SOCIAL MEDIA - THE MIGHTY MEDIA

EVOLVE™

Business Insight

EVOLVE

Shahid Khan
A self-made billionaire from Pakistan

Syed Akbar Ali
Country Manager Reckitt Benckiser, Pakistan

General Elections in Pakistan

Data Privacy
General Data Protection Regulations

Historic meeting of Trump & Kim

Vol. 4, Issue 20 - 2018

Vol. 4, Issue 20 - 2018

AIDING THE ALLIANCE

Rs. 400 | USD. 4.00 | EUR. 3.00 | GBP. 2.50 | AED. 14.00 | SR. 15.00

DATA PRIVACY

DEFINING & SETTING NEW RULES OF GAME: GENERAL DATA PROTECTION REGULATIONS(GDPR)

Personal data has become the life force of business. Flowing from consumer devices into your applications and systems, it shapes the customer experience and strategic decision-making, and trickles into every corner of your business ecosystem. It's not just the big companies like Facebook and Google watching everything we do online and selling advertising based on our behaviors; there's also a large and largely unregulated industry of data brokers that collect, correlate and then sell intimate personal data about our behaviors. If we make the reasonable assumption that authorities are not going to regulate these companies, then we're left with the market and consumer choice. The first step in that process is transparency. The new data protection laws in the world are slowly shining a light on this secretive industry.

General Data Protection Regulations (GDPR) approved by the EU Parliament in April 2016 and enforceable from May 25, 2018, applies to all of this data and therefore affects most, if not all, business functions, processes, operations and projects. No one is spared – finance, HR, marketing, support – they will all need to pay attention. Crucially, the Regulation includes numerous new requirements that add an entirely new dimension to the mandates outlined in the Data Protection Act 1998 (DPA), a UK Act of parliament. Therefore, every company should familiarize themselves with the elements of the GDPR and make note of the changes that might have the biggest impact on their organization.

IMPLICATIONS OF THE GDPR

In comparison to the existing EU data protection rules, the GDPR places greater emphasis on the obligations of data controllers (that is, those who determine when, how and for what purpose personal data is to be processed). It also imposes a significant number of new requirements directly on data processors (that is, those who process data on behalf of data controllers), which currently are subject only to the contractual obligations imposed on them by data controllers. A new accountability principle will apply that will require companies that process EU personal data to create and maintain records demonstrating their compliance with the relevant GDPR requirements. In some cases, significant business process and even business model change will be required to meet the new obligations imposed by the GDPR. National Data Protection Authorities will have audit and investigatory powers to ensure that the requisite procedures are being followed. The GDPR will reinforce and expand the data privacy rights of individuals in a number of important ways. At the same time, it will subject data controllers and processors that fail to comply with the GDPR requirements to potentially severe fines. The maximum penalties will be the higher of €20 million or 4% of annual worldwide turnover. The GDPR also establishes a right to compensation for aggrieved individuals and will enable them to lodge complaints through an organization, association or a not-for-profit body active in the field of data protection, which may represent them and receive compensation on their behalf. The GDPR is applicable de facto to all types of data that pass or may pass through the European Union. The GDPR protects data subjects in the European Union, which means not European citizens or residents but all people whose data passes through Europe.

WHAT IS 'PERSONAL DATA' AND 'CONSENT'

'Personal data' *means any information relating to an identified or identifiable natural person ('data subject'); an identifiable natural person is one who can be identified, directly or indirectly, in particular by reference to an identifier such as a name, an identification number, location data, an online identifier or to one or more factors specific to the physical, physiological, genetic, mental, economic, cultural or social identity of that natural person*

'Consent' *of the data subject means any freely given, specific, informed and unambiguous indication of the data subject's wishes by which he or she, by a statement or by a clear affirmative action, signifies agreement to the processing of personal data relating to him or her*

WHAT ARE THE KEY NEW REQUIREMENTS?

• **Direct liability for data processors** – For the first time, organizations that process the personal data of other companies in the course of providing a service (such as cloud providers or website hosts) will have direct liability for breaches of the GDPR, including the risk of being fined. In addition, more extensive obligations will be required in processor agreements than are compulsory at present, and indemnities and limitation of liabilities will most likely become subject to renegotiation.

• **Data breach reporting** – It will be mandatory for data controllers to notify, within 72 hours where feasible, the relevant Data Protection Authority about data breaches that may result in a risk to the rights and freedoms of individuals whose data is compromised; individuals may also need to be notified without delay if there is a "high risk" to their rights and freedoms.

• **New and expanded individual rights** – The GDPR gives individuals a new "right to be forgotten" (have their personal data removed), a new right of data portability (have their personal data copied and transmitted to another organization for further use, including competitors) and enhanced data subject access rights. Individuals will also have expanded rights to object to processing, including an absolute right to object to direct marketing, which might have significant implications for businesses that rely on data analytics.

• **Appointment of Data Protection Officers (DPOs)** – It will be mandatory for organizations, both data controllers and data processors alike, to appoint a DPO with expert knowledge in data protection reporting directly to the highest management levels, if (a) the organization is a public body, or (b) its core business requires regular and systematic monitoring of individuals on a large scale or consists of the large-scale processing of sensitive personal data or criminal records.

• **Mandatory "data mapping" and documentation requirements** – Controllers and processors will have to prepare and maintain comprehensive records of their processing activities, such as the purposes for processing, categories of data subjects and personal data, recipients of personal data, records of international transfers of data, records of data breach incidents, developing and maintaining privacy notices for each product line, storing verifiable consents, etc.

• **Consents** – The GDPR sets out strict new requirements for obtaining valid and verifiable consents for the processing of personal data from data subjects, where consent is used as the basis for processing EU personal data.

• **Enhanced Privacy notices** – The GDPR sets out specific information to be included in privacy notices and requires individuals to be given clear information as to what is done with their data in an easily accessible form.

• **Data protection Impact Assessments** – These will be mandatory before undertaking "high risk" processing, including profiling or heavy use of sensitive personal data (such as health records). Further guidance will be provided by national regulators as to what constitutes "high risk" processing, but the scope is expected to be relatively broad.

WHAT NEEDS TO BE DONE?

• Assess the overall impact about the data-landscape of your business to determine exactly what data you hold, whether that is employee, end-user or customer data.

• Establish how data was obtained and whether fully informed consent was given. Remember, if you can't prove consent, you don't have consent.

• Determine your legal basis for processing personal data.

• Create a data-processing register, detailing how data is stored and transferred, what it is used for and who has access to it. This includes third party suppliers such as Cloud Service Providers.

• Be able to recognize and respond to requests from data subjects, for example, the right to object or the right to be forgotten. All processes must be clearly documented and become part of your business processes.

• Ensure that employees are suitably trained to respond to vulnerabilities and data breaches. Remember, data breaches need to be reported within 72 hours of becoming aware.

• Always tell individuals who your organization is and name any third parties that the data will be shared with. If you share data with third parties, including Cloud Service Providers, you must ensure that they are GDPR compliant.

• Review of Existing Business Processes with respect to data protection/privacy policy/privacy statement and then to bring the same in conformity with GDPR.

• Decide who is in charge of your data protection obligations and whether you have a legal duty to appoint a Data Protection Officer.

• Modify, review and update Agreements (in particular Website User Agreement for Online Services Provision).

• Preparation of a Compliance Checklist and its periodic review.

To whom GDPR matters: It's not only the businesses physically present within the European Union, but all those either controlling or processing personal data of the individuals in the European Union wherever in the globe, including European Union multinationals established and working outside the Union but controlling or processing the personal data of Union individuals.

Mr. Saifullah Khan
is an international trade lawyer. He carries specialized experience in WTO laws. Mr. Khan has developed expertise and engaged in the advisory activities in the legal, policy and regulatory framework for e-commerce.