Publisto

General Data Protection Regulation (GDPR)

Introduction

- GDPR will **affect every business** and public body that processes the personal data of EU residents, including individuals on behalf of other business
- It's an **illusion** to have the impression that **only IT Department** is responsible for data protection. **Departments** that are **well impacted** are the ones that receive, hold or process personal data (HR, Accounting etc)

GDPR comes into force on 25 May 2018

What Processing Means

Any operation or set of operations which is performed on personal data or on sets of personal data, whether or not by automated means, such as collection, recording, organisation, structuring, storage, adaptation or alteration, retrieval, consultation, use, disclosure by transmission, dissemination or otherwise making available, alignment or combination, restriction, erasure or destruction

Processing of Personal Data wholly or partly by automated or non automated means.

Personal Data

What do we mean by personal data?

- identification (name, age, residence, occupation, marital status etc.)
- physical characteristics
- education
- labor relations
- economic situation
- electronic traces
- interests, activities, habits.

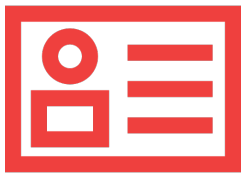
Any information that refers to and identifies a person

The big picture

- the GDPR applies to organizations if they: (i) offer goods or services to EU residents; or (ii) monitor the behavior of EU residents (e.g., organizations that offer online businesses)
- for the most serious violations, privacy regulators will be able to impose penalties of up to €20m or 4% of global revenue (whichever is higher)
- organizations will be under greater obligations to provide assurance to their boards, customers and regulators that their data protection processes and procedures are fit for purpose.

EU Residents, strict penalties, greater obligations

GDPR concerns



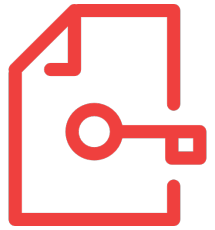
Data profiling directories

Data Protection Officer

Security & data breach notifications

Consent

3rd party processing



Data access requests

Focus areas

Subjects' rights
- New Data Erasure Rights
- Explicit Data Subject Consent

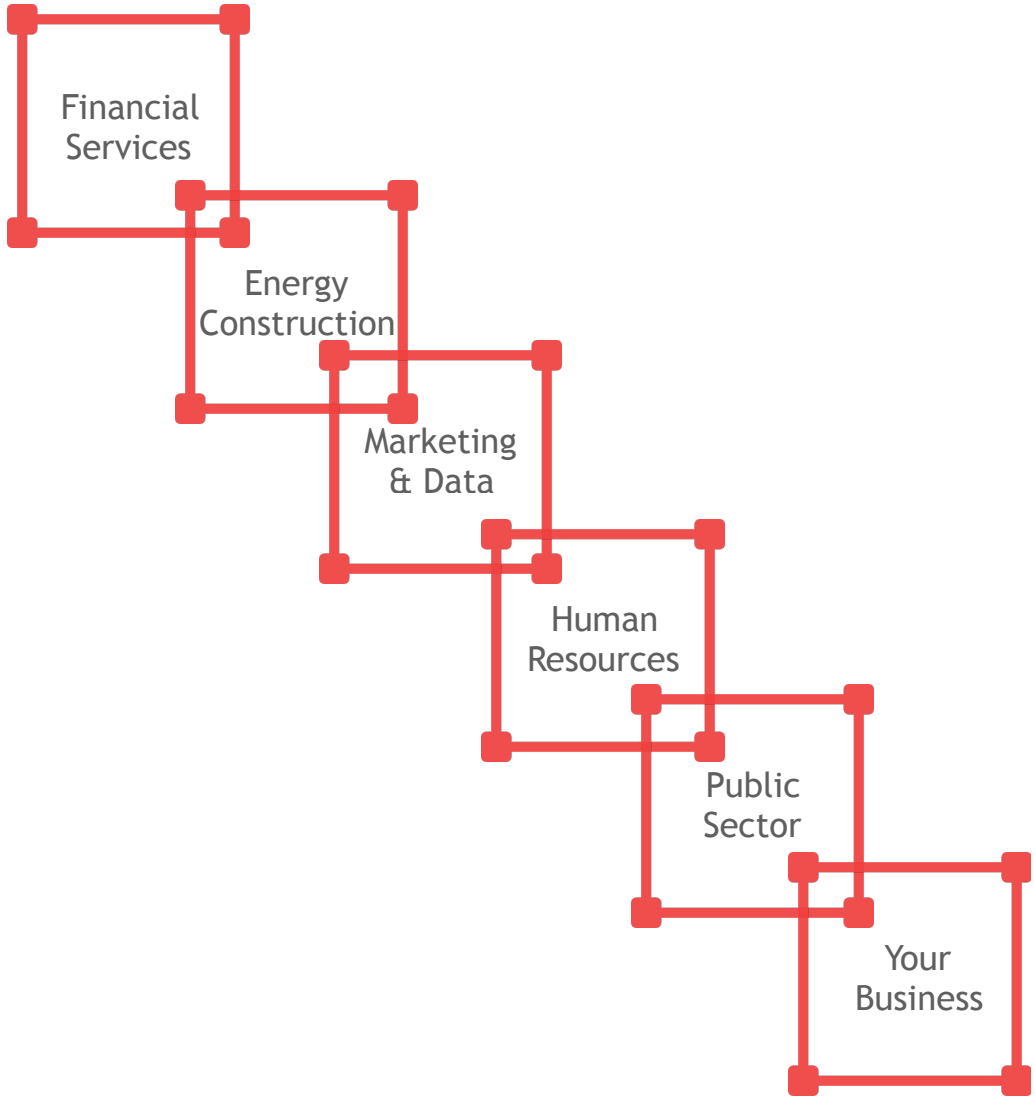
Governance
- Enhanced Transparency Obligations
- Data Protection Officer (DPO) Appointment
- Optimized Governance Structure
- Imposition of large scale penalties

Information Systems & Internal Processes
- Data Protection Impact Assessments (DPIAs)
- Data Breach Notification Obligation
- Internal Data Inventories Requirement
- Security by Design & Risk Consideration

Global Effect
- Global Scope Alignment
- Increased Territorial Scope & Cross-Border Transferal

Key Companies

- Every company that holds or processes personal identifiable information (PII) belonging to an EU citizen, falls under the scope of GDPR, no matter where their headquarters are located.
- Some industries have by default a more direct and significant impact to their operations, due to their nature.
- Such key business areas include consumer businesses, large conglomerates, financial services and any service line processing high volumes of data



Get prepared

- Increase **awareness** to decision makers and key people
- Document the **personal data** you hold.
- Communicate **Privacy Information** on time for GDPR implementation.
- Safeguard **Individuals' rights**.
- Manage **Access Requests**.
- Ensure **Legal Basis** for Processing Personal Data.

- Acquire **Explicit Consent**.
- Manage **Data Breaches**.
- Implement **Data Protection** by Design. Get familiarize on Privacy Impact Assessments.
- Appoint a **Data Protection Officer**.
- **Think Globally** in case your organization operates internationally.

I should act now if…

- Are there any **activities taking place** within the EEA?
- Is your **website directed towards customers based in the EEA**, for example by giving an option to choose a “UK” setting, an EEA currency, or a particular language?.
- Can your **services be bought from within the EEA**?
- Do you have a registered establishment or an **office in the EEA**?

- Is your business currently **registered with an EEA data protection authority**, such as the UK’s Information Commissioner’s Office (the “ICO”)?
- Do you use **servers located in the EEA**?
- Do you **monitor the behavior** of any individuals within the EEA (irrespective of their nationality or habitual residence)? For example, if your website uses tracking cookies, then you are “monitoring individuals” for the purposes of the GDPR

What to do…

- **Conduct a data audit**

Data controllers and processors alike are required to keep records of their personal data processing. Analyze your systems and practices to check what personal data you process, why, how you use them, where they are stored and whether you still need them. Check whether you process them in accordance with one of the permitted legal grounds (e.g. has the individual given their consent, or is the processing necessary for the performance of a contract with the individual, or necessary for a legitimate business interest). “Sensitive” personal data are subject to stricter rules and processing usually requires the individual’s consent.

- **Draft or amend policies and procedures**

The GDPR strengthens and adds to individuals’ rights, adds a new right of “data portability” and shortens timelines for compliance with individuals’ requests. It also imposes new obligations on all data controllers to report personal data breaches “without undue delay”. It introduces a new concept of “privacy by design”, which requires businesses to think about protecting individuals’ privacy at the very beginning of any new project and to conduct “privacy impact assessments” calculating the potential risks to individuals’ privacy rights. Businesses will need to update (or draft) policies and procedures to ensure compliance with these obligations.

What to do…

- **Inform individuals about your processing through fair processing notices**

Individuals must be kept informed about the processing of their personal data. The GDPR increases the amount of information which must be included in these notices. Privacy policies will need to be updated and businesses will need to amend (or draft) notification forms.

- **Amend or put contracts in place with data processors.**

The GDPR requires data controllers to have contracts in place with all of their data processors, containing certain elements specified in the GDPR.

- **Appoint a data protection officer**

Many businesses will be required to appoint data protection officers, or may choose to do so voluntarily, given the increased risks associated with data protection.

1) Data audit
2) Policies and Procedures
3) Processing notices
4) Contract with data processors
5) Data protection officer

What we can do for you...

Assess operational impact on Company’s operations resulting from GDPR requirements - Data processing activities must be identified and documented

Impact assessment, threat analysis, control assessment, risk assessment, DPIA report

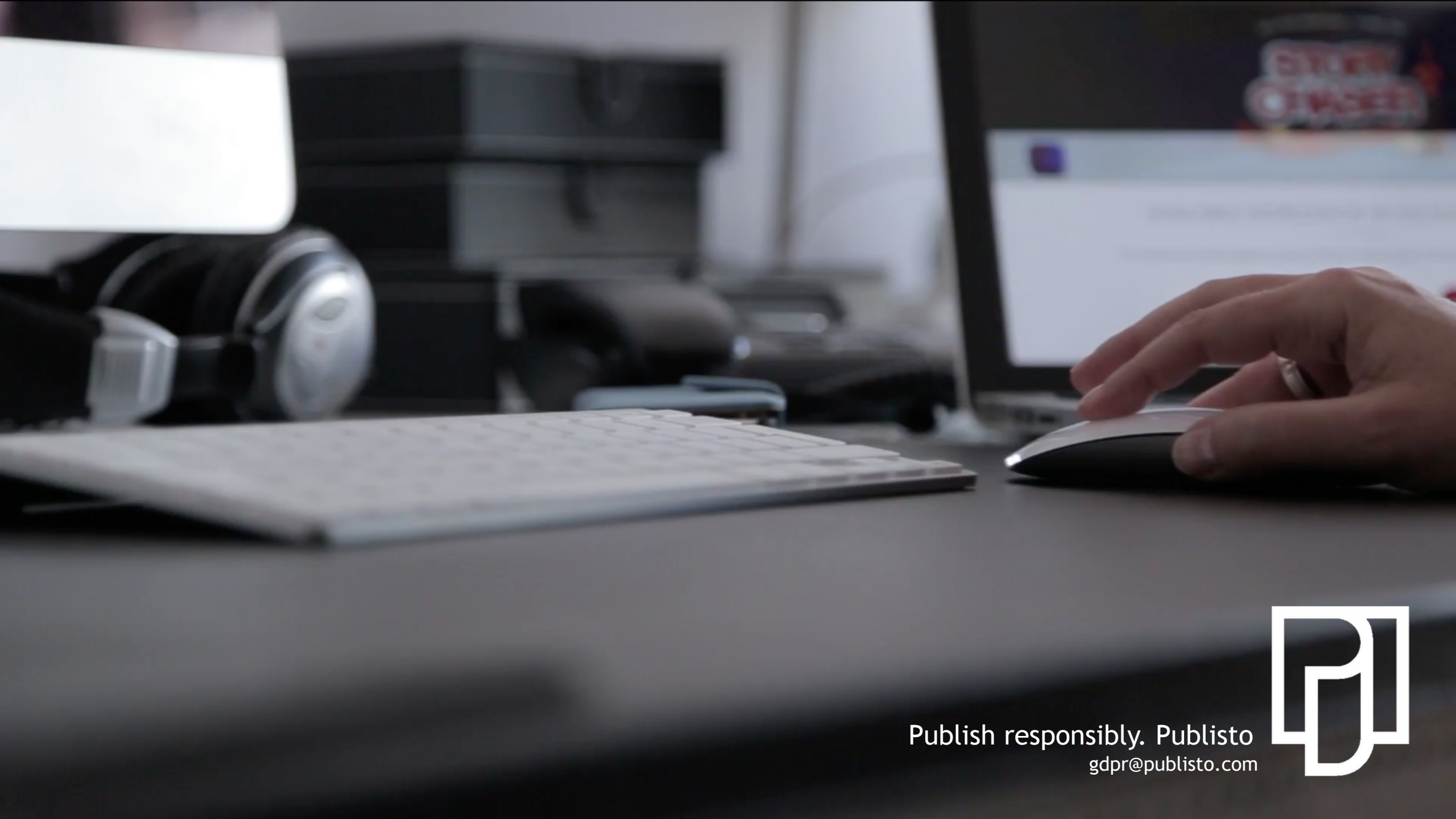
Appropriate data protection processes to ensure the rights of the data subject must be implemented.

GDPR project will change the business, it is not only about IT or Legal to become compliant

IT-Legal-Consultant: an ideal team for GDPR results

We aim to protect our clients by changing the way they think about data. Our team comprises with the rights mix of established GDPR legal experts, hardcore IT professionals and seasoned business consulting persons.

We are looking forward to your inquiries about our credentials and method.


Publish responsibly. Publisto
gdpr@publisto.com