MASTERING GDPR

COMPLIANCE, RISK MANAGEMENT, TRENDS & CHANGES

Harald Lavric

Owner of GRIFFOX Consulting

Background

- Master's Degree in Economics
- M. A. in Business Coaching & Change Management
- Certified Data Protection Auditor
- Certified Change Management Professional™
- Prosci Change Practitioner
- Certified Project Manager
- 20+ years experience as C-Level-Manager
- 10 years of experience in Data Privacy Management

Focus

- Organizational Change Management
- International Data Privacy Management
- Business Coaching
- Risk Management
- Process Improvement
- Organizational Assessments
- Training & Development
- Leadership Coaching

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

GDPR Risk Management

2023: Important Trends and Changes

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Understanding the Core Components of the GDPR

How to start?

7 principles	6 lawful bases of data processing	Privacy by Design	Privacy by Default	Who is the Controller?
Rights of the Data Subject (your client in Europe)	Worldwide impact	Technical Measurements	Organizational Measurements	Non-Compliance

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

7 Principles

- Lawfulness, Fairness, and Transparency
- Purpose Limitations
- Data Minimization
- Accuracy
- Storage Limitation
- Integrity and Confidentiality
- Accountability

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

6 Lawful Bases of Data Processing

- ✓ Consent
- ✓ Contract
- ✓ Compliance with legal obligation to which the controller is subject
- ✓ Vital interests of the data subject or another natural person
- ✓ Performance of a task conducted in the public interest or in the exercise of official authority
- ✓ Processing is necessary for the legitimate interest pursued by the controller or by a third party

Understanding the Core Components of the GDPR

Privacy by Design

Taking into account

- the state of the art,
- the cost of implementation, and
- the nature, scope, context, and purposes of processing as well as
- the risks of varying likelihood and
- severity for rights and freedoms of natural persons posed by the processing,

the controller shall, both at the time of the determination of the means for processing and at the time of the processing itself, implement appropriate technical and organizational measures, such as pseudonymization, which are designed to implement data-protection principles, such as data minimization, effectively and to integrate the necessary safeguards into the processing to meet the requirements of this Regulation and protect the rights of data subjects.

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Privacy by Default

The controller shall

- implement appropriate technical and organizational measures to ensure that,
- by default,
- only personal data that are necessary for each specific purpose of the processing are processed.

That obligation applies to the amount of personal data collected, the extent of their processing, the period of their storage, and their accessibility.

In particular, such measures shall ensure that by default personal data are not made accessible without the individual's intervention to an indefinite number of natural persons.

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Who is the Controller?

Is there only one controller or are there many controllers?

- From the point of view of the GDPR, the question of who is responsible can be solved relatively easily.
- *Art. 4 (7) - Controller means the natural or legal person […], which, alone or jointly with others, determines the purposes and means of the processing of personal data […].*

So the final question is: **Who is in charge?**

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Rights of the
Data Subject
(your client in Europe)

- Access (Obtain information)
- Rectification (Correction of data stored)
- Erasure (Right to Be Forgotten)
- Restriction of Processing (inaccurate/unlawful)
- Data Portability
- Protection against Automated Decision Making

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Worldwide Impact

- The GDPR applies to data processing operations of European citizens that happen on a regular base (more than once) or data processing operations conducted in Europe. This extra-territorial scope therefore also affects companies that are not based in Europe – even if the companies are not settled in a member state of Europe.
- If a company doesn't have a brick-and-mortar location in Europe, it is mandatory to install a GDPR representative who acts as a Single Point of Contact.

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Technical Measurements

- Pseudonymization
- Encryption
- Firewalls
- Protocols (Log Files)
- Password Specifications (US NIST / UK NSCS / GE BSI)
- Access Rights (Need-to-know)

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Organizational Measurements

- Internal Data Protection Policies
- Information Security Policies
- Reviews and Audits
- Due Diligence of external Data Processors (Third Parties)
- Data Protection Officer (DPO as a Service)
- Awareness Raising & Training

GRIFFOX
Solutions for Business & Life

Understanding the Core Components of the GDPR

Non-Compliance

Non-compliance with GDPR can lead to severe penalties.

- Up to 4% of annual global turnover or €20 million (whichever is higher) can be imposed.
- Supervision authorities have investigative, corrective, and advisory powers.
- Additionally, reputational damage and loss of customer trust can have long-lasting effects on an organization's viability.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

GDPR Risk Management

Technical
Risk Management

Organizational
Risk Management

Website
Risk Management

Process
Risk Management

Third-Party
Risk Management

Cross Border Transfer
Risk Management

HR Risk
Management

Strategies

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Technical
Risk Management

- Identify and evaluate technical risks.
- Implement technical measures to mitigate identified risks.
- Continuously monitor and regularly review the effectiveness of measures to ensure ongoing compliance with GDPR.
- Develop and maintain an incident response plan to address data breaches.
- Document risk management processes, measures implemented, and regular reviews conducted, to provide evidence of compliance to supervisory authorities as required under GDPR.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Organizational
Risk Management

- Establish clear structures and policies including the appointment of a Data Protection Officer (DPO), if necessary.
- Conduct regular training and awareness programs to ensure that employees and other stakeholders are aware of their responsibilities.
- Assess and manage the risks associated with third-party vendors.
- Monitor compliance with GDPR on an ongoing basis, reviewing and updating risk management processes and measures to address any changes in the organizational context or legal framework.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Website
Risk Management

- Ensure that the website only collects the necessary personal data required for its operation or service provision.
- Implement clear consent mechanisms for data collection, ensuring users have the ability to opt in and opt out easily.
- Deploy robust security measures such as HTTPS, anti-malware tools, and firewalls to protect against data breaches and other cyber threats.
- Clearly inform visitors about the use of cookies and trackers, obtain consent where required, and provide easy-to-use options for users to manage their preferences in alignment with GDPR requirements and keep this information up-to-date.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Process
Risk Management

- Use a record of processing activities to get an overview of those activities and implement Privacy by Design / Privacy by Default. Identify where personal data is being processed, stored, and transmitted to ensure a thorough understanding and management of the risks involved.
- Perform regular audits and reviews of data processing activities to ensure they remain compliant with GDPR requirements, and to identify any emerging risks or areas for improvement in the risk management process.
- Develop and maintain a robust incident response plan to address any data breaches or non-compliance issues, ensuring timely notification to supervisory authorities and affected individuals as per GDPR mandates.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

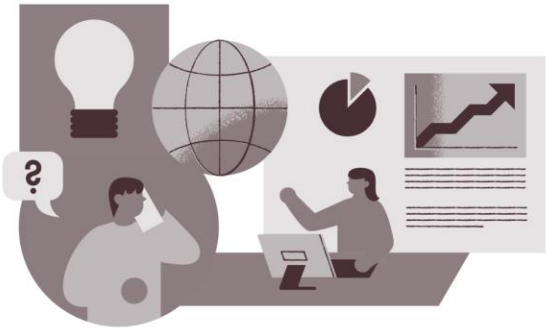
Third-Party
Risk Management

- Conduct thorough assessments of third-party vendors.
- Establish clear contracts and Data Processing Agreements (DPAs) with third parties, outlining their data protection responsibilities, liability, and the standards they need to adhere to under GDPR.
- Implement continuous monitoring and auditing mechanisms to ensure third parties remain compliant with GDPR.
- Ensure appropriate safeguards are in place for cross-border data transfers to third-party countries, such as Standard Contractual Clauses (SCCs).

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Cross Border Transfer
Risk Management



- Check if the destination country has an adequacy decision from the EU Commission, which confirms that the country provides a comparable level of data protection to the GDPR, simplifying the transfer process.
- Utilize Standard Contractual Clauses (SCCs) approved by the EU with overseas recipients to ensure an adequate level of data protection.
- Establish Binding Corporate Rules (BCRs) for intra-group cross-border data transfers, ensuring all entities within the corporate group maintain GDPR-compliant.
- Conduct Data Transfer Impact Assessments (DPIAs) to identify and mitigate risks.
- Maintain detailed records of cross-border data transfers and any additional safeguards implemented.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

HR
Risk Management

- Collect and process only the necessary personal data required for HR purposes.
- Implement strict access control measures to ensure only authorized personnel can access personal data, coupled with regular training on GDPR compliance for HR staff.
- Provide clear and concise privacy notices to employees, detailing how their personal data will be processed, stored, and protected.
- Establish and enforce data retention policies to ensure personal data is kept only for the required duration.

GRIFFOX
Solutions for Business & Life

GDPR Risk Management

Strategies

- Use records of processing activities
- Understand rules and regulations
- Use a Consent Management System
- Take care of User Rights and Website Compliance
- Comply with the different Data Protection Laws (Europe, UK, Brazil…)
- Implement Privacy by Design / Privacy by Default in the Development Process

GRIFFOX
Solutions for Business & Life

2023: Important Trends and Changes

2023: Important Trends and Changes

EU-US-Data-Privacy-Framework (DPF)

Self-certifying to DPF as an organization

Not eligible for the DPF?

Countries with similar rules like the GDPR

USA – California and Virginia

USA - Florida

GRIFFOX
Solutions for Business & Life

EU-US-Data-Privacy-Framework (DPF)

2023: Important Trends and Changes

- EU-US-Data-Privacy-Framework (DPF): launched in July 2023
  - DPF ensures data protection that is consistent with EU, UK, and Swiss law
  - DPF gives participating organizations a binding framework to self-certify.
  - DPF is only for those companies subject to the jurisdiction of either the Federal Trade Commission (FTC) or the US Department of Transportation (DOT).
- First Lawsuit against the DPF in September 2023
- Additional Lawsuits are planned by Max Schrems (Safe Harbour/Privacy Shield)

GRIFFOX
Solutions for Business & Life

2023: Important Trends and Changes

Self-certifying to DPF as an organization

https://www.dataprivacyframework.gov

- **Notice** – inform individuals about participation, purpose, type of data, …
- **Choice** – option to opt-out and opt-in
- **Accountability for Onward Transfer** – comply with Notice & Choice / enter into a contract with a third-party controller (Purpose limitation)
- **Security** – Implement appropriate safeguards
- **Data Integrity and Purpose Limitation**
- **Access** – User Rights to access, amend, correct, or delete stored information
- **Recourse, Enforcement, and Liability**
- 16 additional supplemental principles

GRIFFOX
Solutions for Business & Life

Not eligible for the DPF?

2023: Important Trends and Changes

- Ensure sufficient safeguards according to Art. 46 GDPR, for example, Standard Contractual Clauses (SCCs) or Binding Corporate Rules (BCRs) for intra-group cross-border data transfers
- Transfer Impact Assessment (TIA); TIA assesses whether the personal data in the recipient country is protected within an equivalent level of data protection as in the EU. If necessary, companies can take additional measures to guarantee the protection of the personal data of the data subjects.

GRIFFOX
Solutions for Business & Life

2023: Important Trends and Changes

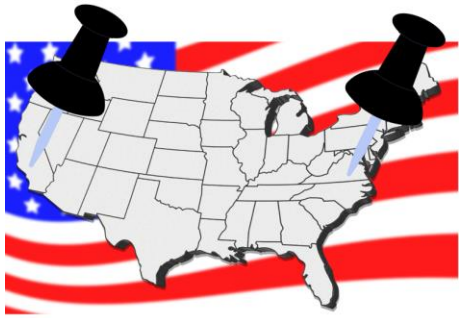
Countries with similar rules like the GDPR

- **Argentina** (Personal Data Protection Act No 25,326)
- **Bahrain** (Personal Data Protection Law)
- **Brazil** (General Data Protection Law LGPD)
- **Canada** (Personal Information Protection and Electronic Documents Act (PIPEDA)
- **China** (Personal Data Protection Law)
- **Israel** (Data Security Regulations)
- **Japan** (Act on the Protection of Personal Information)
- **Kenya** (Data Protection Act)
- **Mauritius** (Data Protection Act)
- **New Zealand** (Privacy Act)
- **Nigeria** (Data Protection Regulation)
- **Qatar** (Law No. 13)
- **Singapore** (Personal Data Protection Act)
- **South Africa** (Protection of Personal Information (POPI) Act)
- **South Korea** (Personal Information Protection Act)
- **Switzerland** (Personal Data Protection Law)
- **Thailand** (Personal Data Protection Act)
- **Turkey** (Law on Protection of Personal Data No. 6698)
- **Uganda** (Data Protection and Privacy Act, 2019)
- **Uruguay** (Act on the Protection of Personal Data and Habeas Data Action)

GRIFFOX
Solutions for Business & Life

2023: Important Trends and Changes

USA – California and Virginia



- **California** Privacy Rights Act (CPRA) modifies the scope outlined by the CCPA (Gross annual revenue/information of 100,000 or more California residents / Generates at least 50 % of their annual income from selling or sharing information from California residents)
- **Virginia** Consumer Data Protection Act (CDPA); companies that control or process the personal data of at least 100,000 consumers during a calendar year or control or process the personal data of at least 25,000 consumers and make at least 50% of its gross revenue from the sale of personal data

GRIFFOX
Solutions for Business & Life

2023: Important Trends and Changes

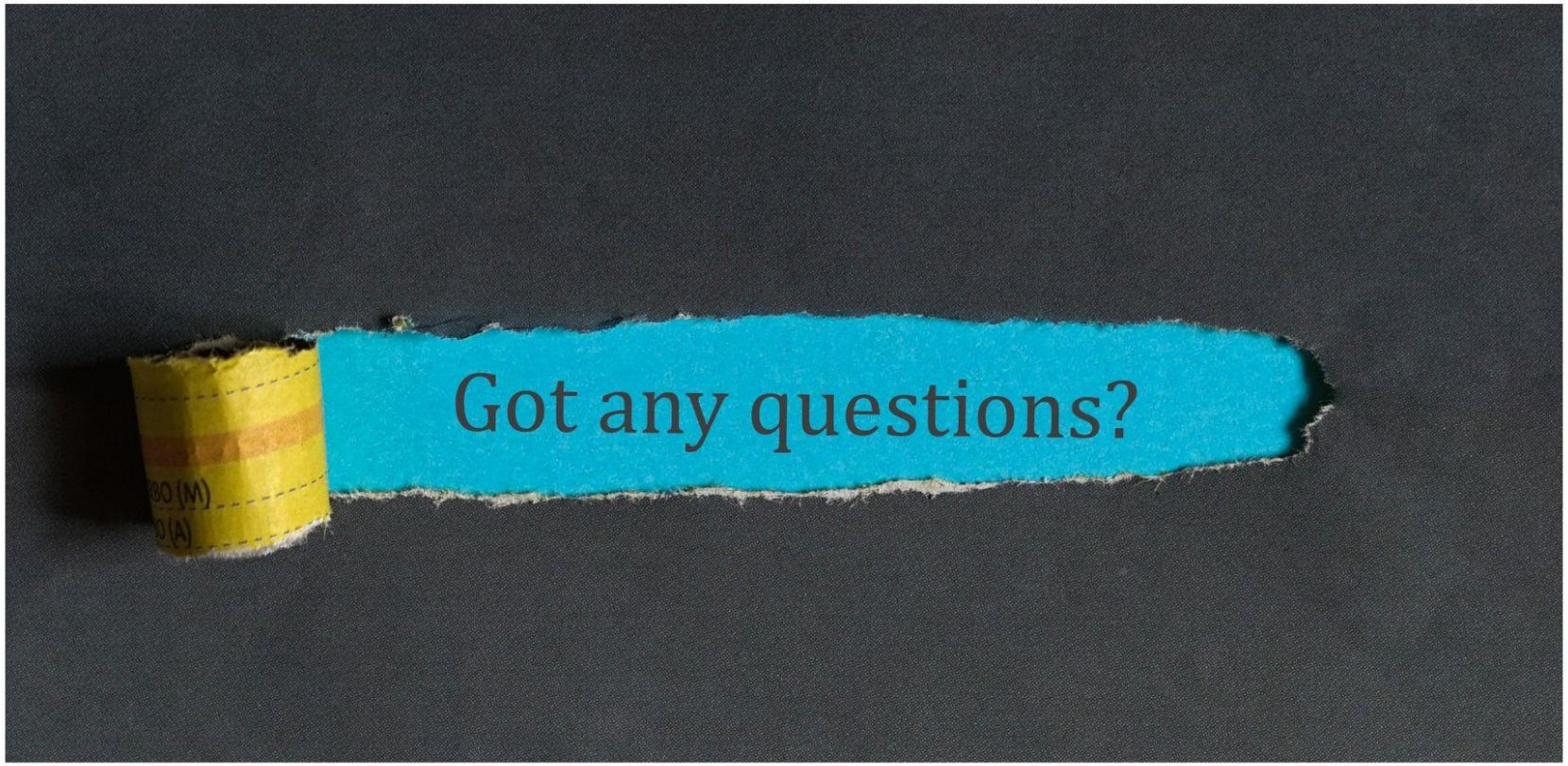
USA - Florida

- The **Florida Digital Bill of Rights** (FDBR) was signed into law by Governor Ron DeSantis on June 6, 2023, making Florida the tenth state to enact a consumer data privacy law along with California, Virginia, Colorado, Connecticut, Utah, Iowa, Indiana, Tennessee, and Montana.
- The FDBR, which goes into effect on **July 1, 2024**, generally adheres to the "Virginia model" of consumer privacy legislation.
- The law does not apply to businesses with less than $1 billion in gross annual revenue.
- Other thresholds further limit the law's coverage to those that derive half their revenue from digital ad sales, operate certain app stores or digital distribution platforms, or offer certain smart home speakers with a virtual assistant.

GRIFFOX
Solutions for Business & Life

THANK YOU!

GRIFFOX
Solutions for Business & Life



Let's talk about your challenges

GRIFFOX

Solutions for Business & Life

contact@griffox.com

(850) 376 7843

Milton, FL

www.griffox.com