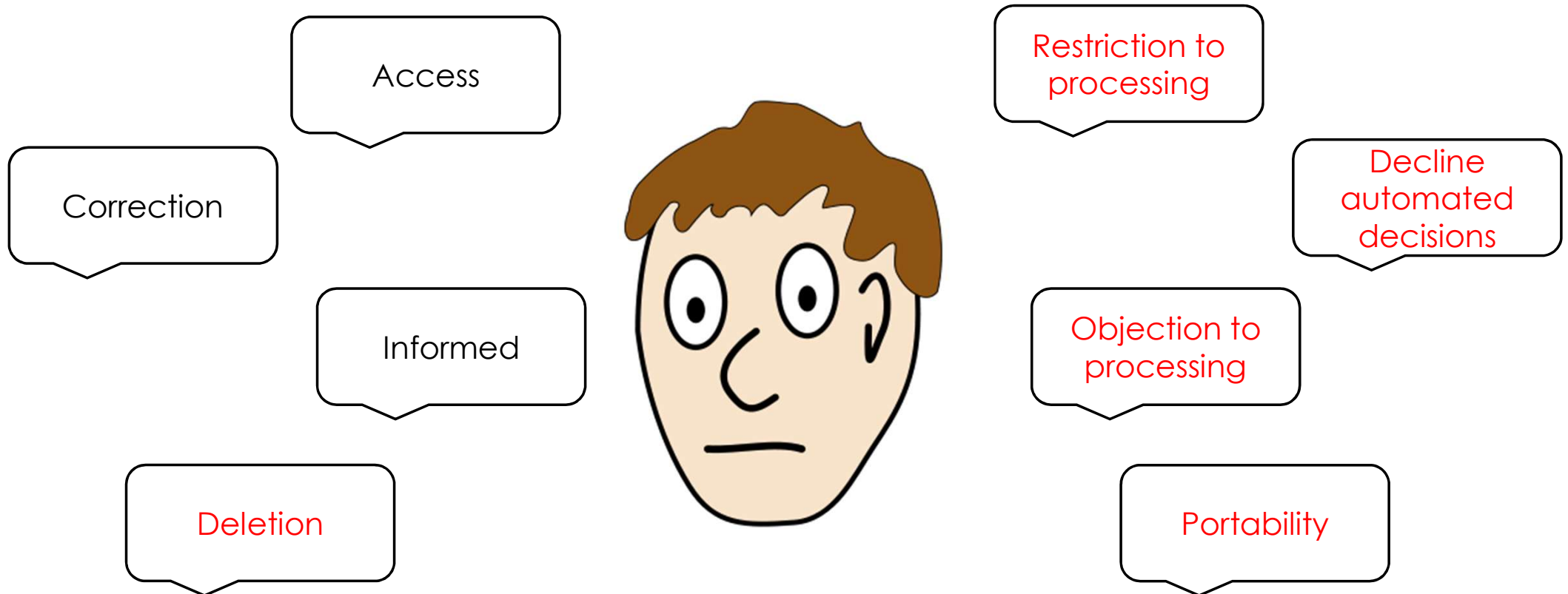
The GDPR expands liability beyond data controllers



The GDPR requires 'Privacy by Design'

# What rights does an individual have?

12



BIOMETRICS

DATA  
REGULATIONPERSONAL  
FILE STORAGE

PRIVACY POLICY

GLOBAL  
COMPLIANCETECHNICAL  
SECURITY

PROTECTION

# What is the impact of Brexit?



# What happens if there is a no deal?

- One Stop Shop
- Transfers to the UK
- Binding Corporate Rules
- Representatives
- Breach reporting

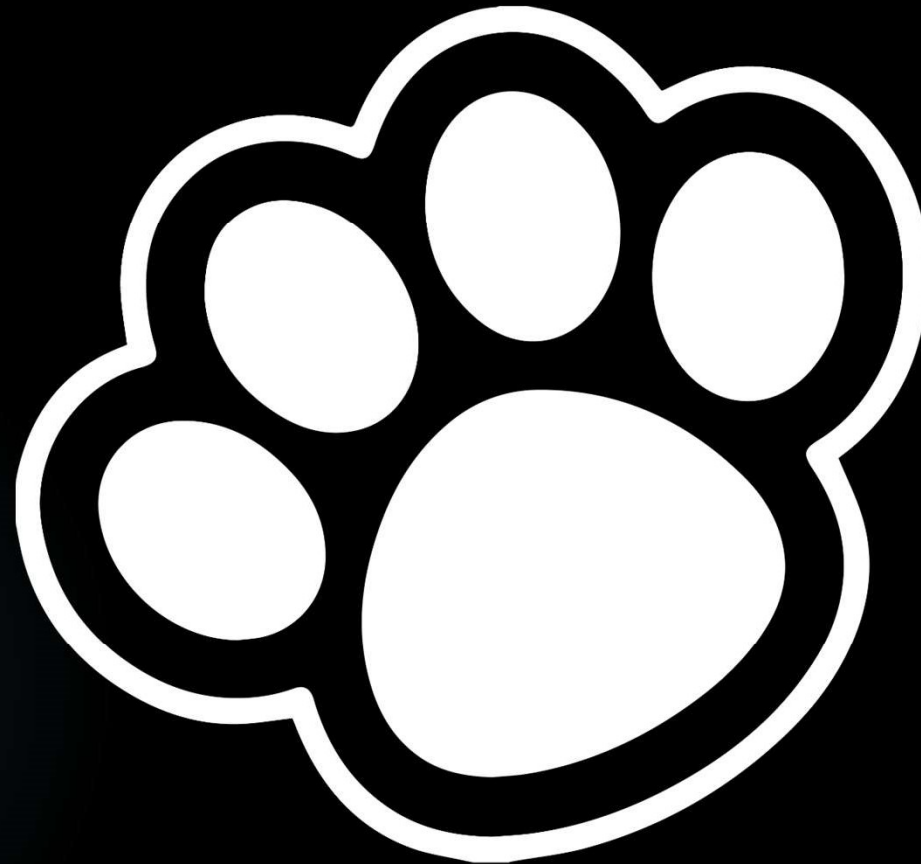


The UK Government intends to remain the extraterritorial scope within their legislation.

# Questions

15





[www.twoblacklabs.co.nz](http://www.twoblacklabs.co.nz)