WOLF THEISS

Supporting the international growth and development of Entrepreneurial Businesses

Data Protection and Privacy

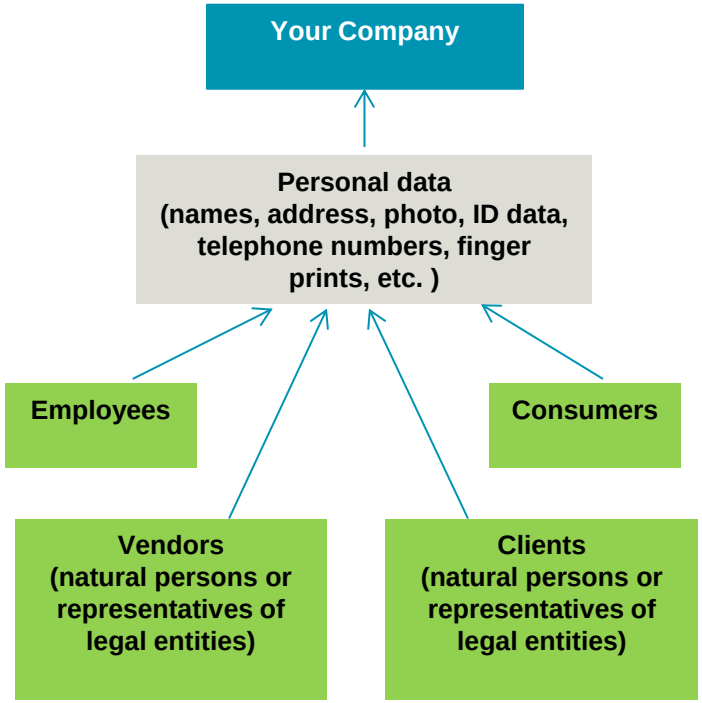
September 2016

Why a Business Should Consider the Data Protection Rules

What is Personal Data?

Personal data is ***any data*** related to a ***natural person*** which may reveal his/her ***identity*** .

Below are the main groups of individuals whose personal data is processed by companies on a daily basis:



Do Data Protection Laws Apply to Your Company?

Processing of personal data is regulated under Bulgarian and EU law.

If you are a business which processes personal data in Bulgaria or maintains local means by which personal data is processed (e.g. servers, data centers, etc.), on ***its own account*** and for ***its own purposes***, Bulgarian data protection law will most likely apply to you.

Main Obligations of Data Controllers

If the above criteria is met, your company would qualify as a ***data controller*** and have the following main obligations**:**

1. Register as data controller with the Bulgarian Commission for Personal Data Protection ('**CPDP**')
2. Register the separate registers with personal data with the CPDP (e.g. Register HR, Register Clients, etc.)
3. Determine appropriate organizational and technical safety measures
4. Adopt Internal Rules on Data Processing setting the internal organization, appropriate compliance measures and responsible persons

Personal Data in Employment

Dealing with data protection and privacy rules in employment

Employment data is one of the main categories of personal data a business normally processes. Also it is one of the categories of personal data that is most regulated. Below are some Q&As, illustrating data protection requirements in various employment situations:

Processing of employees' data upon entering into employment

- Is the consent of the employees needed for processing their personal data? **–** No, if processing is limited only to statutory required data and used only for statutory required purposes (labour, tax, social security). Otherwise consent is required.
- How far can you go in recruitment procedures? **–** Only to the extent relevant for the position. If requested data or other measures (investigations, interviews with referees, etc.) are excessive, there would be a breach of the person's privacy.
- Can you take a copy of the ID card of your employees? – Only with the consent of the employee.
- Can you disclose the personal data of your employees to third parties without their consent? – Only in limited cases, specified under law . Otherwise, consent is required.
- Can you disclose personal data of your employees for the purposes of due diligence report in the course of a transaction? – Only with the consent of the employees.

Monitoring of employees' correspondence

- Is the consent of the employees needed for monitoring of their correspondence? - Employers don't need consent for monitoring professional correspondence but if employees also have personal correspondence (e.g. used the corporate e-mail for personal purposes), their consent will be required.
- How do you know if the correspondence is personal or professional? – You don't, until the correspondence is accessed (which may already qualify as a breach). Thus, most employers set explicit rules on personal use of communication.
- Do you have to inform the employees, even if only professional correspondence is monitored? - Yes, employees should be informed that their correspondence is monitored as well as of the purposes and intensity of such monitoring.

Video surveillance of employees

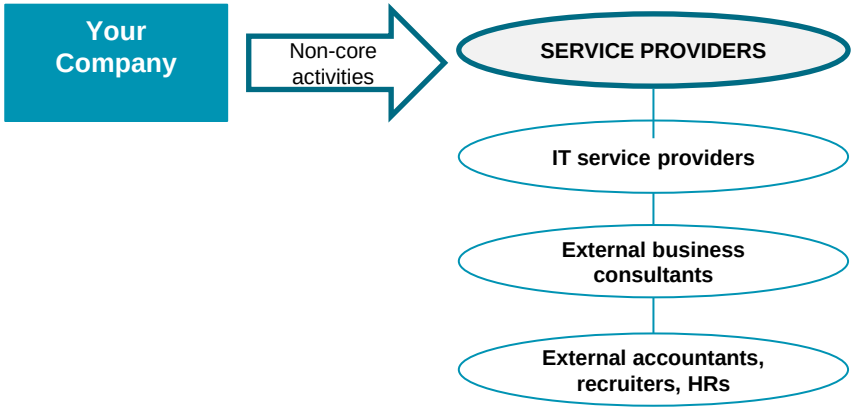
- Is the consent of the employees needed for implementing video surveillance in the office premises? – Unless the video surveillance is required under law (e.g. for banks, etc.), the consent of the employees shall be prior obtained.
- What if only part of the employees consent? – Then the employer can implement video surveillance only to those employees who have consented.
- Other requirements for video surveillance? – Employees shall be always informed of the video surveillance as well as of the purposes, of surveillance, the types of data, etc.

Personal Data and Privacy in Relations with Vendors

What data protection considerations should a business have in mind when contracting with vendors?

A business may outsource some of its non-core activities to external providers, or use service providers for specific activities.

From a data protection perspective, since external providers would process personal data on behalf of the business (not for their own) purpose , the business remains jointly liable with the provider for how data is processed.



Relations with service providers under Bulgarian law

- Service providers , generally, do not have all obligations of data controllers when processing data
- Thus, the data controller has the obligation to take necessary measures and ensure that personal data would be lawfully processed
- The scope, purposes and operations of the service provider towards the disclosed personal data shall be arranged in a written agreement with the data controller
- For breach of data protection rules, the service provider and the business undertaking are jointly liable

Considerations when using cloud services

- Use a trustworthy cloud providers - the cloud service provider is a regular service provider, thus the business undertaking is jointly liable for any data breaches;
- Make sure to know where the cloud is – if it is outside EU, storing the data on the cloud would qualify as data transfer and require additional measures (consent, permits, etc.);
- Define the access and purposes of access to the data by the cloud provider – the cloud provider should have limited access to the data, otherwise the concerned individuals may need to provide additional consent;
- Impose strict safety measures on the cloud provider – if it is outside EU, ensure that organizational and technical measures comply with the EU standards
- Ensure that data breaches/leakage will be notified in short term – under the new EU Regulation there are notification obligations in case of data leakage and high fines for delay

Transfers of Personal Data to Other Countries

Does your company conducts transfers of personal data?

In daily operation, business undertakings usually make a number of data transfers. Even sending an-email with personal data to another country qualifies as data transfer.

Transfers of personal data in a nutshell

- Transfer of personal data means ***the export of personal data*** , in hard copy or electronically (via e-mail, by storing documents in clouds, etc.), ***from one country to another.***
- Transfers of personal data to companies in other ***EU countries are free***.
- Transfers of personal data to countries ***outside EU are subject to prior permission*** by the CPDP, with some exceptions.
- Under Bulgarian law even ***intra-group transfers*** outside EU are subject to the same permission procedures.
- In some cases, transfer of personal data may require ***the consent of the concerned individuals*** whose data is transferred

How to make data transfers to third countries without need of permission

- ***Countries where adequate level of data protection has been ensured –*** if your company transfers data to some of the third countries for which the European Commission (EC) has confirmed that they adequate level of protection, no permission will be required. Such third countries include Switzerland, Israel, New Zealand, etc.

- ***Transfers under Standard Contractual Clauses, adopted by the European Commission -*** EC has developed standard contractual clauses for transfers of personal data to third countries which contractually ensure that adequate safeguards to the privacy and fundamental rights of individuals are put in place. Data transfers based on the EC standard contractual clauses are exempted from additional permissions.

- ***The new EU-US Privacy Shield –*** the EU and US government bodies recently reached an agreement on data transfers - the EU–US Privacy Shield. US companies who sign up to comply with the principles and requirements of the Privacy Shield, may receive personal data from EU under a facilitated regime. The Bulgarian CPDP is currently preparing a guidance on how the Privacy Shield would be applied in Bulgaria.

New EU Regulation on Personal Data

"Citizens and businesses will profit from clear rules that are fit for the digital age, that give strong protection and at the same time create opportunities and encourage innovation in a European Digital Single Market."

Věra Jourová, Commissioner for Justice, Consumers and Gender Equality

What you need to know about the new Regulation:

- Applies as of 25 May 2018
- Unifies data protection rules across EU Member States
- Applies also to businesses established outside the EU if they process personal data of EU citizens
- Imposes higher standards on data controllers to demonstrate compliance
- Introduces obligation for designation of Data Protection Officers
- Imposes Data Breach Notification Obligations in case of data breaches and data leakages
- Higher sanctions for breach of data rules - up to 4% of annual worldwide turnover of the data controller or EUR 20 million (whichever is greater)
- In Bulgaria, the CPDP has set up a Working Group to initiate the required amendments in Bulgarian law and align it with the Regulation. A Guidance on the application of the Regulation is expected.

Main benefits to businesses under the new Regulation:

- ***One stop shop:*** The Regulation aims to simplify the interactions of multinational companies which operate in a number of Member States with the separate national data protection regulators, by establishing the principle of having one "Lead Supervisory Authority" in EU. The competency of the Lead Supervisory Authority is determined by the data controller's country of "main establishment".
- ***Less Administrative Burden:*** In many cases the requirement to notify or seek approval from the national Data Protection Authorities would be replaced with self-regulation by the data controllers - to internally put in place effective procedures and safeguards
- ***More Options for Data Transfers:*** the new Regulation introduces new 'appropriate safeguards' for data transfers, including : approved codes of conduct, certification mechanisms, seals and marks and a new prescribed process for Binding Corporate Rules. Where relying on consent of the individuals, that consent must be explicit and the data subject must have been informed of the risks of the transfer.
- ***Benefits for SMEs:*** Start-ups and smaller companies may benefit from further regulatory and administrative exemptions, e.g. – SMEs may not be obliged to appoint a Data Protection Officer (unless the SME processes highly risky data); SMEs would also have less internal documentation obligations, etc.

Wolf Theiss: Strategic advice to clients across the region

- Real presence on the ground – our offices in 13 countries in the CEE/SEE region enable us to provide our clients with fully integrated and efficient service, irrespective of the jurisdictions involved
- One of the largest and most experienced teams in the CEE/SEE region – over 340 lawyers, focused on not only meeting but exceeding clients' expectations wherever possible
- Comprehensive full-scope legal advice to help make your opportunities happen
- OUR VISION: To be instrumental in building and safeguarding the future prosperity and success of our clients, our people and the markets in which we choose to operate

CHAMBERS AND PARTNERS

Austrian Law Firm of the Year: 2009, 2012 & 2013
Austrian Client Service : Law Firm of the Year 2011

THE LAWYER
www.thelawyer.com

Law Firm of the Year: Austria, 2014
Law Firm of the Year: Central Europe 2010 & 2014
Law Firm of the Year: Eastern Europe & The Balkans, 2009, 2012 & 2015

IFLR
INTERNATIONAL FINANCIAL LAW REVIEW

Austrian Law Firm of the Year: 2011, 2012, 2015 & 2016
Czech Republic Law Firm of the Year: 2010
Hungarian Law Firm of the Year: 2009

WOLF THEISS

Our data protection practice

Wolf Theiss has one of the strongest practices across CEE region providing unique expertise on data protection, IP and IT legal matters. Our expert lawyers advise on all aspects of data protection and privacy, offering practically oriented solutions and support in structuring and maintaining the overall data operations within a business undertaking. And because we provide tailor made advices to the particular client., Wolf Theiss have become the trusted advisor for data protection compliance of one of the biggest international companies operating across CEE in various industries - from pharmaceutical companies to financial institutions, hotel chains, outsourcing companies, etc.

In particular, our expertise includes :

- Support in all registration and notification procedures before the local Data Protection Authority
- Risk assessment of processed data and determining adequate technical and organizational measures
- Preparation of internal documents related to data processing
- Structuring relations with data processors and vendors
- Data protecting compliance in employment relations, preparing consent and information forms, etc.
- Structuring data transfers in the most suitable way from regulatory and business perspective;
- Obtaining approvals,/authorizations from the national Data Protection Authority.
- Legal representation in disputes before the Data Protection Authority
- Monitoring legislative changes and change in practice of the relevant authorities,

)

Wolf Theiss' 'professional and pragmatic' practice group is 'highly responsive and very strong in terms of strategy'. Its expertise covers a wide range of contentious and non-contentious IT matters, including cloud-computing, software license agreements, data protection, search engine liability, e-health and ecommerce

L *(Legal 500 EMEA 2015)*

"The quality of the work from this law firm is outstanding – truly comprehensive and complete. The communication is clear, and the lawyers were proactive in providing solutions to the issues."

(Chambers 2016)

"Wolf Theiss has a very international outlook and many talented people. That is really important if you are a company with activities in other countries. It is able to handle all of our issues, from general corporate matters to serious disputes with governments. To be able to work with just one firm is a huge benefit for us."

(Chambers 2015)

"The attorneys at Wolf Theiss are very dedicated and easy to work with. They understood our business, and really went the extra mile when needed."

"I have a positive impression of the firm. It has an organic approach, with good offices in many countries."

(Chambers 2014)

Supported by a comprehensive legal foundation

TAX

- Tax Advice in M&A
- Tax Disputes & Litigation
- Fiscal Criminal Law
- Tax Planning
- Private Clients
- Financial Products

BANKING & FINANCE

- Finance/Project Finance
- Financial Institutions
- Derivatives
- Loan Portfolio Transactions
- Deleveraging, Restructuring, Insolvency
- Asset Management
- Capital Markets & Securities
- Regulatory

REGULATORY & PROCUREMENT

- Public Procurement
- Compliance
- Environmental Law
- Data Protection
- Dispute Resolution
- Sector-Specific Regulation
- PPP & Concession Law
- Constitutional, National & EU Law

COMPETITION & ANTITRUST

- Abuse of Dominance
- Cartels
- Competition Compliance
- Competition Litigation
- Vertical & Cooperation Agreements
- Merger Control
- Private Enforcement
- State Aid

REAL ESTATE & CONSTRUCTION

- Real Estate Transactions
- Project Development
- Planning & Construction
- Dispute Resolution
- FIDIC Contracts
- Leasing
- Finance

CORPORATE / M&A

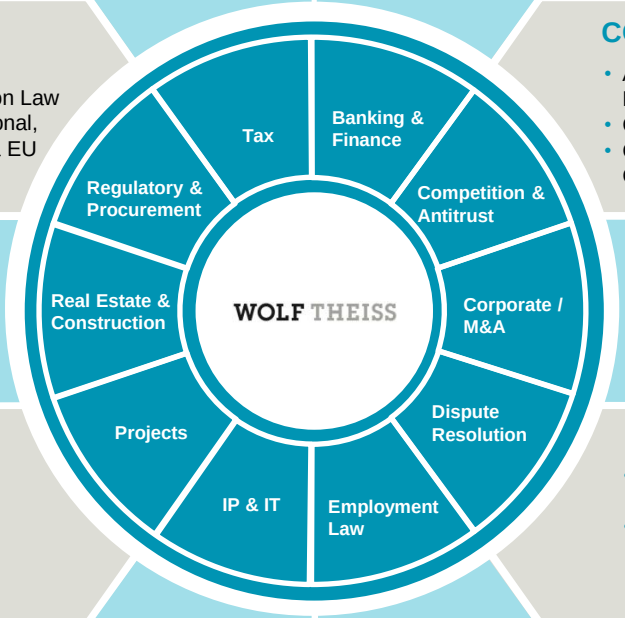
- Public, Private & Distressed M&A
- Privatization & Liberalization
- Governance & Compliance
- Joint Ventures
- Private Equity
- Venture Capital & Start-Ups

PROJECTS

- Development & Structuring
- Finance
- Regulatory
- Commercial Contracts
- Dispute Resolution
- M&A and Corporate

DISPUTE RESOLUTION

- Commercial Litigation
- Financial Services Litigation
- Corporate Disputes
- White Collar Crime
- Compliance
- Internal Investigations
- Commercial & Investment Arbitration



IP & IT

- Trademarks
- Patents
- Copyrights
- Unfair Competition
- IP Litigation
- Life Sciences
- Information Technology
- Data Protection & Privacy

EMPLOYMENT LAW

- Agreements & Policies
- Litigation & Administrative Proceedings
- Pensions & Benefits
- Restructuring & Outsourcing
- Organizational Changes
- Day-To-Day Management

WOLF THEISS

If you have any questions regarding WOLF THEISS, please do not hesitate to contact our experts:

Anna Rizova, Managing Partner

Rainbow Plaza Center
29 Atanas Dukov Str.
1704, Sofia, Bulgaria
T: +359 2 86 13 700
anna.rizova@wolftheiss.com