Latest Developments in Data Protection Regulations and Case Law

USE OF DATA PROCESSORS

Radoslava Makshutova

ATTORNEY, CIPP/E, PHD CANDIDATE

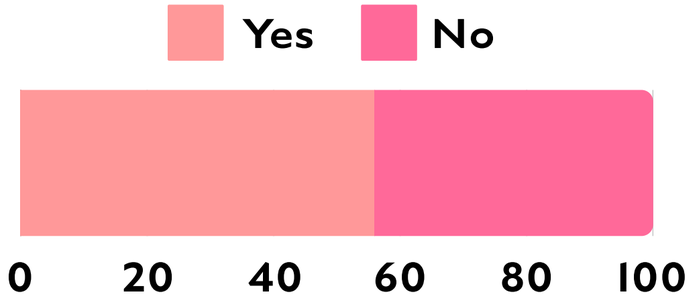
VEDA Legal

EMPOWERING ENTREPRENEURS.
PROTECTING INNOVATION.

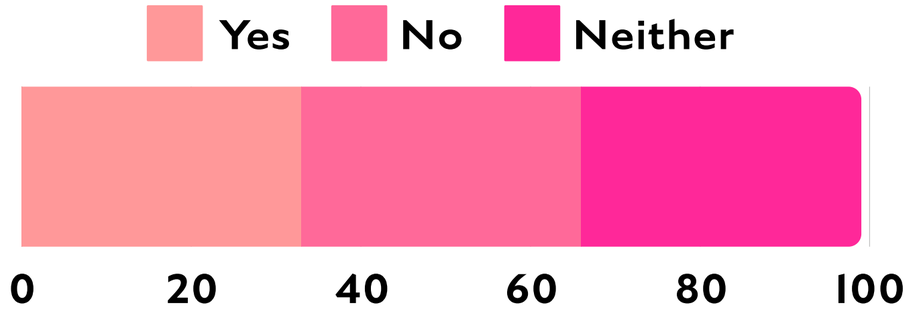
SOME STATISTICS FOR BEGINNING

VEDA LEGAL

Do you avoid using certain websites, apps or social media due to privacy concerns?



Do you feel that you have control over your personal information online?



OECD (2024), OECD Digital Economy Outlook 2024 (Volume 2): Strengthening Connectivity, Innovation and Trust, OECD Publishing, Paris,

WHY THIS TOPIC?

- Every business uses at least one data processor, most use multiple
- Rules for engagement of processors are hard to apply in practice, making this one of the most challenging aspects of personal data protection
- Data is as a rule most vulnerable when transmitted
- Controllers are obliged to have an extensive data processing agreement with mandatory requisites with each of their processors
- In case of data breaches involving processors detailed data processing agreements are key for protection of the controller’s interests

USE OF PROCESSORS OVERVIEW

In brief data processor (or just processor) is a separate entity (a natural or legal person, public authority, agency or other body) which:

- processes personal data on behalf of the controller and under its instructions
- does not determine the means and purposes of the processing
- acts in accordance with a contract with the controller (or other legal act)

Frequent examples of processors used by most organisations:

- Cloud hosting
- External IT support
- External customer support centres
- External payroll
- Email marketing

SO WHAT IS NEW?

In October 2024 the European Data Protection Board issued a new opinion on controller's obligations in respect to processors after request of the Danish data protection authority to clarify certain matters.

In January 2025 the Bulgarian Commission for Personal Data Protection issued further guidelines to controllers who engage processors.

OPINION OF THE BOARD

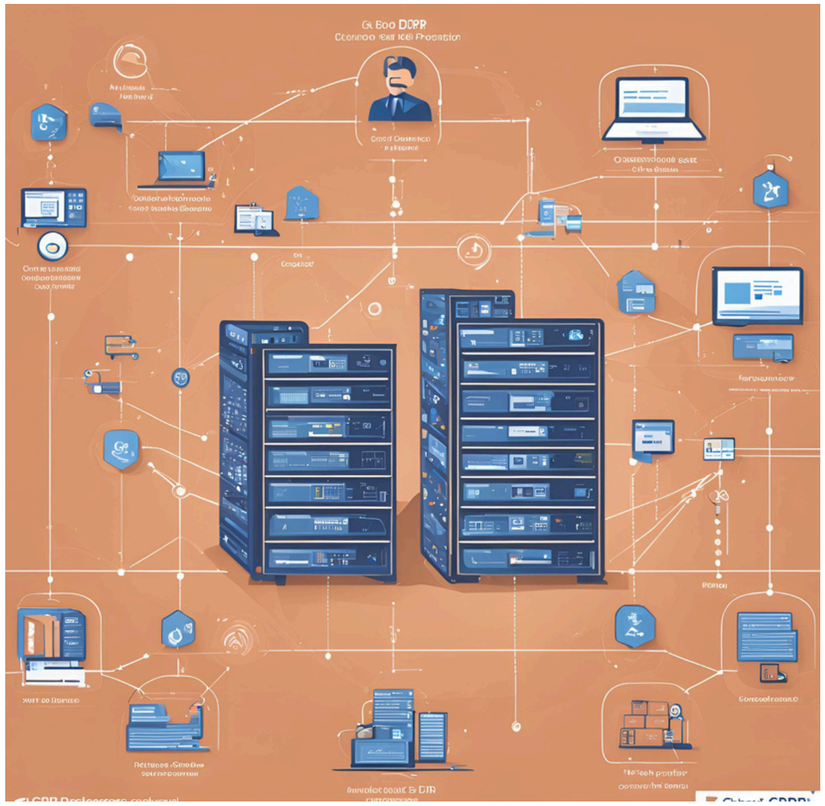
Most important takeaway

The engagement of processors should not lower the level of protection for the rights of data subjects compared to a situation where the processing is carried out directly by the controller.

OPINION OF THE BOARD

Q: Must the controller identify all of the processor's sub-processors, throughout the chain?

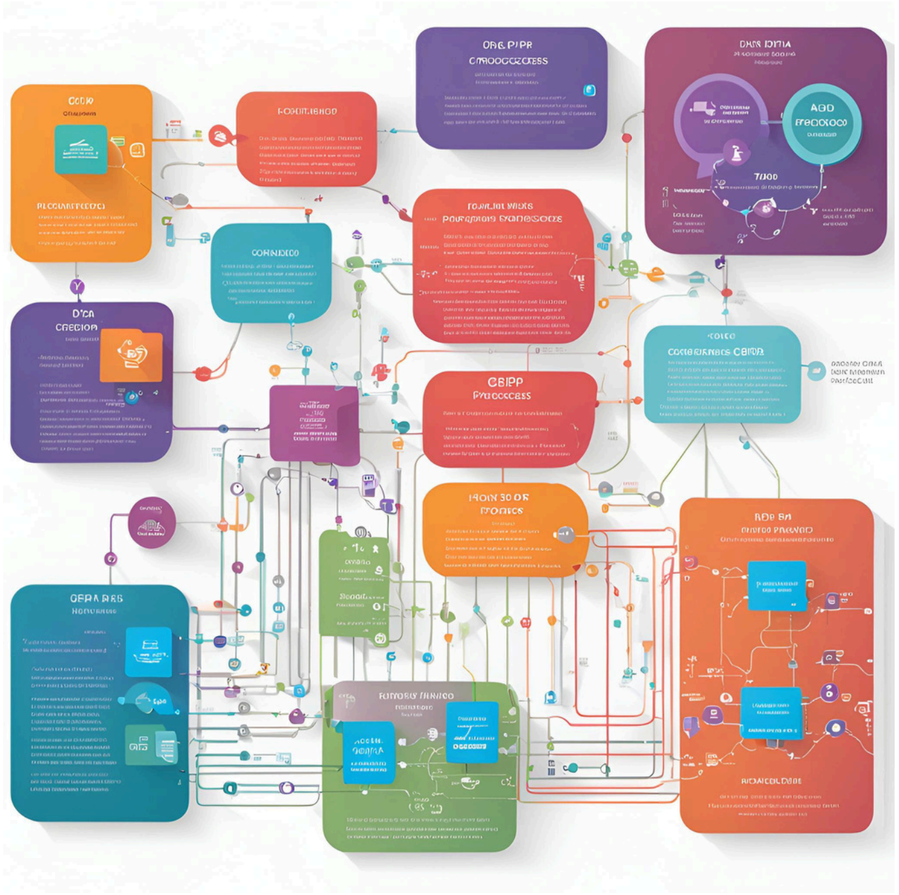
A: the short answer is yes.
Controllers should have the information on the identity (i.e. name, address, contact person) of all processors, sub-processors etc. readily available at all times, regardless of the risk associated with the processing activity. The processor should proactively provide to the controller all this information and should keep it up to date at all times.



OPINION OF THE BOARD

Q: To what extent and in which level of detail must the controller verify and document the technical and organisational measures taken by processors and subprocessors?

A: The extent of such verification will in practice vary depending on the nature of the organisational and technical measures based on, among other criteria, the risk associated with the processing.



GUIDELINES OF THE CPDP

Most important takeaway

Controllers must undertake numerous steps before providing personal data to a processor.

GUIDELINES- BUGARIAN CPDP

The controller must determine which personal data will be processed on the controller's behalf, in what form and to what extent, including to:

- carry out an initial risk analysis and to take the outcome of this analysis into account in its subsequent actions
- define the access limits of the processor for which two principles may be applied:
  - "need to know"
  - "need to use"

GUIDELINES- BUGARIAN CPDP

The controller must assess whether the safeguards provided by the processor are sufficient to ensure compliance with GDPR, including:

- to take into account the following elements:
  - the expertise of the processor (e.g. technical and expertise on security measures and data breaches),
  - the reliability of the processor, including its reputation in the market,
  - the resources of the processor.
- to be able to provide the analysis/risk assessment and its conclusions, and to carry it out again at appropriate intervals.

GUIDELINES- BUGARIAN CPDP

The processor must demonstrate to the satisfaction of the controller that it will implement specific rules to certain aspects of personal data protection:

- adaption to the particular categories of personal data to be processed;
- physical location of the records (servers);
- ongoing confidentiality, integrity, availability and resilience of the processing systems and services;
- means of accessing and making available personal data;
- control mechanisms, including access control, monitoring, reporting and auditing
- an explicit list of the processor's employees authorised to access or receive information, including employee declarations
- procedures for managing personal data breaches.

GUIDELINES- BUGARIAN CPDP

The data processing contract must include (in addition to GDPR's requirements):

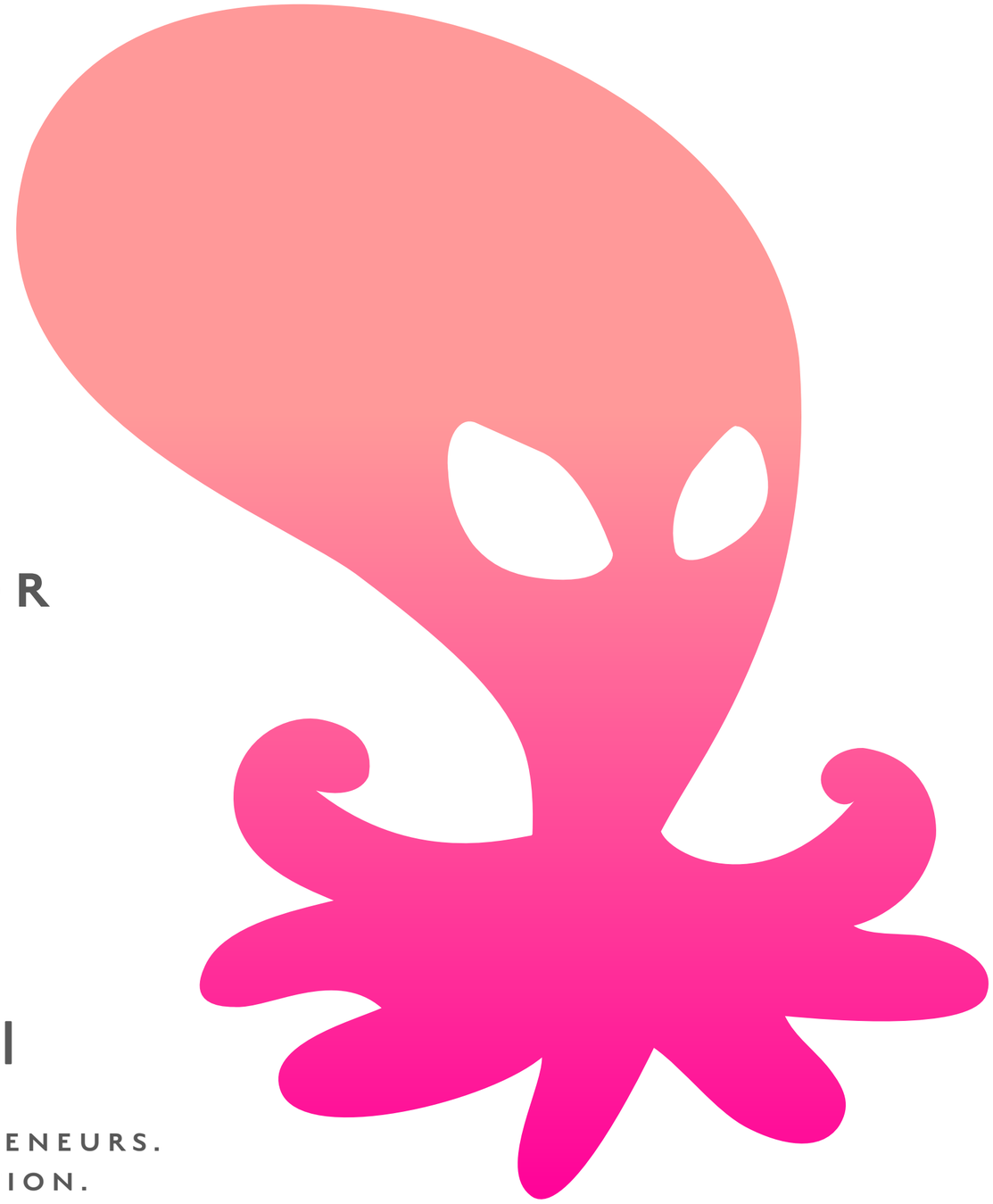
- manner of provision of personal data
- keeping of logs of processing activities in automated processing systems
- staff training
- processes and procedures for monitoring compliance with agreed processing security requirements
- conditions and actions in the event of a contract change
- portability - how and for how long data is stored after transmission
- actions in case of security breaches, including restoring the availability of data
- grounds for termination of the contract

GUIDELINES- BUGARIAN CPDP

In case of technical service, a Service Level Agreement (SLA) must be signed and must include:

Description of the service provided	Communication channels	Backup policy
Efficiency/quality of the service	Backup policy;	Scope of the service - development, test, production, etc.
Availability - time period and failover time	Security measures and security levels	Monitoring and audits
Change management	Termination of service	Deletion and destruction
Incidents and breaches	Sanctions for non-compliance with SLA	SLA review

THANK YOU AND I AM HERE FOR YOUR QUESTIONS!



Radoslava Makshutova

ATTORNEY, CIPP/E, PHD CANDIDATE

VEDA Legal

EMPOWERING ENTREPRENEURS.
PROTECTING INNOVATION.