FIELD GUIDE

A PRACTICAL GUIDE TO THE GENERAL DATA PROTECTION REGULATION (GDPR)

CREATED BY

WWW.VENZAGROUP.COM

GDPR FIELD GUIDE SERIES VOL. 1

CLICK TO NAVIGATE

TOPICS:

CLICK TO NAVIGATE

GDPR ENFORCEMENT 25 MAY 2018

GDPR BASICS & IMPORTANT TERMS

What Is GDPR?

- An EU "regulation" (meaning = law)
- An extra-territorial standard for organizations that:
  - Offer goods/services to EU citizens (e.g. hotel rooms)
  - Monitor behaviors of EU citizens (e.g. loyalty programs)
- A compliance framework for transborder data transfers

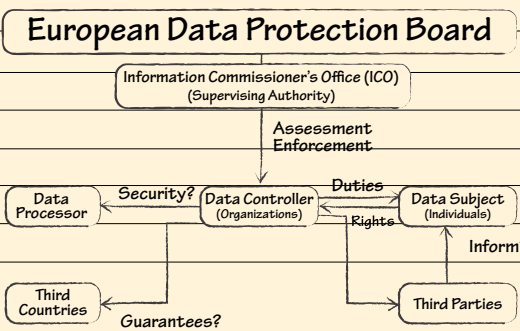
Why?

- To protect data privacy of EU citizens
- An EU directive from '95 didn't do enough to protect rights

Important Terms & Phrases to Know:

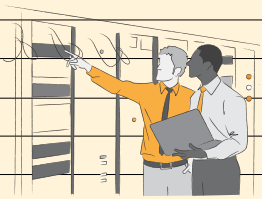
- Data subjects = natural persons
- Data protection Officer (DPO) = an independent privacy advocate
- Data Protection Impact Assessment (DPIA) = a risk evaluation
- Privacy By Design (PbD) = a guiding principle for:
  - Minimal data collection & retention
  - Capturing consent

Data Protection Model



1. DPO Designation (Article 37)

- Position Essentials (Article 38)
  - Must be independent... no conflict of interest!
  - Reports to executive leadership
- Must understand:
  - GDPR legal
  - Controller's business
  - Operation's information systems
- DPO tasks (Article 39)
  - Advise
  - Monitor compliance
  - Raise awareness & train staff



2. Contracts & Policies Review

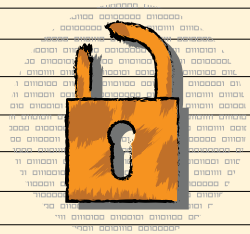
(Articles 6, 12, 13, 14, & 96)

- Privacy Policy
- Agreements with:
  - Suppliers
  - Vendors
  - Partners
  - Employees, etc.

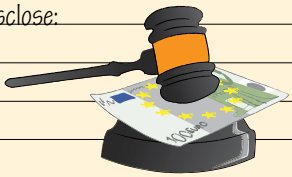
3. Processing Operations Evaluation

(Articles 6 & 35)

- Where are the data?
- How are they collected?
- For how long?
- With whom are they shared?
- Etc.



4. Limitation of Purpose (Articles 5,13 & 14)



- As for data processing, must disclose:
  - Processing purpose
  - Storage period
- You must:
  - Respect data (Article 5)
  - Determine applicability of legitimate interest (Article 6)
- In case of abuse, supervisory authorities can impose processing ban!

5. Consent Management

- You must:
  - Inform of consent (Articles 5, 6, 7, 11, 13 & 14)
  - Manage direct marketing objections (Article 22)
  - Implement withdrawing consent (Articles 7 & 17)
  - Keep records! (Article 7)

6. Breach Response (Article 12)

- For people, breaches can result in:
  - Limiting rights
  - Identity theft
  - Fraud/financial loss
  - Reputational damage
- You must:
  - Present appropriate notice within 72 hrs. (Recital 85 & Article 33)
  - Notify supervisory authority (Article 33)

The Controller

- Monitor data processing
- Adopt internal privacy policies and adhere to codes of conduct (Recital 78, Article 24)
- Implement measures for data protection (Article 24)
- Secure and maintain record of processing (Articles 30 & 32)
- Consult with supervisory authority and notify in the case of a data breach within 72 hours (Articles 33 & 36)

The Processor

- Comply with the controller's processing contract (Article 28)
- Refrain from engaging 3rd-party processors, unless authorized (Article 28)
- Secure and maintain record of processing (Articles 30 & 32)
- Notify the controller in the case of a data breach (Article 33)

NOTE: If a processor determines the purpose and/or means of processing, they will be considered a controller. (Article 28)

Fines

- €10 million (or 2% of global turnover) for not adhering to requirements (Article 83)
- €20 million (or 4% of global turnover) for not adhering to core principles (Article 83)

NOTE: EU Member States may levy additional penalties! (Article 84)

The Data Protection Officer (DPO)

- Monitor compliance and awareness . . . train employees!
- Inform and advise the controller or the processor (Article 39)
- Cooperate with the supervisory authority (Article 39)

NOTE: The DPO is not subject to fines due to non-compliance!

GDPR COMPLIANCE IS A JOURNEY.

WE'RE THE GUIDE.

venza®
Better Visibility. Better Defense.

Global Headquarters
10886 Crabapple Road, Suite 100
Roswell GA. 30075
+1 770.685.6500
+1 770.685.6553 Fax
+1 800.684.6132 Toll Free

EU Office
Prinses Margrietplantsoen 33
2595 AM
The Hague, Netherlands
+1 404.432.4263