<u>כשחובת הגנת הפרטיות הופכת לסיכון אישי של הדירקטורים והמנכ"ל! / אסנת נתאי, עו"ד</u>*

מנכ"ל חברה נדהם לקבל דרישת אבחון רשמית מרשות הגנת הפרטיות[1]. הבעיה לא הייתה השאלון עצמו, אלא העובדה המדאיגה שמעולם לא בוצע בארגון אבחון מקדים של צרכים וסיכונים, הפערים לא מופו והתיקונים הטכנולוגיים והמשפטיים הנדרשים בחוק לא הוטמעו מבעוד מועד. האם ניתן בכלל לגשר על פערים של שנים ולהפוך מערכת נתונים פרוצה למבצר של ציות ופרטיות, כששעון החול של הרשות כבר התהפך ?

תיקון 13 לחוק הגנת הפרטיות מהווה כיום נדבך מרכזי בחיזוק יכולת ההרתעה והאכיפה של הרשות הישראלית להגנת הפרטיות. מדובר בשינוי פרדיגמה: מעבר ממודל של "המלצות" למודל של אכיפה מנהלית תקיפה, הכולל עיצומים כספיים כבדים, גם על דירקטורים ונושאי משרה, ומתן הנחיות מקצועיות מחייבות לבעלי שליטה במאגרי מידע. בעידן זה, הרשות אינה מסתפקת רק בבדיקת אירועי פריצה, אלא פועלת באופן יזום כדי לוודא שארגונים פרטיים וממשלתיים כאחד עומדים בסטנדרטים המחמירים של חוק הגנת הפרטיות, כאשר קיימת לרשות גם האפשרות להטיל קנסות אישיים על בעלי תפקידים בארגון, בסכומים של עד 150,000 ש"ח.[2]

אחד השינויים הגדולים בתיקון 13 הוא חובת מינוי ממונה הגנה על הפרטיות (DPO), אשר אינה חלה רק על גופים ציבוריים אלא גם על קבלנים העובדים מטעמם, גופים שעיסוקם העיקרי הוא סחר במידע אישי, גופים העוסקים בניטור שיטתי ומתמשך של התנהגות בני אדם כחלק מעיסוקם המרכזי, ועל גופים המעבדים בהיקף משמעותי מידע ברגישות מיוחדת, כגון נתונים רפואיים, ביומטריים, פליליים, נתוני אשראי או נטייה מינית. ה-DPO פועל כפונקציה מקצועית ועצמאית המדווחת למנכ"ל ולדירקטוריון, והוא מבצע את הפיקוח על אבטחת המידע בארגון.

גם ללא חובת מינוי DPO על הדירקטוריון מוטלת חובה אקטיבית לוודא את אבטחת המידע בארגון ולכן עליו לאשר הגדרות ונהלים, לבחון סיכונים ולוודא יישום מדיניות ציות הכוללת מנגנוני בקרה וחובת דיווח מידי על אירועי אבטחה. כך, גם כאשר לא קיימת חובה, מומלץ למנות DPO כדי לוודא עמידת הגוף בדרישות החוק באופן שוטף ולהקטין את החשיפה של דירקטורים ונושאי משרה במקרה שקרה אירוע של דלף מידע.[3] התעלמות מהמלצות ה DPO או כשל בפיקוח השוטף (לרבות אי-הקצאת משאבים מתאימים) עשויים להיתפס כהפרה של חובת הזהירות. בין בעת ביקורת רגולטורית ובין אם קרה אירוע של דלף מידע או אירוע אחר, מחדלים אלו עשויים לגרום לאחריות אישית של דירקטורים ונושאי משרה, ללא תלות באחריות החברה.

טעות נפוצה של מנהלים היא התפיסה שפרטיות היא "פרויקט" זמני לקראת ביקורת. תיקון 13 מבהיר כי האחריות הסופית מוטלת על הדירקטוריון, תוך חשיפת נושאי משרה לעיצומים כספיים אישיים כבדים, שלא לדבר על היתכנות לחקירה פלילית. לפיכך, מומלץ לנושאי המשרה לפעול ללא דיחוי להבטחת ציות מלא וגיבוש נוהלי אבטחה כתובים להגנה על המידע. לאור הסיכון המשפטי והאישי, מומלץ שלא להסתפק בספק שירותי DPO חיצוני רגיל (ולאחר תיקון 13 צצו שרלטנים כפטריות אחרי הגשם והרשת מלאה בפרסומות שלהם), אלא להשתמש בשירותי משרד עורכי דין בעל מומחיות בתחום הגנת הפרטיות לליווי מקצועי שוטף ואספקת שירותי DPO חיצוניים.

***עו"ד אסנת נתאי** הינה חלק מצוות משרד אפיק ושות' (www.afiklaw.com), שהינו חלק מרשת המשרדים BOKS International (www.boks-international.com). אסנת בוגרת הפקולטה למדעי החברה באוניברסיטה העברית בירושלים ובוגרת תואר במשפטים, בעלת תעודת גישור במשפחה מטעם מרכז גבים. אסנת מוסמכת מטעם משרד המשפטים בישראל להפקת ייפויי כוח מתמשך והיא בוגרת הכשרה של משרד המשפטים בנושא הגנה על הפרטיות. אין בסקירה כללית זו משום ייעוץ משפטי כלשהו ומומלץ להיוועץ בעורך דין המתמחה בתחום זה בטרם קבלת כל החלטה בנושאים המתוארים בסקירה זו. לפרטים נוספים: 03-6093609, או באמצעות הדואר האלקטרוני: afiklaw@afiklaw.com.

[1] ראו: https://he.afiklaw.com/updates/19311

[2] ראו: <u>פרטיות ממונה ומה שבתיקון?</u>/עו"ד עדי מרכוס, פורסם באפיק משפטי 445 06.08.2025 - https://he.afiklaw.com/articles/a445

[3] ראו: <u>כשהדירקטור נכנס לאטרף מכיוון שפרצו לך למאגר המידע</u>/עו"ד אסנת נתאי, פורסם באפיק משפטי 424 16.10.2024 - https://he.afiklaw.com/articles/a424

When Privacy Compliance Becomes a Personal Risk for the Board and CEO! / Osnat Nitay, Adv. [*]

A company CEO was surprised to receive a formal diagnostic demand from the Israeli Privacy Protection Authority (PPA).[1] The issue was not the questionnaire itself, but the alarming fact that the organization had never conducted a preliminary assessment of needs and risks, gaps were never mapped and the technological and legal rectifications required by law were not implemented in time. Is it even possible to bridge years of gaps and transform a breached data-system into a fortress of compliance and privacy when the Authority's hourglass has already been turned?

Amendment 13 to the Israeli Privacy Protection Law currently serves as a central pillar in strengthening the deterrence and enforcement capabilities of the PPA. This represents a paradigm shift: a transition from a "recommendations-based" model to a model of firm administrative enforcement, which includes heavy financial sanctions and the issuance of binding professional directives to database controllers. In this era, the PPA does not merely settle for investigating security breaches; it acts proactively to ensure that both private and governmental organizations comply with the rigorous standards of the Privacy Protection Law, with the PPA having the power to impose personal fines on company executives of up to ILS 150,000.[2]

One of the most significant changes introduced by Amendment 13 is the mandatory appointment of a Data Protection Officer (DPO). This requirement is no longer limited to public bodies; it now applies to contractors working on their behalf, entities which primary business is trading in personal data, organizations engaged in systematic monitoring of human behavior and entities processing significant volumes of sensitive data (such as medical, biometric, criminal, credit data, or information regarding sexual orientation). The DPO acts as an independent professional function, reporting directly to the CEO and the Board of Directors and is charged with overseeing the organization's data security.

However, even when appointing a DPO is not mandatory, the Board of Directors bears an active duty to ensure data security. They must approve definitions and procedures, assess risks, and verify the implementation of a compliance policy that includes control mechanisms and immediate reporting of security incidents. Therefore, even in the absence of a statutory obligation, appointing a DPO is highly recommended to ensure ongoing compliance and mitigate the exposure of directors and officers in the event of a data breach.[3] Ignoring the DPO's recommendations or failing in ongoing oversight (including the failure to allocate appropriate resources) may be perceived as a breach of the duty of care. Whether during a regulatory audit or in the aftermath of a leak, such failures can lead to personal liability for directors and officers, independent of the company's corporate liability.

A common executive error is viewing privacy as a temporary "project" in preparation for an audit. Amendment 13 clarifies that ultimate responsibility lies with the Board, exposing officers to heavy personal financial sanctions and potential criminal investigations. Consequently, officers are advised to act without delay to ensure full compliance and formulate written security procedures. Given the legal and personal risks involved, it is advisable not to settle for a standard external DPO provider (especially given the recent influx of inexperienced providers "popping up like mushrooms" post-Amendment 13). Instead, organizations should engage a law firm with specific expertise in privacy protection to provide ongoing professional guidance and external DPO services.

---

[*] **Osnat Nitay, Adv.** is part of the legal team of Afik & Co. (www.afiklaw.com), which is part of BOKS International (www.boks-international.com). Osnat is a graduate of the Faculty of Social Sciences at the Hebrew University of Jerusalem and has a degree in law. She holds a family mediation certificate from the Gevim Center. Osnat is certified by the Israeli Ministry of Justice to create lasting powers of attorneys and graduated a training of the Ministry of Justice on privacy protection. This overview does not constitute any legal advice and it is recommended to consult a lawyer who specializes in this field before making any decision on the issues described in this overview. For more details: 03-6093609, or by e-mail: afiklaw@afiklaw.com

[1] See: https://www.afiklaw.com/updates/19312

[2] See: Privacy, DPO and what's in the Amendment / Adi Marcus, Adv., Published in Afik Law 445 08.06.2025 - https://www.afiklaw.com/articles/a445

[3] See: When a Director "Enters an Atraf State" (Goes Frenzy) Because of a Data Breach/Osnat Nitay, Adv., Published in Afik news 424 16.10.2024 - https://www.afiklaw.com/articles/a424

¡Cuando el cumplimiento en materia de privacidad se convierte en un riesgo personal para la Junta Directiva y el CEO! / Osnat Nitay, Abg.*

El CEO de una empresa se sorprendió al recibir una demanda formal de diagnóstico por parte de la Autoridad de Protección de la Privacidad de Israel (PPA, por sus siglas en inglés).[1] El problema no era el cuestionario en sí, sino el hecho alarmante de que la organización nunca había realizado una evaluación preliminar de necesidades y riesgos, nunca se habían mapeado las brechas y no se habían implementado a tiempo las rectificaciones tecnológicas y legales requeridas por la ley. ¿Es posible siquiera cerrar años de brechas y transformar un sistema de datos vulnerado en una fortaleza de cumplimiento y privacidad cuando el reloj de arena de la Autoridad ya se ha dado la vuelta?

La Enmienda 13 a la Ley de Protección de la Privacidad de Israel sirve actualmente como pilar central en el fortalecimiento de las capacidades de disuasión y aplicación de la PPA. Esto representa un cambio de paradigma: una transición de un modelo "basado en recomendaciones" a un modelo de aplicación administrativa firme, que incluye severas sanciones financieras y la emisión de directrices profesionales vinculantes para los responsables de las bases de datos. En esta era, la PPA no se conforma simplemente con investigar brechas de seguridad; actúa de manera proactiva para garantizar que tanto las organizaciones privadas como las gubernamentales cumplan con los rigurosos estándares de la Ley de Protección de la Privacidad, teniendo la PPA la facultad de imponer multas personales a los ejecutivos de la empresa de hasta ILS 150.000.[2]

Uno de los cambios más significativos introducidos por la Enmienda 13 es el nombramiento obligatorio de un Delegado de Protección de Datos (DPO, por sus siglas en inglés). Este requisito ya no se limita a organismos públicos; ahora se aplica a contratistas que trabajan en su nombre, entidades cuyo negocio principal es el comercio de datos personales, organizaciones dedicadas al monitoreo sistemático del comportamiento humano y entidades que procesan volúmenes significativos de datos sensibles (como datos médicos, biométricos, penales, crediticios o información sobre orientación sexual). El DPO actúa como una función profesional independiente, reportando directamente al CEO y a la Junta Directiva, y está encargado de supervisar la seguridad de los datos de la organización.

Sin embargo, incluso cuando el nombramiento de un DPO no es obligatorio, la Junta Directiva tiene el deber activo de garantizar la seguridad de los datos. Deben aprobar definiciones y procedimientos, evaluar riesgos y verificar la implementación de una política de cumplimiento que incluya mecanismos de control y la notificación inmediata de incidentes de seguridad. Por lo tanto, incluso en ausencia de una obligación legal, se recomienda encarecidamente nombrar un DPO para asegurar el cumplimiento continuo y mitigar la exposición de los directores y funcionarios en caso de una filtración de datos.[3] Ignorar las recomendaciones del DPO o fallar en la supervisión continua (incluyendo la falta de asignación de recursos adecuados) puede percibirse como un incumplimiento del deber de diligencia (*duty of care*). Ya sea durante una auditoría regulatoria o tras una filtración, tales fallos pueden derivar en responsabilidad personal para los directores y funcionarios, independientemente de la responsabilidad corporativa de la empresa.

Un error común de los ejecutivos es ver la privacidad como un "proyecto" temporal en preparación para una auditoría. La Enmienda 13 aclara que la responsabilidad final recae en la Junta Directiva, exponiendo a los funcionarios a fuertes sanciones financieras personales y posibles investigaciones penales. En consecuencia, se aconseja a los funcionarios actuar sin demora para garantizar el pleno cumplimiento y formular procedimientos de seguridad por escrito. Dados los riesgos legales y personales involucrados, es aconsejable no conformarse con un proveedor de DPO externo estándar (especialmente dada la reciente afluencia de proveedores inexpertos que "surgen como hongos" tras la Enmienda 13). En su lugar, las organizaciones deben contratar un despacho de abogados con experiencia específica en protección de la privacidad para proporcionar orientación profesional continua y servicios de DPO externo.

---

* **Osnat Nitay** forma parte del equipo jurídico de Afik & Co. (www.afiklaw.com) , que forma parte de BOKS International (www.boks-international.com). Osnat es licenciada en Derecho por la Facultad de Ciencias Sociales de la Universidad Hebrea de Jerusalén y posee un certificado de mediación familiar del Centro Gevim. Osnat está certificado por el Ministerio de Justicia de Israel para crear poderes notariales duraderos y se graduó de una capacitación del Ministerio de Justicia sobre protección de la privacidad. Esta descripción general no constituye asesoramiento legal y se recomienda consultar a un abogado especializado en este campo antes de tomar cualquier decisión sobre los temas descritos en esta descripción general. Para más detalles: 03-6093609, o por correo electrónico: afiklaw@afiklaw.com

[1] Ver: https://es.afiklaw.com/updates/19581

[2] Ver: Privacidad, DPO y qué hay en la Enmienda/Adi Marcus, Adv., Publicado en Afik Law 445 08.06.2025 - https://es.afiklaw.com/articles/a445

[3] Ver: Cuando un director "entra en estado de Atraf" (se vuelve frenético) debido a una filtración de datos/Osnat Nitay, Adv., Publicado en Afik news 424 16.10.2024 - https://es.afiklaw.com/articles/a424

Quando a conformidade com privacidade se torna um risco pessoal para o Conselho de Administração e para o CEO! / Osnat Nitay, Abg.[*]

O CEO de uma empresa foi surpreendido ao receber uma demanda formal de diagnóstico por parte da Autoridade de Proteção da Privacidade de Israel (PPA, na sigla em inglês).[1] O problema não era o questionário em si, mas o fato alarmante de que a organização nunca havia realizado uma avaliação preliminar de necessidades e riscos, as lacunas nunca haviam sido mapeadas e as retificações tecnológicas e legais exigidas por lei não haviam sido implementadas a tempo. Será sequer possível fechar anos de lacunas e transformar um sistema de dados vulnerado em uma fortaleza de conformidade e privacidade quando a ampulheta da Autoridade já virou?

A Emenda 13 à Lei de Proteção da Privacidade de Israel serve atualmente como pilar central no fortalecimento das capacidades de dissuasão e aplicação da PPA. Isso representa uma mudança de paradigma: uma transição de um modelo "baseado em recomendações" para um modelo de aplicação administrativa firme, que inclui severas sanções financeiras e a emissão de diretrizes profissionais vinculantes para os controladores de bancos de dados. Nesta era, a PPA não se contenta simplesmente em investigar violações de segurança; age de maneira proativa para garantir que tanto as organizações privadas quanto as governamentais cumpram os rigorosos padrões da Lei de Proteção da Privacidade, tendo a PPA o poder de impor multas pessoais aos executivos da empresa de até 150.000 ILS.[2]

Uma das mudanças mais significativas introduzidas pela Emenda 13 é a nomeação obrigatória de um Encarregado de Proteção de Dados (DPO, na sigla em inglês). Este requisito já não se limita a organismos públicos; agora aplica-se a contratados que trabalham em seu nome, entidades cujo negócio principal é o comércio de dados pessoais, organizações dedicadas ao monitoramento sistemático do comportamento humano e entidades que processam volumes significativos de dados sensíveis (como dados médicos, biométricos, penais, de crédito ou informações sobre orientação sexual). O DPO atua como uma função profissional independente, reportando-se diretamente ao CEO e ao Conselho de Administração, e está encarregado de supervisionar a segurança dos dados da organização.

No entanto, mesmo quando a nomeação de um DPO não é obrigatória, o Conselho de Administração tem o dever ativo de garantir a segurança dos dados. Devem aprovar definições e procedimentos, avaliar riscos e verificar a implementação de uma política de conformidade que inclua mecanismos de controle e a notificação imediata de incidentes de segurança. Portanto, mesmo na ausência de uma obrigação legal, recomenda-se fortemente nomear um DPO para assegurar a conformidade contínua e mitigar a exposição dos diretores e executivos em caso de vazamento de dados.[3] Ignorar as recomendações do DPO ou falhar na supervisão contínua (incluindo a falta de alocação de recursos adequados) pode ser percebido como uma violação do dever de diligência (duty of care). Seja durante uma auditoria regulatória ou após um vazamento, tais falhas podem resultar em responsabilidade pessoal para os diretores e executivos, independentemente da responsabilidade corporativa da empresa.

Um erro comum dos executivos é ver a privacidade como um "projeto" temporário em preparação para uma auditoria. A Emenda 13 esclarece que a responsabilidade final recai sobre o Conselho de Administração, expondo os executivos a pesadas sanções financeiras pessoais e possíveis investigações criminais. Consequentemente, aconselha-se aos executivos que ajam sem demora para garantir a conformidade total e formular procedimentos de segurança por escrito. Dados os riscos legais e pessoais envolvidos, é aconselhável não se contentar com um prestador de serviços de DPO externo padrão (especialmente dada a recente afluência de prestadores inexperientes que "surgem como cogumelos" após a Emenda 13). Em vez disso, as organizações devem contratar um escritório de advocacia com experiência específica em proteção da privacidade para fornecer orientação profissional contínua e serviços de DPO externo.

---

[*]**Osnat Nitay** faz parte da equipe jurídica da Afik & Co. (www.afiklaw.com), que faz parte da BOKS International (www.boks-international.com). Osnat possui diploma em Direito pela Faculdade de Ciências Sociais da Universidade Hebraica de Jerusalém e certificado em mediação familiar pelo Centro Gevim. Osnat é certificado pelo Ministério da Justiça de Israel para criar procurações duradouras e formou-se em um treinamento em proteção de privacidade por um Ministério da Justiça. Esta visão geral não constitui aconselhamento jurídico e recomenda-se que você consulte um advogado especializado nesta área antes de tomar qualquer decisão sobre as questões descritas neste resumo. Para mais detalhes: 03-6093609, ou por e-mail: afiklaw@afiklaw.com

[1] Ver: https://pt.afiklaw.com/updates/19582

[2] Ver: Privacidade, DPO e o que há na Emenda/Adi Marcus, Adv., Publicado no Afik Law 445 08.06.2025 - https://pt.afiklaw.com/articles/a445

[3] Ver: Quando um diretor "entra em estado de Atraf" (fica frenético) devido a um vazamento de dados/Osnat Nitay, Adv., Publicado en Afik news 424 16.10.2024 - https://pt.afiklaw.com/articles/a424

Quand la conformité en matière de vie privée devient un risque personnel pour le Conseil d'Administration et le PDG ! / Osnat Nitay, Abg.*

Le PDG d'une entreprise a été surpris de recevoir une demande formelle de diagnostic de la part de l'Autorité israélienne de protection de la vie privée (PPA, pour son acronyme anglais).[1] Le problème n'était pas le questionnaire en soi, mais le fait alarmant que l'organisation n'avait jamais réalisé d'évaluation préliminaire des besoins et des risques, que les lacunes n'avaient jamais été cartographiées et que les rectifications technologiques et juridiques requises par la loi n'avaient pas été mises en œuvre à temps. Est-il même possible de combler des années de lacunes et de transformer un système de données vulnérable en une forteresse de conformité et de confidentialité alors que le sablier de l'Autorité s'est déjà retourné ?

L'Amendement 13 de la Loi israélienne sur la protection de la vie privée sert actuellement de pilier central dans le renforcement des capacités de dissuasion et d'application de la PPA. Cela représente un changement de paradigme : une transition d'un modèle « basé sur des recommandations » vers un modèle d'application administrative ferme, qui inclut de sévères sanctions financières et l'émission de directives professionnelles contraignantes pour les responsables de bases de données. À notre époque, la PPA ne se contente pas simplement d'enquêter sur les failles de sécurité ; elle agit de manière proactive pour garantir que tant les organisations privées que gouvernementales respectent les normes rigoureuses de la Loi sur la protection de la vie privée, la PPA ayant le pouvoir d'imposer des amendes personnelles aux dirigeants de l'entreprise pouvant aller jusqu'à 150 000 ILS.[2]

L'un des changements les plus significatifs introduits par l'Amendement 13 est la nomination obligatoire d'un Délégué à la Protection des Données (DPO). Cette exigence ne se limite plus aux organismes publics ; elle s'applique désormais aux sous-traitants travaillant pour leur compte, aux entités dont l'activité principale est le commerce de données personnelles, aux organisations dédiées à la surveillance systématique du comportement humain et aux entités traitant des volumes significatifs de données sensibles (telles que des données médicales, biométriques, pénales, de crédit ou des informations sur l'orientation sexuelle). Le DPO agit en tant que fonction professionnelle indépendante, rendant compte directement au PDG et au Conseil d'Administration, et est chargé de superviser la sécurité des données de l'organisation.

Cependant, même lorsque la nomination d'un DPO n'est pas obligatoire, le Conseil d'Administration a un devoir actif de garantir la sécurité des données. Ils doivent approuver les définitions et procédures, évaluer les risques et vérifier la mise en œuvre d'une politique de conformité incluant des mécanismes de contrôle et le signalement immédiat d'incidents de sécurité. Par conséquent, même en l'absence d'obligation légale, il est fortement recommandé de nommer un DPO pour assurer une conformité continue et atténuer l'exposition des administrateurs et dirigeants en cas de fuite de données.[3] Ignorer les recommandations du DPO ou manquer à la supervision continue (y compris l'absence d'allocation de ressources adéquates) peut être perçu comme une violation du devoir de diligence (*duty of care*). Que ce soit lors d'un audit réglementaire ou après une fuite, de tels manquements peuvent entraîner une responsabilité personnelle pour les administrateurs et dirigeants, indépendamment de la responsabilité corporative de l'entreprise.

Une erreur courante des dirigeants est de considérer la vie privée comme un « projet » temporaire en préparation d'un audit. L'Amendement 13 précise que la responsabilité finale incombe au Conseil d'Administration, exposant les dirigeants à de lourdes sanctions financières personnelles et à d'éventuelles enquêtes criminelles. Par conséquent, il est conseillé aux dirigeants d'agir sans délai pour garantir une conformité totale et formuler des procédures de sécurité par écrit. Compte tenu des risques juridiques et personnels impliqués, il est conseillé de ne pas se contenter d'un fournisseur de services DPO externe standard (surtout compte tenu de l'afflux récent de prestataires inexpérimentés qui « poussent comme des champignons » après l'Amendement 13). Au lieu de cela, les organisations devraient engager un cabinet d'avocats disposant d'une expertise spécifique en protection de la vie privée pour fournir une orientation professionnelle continue et des services de DPO externes.

---

*__Osnat Nitay__ fait partie de l'équipe juridique d'Afik & Co. (www.afiklaw.com), qui fait partie de BOKS International (www.boks-international.com). Osnat est titulaire d'un diplôme de droit de la Faculté des sciences sociales de l'Université hébraïque de Jérusalem et d'un certificat en médiation familiale du Centre Gevim. Osnat est certifié par le ministère israélien de la Justice pour créer des procurations durables et a obtenu une formation en protection de la vie privée dispensée par un ministère de la Justice. Ce résumé ne constitue pas un conseil juridique et il est recommandé de consulter un avocat spécialisé dans ce domaine avant de prendre toute décision sur les questions exposées dans ce résumé. Pour plus de détails : 03-6093609, ou par email : afiklaw@afiklaw.com

[1] Ver: https://fr.afiklaw.com/updates/19580

[2] Ver: Vie privée, DPO et ce que contient l'Amendement/Adi Marcus, Adv., Publicado no Afik Law 445 08.06.2025 - https://fr.afiklaw.com/articles/a445

[3] Ver: Quand un directeur « entre en état d'Atraf » (devient frénétique) à cause d'une fuite de données/Osnat Nitay, Adv., Publicado en Afik news 424 16.10.2024 - https://fr.afiklaw.com/articles/a424