# Global Data Protection Day

by Copenhagen Compliance®

January 28, 2021, Online Conference

Kersi Porbunderwala
The E-Compliance Academy

**The Biggest GDPR Fines of 2021**

**Review of violations and fines levied in 2021**

- **The most common violations**
- **Growing lack of consent and transparency.**

Global Data Protection Day by Copenhagen Compliance

# Agenda

- GDPR is designed to make non-compliance a costly mistake
  - €10 million or 2% of a firm's annual revenue
  - 4% of annual revenue from the preceding year, whatever is higher
- Review of violations and fines levied in 2021
- The most common violations
  - Growing lack of consent and transparency.
- The trend in 2022.

# Step 1: Obtain the buy-in

## Key factor for success

## Fines + Reputation


**Board members**
**Senior managers**
**Chief compliance officer**
**Chief risk officer**
**Chief legal officer**
**Chief information offices**
**Chief security information officer**

Global Data Protection Day by Copenhagen Compliance®

# The Progression of fines

# Step 2. Why is GDPR important?

COPENHAGEN COMPLIANCE

## Fines!

NEW

**20M EUR up to 4% global revenue in the last year**

Failure to implement core principles, infringement of personal rights and the transfer of personal data to countries or organisations without adequate protection

**10M EUR up to 2% global revenue in the last year**

Failure to comply with technical and organisational requirements such as impact assessment, breach communication and certification

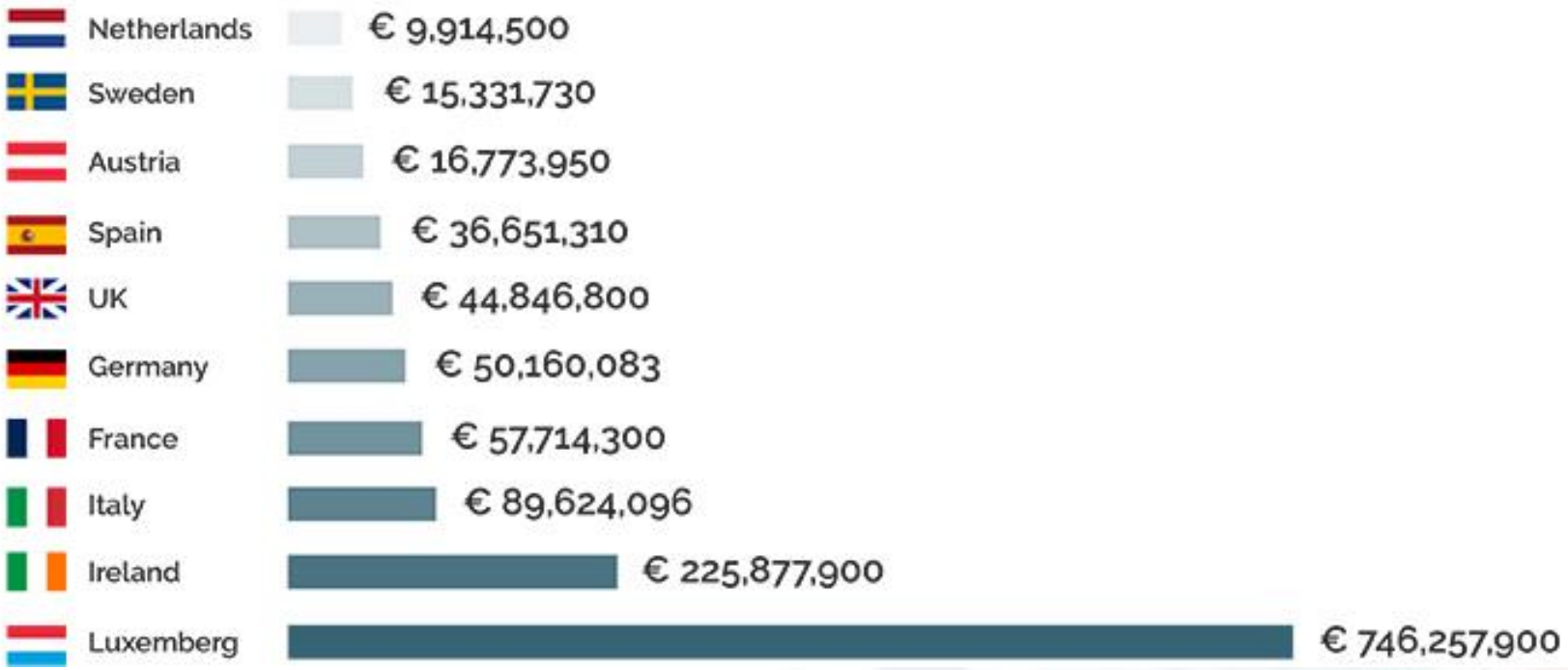
**Reduced with appropriate technical and organisational measures**

Global Data Protection Day

by Copenhagen Compliance®

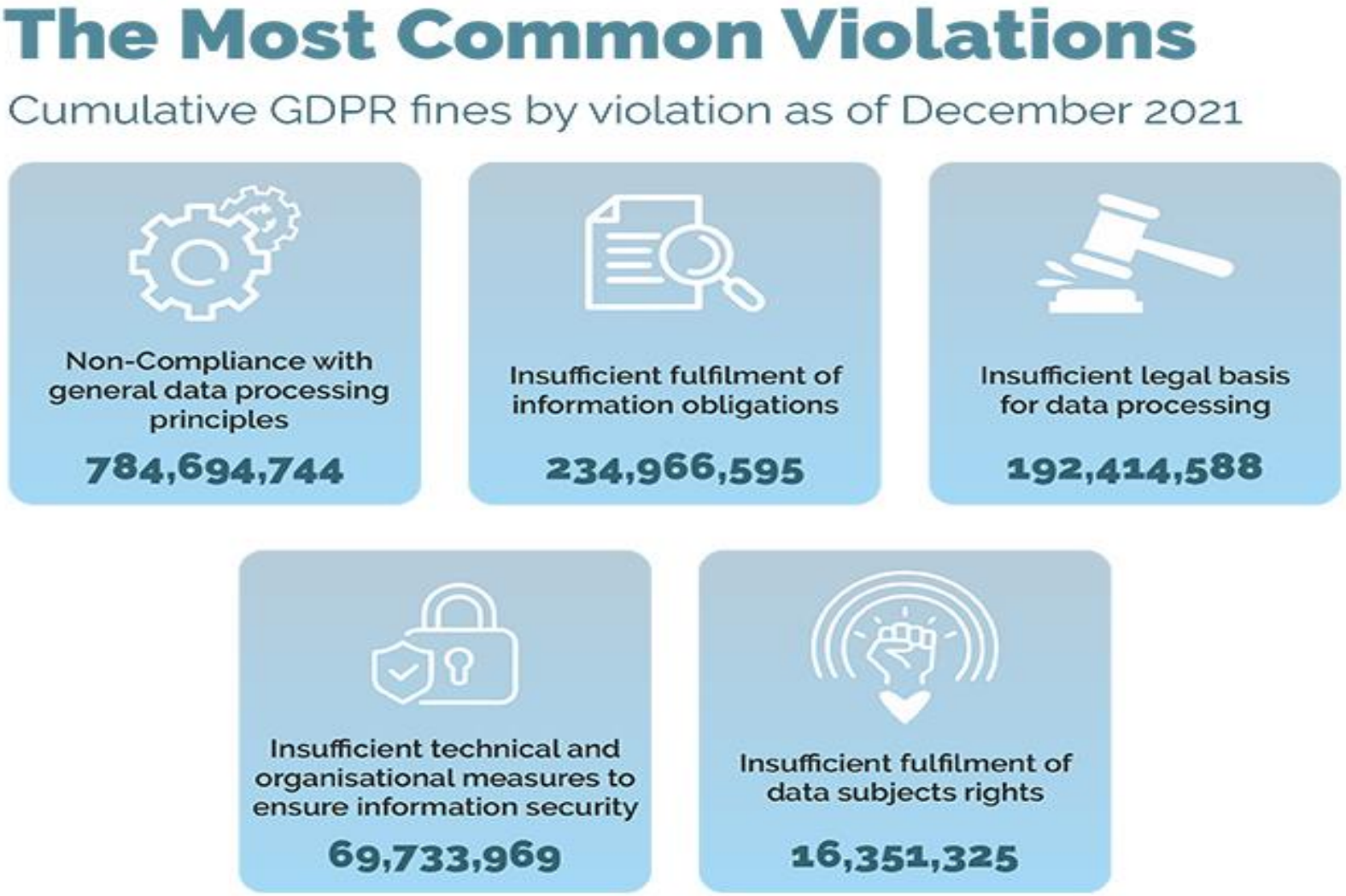
# Highest GDPR Fines by Country

Total sum of GDPR fines imposed by country as of December 2021



Global Data Protection Day by Copenhagen Compliance

# GDPR Non-Compliance



# Principles

GDPR MASTERCLASS

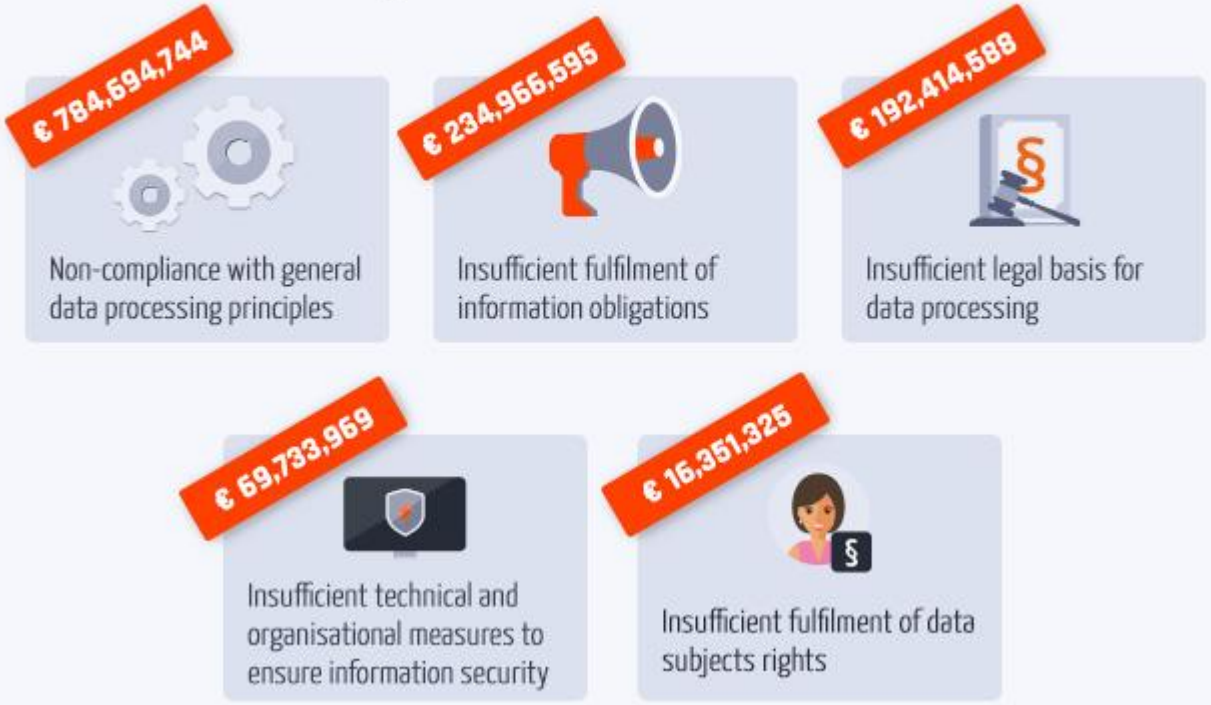
- Processed lawfully, fairly and transparently
- Processed in a manner that ensures appropriate security
- Collected for specified, explicit and legitimate purposes
- Accurate and, where necessary, kept up to date
- Adequate, relevant and limited to what is necessary
- Kept for no longer than is necessary

Global Data Protection Day

by Copenhagen Compliance®

# THE MOST COMMON VIOLATIONS

Cumulative GDPR fines by violation as of December 2021



# Privacy Information (data Subject)

GDPR MASTERCLASS

## Consent

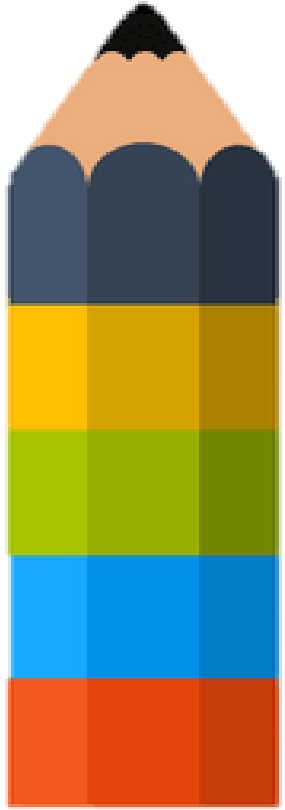
***Data subjects understand and explicitly or implicitly agree with the uses of personal information***

## Notice

***Data subjects receive a clear statement on the reason, retention period, access and the rights of personal information***

## Right to be forgotten

***Data subjects are allowed to erase personal information from data controllers and third parties***



## Access and correction

***Data subjects access and correct personal information to ensure is accurate, complete and relevant***

## Choice

***Data subjects make an informed decision regarding the permits on personal information***

## Sensitivity

***Data subjects are more sensitive to personal data involving health, lifestyle, criminal records..***

## Anonymity

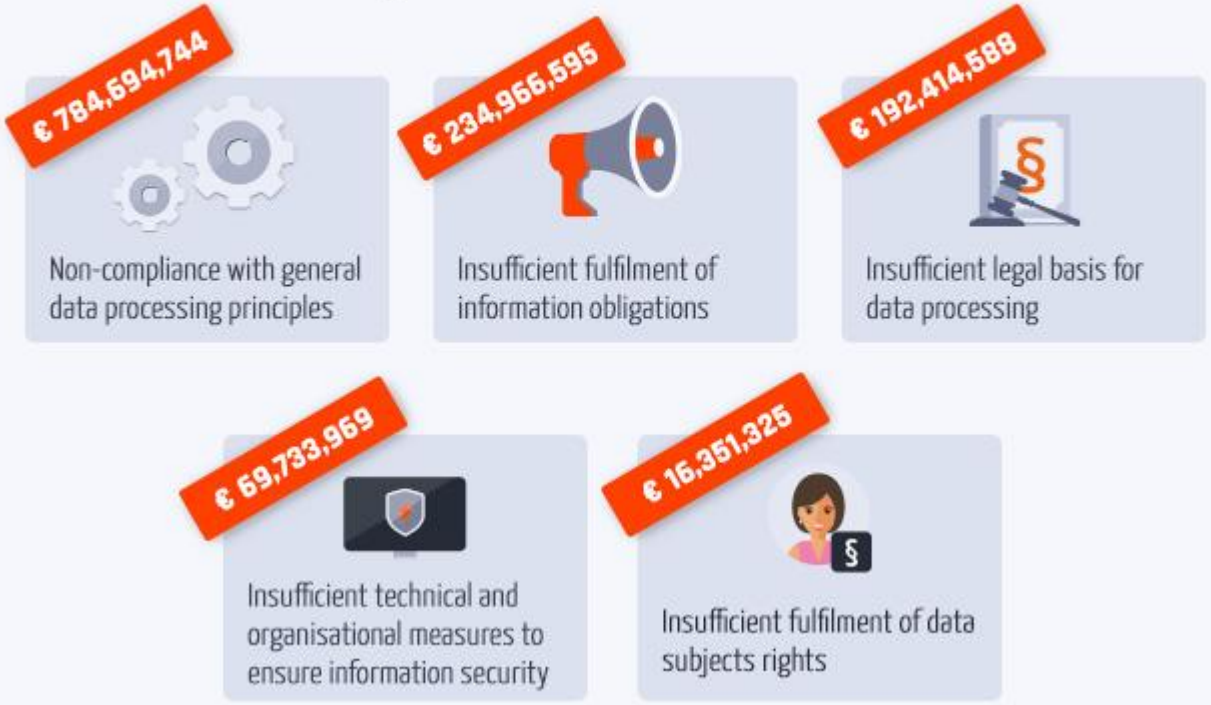
***Data subjects have the option of not identify themselves***

Global Data Protection Day

by Copenhagen Compliance®

# THE MOST COMMON VIOLATIONS

Cumulative GDPR fines by violation as of December 2021




GDPR Principles

# GDPR Principles

COPENHAGEN COMPLIANCE

- Processed lawfully, fairly and transparently
- Processed in a manner that ensures appropriate security
- Collected for specified, explicit and legitimate purposes
- Accurate and, where necessary, kept up to date
- Adequate, relevant and limited to what is necessary
- Kept for no longer than is necessary

# Principles


the controller be able to demonstrate **accountability**

- Being able to demonstrate best efforts to comply with the GDPR principles
- Proactive approach to properly manage personal data and to address privacy risks by a structured privacy management program

# Principles

**Proportionality**

processing only if necessary, for the attainment of the stated purpose

- Personal data must be adequate, relevant and not excessive in relation to the purposes
- By the data processor and controller
- Requires to use the less intrusive means of processing


# GDPR Principles

Global Data Protection Day by Copenhagen Compliance

# Data Controller Obligations

- Ensure data is processed lawfully and in a transparent manner to the data subject.
- Ensure data collected and processed for specific purposes, and not in a manner incompatible with original purposes.
- Ensure collected data is accurate and up-to-date.
- Ensure you are able to demonstrate compliance.

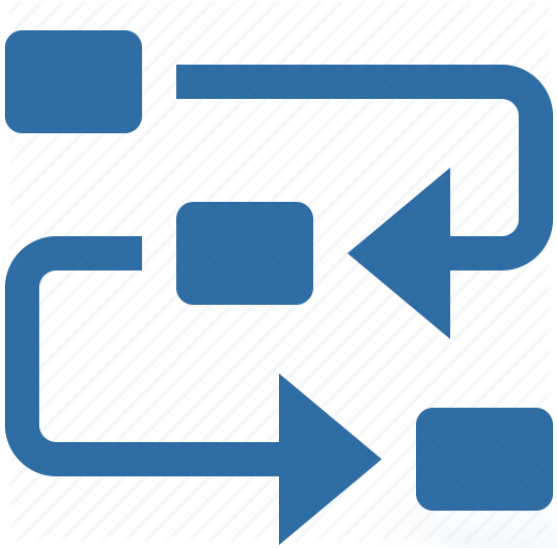
https://ec.europa.eu/info/sites/default/files/data-protection-factsheet-sme-obligations_en.pdf

# GDPR Principles

# Legal Bases For Processing Personal Data

GDPR MASTERCLASS

- Legitimate Interest
- Compliance with Legal Obligation
- Vital Interest of Individual



- Contract
- Consent
- Public Interest

*If it is hard to obtain a valid consent, then another more appropriate legal basis should be used*

Difficulties collecting consent = more appropriate legal basis should be used

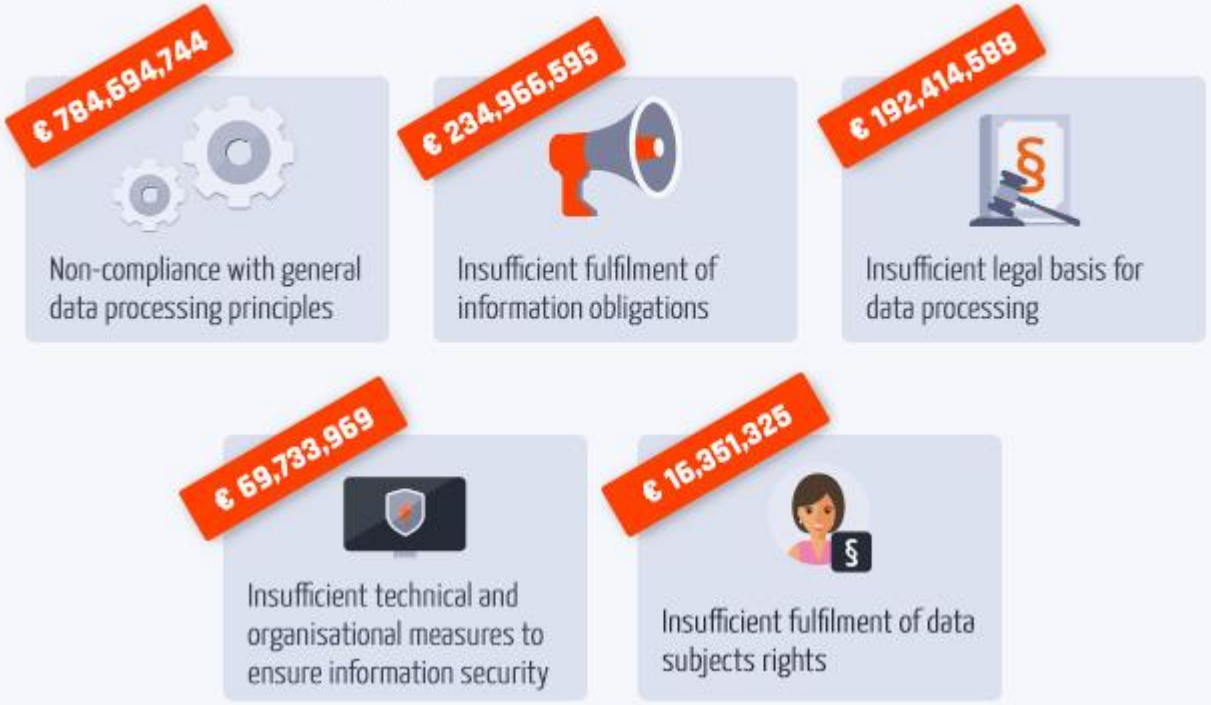
Consent is not appropriate = may be considered unfair and misleading

Global Data Protection Day

by Copenhagen Compliance®

# THE MOST COMMON VIOLATIONS

Cumulative GDPR fines by violation as of December 2021



# GDPR Principles

# Data Subject Rights

COPENHAGEN COMPLIANCE

**Right to be informed**

*Article 13, 14*

*Recitals 60-62*

**Right of Access by the Data Subject**

*Article 15*

*Recitals 63 & 64*

**Right to Rectification**

*Article 16, 19*

**Right to Erasure (RTBF)**

*Article 17, 19*

*Recitals 65 & 66*

**Right to Restrict Processing**

*Article 18, 19*

*Recital 67*

**Right to Data Portability**

*Article 20*

*Recital 68*

**Right to Object**

*Article 21*

*Recital 69 & 70*

**Automated Decision Making**

*Article 22*

*Recital 71 & 72*

**Right to Withdraw Consent**

*Article 7*

*Recital 32, 33, 41, 43*

# GDPR Principles

# Step 2. Why is GDPR important?

COPENHAGEN COMPLIANCE

## Fines!

NEW

**20M EUR up to 4% global revenue in the last year**

Failure to implement core principles, infringement of personal rights and the transfer of personal data to countries or organisations without adequate protection

**10M EUR up to 2% global revenue in the last year**

Failure to comply with technical and organisational requirements such as impact assessment, breach communication and certification

**Reduced with appropriate technical and organisational measures**

Global Data Protection Day by Copenhagen Compliance

- **GDPR Enforcement Tracker**
  GDPR Enforcement Tracker is an overview of fines and penalties which data protection authorities within the EU have imposed under the EU General Data Protection Regulation (GDPR, DSGVO).
  All fines are made public, therefore the list is not complete, and does not include fines imposed under national / non-European laws, under non-data protection laws (e.g. competition laws / electronic communication laws) and under "old" pre-GDPR-laws.

GDPR Enforcement Tracker - list of GDPR fines

Global Data Protection Day by Copenhagen Compliance®

COPENHAGEN COMPLIANCE
Global GRC Solutions
www.copenhagencompliance.com
Global Standards, Global Compliance Platform

Kersi F. Porbunderwalla is the Secretary General of Copenhagen Compliance® and Managing Partner of E-Compliance Academy, Information Security Institute and EUGDPR Institute®. Kersi is a global consultant, teacher, instructor, researcher, commentator and practitioner on GDPR, Corporate Governance, Risk Management, Compliance and IT-security (GRC), Bribery, Fraud and anti-Corruption (BFC) and Corporate Social Responsibility (CSR) issues. Kersi lectures at The Govt. Law College (Thrissur, India) Georgetown University (Washington) Cass Business School (London), Fordham University (New York) and Renmin Law School (Beijing). Kersi has conducted several hundred workshops, seminars and international speaking assignments on Regulatory Compliance, GDPR, GRC, CSR, and BFC issues.

EU GDPR INSTITUTE
GDPR Training and Certification

E-Compliance Academy
EU GDPR INSTITUTE
E-learning platform for Insights/Online Seminars

information security institute

**Disclaimer:** This presentation is prepared for The Data Protection Day.. The content together with the links to narratives, brochures and information on our websites, is for general informational purposes only. Please refer to Copenhagen Compliance® for specific advice on regulatory compliance and other GRC issues. As always refer to your counsel for legal advise, we are not licensed to provide legal advise.