
MOORE STEPHENS
2018
Moore Stephens KSC
GDPR Implementation
Event Recap Booklet

TABLE OF CONTENTS

About our event

The General Data Protection Regulation changes the economic landscape

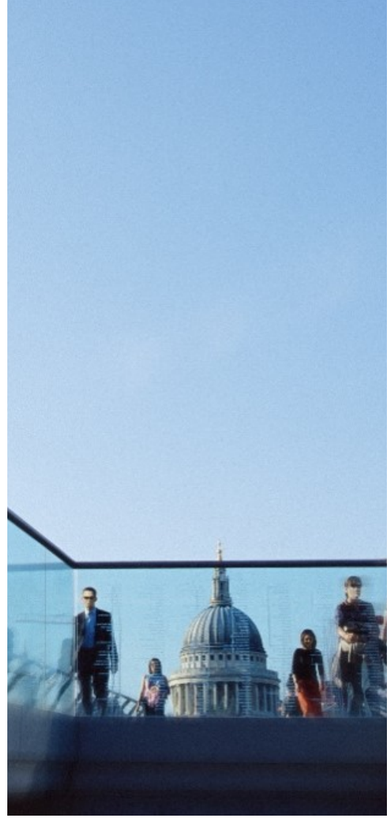
On 26th February 2018 British Romanian Chamber of Commerce (BRCC) and Moore Stephens KSC arranged an event on the General Data Protection Regulation (GDPR).

The objective of event was to give participating entities a comprehensive introduction to the GDPR and a practical understanding of the implications and legal requirements for organisations - helping them to prepare correctly and avoid the applicable fines for non-compliance.

Amongst the keynote speakers of the event were Mr. Thomas Baekelandt-the Ambassador of Belgium to Romania, Mr. Dimitris Hatziargyrou-the Ambassador of Cyprus to Romania, Mr. Gerard Healy – Head of Economic Diplomacy British Embassy, Mr.Mamas Koutsoyiannis– CEO, Moore Stephens KSC & Board Member of the BRCC, Ms.Oana Luisa Dumitru-Head of International Affairs Department National Supervisory Authority for Personal Data Processing, Ms.Valentina Ion-IT Audit & IT Advisory Partner, Moore Stephens KSC & Managing Partner of BIT Advisory Services,Mr.Andrei Stan-Partner, Moore Stephens KSC, Ms.Andreea Tigau–Chief Liability Underwriter, CertAsig, Mr.Mihai Bizineche- Chief Underwriting Officer, CertAsig.

In less than six months, Europe's data protection rules will undergo their biggest changes in two decades. The GDPR's focus is the protection of personal data, i.e. data about individuals, and builds on existing data protection laws, setting out the responsibilities of businesses in relation to the personal data they collect, hold, transmit and otherwise use. The GDPR is extra-territorial in nature and applies not just to organizations within the EU who process the data of individuals but also organizations outside the EU who offer goods or services to individuals in the EU, or who monitor the behavior of individuals in the EU.

Organisations have until 25 May 2018 to fully comply with the new GDPR regulations and it is imperative that organisations fully understand the requirements of GDPR and prepare well in advance to avoid being hit with heavy fines. Breaches within the regulation around the collection, usage and maintenance of personal data are significant, but the loss of customer and stakeholder confidence leading to a loss of reputation could be terminal. The possible fines for non-compliance can start from 2-4% of the global turnover up to EUR 20 million, depending on which of them is higher.



GENERAL DATA PROTECTION REGULATION'S NOVELTIES IMPLICATIONS ON DATA CONTROLLERS' ACTIVITY

Material scope

- By a natural person in the course of a purely personal or household activity
- By competent authorities for the purpose of prevention and prosecution of offences – Directive 2016/680
- Activity which falls outside the scope of Union law
- Activities which fall within the scope of Chapter 2 of Title V of the TEU

Territorial scope

GDPR is applicable to:

- Processing of personal data by a controller / processor within EU
- Processing of personal data of data subjects who are in the Union by a controller/processor outside EU if the processing is related to:
- Offering of goods or services to persons who are in the EU
- Monitoring the behavior of the EU persons

Data Protection Officer

Mandatory:

- public authorities and bodies, except courts
- regular and systematic monitoring of data subjects on a large scale
- processing on a large scale of special categories of data pursuant to Article 9 and personal data relating to criminal convictions and offences referred to in Article 10

(eg. racial or ethnic origin, political opinions, genetic data, biometric data, health data, criminal convictions)

GENERAL DATA PROTECTION REGULATION'S NOVELTIES IMPLICATIONS ON DATA CONTROLLERS' ACTIVITY

Data Mapping

Article 30 of GDPR is applicable:

- Data controllers from public sector
- Data processors
- Data controllers from private sectors with more than 250 employees

DPIA

Required for processing likely to result in a high risk:

- Systematic and extensive evaluation through automated processing on which decisions are based that produce legal effects concerning the natural person (e.g. profiling, predicting)
- Processing on a large scale of special categories of data (e.g. biometric data, genetic data) or of personal data relating to criminal convictions and offenses
- Systematic monitoring of a publicly accessible area on a large scale (e.g. CCTV).

Consultation ANSPDCP

Review of the impact assessment

Rights (currently)	Rights (after May 25, 2018)
Information (Article 12)	Information (Article 13, Article 14
Access (Article 13)	Access (Article 15)
Intervention (Article 14)	Rectification (Article 16, Article 19)
-	Deletion (Article 17, Article 19)
-	Restriction (Article 18, Article 19)
-	Portability (Article 20)
Oppose (Article 15)	Oppose (Article 21)
Individual automated decisions (Article 17)	Automated decisions, profiling (Article 22)
Restrictions (Article 16)	Restrictions (Article 23)

HOW TO IMPLEMENT GDPR?

Gap Analysis

- **Resources**
- **People**
- **Data**
- **Processes**

Readiness assessment

GDPR Implementation

- **Data Flow Mapping**
- **Update organizational structures, policies and procedures organizational**
- **Change in IT systems**
- **Staff Training**
- **Regular Assessments and updates**

READINESS ASSESSMENT

Legal Basis for Processing

- Has a legal basis been documented for each processing activity?
- Are there processing activities that exceed the initial scope?
- Have a consent mechanisms been reviewed in order to ensure they remain valid

Data Security and Integrity

- Has data been properly identified/ classified?
- Are regular security assessments being performed?
- Have you adopted security measures such as: encryption and pseudonymization
- Have you implemented a proper BCP/DRP procedure?

Data Subjects Rights

Have procedures been implemented so data subjects can practice their rights to:

- Access
- Rectification of inaccurate or incomplete data
- Blocking of data whose accuracy is contested
- Erasure of data (right to be forgotten)
- Portability

Data Protection by Default and by Design

- Have you property analyzed risks and have you implemented proportional controls?
- Do you practice data protection by design and by default (e.g. when implementing new applications)
- Have you implemented security mechanisms (encryption etc) by default?
- Are there processors to identify an external party (eg. processor data breach?

Transparency

- Has the right to object to processing for direct marketing been communicated clearly to the data subject?
- Are notices given in a clear and transparent manner?
- Have the notices been reviewed and updated to ensure GDPR-compliance?

DPIA

- Have you defined a procedure to ensure a DPIA is performed whenever necessary?
- Are you aware of the cases when DPAs must be noted?
- Are you properly involving the DPO in carrying out DPIAs?

Controllers Obligation

- A representative been named in the EU?
- Are data flows properly documented?
- Are data protection mechanisms regularly updated?
- Has your Organization adhered to specific GDPR codes of conduct or certification?

DPO

- Is your Organization required to name a DPO and have you named one?
- Has the DPO role been properly defined?
- Is the DPO properly involved in data protection activities in your Organization?

Data breaches

- Have you defined adequate procedures to identify and notify appropriate parties (DPAs, data subjects) in the event of a data breach?
- Have you defined a Security incident response plan?
- Are there processors to identify an external party (eg. processor data breach?

Data Transfers

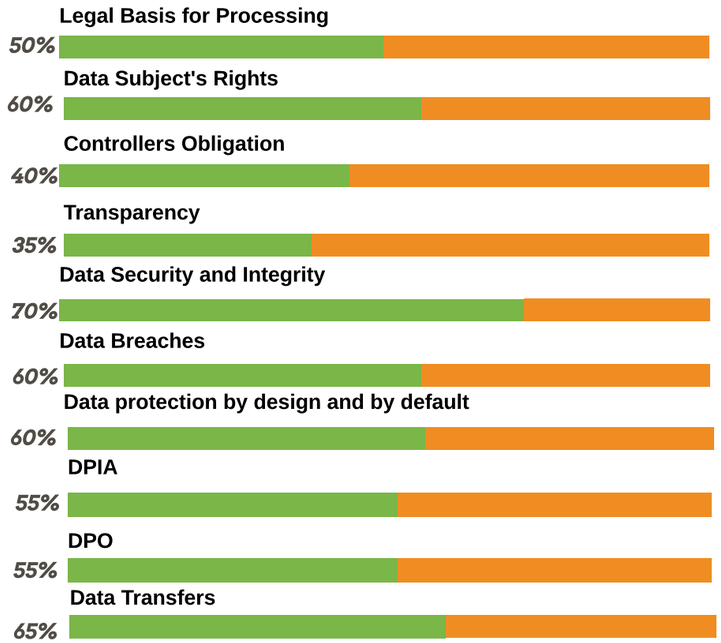
- Have all transfers been properly documented?
- Are you implementing adequate safeguards for third countries transfers?
- Are you requiring suppliers to implement adequate security measures?

GDPR READINESS ASSESSMENT-SAMPLE REPORT

Overall Readiness:55%

Assessment Summary

72	43	29	0
Questions	Compliant	Gaps	Unanswered



GDPR IMPLEMENTATION CHALLENGES

- **Breach notification**

Notification of breaches becomes mandatory in all member states when as a result of a breach there is a risk that the rights and freedoms of individuals could become compromised. Under GDPR, the notification must be reported within 72 hours of the breach being identified.

Data processors are also required to notify their customers, the controllers, “without undue delay” after identifying any breach.

- **Data portability**

GDPR introduces data portability – the right for a data subject to receive the personal data concerning them, which they have previously provided in a commonly used and machine readable format and have the right to transmit that data to another controller.

- **Right to access**

The rights of data subjects have been strengthened somewhat under GDPR. The data subject now has a right to obtain confirmation where and how their personal data is being processed, and for what purpose, from the data controller.

As a result of this request, the data controller must provide a copy of the personal data held, free of charge, in an electronic format further strengthening data transparency requirements.

- **Right to be forgotten**

Under GDPR, the data subject now has the right to be forgotten which entitles the data subject to have the data controller erase their personal data, cease further dissemination of the data, and potentially have third parties halt processing of the data.

The conditions for erasure include the data held no longer being relevant for the original purposes it was collected for processing, or a data subject withdrawing their consent for the data to be used.

It should be noted that data controllers should compare the data subjects rights to the “public interest in the availability of the data” when considering such requests.

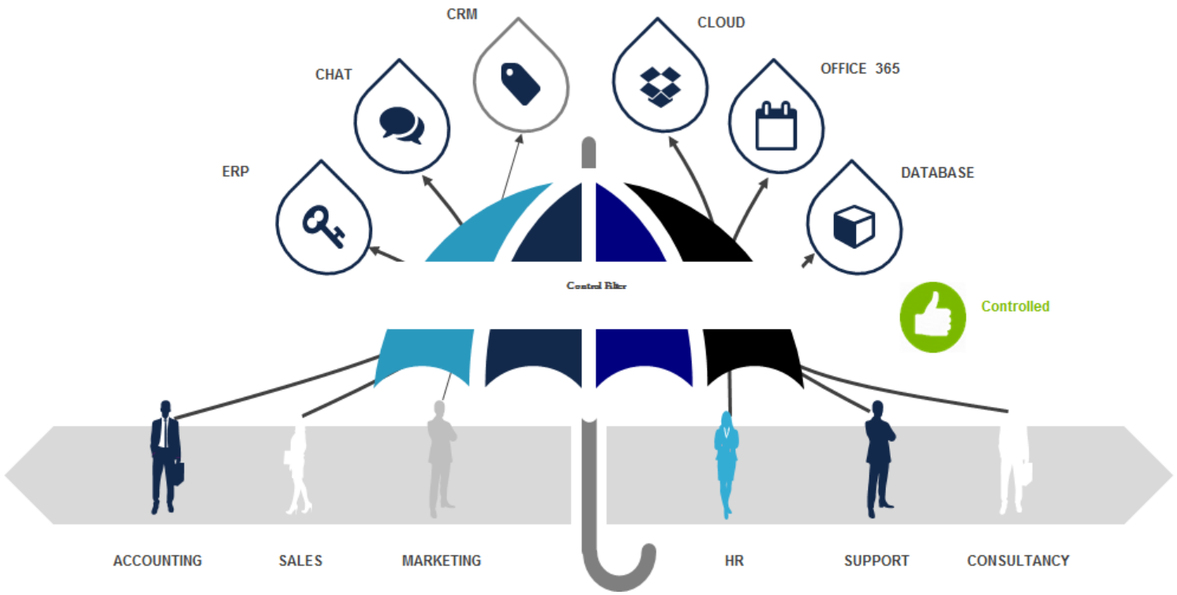
- **Privacy by design**

Now a legal requirement within GDPR, privacy by design calls for the inclusion of data protection from the onset of the designing of systems, rather than an addition.

This will ensure that the controller meets the requirements of this regulation and protects the rights of data subjects.

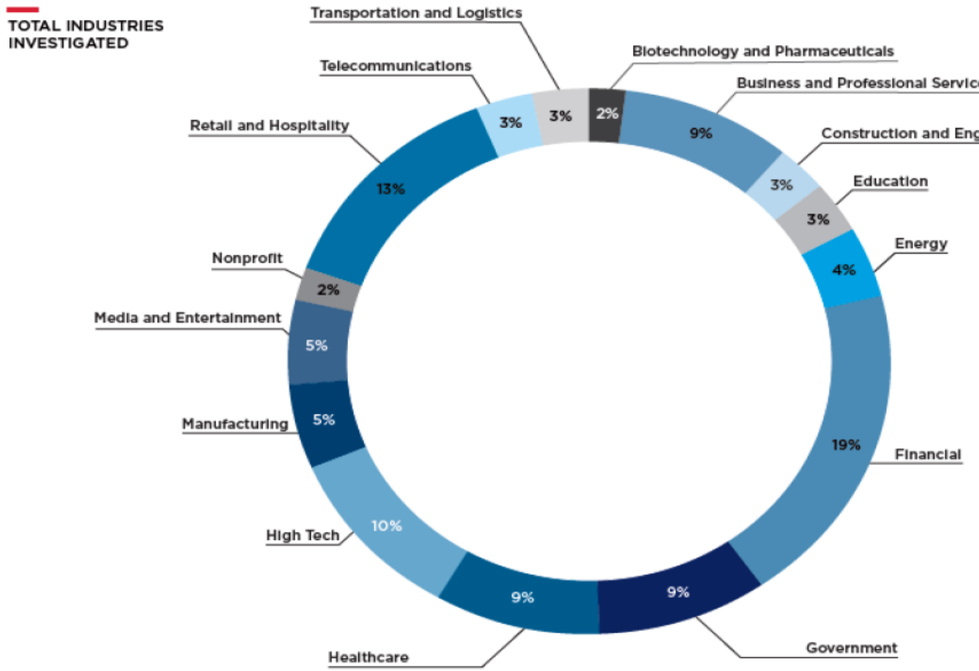
To do this, controllers are to hold and process only the data absolutely necessary for the completion of its duties, as well as limiting the access to personal data to those needing to act out the processing.

ORIGINATION OF DATA



CYBER RISK

60% of SMEs are bankrupt in 6 months from a cyber attack.



CYBER RISK

Over 90% of the cost of cyber-attacks are hidden for Business

Above the Surface- Cyber Incident Response Expenses	Below the Surface- Hidden or less visible costs
Incident response manager fees	Operational disruption or destruction
Customers breach notifications	Increased cost to raise debt
Post-breach customer protection (e.g.: Costs to set up and operate a call center)	Lost value of customer relationships
Regulatory compliance (fines)	Value of lost contract revenue
Public relations/Crisis communications expert fees	Devaluation of trade name
Incident response manager fees	Loss of intellectual property (IP)
Attorney legal fees and litigation	Insurance premium increases
IT forensics investigation costs	-
Cyber-security improvements	-

HOW MOORE STEPHENS CAN HELP?

There are a number of aspects to the GDPR that will take some organisations considerable time to achieve and all organisations should be looking at this now. This draws on a range of governance, risk and assurance capabilities as well as in-depth technical and data protection skills. Our cost effective services help you to:

- **Educate**: your senior management and employees on the changes that the GDPR will bring: ensuring that they are fully aware of regulations and how the changes will affect the organisation.
- **Architect** your risk, policy and procedure environments to help you ensure your business operates effectively in line with the GDPR regulation requirements.
- **Assure** the processes you have in place around GDPR giving you independent and timely information on the state of your management in relation to GDPR regulation requirements.
- **Manage** your GDPR requirements and objectives, making sure you blend education, architecture and assurance in a way that is appropriate to your operation

Educate

GDPR Organizational Culture

Benchmarking

Board Awareness

Staff Training

Assure

Processes

Third Parties

Architect

Policies

Procedures

Expected Best Standards

Risk Management

Manage

DPO Outsourcing

CONTACT US

We have offices located in Romania and the R.Moldova who can provide tailored services to your business. For more information on how we can help you succeed contact us on the information below

Moore Stephens KSC

Bucharest Office

014472, 175 Calea Floreasca, Floreasca Tower building, 13th Floor, District 1 Bucharest – Romania

T: +4 0374 490 074

F:+4 0374 094 191

E: info@moorestephens-ksc.ro

www.moorestephens-ksc.ro

Timisoara Office

30056, 1 Ionel Bratianu Square, Bratianu Real Estate Timisoara – Romania

T: +4 0374 490 074

F:+4 0374 094 191

E: info@moorestephens-ksc.ro

www.moorestephens-ksc.ro

Chisinau Office

MD 2004, 202 Stefan cel Mare Bvd., Kentford building, 9th floor Chisinau – Moldova

T +373 22 022 555

F: +373 22 022 556

E:info@moorestephenes-ksc.md

www.moorestephens-ksc.md