GOBERT UND PARTNER
RECHTSANWALTSKANZLEI

Róbert Károly krt. 70-74, "B" 8. Stock
1134 Budapest
UNGARN
Telefon: + 36 (1) 270 9900
Telefax: + 36 (1) 270 9990
E-Mail: office@gfplegal.com

GDPR NEWSLETTER

DER

DER RECHTSANWALTSKANZLEI
BWSP GOBERT & PARTNER

SONDERAUSGABE

Budapest

2018

GDPR UMSETZUNG IN DER PRAXIS - DIE ZEIT IST REIF FÜR PLÄNE!

Vorbereitung auf die neue EU-Datenschutz-Grundverordnung in Ungarn

Der Schutz der Privatsphäre wird eine besonders hervorgehobene Rolle in der unmittelbar anwendbaren Datenschutz-Grundverordnung Nr. 679/2016 (**GDPR**) des Europäischen Parlaments und Rates spielen. Die neue Verordnung regelt die Behandlung von personenbezogenen Daten nicht weniger streng und nicht mit geringerer Bedeutung, als den Besitz von einer neuen wirtschaftlichen Ressource. Die ungarische Behörde beurteilt es ähnlich, denn die Mitarbeiter der Nationalen Datenschutz- und Informationssicherheitsbehörde (**NAIH**) äußern gewöhnlich bei ihren Vorträgen vor dem Fachpublikum, dass „die Daten das Öl der Informationsgesellschaft sind". Die, in den 28 Mitgliedstaaten der EU unmittelbar anwendbare und die nationalen Rechtsvorschriften überschriebene GDPR muss in Ungarn zusammen mit den Anordnungen des 2011. CXII. Gesetzes über das Informationsselbstbestimmungsrecht und die Informationsfreiheit (**InfoG.**), anderer Brancherechtsvorschriften, sowie mit der Praxis der ungarischen Datenschutzbehörde ausgelegt werden; und sie muss ab 25. Mai 2018 in allen Unternehmen mit einem ungarischen Sitz im Alltagsbetrieb des Verarbeitungssystems der Daten in Papier- und digitalisiertem Format angewendet werden. Die Vorschriften der GDPR betreffen jedoch nicht nur die Unternehmen, die ihre zentrale Geschäftstätigkeit in den EU-Mitgliedsstaaten ausüben, sondern der Geltungsbereich der GDPR erstreckt sich auch auf solche Unternehmen, die sich außerhalb der EU mit der Datenverarbeitung beschäftigen und deren Datenverarbeitungstätigkeit sich an die Bereitstellung von Waren oder Dienstleistungen an Kunden, die sich in einem beliebigen EU-Mitgliedsstaat befinden, knüpft; oder die Datenverarbeitung solcher Unternehmen sich an die Überwachung des Verhaltens natürlicher Personen innerhalb des EU-Territoriums knüpft (z.B. Profilbildung, Vorhersage von persönlichen Präferenzen, Monitoring auf dem Internet usw.).

Komplexe juristische und informationstechnische Maßnahmen sind erforderlich, mit denen man nicht früh genug beginnen kann, um sich auf die neue europäische Datenschutz-Grundverordnung vorzubereiten. Nach dem Inkrafttreten sind die europäischen Datenschutzbehörden berechtigt, beispiellos hohe Geldstrafen in Höhe von bis zu 20 Millionen Euro oder 4 % des weltweiten Umsatzes der Firma im Vorjahr zu verhängen. Das bedeutet, dass die finanzielle Risiken der Unternehmen, die sich auf dem EU-Territorium mit Datenverarbeitung beschäftigen, bei Nichtbefolgung der neuen Rechtsvorschriften beachtlich vergrößern werden.

I. WAS ENTHÄLT EIN WIRKSAMER AKTIONSPLAN BEI DER VORBEREITUNG AUF DIE GDPR?

Es stellt sich die Frage, was wir genau in den verbleibenden Monaten für das Erreichen eines GDPR-konformen Datenschutz- und Datensicherheitsniveau tun können, und wie wir die finanziellen Risiken unserer Firma minimieren können. Die geschäftsführenden Partner unserer Kanzlei schlagen den folgenden Aktionsplan vor, der im Rahmen eines Dienstleistungspakets für die Vorbereitung auf die GDPR von den Datenschutzexperten unserer Kanzlei ausgearbeitet wurde:

1. Audit der gegenwärtigen Praxis der Datenverarbeitung und der Datenschutzdokumentation der Firma aus Datenschutzhinsicht (Audit, Folgenabschätzung, IT-Audit, Datenkarte);
2. Angemessenheitsuntersuchungen, Interessenabwägungstests, Errichtung von Datenschutzstufen auf der Rechtsbasis der neuen GDPR für die Verarbeitungseinwilligungen, Sicherstellung der Rechte der Betroffenen, Handhabung von Verletzung des Schutzes personenbezogener Daten, Pseudonymierung und andere datenverarbeitungsbezogene Firmenpraxis;
3. Vorbereitung der GDPR-konformen juristischen Dokumentation (z.B. Vorschriften für die Angestellten und Klienten, Merkblätter, Einverständniserklärungen, Formulare, Plan für die Handhabung von Verletzung des Schutzes personenbezogener Daten, Informationssicherheitsregelung usw.);
4. Vorbereitung der juristischen Dokumentation und Vorgehensweise für eine angemessene Verständigung der Betroffenen, Aktualisierung und kontinuierliches Monitoring der Datenkarte;
5. Überprüfung, Bearbeitung und Gestaltung der Firmenwebseite aus Datenschutzhinsicht;
6. Einbindung der Sicherheitspraxis in den Betrieb und das IT-System der Firma, die vom „Privacy by Design" Grundprinzip verlangt wird;

7. Gestaltung von Vertragsmustern der Datenverarbeitung und Gefährdungsbeurteilungsmaßnahmen in Bezug auf den Auswahlprozess der Vertragspartner;
8. Prüfung der Cloud-basierten Datenspeicherung und die Gestaltung ihrer GDPR-Angemessenheit;
9. Erarbeitung von Verfahren und Maßnahmen für den besonderen Schutz von Kinderrechten;
10. Ernennung eines Datenschutzbeauftragten, wenn es die GDPR für das Unternehmen vorschreibt;
11. Mitteilung der anmeldepflichtigen Datenverarbeitung an die NAIH im Einklang der neuen Verordnung noch vor dem 25. Mai 2018;
12. Sicherstellung der Schulung von Geschäftsführern und Datenschutzangestellten innerhalb der Firma, Steigerung des Datenschutzbewusstseins, Erstellung von innerhalb der Firma anwendbaren E-Learning Tests und Prüfungen;
13. Fortlaufender Kontakt zur NAIH, Genehmigung von Interessenabwägungstests, Durchführung von vorherigen Folgeabschätzungen;
14. Erarbeitung von obligatorischen internen Datenschutzregistern;
15. Erarbeitung einer Verbindlichen Organisatorischen Regelung (BCR) innerhalb der Unternehmensgruppe; Prüfung der, in dem „Privacy Shield" tätigen Firmen;
16. Monitoring des Firmenbetriebs gemäß der Datenschutzverordnung.

II. WAS LOHNT SICH ZU WISSEN ÜBER DIE GDPR VERORDNUNG?

Alle Unternehmen, die mit natürlichen Personen durch jeglichen Kontakt personenbezogene Daten aufnehmen, sammeln, benutzen oder speichern, gelten als sog. „Datenverarbeiter" personenbezogener Daten – das sind 99% aller funktionierenden Firmen und so sind sie verpflichtet, die GDPR-Vorschriften einzuhalten. Wenn ein Unternehmen die, in der GDPR bestimmten Datenverarbeitungstätigkeit mit Wirkung auf Ungarn ausübt, muss es die GDPR-Vorschriften, die nationalen Rechtsvorschriften bezüglich des Datenschutzes und die strenge NAIH-Praxis vor Augen halten.

GDPR definiert den Begriff der „**personenbezogenen Daten**" breiter, als die gültige europäische Richtlinie und die nationalen Regelungen. Laut GDPR können nämlich personenbezogene Daten **auf eine natürliche Person bezogene Informationen** sein, **mit denen die Person mittelbar und unmittelbar identifiziert werden kann**. Als personenbezogene Daten gelten demzufolge nicht nur der Name, der Personalausweis, der Geburtsort, die E-Mail-Adresse, Fotos oder Tonaufnahmen natürlicher Personen (**Betroffenen**), sondern auch geistiges, wirtschaftliches, kulturelles oder soziales Knowhow, als ortsangebende Daten die GPS-Daten ihres Fahrzeuges und Mobilfunkgerätes, oder ihre Browserdaten am Arbeitsplatz, sogar auch die IP-Adressen und Cookies. **Wie kann man die datenschutzbewusste Handhabung der, durch die GDPR beachtlich erweiterten personenbezogenen Daten in der Praxis so ausführen, dass sie den Vorschriften restlos entsprechen?** – fragen uns regelmäßig unsere Mandanten. Selbst die Ansicht (d.h. Kennenlernen) dieser personenbezogenen Daten bedürfe einer unternehmensinternen Verarbeitungsregelung, Verständigung und Regelung bezüglich der Formen des Monitoring der Angestellten (z.B. Internetbenutzung, Firmennummer, Kameragebrauch, GPS), Verarbeitungsregister, sowie einen rechtmäßigen Zweck und nachträgliche Verifizierbarkeit, welche Anforderungen ab dem 25. Mai 2018 von kritischer Bedeutung werden.

Eines der zentralen Elemente der neuen Datenschutzverordnung ist die zweckgebundene Datenverarbeitung und das Grundprinzip der Zweckbindung. Das bedeutet, dass jede einzelne Verarbeitung einem konkreten Zweck dienen soll. Wenn also eine Firma für die Erhebung und Speicherung von personenbezogenen Daten auch nachträglich keinen konkreten und umschriebenen Zweck gemäß den Verordnungen nachweisen kann, besteht die Gefahr, dass die Datenschutzpraxis juristische Bedenken aufwirft. **Der erste essentielle Schritt bei der Vorbereitung auf die GDPR ist, dass die gegenwärtigen Zwecke der einzelnen Datenaufnahmen der Unternehmen gemäß der GDPR-Prinzipien überprüft werden.** Neben dem Grundprinzip der Zweckbindung, spielen auch das

Verhältnismäßigkeitsprinzip und die Notwendigkeit eine hervorgehobene Rolle. Darüber hinaus müssen die neuen, besonders sensitive Daten geprüft werden, so die Verarbeitung von medizinischen oder biometrischen (z.B. Porträt, Fingerabdruck), bzw. genetischen Daten. Laut NAIH kann die Verarbeitung dieser Daten ausschließlich aufgrund von berechtigten Interessen geschehen. Im Fall der modernen Eintrittssysteme (externer Systemzugang) können solche berechtigten Interessen nicht geringer sein, als wenn beispielsweise ein „tödlicher Virus" im Datenraum selbst untersucht wird.

Bei der Vorbereitung auf die GDPR muss man besonders auf die Überprüfung der Datenschutzpraxis gemäß der entsprechenden Rechtsgrundlage achten. **Laut der neuen Regelung kann die Rechtsgrundlage der Datenverarbeitung die freiwillige Einwilligung der Betroffenen oder eine Rechtsvorschrift, bzw. andere neue Rechtsgrundlagen sein, z.B. berechtigtes Interesse, die Wahrnehmung einer Aufgabe, die im öffentlichen Interesse liegt oder in Ausübung öffentlicher Gewalt erfolgt.** Von den neuen Rechtsgrundlagen ist das berechtigte Interesse hervorzuheben, d.h. laut GDPR kann die Verarbeitung das berechtigte Interesse der Verarbeiter oder eines Dritten rechtfertigen. Diese Rechtsgrundlage wird voraussichtlich regelmäßig in Zusammenhang mit der Datenverarbeitung der Angestellten, bzw. dem Vertragsschluss und dessen Erfüllung angewendet.

Bezüglich der Anwendung der GDPR müssen sich die Geschäftsführer und Datenschutzangestellten der Unternehmen ausdrücklich darüber bewusst sein, welche Rechte den Betroffenen zustehen (Recht auf Verständigung, Berichtigung und Löschung usw.), denn die Erfüllung der Rechte der Betroffenen taucht weiterhin als eine Verpflichtung seitens des Unternehmens als verantwortlichem Datenverarbeiter auf.

III. WELCHEN TYPISCHEN DATENVERARBEITUNGSTÄTIGKEITEN GIBT ES IN EINEM UNTERNEHMEN?

Die untenstehenden Geschäftstätigkeiten gelten als tagtägige Verarbeitungsprozesse aller Unternehmen, daher haben wir unsere praktischen und nützlichen Ratschläge aufgelistet, die der Erfüllung der GDPR-Vorschriften nach 25. Mai 2018 dienen.

1. Verständigungs-, Angebotsersuchen; Terminbuchungsbehandlung, Lebensläufe von Kandidaten

Die Zweckbindung, das Verhältnismäßigkeitsprinzip und die Notwendigkeit sollen sich auch auf den ganzen Prozess und Zeitraum der Datenverarbeitung beziehen. Wenn eine E-Mail, die ein Verständigungs- oder Angebotsersuchen, eine Terminbuchung (und dadurch die personenbezogene Kundendaten) beinhaltet, von dem Unternehmen nicht mehr gebraucht wird, so muss sie von allen Datenbanken der Firma gemäß der Praxis der NAIH gelöscht werden. Obwohl wir bei einer Terminbuchung den Namen, bzw. die Telefonnummer des Kunden gewöhnlich notieren, müssen alle personenbezogene Daten endgültig aus der Datenbasis gelöscht werden, wenn sie ihren Zweck erfüllt haben; es sei denn, die Firma kann ihr legitimes Interesse der Beibehaltung der Daten nachweisen, oder der Betroffene hat der Firma seine ausdrückliche Einwilligung für die Beibehaltung der Daten nach ihrer Zweckerfüllung erteilt.

2. Betrieb von Kamerasystemen

Bitte beachten Sie, dass ein Kamerasystem zurzeit oder nach dem Inkrafttreten der GDPR im öffentlichen Raum, auf dem Privatgelände, bzw. am Arbeitsplatz zur Beobachtung der Angestellten nur dann betreiben werden kann, wenn der Betrieb der Einhaltung gewisser Garantien entspricht und die Betroffenen, Angestellten angemessen informiert wurden. Mit einem Kamerasystem am Arbeitsplatz darf man nicht das Privatleben beobachten, oder die Arbeitsverrichtung durch die Kameras beeinflussen.

Bei der Einrichtung von Kamerasystemen ist die Erfüllung der Datenschutzvorschriften äußerst wichtig. NAIH kann unter der Anwendung der Notwendigkeit und des Verhältnismäßigkeitsprinzips, neben der Erhebung einer Geldstrafe, das Abmontieren von unnötigen Kameras aufgrund einer „überproportionalen Beobachtung" des beobachteten Bereiches anordnen, z.B. das Abmontieren von Kameras in einer Hotellobby (2 von 4 Kameras sind erlaubt), welche unnötig sind, um den Zweck zu erfüllen. Die Filmaufnahmen – wenn ungenutzt – können 3 Tage,

oder in speziellen Fällen 30 oder 60 Tage aufbewahrt werden, wenn die Voraussetzungen des Gesetzes CXXXIII. 2005 über den Schutz der Personen und Vermögen, und die Aktivitäten von Privatdetektiven bestehen.

Wenn ein Unternehmen auf dem Betrieb von Kameras besteht, muss ein, mit den, vom NAIH vorgeschlagenen Anhängen versehene Kameravorschrift für die Betroffenen, die den beobachteten Bereich betreten, erstellt werden. Laut NAIH sind alle Personen, Kunden und Angestellten vor dem Betreten des Gebäudes berechtigt, über den Betrieb des Kamerasystems informiert zu werden. Ferner stellt sich die praktische Frage von Fall zu Fall, ob die Kamerabilder (z.B. die internen Bereiche einer Bank) als Geschäftsgeheimnis gelten.

Der sog. **Interessenabwägungstest** muss als ein integraler Bestandteil der GDPR-konformen Datenverarbeitung betrachtet werden. Die Essenz des Interessenabwägungstests besteht darin, dass der Datenverarbeiter bei der Datenverarbeitung aus besonders berechtigtem Interesse sich selbst die Frage stellen muss, ob die Datenverarbeitung tatsächlich nötig ist und er die Interessen der Betroffenen mit den seinen vergleichen muss. Nur solche Datenverarbeitungen, die diesen Test bestehen und von NAIH genehmigt wurden, sind in der Praxis auch empfohlen.

Vor der Datenverarbeitung müssen die Vorschriften und Merkblätter auf der Webseite des Unternehmens oder im Papierformat für die Betroffenen unbedingt zugänglich sein. Im Falle eines Kamerabetriebs müssen alle Räume mit Aufklebern und erklärenden Hinweistafeln versehen werden. Wenn ein Kamerasystem an der Arbeitsstelle betrieben wird, fordert die NAIH streng die vorherige Benachrichtigung der Angestellten über die konkreten Ziele der Beobachtung (niemals die Beobachtung der Angestellten!).

3. Beschwerdemanagementsystem

Laut den wirksamen Verbraucherschutzrechtsvorschriften müssen die Daten bezüglich des Beschwerdemanagements 5 Jahre lang aufbewahrt werden. Dieser Zeitraum kann sich aber in naher Zukunft durch einen aktuell diskutierten Gesetzesvorschlag im ungarischen Parlament ändern.

4. Versenden von Newslettern

Die freiwillige und ausdrückliche Einwilligung der Betroffenen bezüglich der Bestellung von Newslettern kann die Rechtsgrundlage des Versendens von Newslettern sein. Laut GDPR müssen die Firmen nachweisen, dass die Einwilligung vor dem Versenden gegeben worden ist, deshalb müssen die elektronischen oder auf Papier gesammelten Bestellungsformulare aufbewahrt werden.

Der Standpunkt von NAIH bezüglich von Newslettern ist auch EU-weit relativ streng. Laut NAIH können die Firmen Notwendigkeits- und Verhältnismäßigkeitsprinzipien-konform, die Namen, die E-Mail-Adressen (mit dem Datum der Einwilligung) der Kunden zwecks Versendens von Newsletter sammeln und verzeichnen. Eine Ausnahme bildet, wenn der Inhalt des Newsletters nur über 18 Jahren betrachtet werden kann: In solchen Fällen kann auch das Geburtsdatum verzeichnet werden. Wenn das Unternehmen bezüglich des Newsletters mehrere Daten registriert hat, ist es empfohlen, diese Newsletter-Datenbank bis zum 25. Mai 2018 zu klären.

Laut NAIH werden solche juristischen und praktischen Fragen im Falle eines Unternehmens, das eine Webseite betreibt, auftauchen, wie zum Beispiel das adäquate Format der sog. „checkbox“ der elektronischen Bestellung oder ob die Abbestellung in aller Form – auch per Post auf die Firmenadresse – möglich ist, ob die Datenbank regelmäßig auf Vorschlag der NAIH aktualisiert wird.

5. Gewinnspiel

Unternehmen, die Gewinnspiele anbieten, gelten als Datenverarbeiter, während die Marketingfirmen mit dem Auftrag der Abwicklung von Gewinnspielen als „Auftragsverarbeiter“ gelten. Auftragsverarbeiter tragen ähnliche Verantwortung und Risiken einer Geldstrafe im Falle einer Nicht-Erfüllung der Vorschriften, wie die Datenverarbeiter. Alle Gewinnspiele sind zurzeit anmeldepflichtig und müssen im öffentlich zugänglichen Datenschutzregister der NAIH eingetragen werden. Daneben ist es erforderlich, auch eine Datenschutz- und eine Gewinnspielregelung auszuarbeiten, die öffentlich verfügbar sind (z.B. auf einer Webseite oder ein Link).

6. Verarbeitung von personenbezogenen Daten von Stellenbewerbern und Angestellten

Eine umfassende, ausführliche schriftliche Verständigung der Stellenbewerber und Angestellten einer Firma ist erforderlich, bevor man mit der Datenverarbeitung der Betroffenen beginnt. Im Lichte der GDPR muss man betonen, dass die Firmen die Lebensläufe der erfolglosen Stellenbewerber nach dem Ablauf des Auswahlprozesses ohne ihre vorherige und ausdrückliche Einwilligung nicht aufbewahren dürfen. Die Arbeitgeber dürfen auch keine besonderen Daten (z.B. Vorstrafenregister) ohne die Einwilligung der Kandidaten verlangen, wenn es nicht hauptsächlich mit dem Betätigungsfeld begründet werden kann. Bei der Datenverarbeitung müssen die Arbeitgeber mit verstärkter Vorsicht umgehen, damit sie den untenstehenden Verpflichtungen der Datenverarbeiter, bzw. den Voraussetzungen zur Sicherstellung der Rechte der Betroffenen entsprechend handeln.

IV. WELCHE VERPFLICHTUNGEN HAT DER DATENVERARBEITER?

Die Verpflichtungen des Datenverarbeiters und die Rechte der Betroffenen werden durch die GDPR ab 25. Mai 2018 wesentlich verbreitert. In unserer vorliegenden Zusammenfassung haben wir die Verpflichtungen der Datenverarbeiter gemäß der GDPR zusammengefasst.

1. Verpflichtung der vorherigen Verständigung

Das Recht der Betroffenen auf die vorherige Verständigung ist kein neues Recht, jedoch schreibt die GDPR in erhöhtem Maß vor, dass die vorläufige Verständigung im Falle jeder Datenverarbeitung umfassend bezüglich der Zwecke, des Rechtsgrundes, der Zeitdauer der Datenspeicherung, der Rechtsmittel, der Datensicherheit, der Kontaktdaten des Datenschutzbeauftragten, der Informationen bezüglich der Datenweiterleitung und Auftragsverarbeiter sein sollte. Der Datenverarbeiter ist verpflichtet, im Falle einer eventuellen behördlichen Prüfung bestätigen zu können, dass die ausführliche, vorgeschriebene Verständigung des Betroffenen vor dem Zeitpunkt der Datenverarbeitung in Zusammenhang mit der Datenverarbeitung erfolgte.

Im Falle der zustimmungsgemäßen Datenverarbeitung besteht ein Novum der GDPR darin, dass die „**freiwillige und ausdrückliche**“ zu jeder Zeit durch aktives Verhalten widerrufbare Zustimmung als Forderung vorgeschrieben ist. Unser praktischer Vorschlag für die Datenverarbeitung ausführenden Unternehmen ist, neben der möglichst ausführlichsten schriftlichen Datenschutzverständigung, das Einholen und Aufbewahren der schriftlichen Einwilligung der Betroffenen. Dadurch kann das Unternehmen die rechtmäßige Datenverarbeitungsaktivität später im Fall einer eventuellen behördlichen Prüfung nachweisen. Über die GDPR stellt auch die NAIH strenge und praktische Forderungen bezüglich der Zustimmung aufgrund der vorherigen Verständigung, insbesondere im Falle von „checkbox“ Strukturen und Tonaufnahmen.

Eines der Elemente der GDPR-Angemessenheit ist die Anfertigung von Satzungen und Regelungen. Kernelemente der GDPR-konformen Auskünfte und Regelungen sind laut den Datenschutzexperten unserer Rechtsanwaltskanzlei folgende:

- Falls die Datenverarbeitung bei der NAIH anmeldepflichtig ist, was ist die Nummer ihrer Anmeldung?
- Wer ist der Datenverarbeiter?
- Was ist der Zweck der Datenverarbeitung?
- Was ist die Rechtsgrundlage der Datenverarbeitung?
- Wie lange verarbeitet der Datenverarbeiter die Daten?
- Wie und in welcher Weise läuft die Datenverarbeitung ab?
- Wer und welche Arbeitnehmer können zu den Daten zugreifen und wann und in welchen Fällen sind sie zu dem Zugriff berechtigt?
- Welche Auftragsverarbeiter beschäftigt der Datenverarbeiter?
- Erfolgt eine Datenübermittlung außerhalb der EU?
- Welche Rechte hat der Betroffene und in welcher Weise kann der Betroffene seine Rechte geltend machen?
- Gibt es einen Datenschutzbeauftragten und in welchen Fällen kann sich der Betroffene an ihn wenden?
- Welche Datenschutzmaßnahmen und Verfahren sind in Kraft bei dem Datenverarbeiter?
- Was ist das Verfahren bei Verletzung des Schutzes personenbezogener Daten?

2. Registrationspflicht bei der NAIH und das interne Register der Datenverarbeitungen

Zurzeit ist es obligatorisch – mit einigen Ausnahmen – bestimmte Datenverarbeitungen in das Datenregister der NAIH anzumelden. Davon unabhängig schreibt die GDPR als Verpflichtung für die Datenverarbeiter und für die Auftragsverarbeiter vor, auch ein internes Register über die Datenverarbeitungen zu führen.

Die Organisationen, die weniger als 250 Arbeitnehmer beschäftigen, sind nicht verpflichtet, ein solches Register zu führen; ausgenommen, falls sie risikoreiche ausführen oder sog. „**sensible Daten**" (zum Beispiel: Daten zur rassischen Herkunft, politische Meinung, religiöse oder ideologische Überzeugung, Mitgliedschaft in einer Gewerkschaft oder genetische, biometrische oder gesundheitliche Daten betreffen) oder die strafrechtliche Haftung verursachende Daten verarbeiten.

3. Register der Datenübermittlung

GDPR ermöglicht die Datenübermittlung an Drittländer oder an eine internationale Organisation ähnlich zu den wirksamen Regeln im Falle der Erfüllung der Voraussetzungen, die das angemessene Datenschutzniveau gewährleisten. Es bleibt aufgrund der wirksamen nationalen Datenschutzvorschriften unverändert, dass die Datenverarbeiter, die die Daten weiterleiten, die Datenübermittlung automatisch oder in einem geführten Register eintragen müssen.

Laut GDPR ist die behördliche Genehmigung der Datenübermittlung im Falle der Erfüllung der speziellen Datenübermittlungsgarantien (z.B.: die von den Nationalbehörden genehmigte Verbindliche organisatorische Regelung) nicht erforderlich. Die gesetzmäßige Datenübermittlung kann auch aufgrund der sonstigen, zwischen dem Datenverarbeiter und dem Auftragsverarbeiter aus Drittländern oder in internationalen Organisationen abgeschlossenen Vereinbarung gewährleistet werden, wenn die nationale Datenschutzbehörde durch eine sonstige Genehmigung diese als Garantie des Datenschutzniveaus genehmigt.

Wenn die Kommission offiziell feststellt, dass ein Land ein angemessenes Datenschutzniveau gewährleistet, ist die Erlangung solcher Genehmigung mangels dieser Garantien und der weiteren Garantien der GDPR nicht erforderlich, jedoch existiert ein solches Land mit solcher Qualifikation bisher noch nicht.

4. Register der Datenschutzverletzungen

Die GDPR führt den Begriff der Verletzung des Schutzes personenbezogener Daten ein. Das bedeutet eine solche Verletzung des Datenverwaltungssystems, die den unbefugten Zugriff zu den Daten oder die rechtswidrige Vernichtung der Daten (das Register der Firma ist von Hackern aufgebrochen worden, falls eine E-Mail oder ein Brief an eine andere Person weitergeleitet wird, ein Laptop von dem Arbeitsplatz verschwindet etc.) ergibt. Im Falle der Verletzung des Schutzes personenbezogener Daten sind die Datenverarbeiter zur Anmeldung, Registrierung und Verständigung verpflichtet und zwar laut GDPR nach der folgenden Reihenfolge:

1. **Schnelle Folgenabschätzung.** Falls festgestellt wird, dass die Verletzung der Sicherheit den Betroffenen möglicherweise eine erhebliche Verletzung verursachen kann, und/oder die Verletzung des Schutzes der personenbezogener Daten ein wesentliches Datenschutzrisiko trägt, ist das Unternehmen verpflichtet, den folgenden zweiten und dritten Schritten zu folgen.
2. **Anmeldung binnen 72 Stunden bei der NAIH**, dass das Schutzsystem des Datenverarbeiters verletzt worden ist. In der Anmeldung muss die Beschreibung der Verletzung des Schutzes personenbezogener Daten beinhaltet sein und was der Datenverarbeiter für die Vermeidung der Risiken und der Schäden und für die Vermeidung der nachfolgenden ähnlichen Verletzung des Schutzes der personenbezogenen Daten getan hat.
3. **Verständigung der Betroffenen** über den Erfolg der Verletzung des Schutzes der personenbezogenen Daten mit wahrscheinlich hohen Risiken. Der Datenverarbeiter ist verpflichtet, alle Betroffenen in einer klaren und gemeinverständlichen Weise zu informieren, das das rechtliche Risiko für die Datenverarbeiter trägt, dass die Betroffenen wegen der Verletzung ihrer Rechte zu dem Schutz der personenbezogenen Daten berechtigt sind, Schmerzensgeld von dem Unternehmen vor dem Gericht im Zivilprozessverfahren zu verlangen.

5. Bestellung des internen Datenschutzbeauftragten

Laut GDPR wird es in einzelnen Fällen obligatorisch sein, eine unabhängige Person mit Sachkenntnissen im Bereich des Datenschutzes, einen sog. „Datenschutzbeauftragten" bei den Unternehmen ab 25. Mai 2018 zu beschäftigen, falls:

1. die Datenverarbeiter Organisationen des öffentlichen Rechtes oder Organisationen mit öffentlichen Aufgaben sind,
2. **die Haupttätigkeit des Datenverarbeiters oder des Auftragsverarbeiters mit der regelmäßigen und systematischen Überwachung der personenbezogener Daten zusammenhängt**, oder
3. sensible Daten oder persönliche Daten betreffende Beschlüsse in Zusammenhang mit der Feststellung der strafrechtlichen Haftung der Betroffenen und die Straftaten betreffende Daten von der Organisation verarbeitet sind.

Zwischen den obigen Fällen muss der Zweite betont werden, der national flexibel ausgelegt werden kann, und es stellt sich dabei für die Mehrzahl der Unternehmen die Frage, welche Art der Datenverarbeitung ausführende Unternehmen von dieser Verpflichtung betroffen sind. Bezüglich der Frage in dem zweiten Fall, ob die bestimmte Datenverarbeitung an die Haupttätigkeit des Unternehmens geknüpft ist, können die, in dem Firmenregister angegebenen Aufgabenbereiche in Betracht genommen werden. Mit Rücksicht darauf müssen zum Beispiel Marketingagenturen, Banken, Versicherungsunternehmen, Telefon- und Internetdienstanbietern aber auch viele andere Unternehmen aus unterschiedlichen Branchen einen Datenschutzbeauftragten beschäftigen. Dies ist im Einzelfall zu prüfen!

6. Verbindliche organisatorische Regelungen (Binding Corporate Rules, BCR), Schweiz/EU-USA Datenschutzschild

Die Voraussetzung der Datenübermittlungen an Länder außerhalb des Gebietes der Europäischen Union ist, dass das angemessene Datenschutzniveau durch Garantien zwischen den zwei Ländern gewährleistet werden muss. Eine der Garantien ist die Annahme der von der lokalen Datenschutzbehörde genehmigte „Verbindliche Organisatorische Regelung" für die Unternehmensgruppen, aufgrund dessen die Unternehmen der Firmengruppe sich für die Einhaltung der Vorschriften der GDPR verpflichten, somit erkennen sie praktisch die Vorschriften der GDPR als obligatorisch an.

Ein effizientes – ähnlich zu den obigen – Mittel kann die Verknüpfung zu dem Schweiz/EU-USA Datenschutzschild (**Privacy Shield**) sein, die als Lösung im Falle der transatlantischen kommerziellen Verbindungen bei den Datenübermittlungen an den Geschäftspartnern in die Schweiz/USA gelten kann. Daten dürfen an die, zu der Privacy Shield verknüpften amerikanischen Unternehmen aus der EU oder aus den USA übermittelt werden, falls sie die Einhaltung der GDPR durch die Grundprinzipien der Privacy Shield als verbindlich anerkennen. Die Liste der an der Privacy Shield teilnehmenden Unternehmen kann hier kontrolliert werden: www.privacyshield.gov/welcome.

7. Die fortdauernde Sicherung des täglichen Betriebes laut den Datenschutzregeln, „Privacy by Design"- Grundprinzip

Die GDPR führt die, in der Presse mehrmals betonte generelle Forderung der „Privacy by Design" Denkweise über das Prinzip der Datenminimierung als Neuheit ein. Zwecks der Durchführbarkeit dieser Prinzipien ist es erforderlich, den Betrieb des Unternehmens aus dem Aspekt des Datenschutzes und der Datensicherheit fortdauernd zu überprüfen. **Es bedeutet, dass der Ablauf einer fortdauernden Folgenabschätzung insbesondere im Falle der Entwicklung, Planung, Auswahl oder Verwendung von neuen Produkten sowie Dienstleistungen erforderlich sein wird. Praktisch wird es die fortdauernde Überprüfung des Betriebes des Unternehmens bedeuten.**

V. WELCHE RECHTE UNTERSTÜTZEN DIE AUSÜBUNG DER RECHTE DER BETROFFENEN?

Laut GDPR werden den Betroffenen die folgenden neuen Rechte gewährleistet, deren Geltendmachung die Verpflichtung der Datenverarbeiter und der Auftragsverarbeiter sein wird.

1. Recht auf Verständigung und Zugriff

Die Betroffenen werden berechtigt sein, eine ausführliche Dokumentation von dem Datenverarbeiter bezüglich der Verarbeitung über die, sie persönlich betreffenden und/oder die von ihnen zur Verfügung der Datenverarbeiter gestellten Daten, zu verlangen. In der an den Betroffenen übergebenen Dokumentation muss inbegriffen werden, ob die Verarbeitung der personenbezogenen Daten erfolgte und falls ja, müssen über die konkreten Daten der Betroffenen die einzelnen Datenverarbeitungszwecke, die Zeitdauer der Datenverarbeitung, die Auftragsverarbeiter, im Falle der eventuellen Datenübermittlung die Empfänger, die Rechtsmittel, und falls solches erfolgt war, die Tatsache der automatisierten Profilbildung inbegriffen werden. Falls es von dem Betroffenen gewünscht ist, muss mindestens eine Kopie ihrer persönlichen Daten zu ihrer Verfügung gestellt werden.

2. Recht auf „Vergessenwerden“

Laut GDPR wird das „Recht auf Vergessenwerden“ im Vergleich zu dem Recht auf Löschen ein Zusatzrecht für die Betroffenen sein, das heißt, dass der Datenverarbeiter verpflichtet sein wird, die persönlichen Daten unverzüglich zu löschen, falls irgendeiner der in der GDPR angegebenen Fälle besteht. Mit Rücksicht darauf wird der Datenverarbeiter gemäß dem Wunsch des Betroffenen verpflichtet sein, die persönlichen Daten sowohl aus den Sicherheitskopien, als auch aus den eventuellen Replikationen zu löschen, insbesondere falls der Betroffene der Datenverarbeitung als Kind zugestimmt hat oder falls die Daten überholt sind und ihre Verarbeitung nicht mehr erforderlich oder die Datenverarbeitung rechtswidrig ist.

Der Betroffene muss über die von ihm gewünschten Maßnahmen informiert werden. Falls der Datenverarbeiter die persönlichen Daten eventuell veröffentlicht hat oder an anderen Datenverarbeiter oder Auftragsverarbeiter die persönlichen Daten übermittelt hat, ist es nicht ausreichend die Daten aus der eigenen Datenbank zu löschen, sondern er muss auch die Datenverarbeiter und/oder die Auftragsverarbeiter über den Wunsch des Betroffenen informieren und für die restlose Löschung der persönlichen Daten sorgen. Das von der GDPR eingeführte Recht auf Vergessenwerden wird wegen den umfassenden Verpflichtungen der Datenverarbeiter als effizientes Mittel für uns alle gelten, auch für die Arbeitnehmer, die von ihnen noch als Kind oder Jugendliche online mitgeteilten Fotos und Informationen restlos entfernen möchten.

3. Das Recht auf Datenübertragbarkeit

Im Falle der automatisierten Datenverarbeitung sind die Betroffenen in einzelnen Fällen (falls der Rechtsgrund der von dem Unternehmen ausgeführte Datenverarbeitung eine freiwillige Zustimmung ist oder die verarbeiteten Daten zwecks der Erfüllung des Vertrages erforderlich sind) zu der Datenübertragbarkeit berechtigt. Aufgrund des Rechtes auf Datenübertragbarkeit können die Betroffenen von dem Datenverarbeiter verlangen, die sie betroffenen Daten und/oder die von ihnen zu der Verfügung der Datenverarbeiter gestellten Daten an die Betroffenen weiterzuleiten; und/oder dass der Datenverarbeiter die Daten an einen anderen, von dem Betroffenen bestimmten Datenverarbeiter weiterleiten sollte, z.B. eine Bank an die andere Bank im Falle des Wechsels der Bankfiliale. Die Daten müssen an die Betroffenen oder an die Empfängersorganisation in einem, von Maschinen lesbaren und strukturierten Format ausgegeben oder an sie weitergeleitet werden. Die GDPR unterstützt die Geltendmachung des Rechtes auf die Datenübertragbarkeit dadurch, dass sie den Begriff der „Interoperabilität“, die Datenverarbeitungskooperation zwischen den Organisationen als neue generelle Forderung bezüglich der automatischen Datenverarbeitung ausführenden Datenverarbeiter einführt.

4. Die GDPR trifft Maßnahmen bezüglich der Profilbildung

Die Neuheit der GDPR ist, dass sie ausdrückliche Maßnahmen gegenüber der Profilbildung trifft, gegenüber der Erscheinung, dass die einzelnen Datenverarbeiter aus den sozialen Netzwerken und aus anderen Datenbanken erworbenen Daten Erkenntnisse bezüglich des Betroffenen in Zusammenhang mit den automatisch gesammelten Informationen, die auf Präferenzen und Verhalten hinweisen, Erkenntnisse gewinnen, d.h. sie bilden Profil, aufgrund dessen sie Operationen ausführen. Es gilt als Profilbildung laut den Vorschriften der GDPR, falls z.B. die Versicherungen, Banken, Headhunter die von ihnen aus sozialen Netzwerken (Facebook, LinkedIn) gesammelten

Informationen in ihr System eingeben, und sie stellen als das Ergebnis der automatischen Verarbeitung fest, in welcher Höhe Versicherung oder Darlehen den Betroffenen gewährleistet werden kann oder sie entscheiden sich, für welche Sorten von Arbeiten sie geeignet sind. Die Urheber der GDPR haben während der Regelung der Profilbildung berücksichtigt, dass die für Profilbildung geeigneten informatischen Systeme, Algorithmen sich fortdauernd entwickeln und sie können in der Zukunft erheblich größere Rolle haben. Mit Rücksicht darauf kann die Profilbildung ab dem Zeitpunkt des Inkrafttretens der GDPR nur mit angemessenen Garantien ausgeführt werden, der Datenverarbeiter muss die Verständigung für die Betroffenen vor dem Zeitpunkt der Profilbildung ermöglichen und die Möglichkeit des Einwandes und der Löschung im Falle eines solchen Wunsches der Betroffenen ermöglichen.

Es ist wichtig, sich im Zusammenhang mit der Profilbildungspraxis für HR Zwecke vor Augen zu halten, dass die Überprüfung der Arbeitnehmer und der Arbeitssuchenden durch ihre Facebook-Profile und anderen Sozialnetzwerken ausschließlich in dem Falle nach dem Standpunkt der NAIH erlaubt ist, falls diese Tatsache in dem Stellungsangebot vorläufig von dem Arbeitsgeber angegeben war, und/oder falls der Arbeitssuchende und/oder der Arbeitnehmer über die Tatsache der Profilbildung vorläufig informiert war. Unser praktischer Vorschlag ist im Zusammenhang damit, dass es sich lohnt, eine Bestätigung für die Datenverarbeitung und für die Datenspeicherung per Email zu verlangen.

Die von der GDPR eingeführte neue Rechtsgrundlage der Datenverarbeitung ist das „berechtigte Interesse“, in Bezug dessen die Profilbildung in einzelnen Fällen zwischen engeren Rahmen rechtmäßig sein kann und dessen Schlüssel es ist, die gerechtfertigten Interessen des Datenverarbeiters zu dem konkreten Zweck der Profilbildung zu berücksichtigen. Ein praktisches Beispiel ist, falls Personalberatungsfirmen Daten aus Geschäftszwecken (z.B.: die von dem Betroffenen auf dem LinkedIn Profil veröffentlichten, die frühere Arbeitsplätze und Berufserfahrungen betroffenen persönlichen Daten) verarbeiten. Ihre Voraussetzung ist, dass das Profilbildung ausführende Unternehmen verpflichtet ist, die Betroffenen auf die Tatsache der Datenverarbeitung aufmerksam zu machen und die Geltendmachung der Ausübung der Rechte der Betroffenen zu ermöglichen.

5. Anonymisierung: Die vorgeschlagene Datenschutzpraxis laut der GDPR

Die “Anonymisierung” ist die, in den Vorschriften der GDPR angegebene, vorgeschlagene Datenschutzpraxis, womit der Datenverarbeiter und/oder der Auftragsverarbeiter das Risiko der Datenverarbeitung herabsetzen und ihrer Verpflichtungen aufgrund der GDPR nachkommen können. Die Anonymisierung bedeutet, dass der Betroffene mangels der weiteren, separat gespeicherten Daten aufgrund der anderen persönlichen Daten nicht identifiziert werden kann. Mit Rücksicht darauf identifiziert, und/oder verbindet der Datenverarbeiter die einzelnen persönlichen Daten durch einen Code, z.B. „JGH789”. Die persönlichen Daten werden nach der Verbindung nur durch den Code in den einzelnen Registern oder Unterlagen ersetzt und der Zugriff zu den „dekodischen“ Register – z.B. zu einer Excel Säule, worin in einer Säule die persönlichen Daten, in der anderen Säule die Codes angegeben sind – wird auf dem möglichst geringsten Maße z.B. auf einen zuständigen Arbeitnehmer oder Datenschutzbeauftragten beschränkt.

6. Verrechenbarkeit und Transparenz der Datenverarbeiter aufgrund der GDPR

Die Mandanten unserer Rechtsanwaltskanzlei wenden sich oft an unseren Datenschutzexperten mit der Frage, was die, von der GDPR vorgeschriebenen Forderung der Verrechenbarkeit und Transparenz bedeuten wird. Die Datenverarbeiter sind aufgrund der Verrechenbarkeit verpflichtet, immer durch Unterlagen und Register im Falle der eventuellen Prüfung der Datenschutzbehörde beweisen zu können, dass die Datenverarbeitung rechtgemäß erfolgte. Die Datenverarbeiter sind für diesen Zweck verpflichtet, die „angemessenen technischen und organisatorischen Maßnahmen“ zu vollstrecken, das heißt die Verpflichtungen im Zusammenhang mit der Dokumentation und rechtlichen Verpflichtungen müssen mit der Inanspruchnahme der informatischen technologischen Verfahren erfüllt werden.

Die Transparenz der Datenverarbeitung muss von einfachen, kurzen und verständlichen Verständigungen, Regelungen und falls es nötig ist, die von der NAIH genehmigten Tabellen, Bildzeichen unterstützt werden, die den

Prozess und die Eigenschaften der Datenverarbeitung für die Betroffenen ganz einfach erreichbar machen. Die Erfüllung der Forderung der Transparenz wird essentiell sein, falls Kinder betreffende Daten von dem Datenverarbeiter gesammelt werden.

VI. GEGEN WAS SCHÜTZT DIE FIRMEN DAS „GDPR ANGEMESSENHEITSZERTIFIKAT"?

Die GDPR ermöglicht den Datenschutzbehörden und anderen berechtigten Organisationen der Mitgliedstaaten – in Ungarn der NAIH – die Akkreditierung solcher Zertifikatsorganisationen, die imstande sind Datenschutzaudits bezüglich der Geschäftstätigkeit der Firmen durchzuführen, die den Bedürfnissen der Markt entsprechen, und als Ergebnis des Audits ein Zertifikat über die GDPR Angemessenheit der Firmen überreichen. Solche Zertifikatsorganisationen, Auditor-Unternehmen werden auch voraussichtlich in Ungarn gegründet. Dennoch existiert auf dem ungarischen Markt noch keine solche Organisation, die sich mit der Ausstellung von akkreditierten GPDR Angemessenheitszertifikats betätigt. Unser Büro verfolgt die Situation ständig.

In Zusammenhang mit dem Zertifikat muss hervorgehoben werden, dass der reine Erwerb dessen nur das garantiert, dass die NAIH keine „ex-officio" Prüfung gegen den Datenverarbeiter, d.h. ohne eine Betroffenenbeschwerde anordnet. All das gilt nicht, wenn eine Betroffenenbeschwerde gegen die Firma mit einem Zertifikat eingereicht wird. Somit wird es nicht genug sein, ein Zertifikat zu erwerben, sondern die Firmen müssen auch die konstante GPDR konforme Geschäftstätigkeit aufrechterhalten.

VII. OBLIGATORISCHE FOLGENABSCHÄTZUNG UND VERBINDLICHE KONSULTATION MIT DER NAIH?

Alle Firmen, die sich in Ungarn mit Datenverarbeitung beschäftigen, müssen mit der NAIH in dem Falle konsultieren, wenn das Ergebnis einer internen verbindlichen Folgenabschätzung bevor einer Datenverarbeitung zeigt, dass unter Berücksichtigung der Natur, des Bereiches, Kontexts und der Ziele, die noch nicht eingeführte Datenverarbeitung hohe Risiken gegenüber der Rechte und Freiheit der Betroffenen beinhalten dürfte. Die vorherige Datenschutzkonsultation mit den Behörden, als neues, von der GDPR eingeführtes Rechtsinstitut, hat noch keine Praxis und Erfahrungswerte in Ungarn.

Daneben ist es wichtig über die Risiken der vorherigen Konsultation zu wissen. Im Einklang mit den GDPR Vorschriften kann die NAIH während der vorherigen Konsultation den Firmen nicht nur einen schriftlichen Rat geben, sondern sie kann auch bezüglich des ursprünglichen Betreffs der vorherigen Konsultation andere Prüfungen gegen die Firma anordnen, die sich auf andere Datenverarbeitung erstrecken, bzw. sie kann nach dem Ablauf der Prüfung die Firma für alle entdeckten Rechtsverletzungen anleiten, ermahnen oder mit einer Geldstrafe belegen.

VIII. WIE KANN IHRE FIRMA DIE REKORDHOHEN GELDSTRAFEN VERMEIDEN?

Die GDPR stellt ab 25. Mai 2018 allen Behörden der Mitgliedstaaten, so auch der NAIH, sicher, dass sie nach einem Amtsermittlungsverfahren im Falle einer Rechtsverletzung eine Geldstrafe verhängen können, bei der die Schwere der Datenschutz-Rechtsverletzung, der absichtliche und fahrlässige Charakter, die Dauer und andere Aspekte relativ frei im Rahmen der breit gefassten Rechtsvorschriften der GDPR berücksichtigt werden können. NAIH kann **in weniger ernsthaften Fällen eine Geldstrafe in Höhe von bis zu 10 Millionen Euro (mehr als 3 Milliarden Forint) oder bis zu 2 % des weltweiten Umsatzes der Firma verhängen** (z.B. wenn eine Firma die Anmeldung der Verletzung des Schutzes personenbezogener Daten bei der NAIH unterlässt oder wenn sie bei ihrer Geschäftstätigkeit gegen die Anforderung des „Privacy by Design" Prinzips verstößt), bzw. in **einigen ernsteren Fällen kann die NAIH sogar eine Geldstrafe in Höhe von bis zu 20 Millionen Euro (mehr als 6 Milliarden Forint) oder bis zu 4 % des weltweiten Umsatzes der Firma verhängen** (z.B. wenn die Firma gegen die Grundprinzipien der GDPR verstößt, wenn die Unterschriften der Betroffenen nicht gemäß den Vorschriften besorgt, wenn sie nicht mit der adäquaten Rechtsgrundlage, u.U. mangels einer Rechtsgrundlage Daten verarbeitet). Die GDPR versichert damit den Datenschutzbehörden der Mitgliedstaaten die Zufügung von außergewöhnlich hohen Geldstrafen, die ernsthafte Konsequenzen für die weltweiten Großunternehmen verursachen können. Verschiedene Datenverarbeitungsprozesse, die mit der GDPR nicht konform sind, können mehrmals bestraft werden.

AUFGRUND DER OBIGEN AUSFÜHRUNGEN BLEIBT DIE FRAGE: SIND SIE GENUG VORBEREITET AUF DIE GDPR EINFÜHRUNG?

Damit man die Risiken der Geldstrafe vermeidet, ist es noch nicht zu spät, die Vorbereitungen auf die neue europäische Datenschutz-Grundverordnung aufzunehmen, bzw. zu beschleunigen, die sogar monatelang dauern können. Aber was kann man, was muss man dafür genau tun? – stellt sich jeder verantwortungsbewusster Geschäftsführer in den kommenden Monaten die Frage.

Im Fall von Unternehmensgruppen, in denen die Implementierung der GDPR von der Mutterfirma behandelt wird (z.B. USA, Deutschland), sind die Ratschläge von lokalen Datenschutzexperten unausweichlich. In Ungarn müssen die neuen IT-Systeme, die neuen Vorschriften, Interessenabwägungstests, BCR-s und alle Aspekte der Datenverarbeitung nicht nur GDPR konform sein, sondern auch dem oft strengeren nationalen Privatschutzgesetz und der gewissenhaften NAIH-Praxis entsprechen. **Aufgrund der GDPR Vorschriften, wenn die neuen IT-Systeme, neue Datenverarbeitungsmethode eingeführt werden, können 99% der lokalen Tochterfirmen der multinationalen Firmen die Folgenabschätzung und einer obligatorischen Konsultation mit der NAIH nicht ausweichen.**

Der erste empfohlene Schritt ist das Audit der Geschäftstätigkeit der Firma aus Datenschutzperspektive: Man muss nicht nur die Datenverarbeitungsverfahren, die tatsächlichen Datenverarbeitungsoperationen und Datensicherheitsmaßnahmen überprüfen, sondern auch die verfügbare Datenschutzdokumentation (über welche Vorschriften und Merkblätter verfügt der Datenverarbeiter, gibt es Vorgehensweisen aus Datenschutzgründen, wie konform sind die Arbeitsverträge mit den Datenschutzvorschriften usw.). Die IT-Seite muss auch durchleuchtet werden. In den einzelnen Datenverarbeitungsoperationen müssen entsprechende Vorschriftengarantien eingebaut, im Bedarfsfall neue Vorschriften und Maßnahmen erarbeitet werden.

Wenn verbindlich, muss ein Datenschutzbeauftragter bei der Firma ernannt werden. Nach der Erarbeitung der Vorschriften müssen sie nicht nur veröffentlicht werden, sondern sie müssen auch im Rahmen einer Schulung den Angestellten bekannt gemacht werden.

Zusammenfassend: Firmen müssen für die Erfüllung der Rechtsvorschriften sorgen und sie müssen die Datenschutzbewusstsein bei der alltäglichen Geschäftsführung erhöhen, damit kein Betroffener sich wegen der unangemessenen Datenverarbeitung bei der NAIH beschwert, oder wenn eine Beschwerde eingelegt wird, die Firmen adäquate Antworten während der Ermittlung geben, so dass keine Geldstrafe verhängt wird. Die Nicht-Erfüllung der GDPR Vorschriften trägt reale und beachtliche finanzielle Risiken für die Firmen mit Datenverarbeitungstätigkeit. **Die Risiken sind aber zu vermeiden, deswegen arbeiten die Partner und Datenschutzexperten unserer Rechtsanwaltskanzlei dafür, dass bei vielen Firmen baldmöglichst die Risiken durch Datenschutzaudits verringert bzw. eliminiert werden und unsere Mandanten die höchstmögliche Vorbereitungsstufe bis zum 25. Mai 2018 erreichen.**

Bei weiteren Fragen in Zusammenhang mit der Vorbereitung auf die GDPR stehen unsere Datenschutzexperten unter den folgenden Erreichbarkeiten jederzeit zur Verfügung Ihrer Firma:

Dr. Arne Gobert
Managing Partner, Rechtsanwalt
arne.gobert@gfplegal.com

Dr. Réka Ipacs
Partner, Rechtsanwältin, Datenschutzbeauftragte
reka.ipacs@gfplegal.com

Dr. Veronika Francis-Hegedűs
Rechtsanwältin, Leiterin der Datenschutzgruppe
veronika.francis-hegedus@gfplegal.com