Companies have until May to comply with new EU rules

Serious penalties for data breaches

Interview with Dr. Arne Gobert, managing partner of Gobert & Partners legal and tax advisors, and Dr. Veronika Francis-Hegedűs, data protection expert on the implementation challenges on the new European data privacy regime.

Dr. Arne Gobert, managing partner of Gobert & Partners Legal and Tax Advisors, and Dr. Veronika Francis-Hegedűs, data protection expert, gave us an in-depth interview about the major legal challenges of the General Data Protection Regulation of the EU (GDPR) implementation for organisations in Hungary after 25 May 2018.

What is the purpose of the GDPR and are all companies obliged to comply with it? What happens to the national legislation?

AG: The aim of the GDPR is to decrease data breaches by organisations, achieve greater transparency and empower individuals with new vehicles of redress if privacy rights are infringed. Nevertheless, it will introduce a uniform and harmonised EU data privacy legislation; however, it is no lethal weapon as data security incidents will still occur. We can say that 99% of the companies globally must comply with the GDPR from 25 May 2018, as it is a really wide-ranging legislation

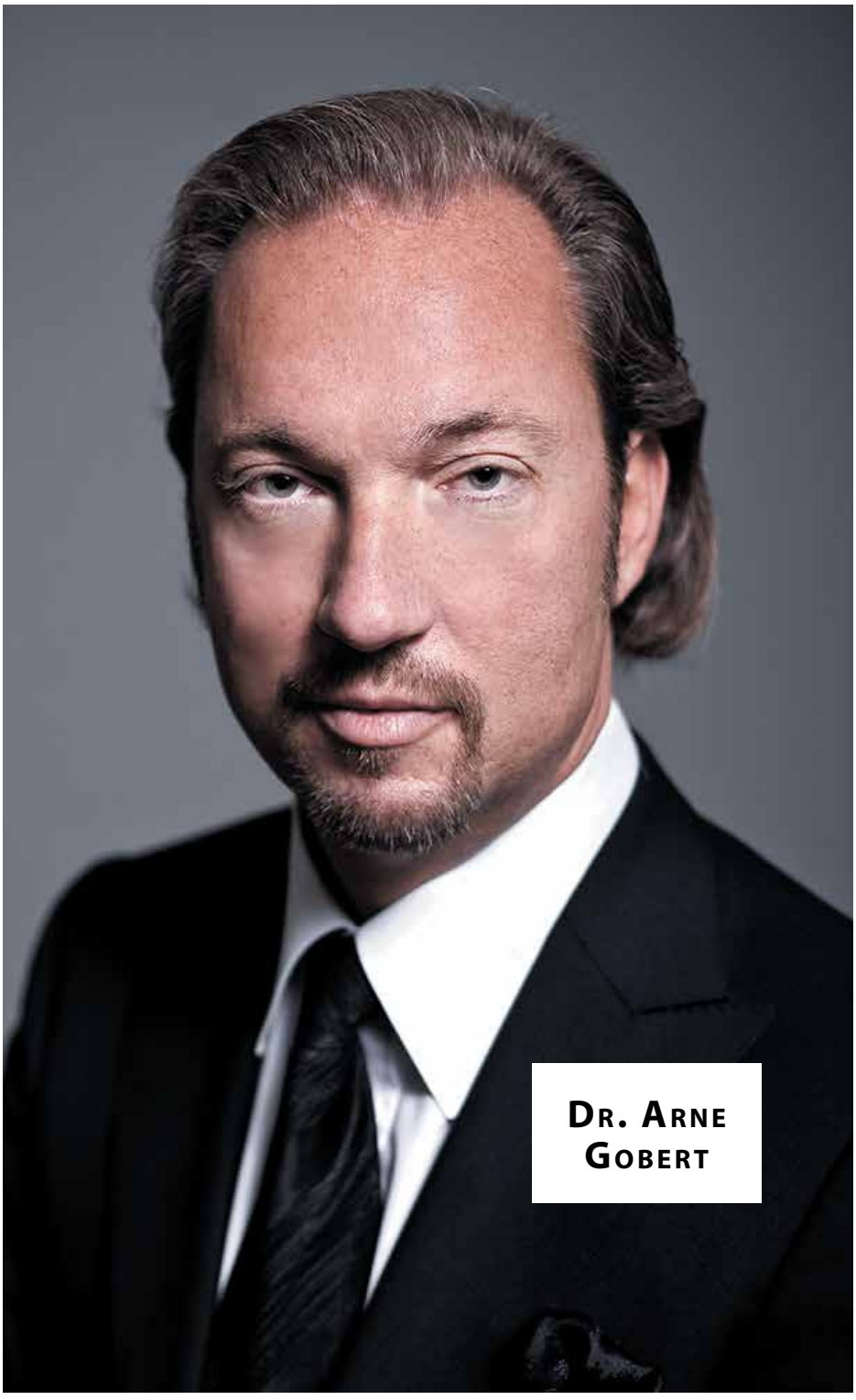
VFH: It must be stressed that the GDPR applies, on one hand, to European-registered companies with a central administration in the EU, as well as to companies that are registered overseas, for example in the US, but conduct business activities related to selling products or rendering services to persons in the EU or concerning the observation of natural persons located in the EU. This means that anyone who collects and processes data of EU citizens is subject to the regulation. It also differs from previous data protection legislation in the EU in a sense that it is a directly applicable regulation. This means that each member state does not need to ratify it into its own national law, compliance is directly expected from 25 May 2018. It cannot be disregarded that EU member state data protection authorities – in Hungary the NAIH – will be in charge with enforcement and they will still have a broad competence on a national level to apply additional strict requirements. Hence, in Hungary, besides the GDPR, the Hungarian privacy act and the stringent guidelines, decisions of the Hungarian data protection authority (NAIH) must be also complied with. Thus, when GDPR compliance is done from the very top of a company group organisation outside of Hungary, Hungarian privacy provisions must be also addressed from the bottom up on the side of the local subsidiary.

Transition to the GDPR era seems to be challenging. What is the final deadline for the compliance, can it be done step-by-step or by one jump? What is the maximum fine the NAIH can impose?

VFH: The GDPR enters into force on 25 May 2018, meaning

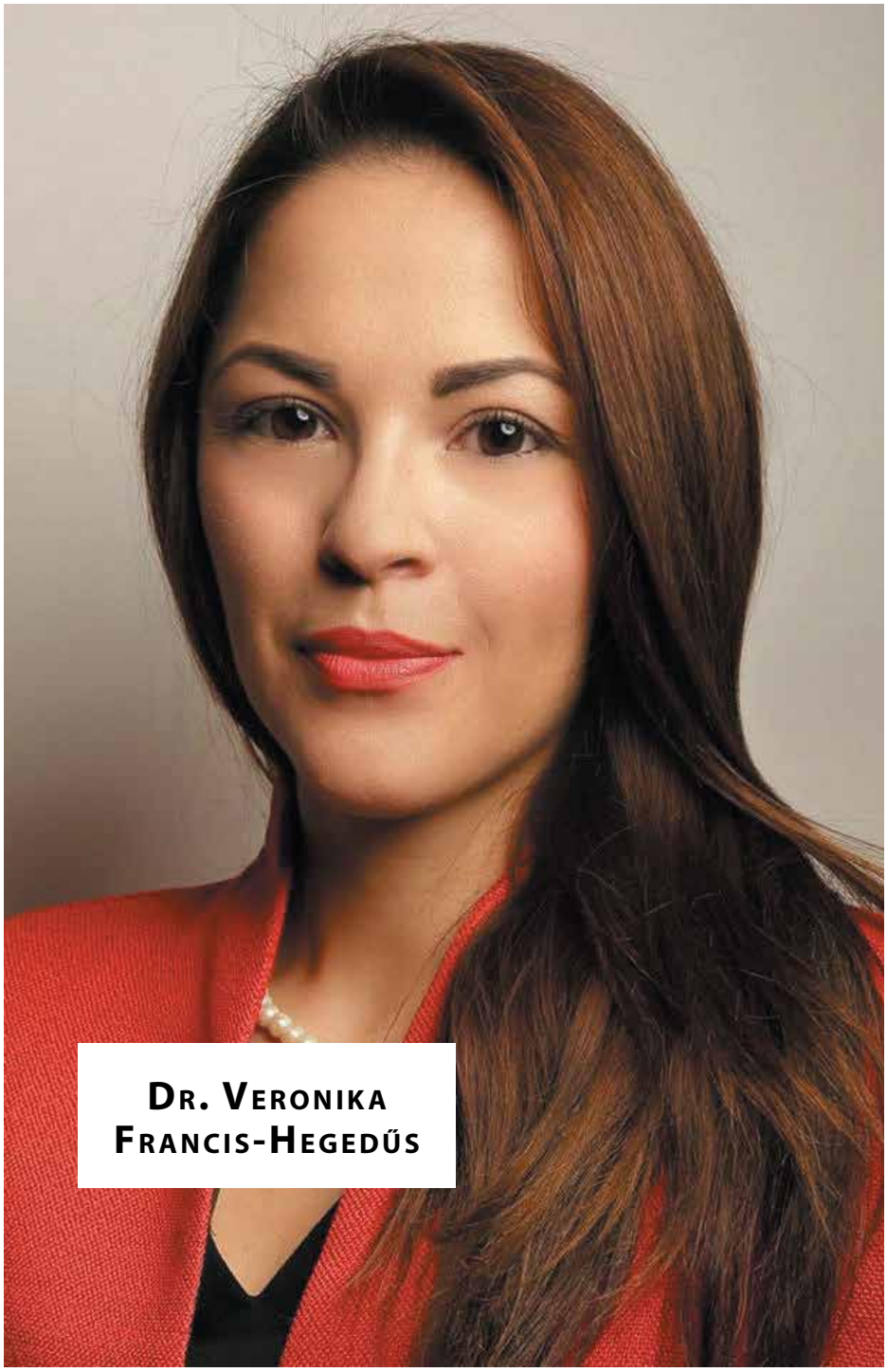
companies who have not started the GDPR implementation process yet still have some time. However, the sanctions for non-compliance after May can be extremely high in the event of a serious data breach (up to EUR 20,000,000, or 4% of the global turnover), besides the serious damaging effect to the brand name of a fine. The GDPR is expected to trigger national data protection authorities, including NAIH, to set an example with any kind of organisation where even a minor data breach can be established. It is highly recommended to start the New Year with addressing the issues of the GDPR era step-by-step, already in January, but not later than March.

AG: The GDPR is not the kind of legislation which can be easily implemented with a one-jump change, and there is no guarantee large organisations can meet this deadline due to the sheer volume of data mixed with challenges posed by mobile devices, cloud-based systems and foreign mother company with numerous subsidiaries. After the deadline, of course the future cannot be predicted, but NAIH has been always following a rather strict policy regarding enforcement of privacy legislation. The authority has already leaked last year that they are increasing significantly the number of inspectors and case handlers. Therefore, for example where a data protection officer is not appointed against the fact that it will be mandatory, the NAIH will not hesitate to impose a large fine based on our experience.



What are the steps to be taken for the GDPR implementation to achieve the most effective GDPR compliant solution?

AG: First of all, in order to being able to protect an individual's personal information, companies and company groups must be able to identify what kind of data, where and how long personal data is kept and is processed, what kind of procedures are used to ensure individual's rights globally in the whole



system. In practice, often different departments do not inform each other or hold precise records about the type of personal data they collect, therefore the data flow related to one individual cannot be easily tracked down. The GDPR will require a system in place which allows locating all personal data intra organisation, which enables deletion securely and immediately from everywhere.

VFH: Therefore, the first step as part of the implementation of the GDPR should be the process of mapping, locating the collected and processed personal data in the scope of an in-depth audit. In case of large multinational company groups, personal data could occur in any documents of any departments, thus the whole database of the organisation must be checked. When the mapping and a comprehensive audit is done, the next technical and legal steps can be identified. However, simultaneously with data mapping, the currently effective global and local privacy notices, policies of the company should be also reviewed in the light of the GDPR and NAIH guidelines regarding the enforcement. This should be followed by appointing a data protection officer (DPO), training staff, implementing new IT system, selecting processors and additional pillars depending on the type of identified issues during the audit.

What is new in the GDPR, what is expected from the new provisions?

AG: In under six months, Europe's old data protection regime will undergo a significant transformation since the 1990s as it will replace the 1995 data protection directive. It will change how businesses and public sector organisations can handle the information of customers, employees. The good news is that organisations already complying with existing data protection laws, the GDPR means an evolution and not a revolution. The problem occurs when organisations do not comply with the current privacy provisions. The novelty is that there are new rights for persons to access and delete information companies hold about them, obliga-

tions for better data management, stricter security requirements and a new regime of fines.

VFH: The GDPR renews already existing rights and enhances them with more content, for example. right to be forgotten, right to access, but there are also new rights e.g. the right to data portability or right to complain to the data protection officer (DPO), right to object to automated decision making, these are novelties. Children's rights and guardian consent under age 16 will be also super important. There are also new legal grounds for lawful data processing, which will require the update of policies, notices and consent declarations. The "legitimate interest" is a new lawful basis for data processing activity; however, it requires a "balance of interest" test approved by NAIH before companies can be sure they are relying on it lawfully. For consent-based data processing, companies must review how consent is sought, managed and documented and they may repaper them for the future. The obligation to designate a data protection officer (DPO) is also a novelty concerning companies whose activity is related to large-scale data collection and processing, the underlying reason is that the rights of data subjects and lawful grounds for processing personal data must be 100% respected. Besides, the GDPR aims to create "trusted data sources". DPOs are key to ensure intra organisation provisions regarding data breaches, retention periods and to education of employees. Furthermore, there are stricter requirement of selection of data processors, and these also serve to ensure a higher level of protection for individual's rights, along with the new principles of "privacy by design", accountability and in certain circumstances mandatory impact assessments. There are also additional requirements regarding the records kept about the collected data.

What are your recommendations for business leaders as homework?

VFH: As we have no crystal ball, we recommend for organisations and business leaders to start evaluating the GDPR situation and the data processing procedures in place of the whole company group and follow a step-by step process. Assessment procedure started at the top of the organisation shall be paired simultaneously with the local, Hungarian level without delay as there may be a considerable amount of work ahead. The work will involve the creation of alignment between IT governance, EU wide data protection legislation, local regulatory and customer demands.

AG: Based on our experience, the GDPR awareness is lower outside of the IT department, which could cause huge problems both in smaller or larger companies. Compliance will require also training staff and key decision makers to maintain GDPR compliance. As the GDPR implementation is a complex process, rethinking and taking action is a must. It's crucial for a business that business leaders up to CEOs and the board of directors, provide and plan the appropriate resources to implement the new IT processes, training and education for staff, meanwhile carrying out an in-depth audit of existing IT technologies and processed personal data. Our office also prepared an in-depth "GDPR Implementation Guide" as a special edition especially helpful for business leaders to start with planning.