



**DATA
LEGAL
DRIVE**
EOS GROUP

GDPR, FADP and now EU-AI-Act

How can I protect my company from data protection violations and high penalties?



Thomas-vini PIRES

Data Protection & AI
compliance specialist



**DATA
LEGAL
DRIVE**
EOS GROUP

Introducing Data Legal Drive

The #1 platform for privacy compliance



10,000+ clients



50,000+ users in 50 countries



10 languages available on our platform



50,000+ employees trained with DLD Learning



98% satisfied users



2018

Creation of Data Legal Drive.



2019

Fundraising with Lefebvre Sarrut Group.



2020

Acquisition of another market player : Captain DPO.



2021

New fundraising with Lefebvre Sarrut Group



2021

Partnership with Vigo Law Firm.



2022

Launch of anti-corruption compliance software



2024

Introduction of AI in the software.



2024




Data Legal Drive's integration into the EQS group.

What do these companies have in common ?



Fines for GDPR infringement (1/2)

Various sectors, various scales, various motives

 Clearview.ai		+103,000,000 CHF (+ 99,000,000 €)			+3,500,000 CHF (+ 3,000,000 €)
		+36,700,000 CHF (+ 35,000,000 €)			+6,686,000 CHF (+ 6,419,000 €)
		+22,900,000 CHF (+ 21,000,000 €)			+14,000,000 CHF (+ 13,000,000 €)
		+21,000,000 CHF (+ 20,000,000 €)			+12,000,000 CHF (+ 5,000,000 €)
		+10,000,000 CHF (+ 9,000,000 €)			+41,000,000 CHF (+ 40,000,000 €)
		+5,000,000 CHF (+ 4,000,000 €)			+8,500,000 CHF (+ 8,500,000 €)

Fines for GDPR infringement ^(2/2)

Various sectors, various scales, various motives

Date	Total sum of fines	Total number of fines
Sept. 2024 (+ 6 y. of application)	€ 4,919,057,151	2185

Sector	Sum of Fines
Media, Telecoms and Broadcasting	€ 3,313,891,366 (at 296 fines)
Industry and Commerce	€ 946,933,077 (at 467 fines)
Employment	€ 349,998,777 (at 144 fines)
Transportation and Energy	€ 173,541,941 (at 120 fines)
Finance, Insurance and Consulting	€ 64,187,258 (at 229 fines)
Public Sector and Education	€ 27,952,463 (at 251 fines)
Accommodation and Hospitality	€ 22,592,648 (at 73 fines)
Health Care	€ 21,327,209 (at 212 fines)
Real Estate	€ 2,702,431 (at 64 fines)
Individuals and Private Associations	€ 1,939,156 (at 301 fines)
Not assigned	€ 1,847,688 (at 138 fines)

Violation	Sum of Fines
Non-compliance with general data processing principles	€ 2,410,164,550 (at 617 fines)
Insufficient legal basis for data processing	€ 1,652,855,412 (at 654 fines)
Insufficient technical and organisational measures to ensure information security	€ 480,011,915 (at 393 fines)
Insufficient fulfilment of information obligations	€ 247,854,260 (at 195 fines)
Insufficient fulfilment of data subjects rights	€ 100,998,646 (at 218 fines)
Unknown	€ 23,267,300 (at 15 fines)
Insufficient cooperation with supervisory authority	€ 6,639,229 (at 124 fines)
Insufficient fulfilment of data breach notification obligations	€ 3,037,392 (at 45 fines)
Insufficient data processing agreement	€ 1,117,110 (at 12 fines)
Insufficient involvement of data protection officer	€ 968,200 (at 22 fines)

1

**GDPR, FADP,
and now... AI ACT?**

Data Protection & AI Regulation - Main features

GDPR 

FADP* 

AI ACT 

Geographical scope

Organizations established in **EU/EEE** or processing data from **EU residents**

Organizations established in **Switzerland** or processing data from **swiss residents**

Organizations established in **EU/EEE** or impacting **EU residents**

Technical scope

Processing of individuals' personal data

Development and/or **use** of AI Systems

Entry into force

May, 25th 2018

Sept, 1st 2023 (last 1992)

August, 1st 2024

Competent authority

National data protection authorities of EU member states

Federal Data Protection and Information Commissioner (FDPIC)

National AI regulatory authorities within the EU

Main rôle in charge

Data Protection Officer (Mandatory)

Data Protection Officer (Best practice)

AI Officer ?
DPO ? Compliance Officer ?

Max. possible sanction

Up to **20 million euros** (22,000,000 CHF) or **4%** of global annual turnover, whichever is higher

Up to **2 million CHF** for legal entities

Up to **35 million euros** (38,500,000 CHF) or **7%** of global annual turnover, whichever is higher

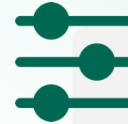
*[The European Commission has classified Swiss data protection as equivalent to the EU General Data Protection Regulation \(GDPR\)](#)

DATA PROTECTION – Fundamental principles



Defined purpose

Make sure that the processing relies on a defined and specific purpose



Data minimization

Make sure that only needed personal data is processed according to the purpose



Retention limitation

Ensure that personal data is kept only for a limited time period according to the purpose



Transparency

Allow users to understand how their data is processed

6 Gold rules of data protection



Security

Ensure that data are organizationally and technically secured



Respect of fundamental rights

Give data subjects possibility to act on their personal data

Data Protection Regulation – Main obligations

RoPA

Maintain a Record of (all) Processing Activities

Privacy by Design

Assess all new processing according to privacy principles

Privacy Impact Assessment (PIA)

Realize a risk assessment for sensitive processing

Transparency

Inform data subjects regarding their data processing

Data Subject Rights

Manage rights exercise (Access, deletion, ...)

Security

Implement technical & organizational security measures

Notification

Notify competent authorities in case of data breach

Third Parties

Evaluate & audit data processors

Data Protection Agreements

Add specific data protection clauses within contracts

Data transfers

Regulate cross-border personal data flows

Awareness

Provide privacy trainings to all employees

Internal control

Perform regular internal control regarding privacy compliance

Cooperation

Cooperate with competent authority in case of control

Accountability

Document EVERYTHING for compliance demonstration

AI REGULATION – Fundamental principles



Autonomy and human control
Respect human autonomy,
human dignity and fundamental
rights



**Societal and environmental
well-being**
Do not cause physical, mental or
environmental damage



Fairness and equity
Prevent bias and discrimination,
promote justice and equity

7 Principles for a Trustworthy AI



Transparency and explainability
Allow users to understand how
they work and to challenge their
decisions



Liability
Make actors responsible for
their actions and the
consequences of their systems



Safety and security
AI systems must be designed to
be safe and secure, and to
minimize the risks of failure or
misuse



Privacy and data protection
Protect the privacy of individuals
and guarantee the security and
confidentiality of their data

AI Regulation – Main obligations

Technical Documentation

Maintain a Record of (High-Risk) AI Systems (HRAIS)

AI Compliance by Design

Assess all AI System according to *trustworthy* AI principles

Risk Management System (RMS)

Realize a risk assessment for HRAIS

Transparency

Inform final users regarding conception & impacts of AI

Data Subject Rights

Manage rights exercise (Access, deletion, ...)

Security

Ensure safety and security of AI Systems

Notification

Notify competent authorities in case of breach

Third Parties

(ante) evaluate & (post) audit suppliers

Agreements

Add specific clauses within contracts

Data transfers

Regulate cross-border personal data flows

Awareness

Provide privacy trainings to all employees

Conformity assessment

Perform internal regular assessment on every HRAIS

Registration

HRAIS CE Marking + Registration in EU Databases

Quality Management System (QMS)

Document EVERYTHING for compliance demonstration

2

HOW TO COMPLY WITH?

How to comply with these regulations ? ^{1/2}

Apply the 5 main compliance steps...

APPOINT A LEADER

A conductor (and his orchestra)

MAP PROCESSINGS & AI SYSTEMS

Map the existing to adopt a risk approach

TRAIN & COMMUNICATE

Internally (and externally ?)



DIAGNOSE COMPLIANCE LEVEL

To adapt the global (and local) action plans

PROCESS THE COMPLIANCE

Qualify, assess, document and control

How to comply with these regulations ? ^{2/2}

...and turn a constraint into a strenght



+



Making the principles their own

Spreading corporate culture

CREATING TRUSTED
COMPANIES >>

Q / A time !



*Download our
GDPR checklist*



**DATA
LEGAL
DRIVE**
EQS GROUP

