



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

DATA
PROTECTIONTECHNICAL
SECURITYGLOBAL
COMPLIANCE

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

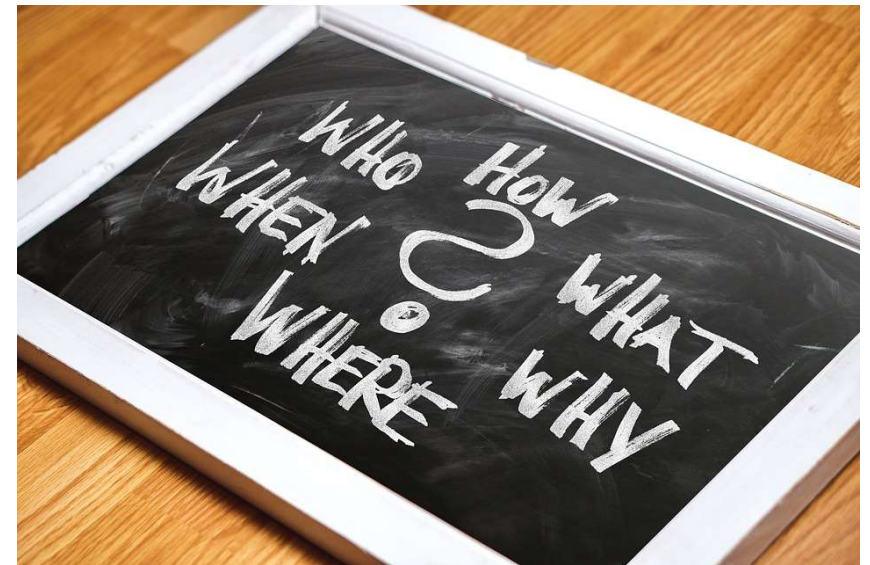
GLOBAL
COMPLIANCETECHNICAL
SECURITY

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.



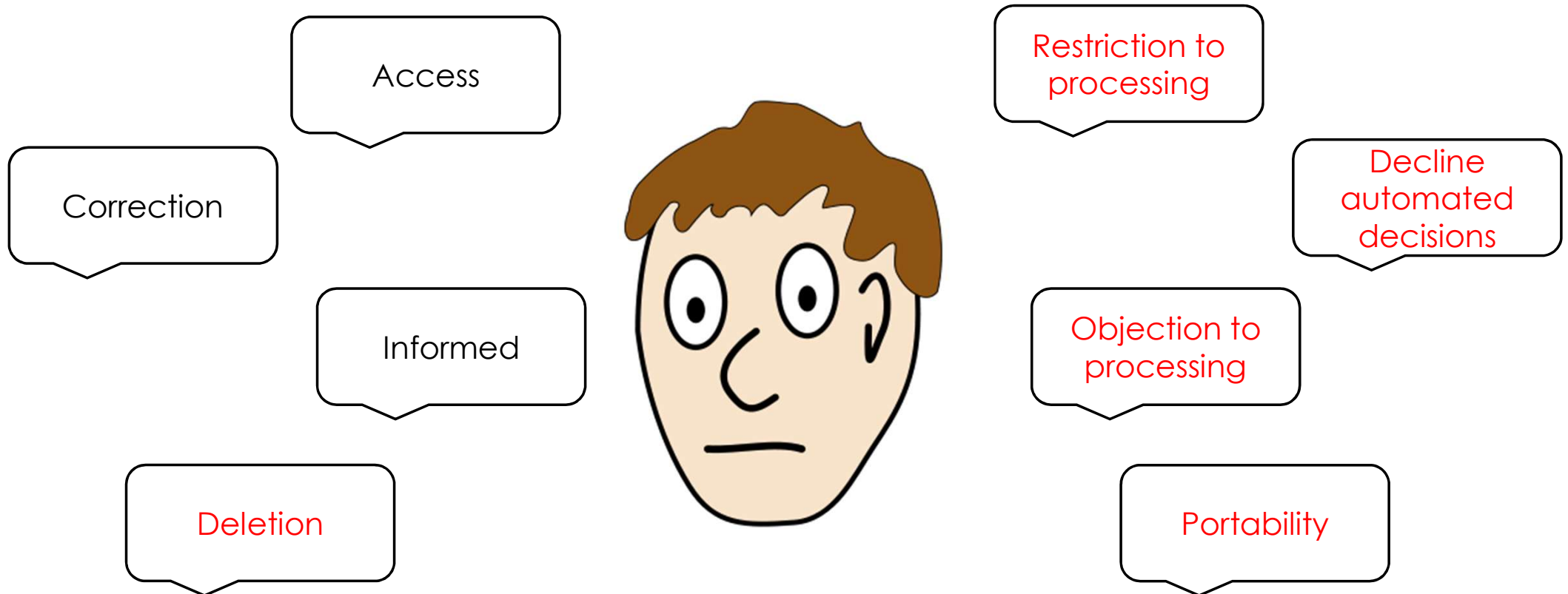
The GDPR expands liability beyond data controllers



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 retain the extraterritorial scope within their legislation.

Questions

15



GDPR APPLIES IF YOU

QUALIFY

DOES GDPR APPLY TO ME?

CONTROLLER OR PROCESSOR

CONTROLLER
IF YOU DECIDE WHAT INFORMATION TO COLLECT, FOR WHAT PURPOSE AND HOW IT SHOULD BE USED. YOU ARE A

PROCESSOR
IF YOU PROCESS INFORMATION ON BEHALF OF A CONTROLLER ON THEIR INSTRUCTIONS YOU ARE A

(DIFFERENT PARTS OF YOUR ORGANISATION CAN BE BOTH)

TRACK THE BEHAVIOUR OF EU RESIDENTS (eg. location, tracking, analytics)?

USE AN EU BASED WEB DOMAIN?

HAVE STAFF IN THE EU?

PROCESS PERSONAL INFORMATION IN THE EU?

TARGET EU RESIDENTS WHEN ADVERTISING?

TAKE PAYMENTS IN EU CURRENCY?

MAKE MARKETING MATERIAL IN EUROPEAN LANGUAGES OTHER THAN ENGLISH?

REFERENCE EU CUSTOMERS IN MARKETING MATERIALS?

DO YOU PROCESS PERSONAL INFORMATION IN THE EU FOR OTHERS?

DO YOU HANDLE INFORMATION ABOUT EU RESIDENTS FOR A CUSTOMER?

HAS A CUSTOMER ASKED YOU TO BE GDPR COMPLIANT?

DO CUSTOMER CONTRACTS MANDATE YOU TO BE GDPR COMPLIANT?

Personal Information in the EU is WIDER than the NZ definition. It includes anonymised and pseudonymised data.

ASSESS

72 HOURS
THE CONTROLLER HAS TO REPORT A BREACH TO THE SUPERVISORY AUTHORITY ONCE AWARE OF THE BREACH

BREACHES
RISK TO INDIVIDUALS
NOTIFY THEM WITHOUT DELAY

DATA PROCESSING AGREEMENTS
PRIOR TO PERSONAL INFORMATION BEING PROVIDED TO A PROCESSOR, THE CONTROLLER IS REQUIRED TO HAVE A DATA PROCESSING AGREEMENT IN PLACE.

ARE YOUR VENDORS GDPR COMPLIANT?
IT'S YOUR RESPONSIBILITY TO MAKE SURE YOUR VENDORS (THE PROCESSOR) ARE COMPLIANT BEFORE PROVIDING INFORMATION.

WRITTEN PROCESS RECORDS
YOU ARE REQUIRED TO KEEP WRITTEN RECORDS OF HOW INFORMATION IS COLLECTED AND HANDLED.

OVERSEA TRANSFERS
IT'S YOUR RESPONSIBILITY TO ENSURE SAFEGUARDS EXIST AND A PERSON'S RIGHTS ARE ENFORCEABLE.

DATA PROTECTION OFFICER
IF YOU REGULARLY DO LARGE SCALE PROCESSING OF PERSONAL INFORMATION, OR PROCESS HIGHLY SENSITIVE INFORMATION, LIKE HEALTH DATA OR POLITICAL AFFILIATIONS, YOU NEED ONE THAT IS SKILLED AND QUALIFIED.

PRIVACY IMPACT ASSESSMENTS
YOU ARE REQUIRED TO COMPLETE A PRIVACY IMPACT ASSESSMENT IF THE PROJECT IS LIKELY TO RESULT IN A HIGH PRIVACY RISK TO A PERSON.

COMPLY

NON-COMPLIANCE
A PERSON CAN FILE A COMPLAINT AND YOU CAN BE FINED

FINES
UP TO €20M OR 4% OF ANNUAL TURNOVER

MAINTAIN

PRIVACY BY DESIGN
MINIMISE RISKS AND BUILD TRUST. DESIGN WITH PRIVACY IN MIND CAN LEAD TO:

BENEFITS

IDENTIFY PROBLEMS EARLY WHEN IT'S SIMPLER & CHEAPER TO FIX

INCREASED AWARENESS OF PRIVACY AND DATA PROTECTION AMONG ORGANISATION

MEET REGULATIONS AND REDUCE FINES

LESS INTRUSIVE ACTIONS ON PRIVACY THAT MIGHT HAVE A NEGATIVE IMPACT ON A PERSON

COMPETITIVE ADVANTAGE THAT DIFFERENTIATES YOU FROM OTHERS

TwoBlackLabs
FOR MORE INFORMATION EMAIL info@twoblacklabs.co.nz

© TwoBlackLabs 2019



www.twoblacklabs.co.nz