DATA PROTECTION IN THE EU

APPLIES TO:

Any organisation in the world processing personal data of EU residents.

PERSONAL DATA BREACH:

Breach of security leading to the unlawful destruction, tampering, or disclosure of any information relating to EU residents.

CONSEQUENCES OF VIOLATIONS:

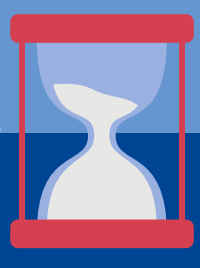
Fines of up to **€20,000,000** or **4%** of global revenue.
€10,000,000 or **2%** for less severe violations.

Permanent suspension from data processing activities.

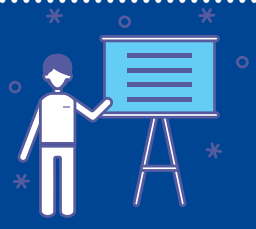
Risk of **class action lawsuits** from affected data subjects

RESPONSIBILITIES OF THE DATA PROTECTION OFFICER:

Required for organizations analyzing subjects' behavior on large scale.



Encase of **data breach**: notify supervisory authority within **72 hours**.



Conduct training & maintain records

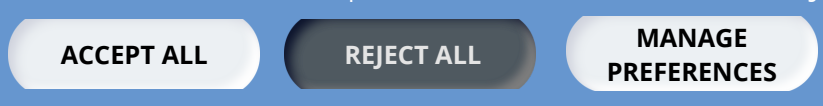
Data Protection Impact Assessments

Serve as contact for authorities + subjects

Monitor compliance with GDPR and carry out internal audits.

GOVERNING PRINCIPLES OF PROCESSING DATA:

- Clear and explicit consent is required from the data subject



- Process data only for the purpose(s) specified to the subject
- Only process the relevant and adequate data for a given purpose
- Maintain personal data with up-to-date and accurate information
- Keep identifiable data for no longer than needed for the purpose
- Ensure proper security with technical & organizational measures

CROSS-BORDER DATA TRANSFER REQUIREMENTS:

Data transfer to third countries is permitted with:

Countries with adequacy status

Usage of standard contractual clauses

Binding corporate rules approved by supervisory authority

FOR MORE INFORMATION ON COMPLIANCE:
US, EU & China's Data Protection Frameworks - Summarized