GOBERT AND PARTNER
ATTORNEYS AT LAW

Róbert Károly krt. 70-74. "B" 8th floor
1134 Budapest
HUNGARY
Telefon + 36 (1) 270 9900
Telefax + 36 (1) 270 9990
E-mail: office@gfplegal.com

GDPR NEWSLETTER

OF THE

BWSP GOBERT & PARTNER LAW FIRM

SPECIAL EDITION

Budapest

2018

APPLICATION OF THE GDPR IN PRACTICE – IT'S TIME FOR PLANNING!

Preparation for the European general data protection regulation in Hungary

The private sphere will be particularly protected by the directly applicable EU Regulation Nr. 679/2016 of the European Parliament and of the Council on the protection of natural persons with regard to the processing of personal data and on the free movement of such data (**GDPR**). The new regulation is not less strict or significant, than the possession of a new economic power source. The opinion of the Hungarian authority concurs, since representatives of the Hungarian National Authority for Data Protection and Freedom of Information (**NAIH**) claim in professional circles "the data is nothing else, than the oil of the information society". The GDPR is directly applicable in 28 Member States of the EU and overwrites the national laws from 25 May 2018. In Hungary it shall be applied along with Act CXII of 2011 on Informational Self-Determination and Freedom of Information (**Privacy Act**), with other sectorial laws and the guidelines of NAIH in the course of daily operation of companies registered in Hungary concerning digital and paper based data processing. However, not only companies with a central administration in the EU will be effected by the GDPR, but also companies, which have central administration outside of the EU and their activity is connected to selling goods and rendering services to data subjects residing in the territory of any member state of the EU, or whose data processing activity relates to the observation of the behaviour of individuals within the territory of the EU (e.g. profiling, forecast of personal preferences, monitoring on the internet etc.).

Complex legal and information technology measures are required, which cannot be started early enough, in order to prepare for the new European data protection regime. From the day of entry into force, the European data protection authorities will be empowered to impose an unprecedently high fine, up to the amount of a maximum 20 million Euros, or the 4% of the global turnover of the last financial year. Conclusively, the financial risk of the legal non-compliance of companies with the GDPR, which carry out data processing over the territory of the EU, will radically increase.

I. WHAT DOES AN EFFECTIVE ACTION PLAN CONTAIN TO PREPARE FOR THE GDPR?

The question arises, what can we do exactly in the upcoming months to reach an adequate level of data protection and security that is in compliance with the GDPR and how can we minimize the financial risk of our company? Managing partners of our firm suggest the following action plan to follow, prepared along with our data privacy experts and available in the scope of our GDPR preparation service package:

1. Audit of the current data processing activities in the company or company group and data protection documentation from a GDPR perspective (audit, impact assessment, IT audit, data mapping);

2. Compliance inspections, balance of interest tests, establishing new data protection levels in line with the legal bases of the GDPR, as well as review of consent to process data, guarantee the rights of data subjects, incidents management, pseudonymisation and other practices of the company regarding data protection;

3. Preparation of legal documents in compliance with the GDPR (e.g. policies for employees and clients, notifications, consent declarations, template forms, incident management plan, information security policy, etc.);

4. Elaboration of legal documentation and procedures to ensure the appropriate notification of data subjects update and permanent monitoring of the data map;

5. Review, update and preparation of the company's website from a data privacy perspective;

6. Incorporate the security practices which are required by the regulation on „Privacy by Design" principle to the operation and IT system of the company;

7. Preparation of agreement template to be concluded by the data controller with data processors, risk evaluation procedure regarding the selection of data processor contractual partners;

8. Inspection of cloud based data storage from legal compliance perspective and establishment of GDPR compliance;

9. Elaboration of procedures for the special protection of children's rights;

10. Appointment of data protection officer by the company, in case it is prescribed by the GDPR;

11. Registration of data processing activities with NAIH in compliance with the new regulation before and after 25 May 2018;

12. Education of company managers and employees performing data processing in the scope of their job function, increase the data protection awareness, preparation of e-learning tests and exams for internal use;

13. Permanent contact with NAIH, ensure NAIH compliant balance of interest tests, conducting preliminary impact assessments;

14. Preparation of mandatory internal registers of data protection;

15. Preparation of Binding Corporate Rules (BCR) inside company group, assisting in the EU/Switzerland – USA Privacy Shield checking of USA based companies;

16. Permanent monitoring of the operation of the company in respect of the regulations of data protection.

II. WHAT SHOULD EVERYBODY KNOW ABOUT THE GDPR?

Every company that records, collects, uses or stores personal data in any respect – 99% of the operating companies – is considered as so-called "data processor" and shall be obliged to comply with the GDPR. In case a company performs any data processing activity defined in the GDPR in the territory of Hungary, it shall take into consideration the provisions of the GDPR, the national privacy laws and the strict practice of NAIH.

The GDPR defines "personal data" more extensively, than the effective European directive and the national Privacy Act. According to the GDPR, **personal data shall be all information, which refers to an individual, and the individual is identifiable directly or indirectly.** With regard to the above, a person's (**data subject**) name, ID card number, place of birth, e-mail address, picture or recorded voice, and any information referring to the intellectual, economic, cultural and social identity of the data subjects, the GPS data of the data subjects' vehicles or any data of their phones, such as GPS data, or the history of the employees' browsers, moreover the IP addresses and cookies shall be regarded as personal data. Our clients ask regularly from us **how they can process this broader scope of personal data in a GDPR compliant manner fully.** In companies, even internally, there is a need for a data processing policy to share (get to know) personal data, furthermore, notification forms and policies are also necessary regarding the types of employee monitoring (e.g. checking the use of internet, business phone, use of cameras, GPS), as well as data processing registers. Equally important that there is a necessity of subsequently verifiable transparency, including a lawful purpose of the data processing activities from 25 May 2018.

An essential element of the new data protection regulation is purposefulness, the purpose limitation principle. This means that the daily data processing must have an exact purpose in pursuance with the GDPR and if the

company is not able to subsequently justify this, the lawfulness of the data processing activity is challengeable. **One of the key steps to prepare for the GDPR is to review the current purposes of each data processing according to the principles of the GDPR.** The principle of necessity and proportionality play also a significant role besides the principle of purpose limitation. Moreover, new types of particularly sensitive data shall be carefully regarded, especially in terms of processing medical, biometric (e.g. facial image, fingerprint), respectively genetic data. According to NAIH, such data may exclusively be processed for a reason of significant legitimate interest. In case of a modern entry gate system, such legitimate interest shall not be less, than examining a "deathly virus" in the back office located beyond the gate system.

In the course of preparation for the GDPR the legal ground of the data processing is another important focus point to be reviewed. **The legal ground of data processing according to the new regulation shall be the voluntary consent of the data subject or statutory provision, respectively other new legal grounds e.g. legitimate interest, exercise of powers in the public interest or by public authority.** One of the new legal grounds, the legitimate interest of the data controller or third party must be emphasised, as pursuant to the GDPR this can justify the data processing. This legal ground shall be regularly applied in data processing in connection with employees, and conclusion or performance of contracts.

Under the application of the GDPR, the management of companies and employees performing data processing on behalf of the data controller must be fully aware of the rights of the data subjects (right of information, rectification, deletion etc.) since the compliance with these rights is a prime obligation of the data controller.

III. COMMON DATA PROCESSING ACTIVITIES IN BUSINESS LIFE

The below daily business activities performed by all companies qualify as data processing activities, thus, we gathered some practical and useful advice to ensure GDPR compliance for the period following 25 May 2018.

1. Information, offer request, management of appointments, CV-s of job applicants

The requirement of purpose limitation, necessity and proportionality shall be applied for the entire course and term of the data processing activity. For instance according to NAIH, subsequent to the request of information or offer, booking appointments (including personal data of the subjects) or the e-mail correspondence containing the CV of a job applicant, the data shall be immediately deleted from the company database in case if there is no reason for further storage. Although, upon setting an appointment we usually record the name, phone number of the client, however, once the purpose is fulfilled all personal data must be immediately deleted, unless there is a legitimate interest of the company to keep the data or the data subject provided express consent to the company to keep their data.

2. Operation of camera system

Please note that currently, or under the GDPR the use of camera systems are allowed to be operated on public or private territory or at workplace for monitoring employees, only by complying with certain guarantees and adequate notification of the data subjects and the employees. Workplace cameras particularly cannot serve the surveillance of private life of the employees (installing cameras in the lounge or smoking area is prohibited) or to influence their work activity with cameras.

Upon installing camera systems, compliance with the regulations of data protection is essential. Applying the principle of necessity and proportionality, NAIH may levy a fine and dismantle the unnecessary cameras due to "disproportionate over-surveillance" of the observed area, for instance dismantling cameras from a hotel lobby (e.g. 2 out of 4 cameras is being permitted), which are unnecessary to fulfil the purpose. The camera footage -

unless being used – may be kept for 3 days, in special cases for 30 or 60 days in accordance with the provisions of Act CXXXIII of 2005 on the rules of security of individuals and property, and activities of private detectives.

Should the company insist on the use of cameras, a respective policy to notify the data subjects entering into the monitored area shall be issued by all means with the annexes recommended by NAIH. According to NAIH, every person, client and employee shall be entitled to be informed about the policy of camera use prior to entering the premises. Another question could arise in practice, which should be considered on a case by case basis, is whether the camera image may or may not (e.g. interior area of a bank) qualify as business secret.

The so called "**balance of interest test" shall be also considered** as an integral part when a GDPR compliant data processing is implemented. The essence of the balance of interest test is that the data controller must pose the question, particularly when personal data is processed based on the legitimate interest of the company, whether the data processing is unavoidable and the controller's interests are not overridden by the privacy rights of the data subjects. Only such data processing which pass the test and NAIH also approves are recommended to follow in practice.

Before the data processing, the data subjects must be provided with the relevant policies, notifications on the website of the company or in paper format. The camera usage must be indicated in the observed area by stickers, explanatory sign-boards. If a camera system is operated at a workplace, NAIH strictly requires prior notification of the employees defining the specific purpose (by no means for the surveillance of the employees!).

3. Complaint management

According to the currently applicable rules of consumer protection all relating data must be kept for a period of 5 years. This period of time may be altered in the near future by a bill debated by the Hungarian Parliament.

4. Sending newsletters

The legal ground of sending newsletters could be the voluntary and expressed consent of the data subject provided upon subscribing to the newsletter. According to the GDPR, companies must be able to prove that prior consent was given, therefore, the records of consent given electronically or in paper format must be kept.

The standpoint of NAIH regarding newsletters is relatively strict EU wide. Pursuant to NAIH, companies shall only collect and keep the names and e-mail addresses of the clients along with the date of approval in order to send newsletters, in line with the principle of necessity – proportionality. Exception may be made if the content of the newsletter is restricted for data subjects over the age of 18, in which case the date of birth can be processed as well. For those companies, which have been processing a broader type of data in connection with newsletters, it is highly advised to adjust their newsletter database previously applied, by 25 May 2018 the latest.

According to NAIH, company run corporate websites may imply further legal and practical questions such as the adequate format of the checkbox for electronic subscription or whether the cancellation of subscription, postal cancellation of the subscription is duly ensured on the address indicated by the controller and the regular database updates are carried out, as recommended by NAIH.

5. Lottery game

Companies offering prize games usually qualify as data controllers, meanwhile, the assigned marketing companies to organize the games qualify as so called "data processors". Data processors according to the GDPR are similarly liable to data controllers and can be fined in case of non-compliance with the data privacy provisions. All prize games are currently subject to notification and must be registered with NAIH in the publicly accessible

data privacy register. Furthermore, a respective data privacy and game policy shall be issued and made available publicly (e.g. on the website or relating link).

6. Processing personal data of job applicants and employees

A comprehensive and detailed notification of job applicants and employees is a must before data processing is started concerning the data of the data subjects. In the light of the GDPR, it must be emphasized that the employers may not keep CV-s of unsuccessful candidates without their prior and explicit consent, after the selection procedure is closed. Employers may also not request special data (e.g. criminal record) without the consent of the candidate, if it cannot be especially justified by the scope of work activity. In the course of data processing employers must proceed with extra caution in order to comply with the below described obligations of the data controller, respectively with the requirements to guarantee the rights of data subjects.

IV. WHAT ARE THE OBLIGATIONS OF THE DATA CONTROLLER?

Obligations of the data controllers and rights of the date subjects will significantly widen from 25 May 2018. In our below summary, we have gathered the obligations of data controllers under the GDPR.

1. Obligation of prior notification

The right of data subjects to prior notification is not new. However, the GDPR particularly requires that the notification is complete including the purpose, legal ground, time period of storage, rights of remedy, data security, contact details of data protection officer, data transfers and data processors. In case of a potential inspection of NAIH, the data controller must be able to verify that the prior, detailed and appropriate notification was provided to the data subjects.

A novelty of the GDPR is the requirement of a consent that is **"voluntary and explicit",** actively given and can be revoked by the data subject anytime. Our general practical advice for data controller companies, besides the detailed written data privacy notifications, is to collect and keep the written consents of the data subjects, enabling the data controller to subsequently verify the lawful data processing activity in case of a NAIH inspection. In addition to the GDPR, NAIH also sets strict requirements as regards the prior notification based consent, in particular concerning consent given via "checkbox" method and sound recording.

The key to GDPR compliance is the application of proper prior notifications and policies. Please read below the essential elements of notifications and policies according to the experts of our office:

- If data processing is subject to NAIH registration, what is the NAIH registration number of the data processing activity?
- Who is the data controller?
- What is the purpose of the data processing?
- What is the legal ground of the data processing?
- What is the time period of the data processing?
- How, in what manner is the data being processed?
- Who, and which employees has access to the data, when and in what cases are they authorized?
- Who are the mandated data processors?
- Is there any data transferred outside the EU?
- What are the rights of the data subject and how are they guaranteed?
- Is there a data privacy officer and when can the data subject request assistance?

- What data security processes and procedures are in effect at the data controller?
- What is the process of breach management of the data controller?

2. NAIH registration obligation and inner data processing record-keeping of data controller

At this moment it is obligatory to register certain types of the data processing activity – with a few exceptions – with NAIH in the publicly available data protection register of NAIH. Irrespective of this, the GDPR prescribes the internal record-keeping obligation of the data processing activities for the data controllers and the data processors.

According to the GDPR, organizations with less than 250 employees are not obliged to keep this internal record, except if the data processing activity carries a high risk or the data processing activity is not carried out on an ad-hoc basis or special type of personal data (e.g. race or ethnical origin, political opinion or religious or ideological conviction, data relating to trade union membership, genetic, biometrical or eventually medical data) or data relating to the criminal liability is collected.

3. Record of data transfers

The GDPR allows the data transfer to third countries or to an international organization similarly to the current provisions in case of fulfilling conditions, which guarantee an adequate data protection level. Based on the national privacy laws, it remained unchanged that the data controllers transferring data must keep an internal record – automatic or updated by an employee – of data transfers.

Pursuant to the GDPR the approval of the data transfer by a member state is not necessary in case of the existence of special data transfer guarantees (e.g. approved Binding Corporate Rules by the national authorities). Lawful data transfer is also possible if there are agreements in effect between the data controller and data processor of a third country or of an international organization and the national data protection authority approves the agreements as a guarantee of adequate data privacy level.

In the absence of these and further GDPR guarantees, if the Commission declared officially that a country guarantees an adequate level of data protection, initial approval of guarantees by the national data protection authorities would not be necessary. However, such country which was qualified like this by the Commission does not exist at the moment.

4. Registration of personal data breaches

The GDPR introduces the term of personal data breach, which means such a security violation of an IT operation system that results in unauthorized access to personal data or the unlawful destruction of the data (e.g. the IT system is breached by hackers; if an e-mail or a letter is sent to unauthorized person than the addressee, a laptop disappears from the workplace). In case of personal data breach, the data controller shall comply with their data notification, registration and notification obligation pursuant to the GDPR according to the following schedule:

1. **Quick impact assessment**: if it is established that the security violation may cause a considerable damage to the rights of the data subject, and/or the personal data breach means a considerable data protection risk, the company shall take the below described second and third steps.

2. **A notification to the National Data Protection Authority within 72 hours:** about that the security system of the data controller was violated. On top of the above referred content, the notification must

contain what kind of measurements the data controller has taken to avoid risks and damages, furthermore, to block similar future personal data breaches.

3. **The notification of the data subjects:** only if the data breach was with high risk to the rights of data subjects. The data controller shall inform all data subjects in clear and plain language, which poses a legal risk for the data controllers that data subjects may demand compensation from the company in a lawsuit at the court due to the privacy violation.

5. Appointment of an internal data protection officer

Pursuant to the GDPR it will be obligatory to employ a qualified, independent data protection officer at the companies from 25 May 2018 in case:

1. the data process is carried out by public sector bodies or public authorities;
2. **the main activity of the data processor and/or data controller is related to the regular, and systematic, large-scale observation of personal data;** or
3. the organization processes special data or data relating to resolutions in connection with the criminal liability of the data subjects

From the cases above we can highlight the second, which may be broadly interpreted and it raises interpretation issues for a considerable amount of companies as it is unclear to which businesses it is of relevance. To decide whether the particular data processing activity is related to the main scope of activity of the company, the data of the company excerpt could give guidance and pursuant to this provision e.g. marketing agencies, banks, insurance companies, phone and internet service providers must employ a data protection officer.

6. Binding Corporate Rules (BCR), Switzerland / EU-USA Privacy Shield

The data transfers to the non-member states of the European Union usually are allowed if NAIH approved guarantees for adequate level of data protection between the two countries are in effect. Company groups could ensure adequate level of data protection by accepting internally Binding Corporate Rules approved by the competent national data protection authorities, in which the companies in the group are undertaking compliance with the provisions of the GDPR and acknowledging it as legally binding.

A similar solution could be the Switzerland/EU-USA data protection shield (**Privacy Shield**), which may provide solution for business partners in relation to data transfers to the USA from Europe or Switzerland in transatlantic commercial relations. This new framework protects the fundamental rights of anyone in the EU or Switzerland whose personal data is transferred to the United States and provides companies a mechanism on both sides to comply with the GDPR requirements. Accordingly, data can be transferred to companies in the USA, if the company registered and undertook as binding the principles of the Privacy Shield. The list of the companies participating in the Privacy Shield is available here: www.privacyshield.gov/welcome.

7. Permanent compliance with data privacy laws during daily operation, Privacy by Design principle

The GDPR introduces the general requirement of the principle “Privacy by Design”, which has been highly emphasised also by the press, besides the principle of data minimization recently. Pursuant to these principles, the operation of the company shall be monitored continuously from the aspect of data protection and data security. **It means continuous running of a data protection impact examination, especially in case of developing, planning, selecting or using new products, services. Practically these requirements mean the continuous audit of the operation of the companies.**

V. WHAT ARE THE RIGHTS OF DATA SUBJECTS?

The GDPR guarantees the following new and renewed rights of the data subjects, the protection of which will be obligatory for the data controllers and data processors.

1. Right to information and access

The data subjects will be entitled to require a detailed documentation of the data processing activity regarding the processing of the personal data provided by them to the data controller. The documentation disclosed to the data subject must contain: whether personal data processing was carried out and if yes, on top of the specific categories of the personal data, the purpose of the data processing, the term of the data processing, data processors; in case of data transfer the recipients, remedy rights, and the fact of profiling, if it was carried out. Based on the request of the data subject at least one copy of the personal data must be provided free of charge.

2. Right to be forgotten

Pursuant to the GDPR the "right to be forgotten" is an additional right to the right of erasure for the data subjects; accordingly, the data controller is obliged to delete personal data without delay if any of the GDPR scenarios subsist. The data controller must delete the personal data even from the backup copies or from the potential copies, for instance, if the consent to the data processing was provided underage, or the data became irrelevant and is no longer necessary or the data processing was unlawful.

The data subject shall be informed on the actions taken based on his request. If the data controller eventually published the personal data or transferred to another data controller, it is not sufficient to remove them from its own database, but it also shall inform the additional data controllers and data processors regarding the deletion request of the data subject and arrange for the removal of the personal data. The right to be forgotten – due to the wide-scope obligations of the data controllers – could be an effective instrument for all of us and especially for employees, who may have publicly accessible e.g. irrelevant online pictures or any information from their childhood.

3. Right to data portability

In case of automatic data processing in some cases (if the legal title for data control is based on voluntary consent or the data is necessary to the fulfilment of the contract) the data subjects are entitled to the right of data portability. Based on this right, the data subjects can request from the data controller that the data relating to them and/or the data disclosed by them shall be forwarded to them or a third party appointed by the data subject, e.g. by one bank to another in case of changing bank. The data shall be disclosed to the data subject and/or the third party organization in a structured, machine-readable format. GDPR encourages the enforcement of the right to data portability by introducing "interoperability", the co-operation between the organizations as new general requirement in relation to the data controllers performing automatic data processing.

4. GDPR takes action against profiling as phenomenon

As a new feature, the GDPR expressly challenges profiling: the phenomenon when a data controller draws conclusions and creates a profile about the data subject based on information related to behaviour and preference patterns collected from social network sites and from other data bases and data controllers execute operations based on this information. Pursuant to the GDPR, the following shall qualify as profiling e.g. if insurance companies, banks, head-hunters collect information from social network sites (Facebook, LinkedIn) to their systems and as a result, upon automatic data processing, they assess the amount of insurance or loan they

can lend to the data subject or jobs the data subject may qualify for. Upon the creation of the GDPR by legislators, it was taken into account that IT systems, algorithms, which are capable of profiling, are developing continuously and they may have a larger role in the future than now. Thus, profiling may be carried out with adequate guarantees, the data controller shall guarantee not only the notification prior to profiling, but also the right to object and the right of erasure based on the request of the data subjects. In connection with the practice of HR profiling, the NAIH's standpoint in the past years was that monitoring employees and potential candidates through their Facebook profiles and other social media is only permitted, if indicated in the job application and/or if the employee was informed in this regard in advance. Our practical advice is to request an e-mail confirmation in case the employer intends to check social media profiles of employees, potential candidates.

Based on one of the new GDPR legal grounds of data processing, namely the "legitimate interest", the lawful profiling will be possible in some cases. The key element of which will be that the profiling shall be in the legitimate interest of the data controller as the particular purpose of the data processing activity. One of the practical examples is when head-hunter companies may process data for business purposes (e.g. the personal data of the data subject disclosed on the LinkedIn profiles of the data subject concerning the previous working places and working experience). However, the company carrying out the profiling must draw the data subjects' attention to data processing and/or guarantee the remedial rights of the data subjects.

5. Pseudonymisation: encouraged practice pursuant to the GDPR

The application of "pseudonymisation" is a recommended data protection practice by the GDPR, which can help for data controllers and data processors to reduce risks and meet their GDPR obligations. The "pseudonymisation" means that the data subject cannot be longer identified by a personal data without additional separately kept information. This means that controller connects or identifies each personal data with a code e.g. "JGH789". The original personal data is substituted by the code in the registrations or documents following the connection; and the data controller minimizes the access right to the „decoding" register including the connections – e.g. to an excel chart in which one column contains personal data, the other column contains the codes - e.g. to one employee or to the data protection officer.

6. Accountability and transparency of the companies as data controllers according to the GDPR

Our clients often turn to our data protection experts with the question of how can the companies as data controllers comply with the requirements of accountability and transparency in their everyday practice? Accountability and transparency imply that in case an official NAIH inspection is initiated, the controllers shall be able to verify the GDPR compliance of their processing activities e.g. with documents and registers at any time. For this purpose the controllers shall use "appropriate technical or organisational measures", namely the controllers shall involve information technology solutions to ensure that all documentation and legal requirements are fulfilled.

The transparency of the data management shall be promoted by concise, intelligible information and regulations using clear and plain language, including graphics if necessary - possibly charts and standardised icons in accordance with the recommendation of NAIH – making it easy to access and understand the data management process for the data subjects. The fulfilment of the requirements of transparency will be also key element of GDPR compliance in case the processed information are collected specifically from children.

VI. WHAT KIND OF PROTECTION IS ENSURED BY A GDPR COMPLIANCE CERTIFICATE FOR COMPANIES?

The GDPR enables the data protection authorities and other authorized organizations of the member states - which is NAIH in Hungary - to accredit such certification bodies that are able conduct audits on the data

protection compliance of the operation of the companies in accordance with the needs of the market, as well as issue GDPR compliance certificates as a result of the audit. Such certification bodies, auditor companies are expected to be established in Hungary. Nevertheless, no such accredited certification issuer has appeared on the Hungarian market yet, which is constantly monitored by our office.

It shall be highlighted in connection with the certification that the mere obtaining of a certificate by the company guarantees only that NAIH does not initiate an ex-officio inspection against the data controller, namely does not investigate the company without any complaint from a data subject. Conclusively, obtaining the certificate will not be sufficient to protect the company against all risks, hence, companies should maintain a GDPR compliant operation constantly.

VII. MANDATORY DATA PROTECTION IMPACT ASSESSMENT AND PRIOR CONSULTATION WITH NAIH?

All companies processing data in Hungary will be obliged to consult with NAIH prior to processing, where a mandatory data protection impact assessment indicates that taking into account its nature, scope, context and purposes, the processing is likely to result in a high risk to the rights and freedoms of data subject natural persons. Until now, there was no such obligation of prior consultation with the authority conclusively there is a lack of common practice of this new process introduced by the GDPR in Hungary.

It is also important to note the risks of the prior consultation. In accordance with the provisions of the GDPR, during the prior consultation, NAIH may not only give advice to the companies in writing, but may also initiate an investigation on the original subject of the prior consultation and extend the scope of the investigation to any other data processing in the company afterwards. Furthermore, as a result of such investigation, NAIH may instruct, warn or fine the company for any infringement detected.

VIII. HOW CAN YOUR COMPANY AVOID THE RECORD-BREAKING FINES?

The GDPR enables all data protection authorities in the member states, such as NAIH, to impose a fine on a company following an official investigation in case of detecting an infringement, where the gravity, the intentional or negligent character, the duration and other aspects of the infringement are considered relatively freely within the broadly defined framework of the provisions of the GDPR. In the event of certain **less serious infringements, NAIH may impose fines up to 10 million EUR (more than 3 billion HUF), or the 2 % of the total worldwide annual company turnover of the preceding financial year** (e.g. if the company fails to notify a personal data breach to NAIH, or violates the requirement of privacy by design during its operation). In case of certain more serious infringements **NAIH could fine up to 20 million EUR (more than 6 billion HUF), or the 4 % of the total worldwide annual company turnover of the preceding financial year** can be imposed (e.g. in case of infringement of the basic principles of the GDPR, if the data subjects' consents are not obtained in accordance with the regulation, if the legal basis of the data processing is not appropriate, or if the company processes data in lack of legal basis).

The GDPR, thus, enables the member states' data protection authorities to impose such extraordinary fine(s) that may have serious consequences even for the operation of large companies in the global market, with special regard to the case of non-compliance of various data processing procedures, in which case fines may be imposed several times.

IN THE VIEW OF THE ABOVE, IS IT WITHOUT QUESTION FOR YOU TOO THAT THE TIME FOR PREPARATION HAS COME?

In order to avoid the risk of a fine, it is still not too late to commence or accelerate the preparations for the new European Data Protection Regulation, which may take even months. But what can be, what should be done exactly for this purpose? – all responsible corporate executives may wonder in the upcoming months.

In case of company groups, where GDPR implementation is handled from the country of the mother company (e.g. US, Germany), the local Hungarian data protection advisory is still unavoidable. **In Hungary, the new IT systems, new policies, balance of interest tests, BCRs and all aspects of the data processing have to comply not only with the GDPR, but also with the often times stricter national Privacy Act and the scrupulous practice of NAIH.** Based on the provisions of the GDPR, especially when new IT systems and data processing practices are implemented, local subsidiaries of multinational companies in 99% cannot avoid the initial risk assessment audit and compulsory NAIH consultation.

The first recommended step is the screening of the company's operation in terms of data protection compliance: it is necessary to examine not only the data management procedures of the company, its actual data management operations and data security measures, but also the available data protection documentation (what regulations and information are already available at the controller, are there any procedural rules for data security, how adequate are the employment protection contracts, etc.). It is also necessary to identify the IT aspects of the compliance. It is essential to incorporate the appropriate safeguards for compliance with the policies of the respective data management operations, and if needed, new policies and procedures shall be created.

A data protection officer shall be designated at the company, if it is mandatory. Once the regulations are prepared, they should not only be published, but also introduced to the workers by education.

Conclusively, the companies should ensure the compliance with the statutory obligations and need to increase overall awareness of data protection law during their day-to-day operation firstly, in order to avoid any complaint on behalf of any data subject on the basis of improper handling of their personal data, secondly, in order to ensure that in case a complaint is filed, we can provide adequate responses to the authority during the investigation so that it closes without any fines being imposed. Failure to comply with the provisions of the GDPR has real and significant financial risks for all companies processing data. **However, risks can be avoided, for which our partners and data protection specialist work together with your company to ensure that the risk assessment with a data protection audit is done as quickly as possible and our clients reach the highest level of GDPR compliance by 25 May 2018.**

In case you have any questions in connection with the preparations for the application of the GDPR our data protection specialists are at your company's disposal at any time on the following contact details:

Dr. Arne Gobert
Managing Partner, Attorney-at-Law
arne.gobert@gfplegal.com

Dr. Réka Ipacs
Partner, Attorney-at-Law, Certified Data Protection Officer
réka.ipacs@gfplegal.com

Dr. Veronika Francis-Hegedűs
Attorney-at-Law, Head of Data Protection Desk
veronika.francis-hegedus@gfplegal.com