Hungary's new Data Protection and Freedom of Information Act entered into force on 1 January 2012. The mere fact that the old law from 1992 was repealed may be cause for celebration. However, in light of EU law and global business trends, the 'new' provisions are at the very least controversial. In this note we give an overview of the new law and flag important new provisions.

On 18 April 2011 the Hungarian Parliament adopted a new constitution which expressly addressed data protection and privacy. The new basic law sets forth that everybody has the right to privacy and access to data in the public interest. The new constitution also provided that from 1 January 2012, a new and independent authority would be placed in charge of the regulation of data protection.

The new Hungarian privacy act was drafted by the Ministry of Public Administration and Justice. Data controllers, NGOs and other entities such as the previous Data Protection Commissioner had very little time to comment on the draft. On 11 July 2011 the Hungarian Parliament, in which the governing party has a two-thirds majority, passed Act CXII of 2011 on the Right to Informational Self-Determination and Freedom of Information (New Privacy Act). There was clearly governmental appetite for revision of the old legislation and the creation of a new and updated legal framework. According to government press releases, the New Privacy Act aims to preserve the previous achievements of the Hungarian data protection framework whilst also ensuring further improvements in line with international developments. The government also claims that the ombudsman style powers of the previous Commissioner were insufficient to investigate and sanction all kinds of violations. Therefore, the new Data Protection Authority has wider powers, including the ability to impose fines. The government also emphasised that the new regime is intended to provide predictable and effective legal protection to data subjects as well as transparent and understandable rules for data controllers.

While some provisions give the law a stronger enforcement focus, such as the new DPA's stronger investigatory rights, and the audit powers that are due to follow in 2013, several areas are still inconsistent with the EU DP Directive or common practice in other EU member states. Furthermore, many of the new provisions remain unclear, especially surrounding the assignment of the functions of the previous Commissioner and his office to the new Data Protection Authority (DPA).

**New legal basis of processing**. While the New Privacy Act retains the general consent requirement it also limits the implementation of Article 7(c) and (f) of EU Data Protection Directive 95/46/EC (Directive) by adding a special balance of interest provision. According to the new regulations, personal data may be processed without consent if it is impossible to obtain the consent of the data subject, or obtaining such consent would require the controller incurring disproportionate expense, and the data processing is necessary either for the controller to comply with its legal obligations or for the pursuit of the controller's (or third party's) legitimate interests. In the latter case, this legitimate interest should also be proportionate to the interference to the privacy of the data subject. Such a limitation is controversial, however, given the recent case law of the Court of Justice of the European Union, which ruled that a similar provision in the Spanish data protection legislation was incompatible with EU law, as Article 7(f) of the Directive has direct effect and member states cannot impose additional requirements (see CJEU ruling of 24 November 2011 in joined cases C-468/10 and C-469/10).

**Registration requirement.** The new regime shifts from the previous notification system to a strict registration and authorisation requirement. This can be considered a setback for data controllers, who will have more onerous filing obligations. Furthermore it also conflicts with the announced amendments to the Directive, with the European Commission's draft EU Data Protection Regulation set to abolish filing requirements in the EU.

Under the new Hungarian rules the Hungarian DPA is required to approve or reject a data processing request within 8 days after its receipt. Data processing may only be commenced after receipt of the DPA's approval. However, if the DPA does not respond within 8 days, data processing can be commenced without approval. Data controllers will also need to pay a fee for registration. The exact amount of this fee has not been disclosed yet, with the governmental decree expected in early January. According to government leaks, the amount of the fee is likely to be minimal (approximately EUR 10). Until this fee is confirmed, however, new registration requests will not be able to be filed. This could result in data processing that commenced on or after 1 January 2012, before the announcement of fees, being in breach of the New Privacy Act. One of the advisors of the new head of the DPA commented that the first weeks of January will be a transitional period and it is unlikely that the new DPA will commence proceedings against a controller until the amount is properly disclosed.

The New Privacy Act also provides for certain exceptions to the authorisation requirements. For example, the processing of employee or customer related data is exempt from the registration requirement, similar to the old rules. However, financial institutions, community service providers and electronic communication service providers are no longer exempt from registration requirement, as they were under the old regime. It is important to note that there is a transitional period to register data processing that commenced before 1 January 2012 but was not notified to the old data protection register. The transitional period does not expire until 30 June 2012, so there will be ample time to achieve compliance. There is obvious controversy on whether it is reasonable to impose a registration requirement upon data controllers if the New Privacy Act is still mainly consent based. Since consent may only be obtained based on a detailed notification to data subjects, they should already have the necessary information regarding the processing of their data. From this point of view the new registration requirement seems to be a mere administrative burden on businesses.

A new section in the filing documents makes registration even more burdensome, as data controllers or processors will have to include general information on their data processing technology. Unfortunately there is no clear guidance on the interpretation of the statement requesting the 'nature of data processing technology applied' so it is uncertain exactly what level of information should be disclosed to the DPA. It is also important to note that this information will be published in the Data Protection Register, so businesses will be wary of disclosing detailed information.

**Data transfer to third countries.** The New Privacy Act still does not resolve one of the biggest constraints of Hungarian law, the regulation of cross-border data transfers. According to the new law, a data transfer to a country outside of the European Economic Area is still subject to the consent of the individual. This is because the New Privacy Act does not provide clear guidance on whether an adequate level of protection, without additional consent, can be considered a valid basis for transfer to a third country, or whether it is necessary to obtain additional consent. Due to the ambiguous provisions and the strict interpretation of the rules under the old DP regime, it is likely that consent to the transfer is still required. Another area of concern is the reduction of the means by which controllers can prove an adequate level of protection. The new law provides that an adequate level of protection can be ensured either by compulsory legal provisions of EU or by a bilateral treaty. The old DP law also contained a reference to decisions of the European Commission, for example on Standard Contractual Clauses (SCCs), but this was removed from the New Privacy Act. Furthermore the New Privacy Act still does not address Binding Corporate Rules (BCRs).

The use of BCRs in Hungary is another highly controversial issue. According to the previous DP Commissioner, Hungary has not been part of the Mutual Recognition system by which national DPAs approve BCRs, and BCRs could not be used for cross-border transfers without additional consent. However, contrary to these remarks, some international companies have claimed that their BCRs were in fact approved by one of the previous Commissioners. In order to resolve this conflict, the New Privacy Act would need to be amended with provisions expressly allowing use of both BCRs and SCCs without specific consent, especially as these solutions are also to be preferred in the European Commission's draft of a new EU Data Protection Regulation.

**Data transfer registry.** Data controllers have to keep a data transfer registry, which shall contain the date, legal basis and addressee of the data transfer, together with the scope of the data transferred.

**Sub-processing.** The other most discussed provision of the old Hungarian data protection law was the express preclusion of sub-processing, i.e. outsourcing by a data processor to another data processor. Unfortunately, the New Privacy Act also contains this odd and outdated requirement which clearly conflicts with the needs of the cloud computing industry and also with EU law (see Commission Decision 2010/87/EU on SCCs for the transfer of personal data to processors established in third countries). Dr. András Jóri, the Hungarian DP Commissioner between 2008 and 2011, also addressed this conflict in his annual report for 2010. According to Dr. Jóri, in this case EU law shall prevail, therefore sub-processing may also be possible in Hungary provided the pre-conditions of Commission Decision 2010/87/EU are met. However, this interpretation has not yet been confirmed by case law, and the New Privacy Act would need to be amended in order to establish a transparent framework that explicitly allows sub-processing.

**New Data Protection Authority.** The New Privacy Act terminated the mandate of the previous Commissioner, Dr. Jóri, with effect from 31 December 2011. He was elected by the Parliament in 2008 and his original term was due to end in 2014. In late November, the Hungarian Prime Minister nominated Dr. Attila Péterfalvi, who had been DP Commissioner between 2001 and 2007, as the head of the new DPA. On 29 November 2011, Dr. Péterfalvi was appointed by the President of Hungary for a period of nine years, as set forth by the New Privacy Act. The new DPA will be part of the public administration and it will have more effective enforcement tools than the previous commissioner. However, several Hungarian NGOs complained to the president of the European Commission to seek protection for the country's current ombudsman system, arguing that the New Privacy Act is contrary to EU law, which requires that the head of a DPA be independent. Viviane Reding, the EU Commissioner for Justice, Fundamental Rights and Citizenship, informed the NGOs in her letter of 30 November 2011 that the complaint will be investigated and the compliance of the New Privacy Act with EU law will also be analysed.

**Fine.** The new DPA has the power to impose fines between HUF 100,000 and HUF 10,000,000 (approx. between EUR 330 and EUR 33,300). This amount might be considered high, especially given under the old DP legislation the Commissioner was not able to impose fines at all. Nevertheless, compared to the level of fines in other member states, this amount is not extraordinary. However, the New Privacy Act does not contain guidelines on the calculation of fines. It is likely that the new DPA will consider the practice of other DPAs, for example the practice of the United Kingdom's ICO, which has issued a detailed guideline on calculation of fines. According to the New Privacy Act, the new DPA has to consider all the circumstances of the case, including the range of data subjects affected by the infringement, its significance and whether it has been a recurring breach. The DPA is also entitled to impose the fine repeatedly. The decisions of the DPA are subject to appeal.

**Procedural rules.** Any data subject is able to initiate proceedings before the new DPA if their personal data were processed unlawfully or there is an imminent threat of such processing. The DPA may also initiate proceedings if it is likely that unlawful data processing will affect a wide range of data subjects or relate to sensitive data or may cause considerable harm or damage. The new DPA is able to impose an order to: (i) amend incorrect data; (ii) block, delete and destroy data processed by illegal means; (iii) prohibit unlawful processing or transfer of data; (iv) provide information to the data subject if this was rejected without legal grounds; (v) impose a fine; and (iv) publish its decision.

**Definition of 'Technical Data Processing'.** The New Privacy Act restates the outdated definition of the old law, which does not comply with the current Directive or the leaked European Commission draft of the new EU Data Protection Regulation. It also uses the term 'technical data processing' which refers to performance of mere technical tasks relating to data processing operations (i.e. data processing performed by a data processor).

**Internal data protection officer.** The provisions of the New Privacy Act on data protection officers (DPO) are almost identical with the old legislation. It is still optional to appoint a DPO in most circumstances, except for certain governmental bodies, financial institutions, electronic communication providers and public utility providers where this is mandatory. Since the New Privacy Act does not contain any constraints in this regard, it is likely that the DPO may be either an internal member of staff or externally appointed/outsourced. The DPO must be a natural person having either a legal, public administration or information technology qualification or equivalent. A new and positive provision of the New Privacy Act is a conference of DPOs which would be organized by the DPA at least annually. At the conference, the DPOs registered with the DPA will be able to raise questions and issues to the DPA. According to the New Privacy Act a DPO: (i) contributes to or assists in making decisions related to data processing and to the enforcement of the rights of data subjects; (ii) monitors compliance with the New Privacy Act and other statutory provisions on data processing, internal data protection, data security and data security requirements; (iii) investigates complaints, and requests that the data controller or data processor cease unlawful data processing; (iv) drafts internal data protection and data security policies, (v) maintains the internal data protection register; and (vi) ensures the training of staff in connection with data protection.

**Children.** The New Privacy Act provides that children over 16 are able to give consent without additional parental approval. Obviously, this facilitates the processing of data relating to younger individuals. Nevertheless it is important to note that, according to the leaked European Commission draft of the new EU Data Protection Regulation, in future children under 18 will not be competent to give consent without parental approval.

According to the government, the New Privacy Act contains transparent and understandable rules, which are also in line with international developments. However, stakeholders, NGOs and others (including some previous DP Commissioners) claim that the New Privacy Act is not only a missed opportunity but also conflicts with EU law. According to these voices, the provisions of the new law are very similar to the outdated provisions of the old legislation. Furthermore, neither European case-law and draft amendments of EU law, nor technological developments, such as cloud computing, social networks, outsourcing were taken into account by the legislator. As a result, the government has been urged to review the provisions of the New Privacy Act and amend it in order to restore Hungary's competitiveness and compliance with EU law. According to unofficial sources, the government is open to such discussions. Nevertheless, it is likely that the actual amendment of the new law will require significant time. Businesses will have to seek compliance with the current provisions of the New Privacy Act without delay, even if they are hopeful of an improved Hungarian framework.