אפיק ושות' עורכי דין ונוטריון
AFIK & CO. ATTORNEYS & NOTARY

גיליון 459: 04 מרץ, 2026
Issue 459: March 04, 2026

הגיליון המקצועי הדו שבועי של אפיק ושות', עורכי דין ונוטריון
The Bi-Weekly Professional Magazine of Afik & Co, Attorneys and Notary

החשמונאים 103, ת.ד. 20144 תל אביב-יפו 6120101, טלפון 03-609.3.609 פקס 03-609.5.609
103 Ha'Hashmonaim St., POB 20144, Tel Aviv 6120101, Israel, Telephone: +972-3-609.3.609

אפיק ושות' מציינת את יום פטירתו של מעצב המשחקים האמריקני ארנסט גֶארי גֶייגֶקס (27 יולי, 1938 - 04 מרץ, 2008) אשר יחד עם דייב ארנסון יצר בשנת 1974 את משחק התפקידים פורץ הדרך "מבוכים ודרקונים" (D&D).

Afik & Co. commemorates the date of demise of American game designer Ernest Gary Gygax (July 27, 1938 - March 4, 2008), who, together with Dave Arneson, created the groundbreaking role-playing game "Dungeons & Dragons" (D&D) in 1974.

1. ניס1 ניס2 – ניס הוא? / עו"ד עדי מרכוס, מר גבריאל מרקוס

NIS1 NIS2 – NIS who? / Adi Marcus, Adv., Mr. Gabriel Marcus

מאמר בנושא התקינה האירופאית העוסקת ברגולציית עולם הסייבר והחשיבות בהקפדה עליה כדי למנוע אחריות אישית לדירקטורים ונושאי משרה בחברה, גם אם החברה אינה אירופאית. את המאמר כתבו עו"ד עדי מרכוס ממשרד אפיק ומר גבריאל מרקוס, ארכיטקט סייבר בכיר, המייעץ לחברות בתחום הסייבר ופועל בשיתוף פעולה עם משרד אפיק ושות' לביצועי סקרי סיכוני סייבר וטיפול בבעיות בנושא. את המאמר בשפה העברית ניתן למצוא בקישור: http://he.afiklaw.com/articles/a460

An article on European standardization concerning cybersecurity regulation and the importance of adhering to it to prevent personal liability for directors and corporate officers, even if the company is not European. The article was written by Adv. Adi Marcus from the Afik Law Firm and Mr. Gabriel Marcus, a senior cyber architect, who advises companies in the cyber sector and collaborates with Afik & Co. to conduct cyber risk assessments and handle related issues. The article in English may be found at the link: https://www.afiklaw.com/articles/a460

2. עדכוני פסיקה

Legal Updates

א. החלטות דירקטוריון שנתקבלו בהעדר קורום ולא זכו אף בדיעבד לתמיכה של הקורום בטלות מלכתחילה

מחוזי מרכז-לוד: בניגוד להחלטות שמתקבלות בישיבות דירקטוריון שחלו פגמים אחרים בכינוסן, במקרה של העדר קורום ואי קבלת הסכמת הנעדרים בדיעבד, ההחלטות חסרות תוקף מלכתחילה. לקריאה נוספת: https://www.afiklaw.com/updates/19874

Board of Directors' resolutions adopted in the absence of a quorum, which did not receive ex post facto support from the quorum, are void ab initio. Read more at: https://www.afiklaw.com/updates/19875

ב. התבטלותו של חוזה מחמת אי-קיום תנאי מתלה איננה מפקיעה את כלל חיוביו

מחוזי תל אביב-יפו: חיובים ראשוניים בחוזה נועדו להגשים את עסקת היסוד, בעוד חיובים משניים מסדירים את היחסים המשפטיים במקרה שהשגת תכלית העסקה כשלה או הסתיימה. לקריאה נוספת: http://he.afiklaw.com/updates/19876

The termination of a contract due to the failure of a condition precedent does not extinguish all of its obligations. Read more at: https://www.afiklaw.com/updates/19878

ג. שינוי חוזה בהתנהגות מחייב גמירות דעת מלאה של הצדדים לשינוי זה

העליון: ניתן לשנות הסכם כתוב בדרך של התנהגות מאוחרת לכריתתו ובלבד שההתנהגות משקפת גמירות דעת ברורה ומפורשת לסטייה זו. קרי, רצון מגובש, כוונה רצינית לשינוי החוזה הקיים והחלטיות. לקריאה נוספת: https://he.afiklaw.com/updates/19879

An alteration of contract by conduct requires the parties' full intent to be bound by this change. Read more at: https://www.afiklaw.com/updates/19880

ד. סירוב לקוח למסירת מידע לפי חוק איסור הלבנת הון מהווה בסיס לסירוב מתן שירות בנקאי

מחוזי מרכז-לוד: הכרת הלקוח על ידי תאגיד בנקאי כוללת את בירור מקור הנכסים הפיננסיים לגביהם ניתנים השירותים וחל איסור על תאגיד בנקאי לתת שירות פיננסי ללקוח אם לא בוצע הליך הכרת הלקוח. לקריאה נוספת: https://he.afiklaw.com/updates/19881

A client's refusal to provide information under the Anti-Money Laundering Law constitutes a basis for the refusal of banking services. Read more at: https://www.afiklaw.com/updates/19882

ה. הסתרת היריון בשימוע וחשיפתו רק לאחר מכן שוללת פיצוי בגין פיטורים במהלך היריון

אזורי לעבודה ב"ש: חוק עבודת נשים אינו חל במקרה של הסתרה מכוונת של ההיריון מהמעסיק טרם החלטת הפיטורים. לקריאה נוספת: https://he.afiklaw.com/updates/19883

Concealing pregnancy during a hearing and revealing it only subsequently negates compensation for dismissal during pregnancy. Read more at: https://www.afiklaw.com/updates/19884

ו. העברת בורר מתפקידו תיעשה רק כאשר הוכח משוא פנים ולא על סמך אמירות שהוצאו מהקשרן

השלום פ"ת: העברת בורר מתפקידו תיעשה במקרים חריגים בלבד שבהם הוכחה תשתית עובדתית מוצקה לקיומו של חשש ממשי למשוא פנים, ולא על סמך תחושות סובייקטיביות או אמירות שנותקו מהקשרן. לקריאה נוספת: https://he.afiklaw.com/updates/19785

The removal of an arbitrator shall be granted only when bias is proven and not on the basis of statements taken out of context. Read more at: https://www.afiklaw.com/updates/19786

1. ניס1 ניס2 – ניס הוא? / עו"ד עדי מרכוס, מר גבריאל מרקוס

NIS1 NIS2 – NIS who? / Adi Marcus, Adv., Mr. Gabriel Marcus

מאמר בנושא התקינה האירופאית העוסקת ברגולציית עולם הסייבר והחשיבות בהקפדה עליה כדי למנוע אחריות אישית לדירקטורים ונושאי משרה בחברה, גם אם החברה אינה אירופאית. את המאמר כתבו עו"ד עדי מרכוס ממשרד אפיק ומר גבריאל מרקוס. עו"ד עדי מרכוס הינה עורכת דין במשרד אפיק ושות' (he.afiklaw.com), שהינו חלק מרשת המשרדים (boks-international.com) BOKS International ומתמקדת במשפט מסחרי ודיני חברות, זכויות יוצרים, דיני תקשורת ואומנים ועסקאות בינלאומיות. עו"ד מרכוס הינה בוגרת הפקולטה למשפטים ובעלת תואר שני בתקשורת באוניברסיטת תל אביב ותואר שני במנהל עסקים בינלאומי מאוניברסיטת בר אילן. היא התמחתה במשרד המשפטי אצל המשנה ליועץ המשפטי לממשלה בתחום הדין האזרחי וזכויות היוצרים, לאחר מכן עבדה כ18 חודש במשרד שלמה כהן בתחום הקניין הרוחני, כ-11 שנה במחלקה המשפטית בגוף התקשורת "רשת נגה בע"מ"(ערוץ 2 של הטלוויזיה), כאשר תפקידה האחרון בטרם מיזוג החברה עם ערוץ 10, כראש תחום במחלקה המשפטית ולאחר כן, טרם הצטרפותה למשרד, כיועצת המשפטית הפנימית של קנלר ייצוג אמנים, בכל נושא היעוץ המשפט של אמנים ואנשי תרבות, בין בישראל ובין במישור הבינלאומי. מר גבריאל מרקוס הינו ארכיטקט סייבר בכיר, המייעץ לחברות בתחום הסייבר ופועל בשיתוף פעולה עם משרד אפיק ושות' לביצועי סקרי סיכוני סייבר וטיפול בבעיות בנושא. את המאמר ניתן למצוא בקישור: http://he.afiklaw.com/articles/a460

An article on European standardization concerning cybersecurity regulation and the importance of adhering to it to prevent personal liability for directors and corporate officers, even if the company is not European. The article was written by Adv. Adi Marcus from the Afik Law Firm and Mr. Gabriel Marcus. Adi Marcus, Adv. is an attorney in the office of Afik & Co. (www.afiklaw.com), which is part of BOKS International (boks-international.com) and who focuses primarily on commercial and corporate law, copyrights, media law and international transactions. Advocate Marcus holds a major in law, an M.A in communication from Tel Aviv University and an international MBA from Bar Ilan University. She completed her internship at the Ministry of justice under the Deputy Attorney General focusing civil law and copyright law, then worked for about 18 months in the office of Shlomo Cohen in the field of intellectual property, about 11 years in the legal department of the communications network "Noga Network" (Channel 2 of TV), with her last position before the company merged with Channel 10, was head of department in the legal department and then, before joining the firm, as Kneller Artists Representation's internal legal advisor, representing in all matters of legal advice to artists and cultural figures, both in Israel and internationally. Mr. Gabriel Marcus is a senior cyber architect who advises companies in the cyber field and works in collaboration with Afik & Co. to perform cyber risk surveys and address issues related to the subject. The article in English may be found at the link:`https://www.afiklaw.com/articles/a460

2. עדכוני פסיקה

Legal Updates

א. החלטות דירקטוריון שנתקבלו בהעדר קוורום ולא זכו אף בדיעבד לתמיכה של הקוורום בטלות מלכתחילה

ת"א 42064-01-25 קיבוץ בוכריץ בע"מ נ' ת. יצחק בנייה ויזמות בע"מ, 23.02.2026, בית המשפט המחוזי מרכז-לוד, כב' השופט אבי סתיו

חברה הגישה תביעה מכח ההחלטה שהתקבלה בישיבת דירקטוריון שנערכה בהעדר מניין חוקי ואף ללא קבלת הסכמת הדירקטור שנעדר מהישיבה להחלטה זו.

בית המשפט דחה את התביעה על הסף בשל בטלות החלטת הדירקטוריון. בניגוד להחלטות שמתקבלות בישיבות דירקטוריון שחלו פגמים אחרים בכינוסן, הניתנות לביטול, הרי שבמקרה של העדר קוורום ואי קבלת הסכמת הנעדרים לאחר מכן, מדובר בהחלטה שאינה ניתנת לביטול, כי אם חסרת תוקף מלכתחילה בבחינת לא נעשה דבר (Non est factum). כאן, מדובר בדירקטוריון עם שני חברים בלבד כאשר אחד מהם נעדר מהישיבה ולא הביע כל הסכמה להחלטה שהתקבלה. משכך, ההחלטה על הגשת התביעה בטלה מלכתחילה, החברה אינה רשאית להגיש את התביעה והיא נדחית על הסף.

Board of Directors' resolutions adopted in the absence of a quorum, which did not receive ex post facto support from the quorum, are void ab initio

A company filed a lawsuit by virtue of a resolution adopted at a board meeting held in the absence of a legal quorum, and without obtaining the consent of the absent director to said resolution.

The Court summarily dismissed the claim due to the board resolution's nullity. In contrast to resolutions adopted at board meetings involving other procedural defects in their convening, which are voidable, in a case of a lack of quorum and the subsequent failure to obtain the absentees' consent, the resolution is not merely voidable but void ab initio, as if "no act was done" (Non est factum). Here, the board consisted of only two members, one of whom was absent and provided no retroactive consent to the resolution. Hence, the resolution to file the lawsuit was void from the outset; the company was not authorized to initiate the proceedings, and the claim was dismissed summarily.

ב. התבטלותו של חוזה מחמת אי-קיום תנאי מתלה איננה מפקיעה את כלל חיוביו

חדלת 21631-10-25 גלובל אוטו מקס בע"מ נ' הממונה על הליכי חדלות פירעון ושיקום כלכלי, 18.02.2026, בית המשפט המחוזי בתל־אביב-יפו, כב' השופט הבכיר חגי ברנר

לאחר כניסת חברה להליכי חדלות הפירעון, הודיע צד שני להסכם על ביטולו בשל אי-קיום תנאי מתלה והחל לפעול ישירות מול יצרן בחו"ל למרות הוראות בהסכם הקובעות אי תחרות.

בית המשפט קבע שההסכם פקע אולם סעיף אי התחרות נשאר בתוקף. תנאי מתלה הוא אירוע חיצוני שרק בהתקיימותו נכנסים חיובי החוזה לתוקף, ואם אינו מתקיים במועד החוזה מתבטל. חיובים ראשוניים בחוזה נועדו להגשים את עסקת היסוד, בעוד חיובים משניים מסדירים את היחסים המשפטיים במקרה שהשגת תכלית העסקה כשלה או הסתיימה. בעוד שביטול חוזה מבטל חיובים ראשוניים, חיובים משניים כמו תניות אי תחרות ובוררות נותרים בתוקפם. בענייננו, ההסכם אמנם בוטל עקב אי-קיום התנאי המתלה במועד, אך הצד השני פעל כדי לזכות בזיכיונות תוך עקיפת הצד הראשון. תניית אי-התחרות הוגדרה כ"חיוב משני" השורד את ביטול ההסכם למשך חמש שנים ונותרת למרות ביטול ההסכם ולכן ניתן צו מניעה האוסר על פנייה עצמאית ליצרן.

The termination of a contract due to the failure of a condition precedent does not extinguish all of its obligations

Following entry of a company into insolvency proceedings, a transaction counterparty announced the termination of the agreement due to the non-fulfillment of a condition precedent and began dealing directly with a foreign manufacturer despite contract terms stipulating non-compete.

The Court held that the contract expired but the non-compete provision is valid. A condition precedent is an external event which occurrence is a prerequisite for the contractual obligations to take effect; should it fail to occur by the stipulated date, the contract is terminated. Primary obligations are intended to realize the fundamental transaction, whereas secondary obligations regulate the legal relationship in the event that the transaction's purpose fails or concludes. While the termination of a contract dissolves primary obligations, secondary obligations such as non-compete and arbitration clauses survive. In this case, although the agreement was terminated due to the non-fulfillment of the condition precedent on time, the counterparty acted to secure franchises while bypassing the first party. The non-compete clause was classified as a "secondary obligation" that survives the agreement's termination for a period of five years. Consequently, an injunction was issued, prohibiting independent contact with the manufacturer.

ג. שינוי חוזה בהתנהגות מחייב גמירות דעת מלאה של הצדדים לשינוי זה

בעמ 57929-12-24 פלונית נ' פלוני, 29.01.2026, בית המשפט העליון בשבתו כבית משפט לערעורים אזרחיים, כב' השופטים דפנה ברק-ארז, גילה כנפי-שטייניץ ויחיאל כשר

בני זוג החליטו להשתתף בהליך הפריה חוץ גופית במהלכו נוצרו והוקפאו עוברים משותפים. קודם לתחילת ההליך חתמו בני הזוג על הסכם המחייב הסכמה משותפת בכל שלב בהליך עד להחזרת העוברים לרחם. אלא שלפני השבת העוברים, סירב בן הזוג להחזרתם וזאת על אף שבמהלך כל ההליך הביע תמיכה בהחזרתם.

בית המשפט קבע כי אין די בהתנהגותו של בן הזוג במהלך ההליך, בכדי לשנות את החוזה. אמנם הדין מכיר באפשרות לשינוי הסכם כתוב בדרך של התנהגות מאוחרת לכריתתו ובלבד והתנהגות זו משקפת גמירות דעת ברורה ומפורשת לסטייה זו. קרי, רצון מגובש, כוונה רצינית לשינוי החוזה הקיים והחלטיות. כאן, מדובר במקרה בו בן הזוג הביע תמיכה בהליך ועודד את בת זוגו, אך בשום שלב לא ויתר באופן מפורש על התניה בהסכם הדורשת הסכמה נמשכת לשימוש בביציות המופרות ומשכך, לא ניתן לטעון כי החוזה שונה בהתנהגות.

An alteration of contract by conduct requires the parties' full intent to be bound by this change

A couple decided to undergo an In Vitro Fertilization (IVF) procedure, during which joint embryos were created and frozen. Prior to commencing the procedure, the couple signed an agreement requiring mutual consent at every stage of the process up to the transfer of the embryos into the uterus. However, before the transfer of the embryos, the male partner refused to consent to the embryos transfer, despite having expressed support for the transfer throughout the entire process.

The Supreme Court held that the male partner's conduct during the procedure was insufficient to alter the contract. While the law recognizes the possibility of modifying a written agreement through subsequent conduct, such conduct must reflect a clear and explicit intent to be bound by this deviation. That is, it requires a definitive will, a genuine intention to change the existing contract, and decisiveness. In this case, although the male partner expressed support for the procedure and encouraged his partner, at no point did he explicitly waive the contractual provision requiring continuous consent for the use of the fertilized eggs. Hence, it cannot be argued that the contract was amended by conduct.

ד. סירוב לקוח למסירת מידע לפי חוק איסור הלבנת הון מהווה בסיס לסירוב מתן שירות בנקאי

תא 23921-09-21 שי-לי אבנבך נ' בנק לאומי לישראל בע"מ, 13.01.2026, בית המשפט המחוזי מרכז-לוד, כב' השופט אלי ברנד

בנק סירב לפתוח חשבון ליורשת לצורך העברה לישראל של כספי ירושה מחשבון חברה פנמית בסינגפור מאחר שלא הוצגו בפניו אסמכתאות למקור הכספים או לזיקת המנוח לחברה הזרה בעלת החשבון ובשל היות היורשת בעלת עבר פלילי הכולל, בין השאר, הרשעות בעבירות מס חמורות.

בית המשפט קבע, כי החלטת הבנק הייתה סבירה ונדרשת בהתאם לחוק איסור הלבנת ההון. בהתאם לחקיקה, חובת "הכרת הלקוח" מחייבת בנקים לברר את מקור הנכסים ואוסרת מתן שירות ללא השלמת הליך זה, במיוחד בפעילות חוצת גבולות המוגדרת בסיכון גבוה. סירוב לפתיחת חשבון נחשב "סביר" ככל שהלקוח אינו מספק פרטים נדרשים או נמנע משיתוף פעולה לצורך יישום מדיניות ניהול הסיכונים של התאגיד הבנקאי. במקרה זה, היורשת בעלת עבר פלילי בעבירות מס, לא הצביעה על מקור הכסף ועל זיקת המנוח לחברה הפנמית, מצב המהווה "דגל אדום" המצדיק סירוב. אי-אספקת מידע על מקור הכסף ועל זהות בעלי החברה, ללא הוכחת ניסיון להשיגו, הצדיקה את סירוב הבנק לפתוח חשבון ליורשת ולכן החלטת הבנק שלא לפתוח חשבון הייתה סבירה.

A client's refusal to provide information under the Anti-Money Laundering Law constitutes a basis for the refusal of banking services

A bank refused to open an account for an heir seeking to transfer to Israel inheritance funds from a Panamanian company's account in Singapore. This refusal was issued as no documentation was provided to verify the source of the funds or the connection between the deceased and the foreign company that owned the account. Furthermore, the refusal was based on the heir's criminal record, which included convictions for serious tax offenses.

The Court held that the bank's decision was reasonable and necessary in accordance with the Israeli Prohibition of Money Laundering Law. Pursuant to legislation, the "Know Your Customer" obligation requires banks to verify the source of assets and prohibits providing service without completing this process, especially in cross-border activities defined as high-risk. Refusal to open an account is considered "reasonable" if the customer fails to provide required details or refrains from cooperating for the purpose of implementing the banking corporation's risk management policies. In this case, the heir, who has a criminal record for tax offenses, failed to substantiate the source of funds or the connection of the deceased to the Panamanian company, a situation that constitutes a "red flag" justifying the refusal. The failure to provide information regarding the source of the money and the identity of the company's owners, without proof of an attempt to obtain it, justified the bank's refusal to open an account for the heir and thus the bank's refusal to open the account was reasonable.

ה. הסתרת היריון בשימוע וחשיפתו רק לאחר מכן שוללת פיצוי בגין פיטורים במהלך היריון

סע"ש (ב"ש) 47968-07-24 נויה דמרי נ' עו"ד ג'אמיל מטאלקה, 10.02.2026, בית הדין האזורי לעבודה בבאר שבע, כב' השופטת אביגיל בורוביץ', נציג ציבור (עובדים) מר חאלד אבו עג'אג' ונציגת ציבור (מעסיקים) גב' עינב מורדוך

עובדת דרשה פיצויים מהמעסיק שפיטר אותה כשהיא בהיריון. המעסיק פיטר אותה מסיבות מקצועיות וקשיים כלכליים בתקופת המלחמה. העובדת גילתה למעסיק שהיא בהיריון רק יום אחרי השימוע ולא הציגה הוכחה לכך.

בית הדין קבע שהעובדת פוטרה כדין. ככלל, חוק עבודת נשים אוסר על פיטורי עובדת בהיריון ללא היתר. עם זאת, החוק דורש התנהלות בתום לב מצד העובדת. אין די באמירה בעל פה כי היא בהיריון כדי להקים חובה אוטומטית למעסיק, ועליה להציג אישור רפואי. מעסיק אינו יכול להיחשב כמי שפעל בניגוד לחוק אם במועד קבלת החלטת הפיטורים כלל לא ידע על ההיריון בשל הסתרתו המכוונת על ידי העובדת. כאן, העובדת נהגה בחוסר תום לב. היא ידעה שהיא בהיריון טרם השימוע, אך בחרה לשתוק במהלך שיחת השימוע. רק למחרת, לאחר שהבינה שהיא מפוטרת, הודיעה למעסיק על ההיריון במטרה לסכל את הפיטורים, ואף לא טרחה להציג אישור רפואי. לפיכך, העובדת פוטרה כדין ואינה זכאית לפיצוי.

Concealing pregnancy during a hearing and revealing it only subsequently negates compensation for dismissal during pregnancy

An employee demanded compensation from the employer who dismissed her while she was pregnant. The employer dismissed her for professional reasons and economic difficulties during the war period. The employee revealed to the employer that she is pregnant only a day after the hearing and did not present proof thereof.

The Labor Court found that the employee was duly dismissed. Generally, the Israeli Employment of Women Law prohibits the dismissal of a pregnant employee without a permit. However, the law requires conduct in good faith on the part of the employee. A verbal statement that a woman is pregnant is not sufficient to establish an automatic obligation on the employer and she must present a medical certificate. An employer cannot be considered as one who acted contrary to the law if, at the time of making the dismissal decision, it did not know about the pregnancy at all due to its intentional concealment by the employee. Here, the employee acted in bad faith. She knew she was pregnant prior to the hearing, but chose to remain silent during the hearing. Only the next day, upon realizing she was being dismissed, did she inform the employer of the pregnancy with the aim of thwarting the dismissal, and did not even bother to present a medical certificate. Therefore, the employee was duly dismissed and is not entitled to compensation.

ו. העברת בורר מתפקידו תיעשה רק כאשר הוכח משוא פנים ולא על סמך אמירות שהוצאו מהקשרן

ת"א 38258-01-25 ד. ניב בניה ופיתוח בע"מ נ' הבונים ע.מ, 21.01.2026, בית משפט השלום בפתח תקווה, כב' השופטת זהבית אלדר

צד לבוררות הגיש בקשה להעברת בורר (מהנדס בניין) מתפקידו לאחר ארבע שנות דיונים, בטענה למשוא פנים שהתבטא בין היתר באמירות מזלזלות.

בית המשפט דחה את הבקשה וקבע כי לא נמצאה עילה להעברת הבורר מתפקידו בשל היעדר הוכחה לחשש ממשי למשוא פנים. לפי חוק הבוררות בית המשפט רשאי להעביר בורר מתפקידו אם נתגלה שאינו ראוי לאמון הצדדים, כאשר המבחן המיושם הוא אובייקטיבי בדומה למבחן פסלות שופט. יש לגלות זהירות יתרה בבקשות המוגשות בשיהוי ניכר, במיוחד בשלב בו הסתיימו הדיונים והבוררות הגיעה לשלב הגשת הסיכומים. במקרה זה, נעשה ניסיון להיתלות באמירות שנאמרו על ידי הבורר (כגון: "הייתי חוסך את התיק הדפוק הזה") בניסיון להשתלט על אווירה טעונה ודיונים קולניים בין הצדדים, אשר צוטטו במנותק מהקשרן הדינמי. הבורר פעל לקידום הליך יעיל ורציף והטענות שהועלו בדיעבד היו נגועות בשיהוי מהותי ומשכך, הבקשה נדחתה.

The removal of an arbitrator shall be granted only when bias is proven and not on the basis of statements taken out of context

A party to an arbitration filed a motion to remove the arbitrator (a civil engineer) after four years of proceedings, alleging bias expressed, *inter alia*, through disparaging remarks.

The Court rejected the motion and held that no grounds for the arbitrator's removal were found due to lack of evidence of a real concern of bias. According to the Israeli Arbitration Law, the Court may remove an arbitrator from office if it is discovered that it is unworthy of the parties' trust, applying an objective test similar to the disqualification of a judge. Extreme caution must be exercised regarding applications filed with significant delay, particularly at a stage where hearings have concluded and the arbitration has reached the summary submission phase. In this case, an attempt was made to rely on statements made by the arbitrator (such as: "I would have saved this messed up case") in an effort to control a charged atmosphere and loud discussions between the parties, which were quoted out of their dynamic context. The arbitrator acted to promote an efficient and continuous process and the claims raised retrospectively were tainted by substantial delay. Therefore, the motion was rejected.

ניס1 ניס2 – ניס הואז? / עו"ד עדי מרכוס, מר גבריאל מרקוס*

בעולם העסקי של 2026, אבטחת מידע אינה עוד סוגיה טכנית המצויה באחריותם הבלעדית של אנשי הפיתוח והמחשוב. עם כניסתם לתוקף של התיקונים האחרונים לדירקטיבת NIS2 באירופה ופרסומו של תזכיר חוק הגנת הסייבר הלאומי (התשפ"ו-2026)[1] בישראל, האחריות המשפטית על אירועי סייבר עברה מחדר השרתים ישירות לשולחן הדירקטוריון.

בעשור האחרון עברה רגולציית הסייבר העולמית תהליך התבגרות מואץ. עבור חברות ישראליות הפועלות בזירה הבינלאומית, הבנת ציר הזמן הרגולטורי אינה עוד שאלה של "ציות טכני", אלא תנאי סף לשרידות עסקית ומשפטית. ראשיתו של התהליך בשנת 2016, עם אימוץ דירקטיבת NIS1[2]. דירקטיבה זו התמקדה ב"מפעילי שירותים חיוניים" (תשתיות לאומיות) והייתה וולונטרית במידה רבה עבור המגזר העסקי הרחב. ואולם, המפנה הדרמטי התרחש בשנת 2024 עם כניסתה לתוקף של דירקטיבת NIS2[3] שהרחיבה את תחולת הרגולציה ל-18 מגזרים שונים ובהם ייצור, מזון, ניהול פסולת ושירותים דיגיטליים, הטילה חובות דיווח נוקשות וקבעה כי הנהלת החברה נושאת באחריות ישירה לאימוץ אמצעי הגנה הולמים. למרות היותה חקיקה אירופית, השפעתה על המשק הישראלי קריטית: כל חברה ישראלית המספקת שירותים לאיחוד, פועלת בתחומיו או מהווה חוליה בשרשרת האספקה של גוף אירופי, מחויבת לעמוד בסטנדרטים אלו.

בינואר 2026, הכניס האיחוד האירופי שינויים משמעותיים ("חבילת הסייבר 2026"[4]) שנועדו להתמודד עם סיכונים גיאופוליטיים ומתקפות כופר. במקביל, בישראל, תזכיר חוק הגנת הסייבר משנת 2026 מטיל חובות דומות על גופים המוגדרים כ"ספקי שירותים דיגיטליים" ו"תשתיות חיוניות" ומבקש לחייב חברות לבצע בדיקת נאותות סייבר (Cyber Due Diligence) לכל ספק בשרשרת האספקה שלהן. ככל שחברה פועלת כספקית תוכנה או IT, סביר כי לקוחותיה ידרשו הוכחות לעמידה בתקני NIS2 כתנאי להתקשרות חוזית.

הרגולציה העדכנית דורשת גם דיווח בתוך 24 שעות על כל אירוע סייבר משמעותי, לרבות פירוט על תקיפות כופר, תוך חשיפה נרחבת של פעילות החברה בזמן משבר. מעבר לכך, לא ניתן עוד להאציל את האחריות באופן בלעדי למנהל אבטחת המידע (CISO) והמנהלים הבכירים מחויבים כעת לעבור הכשרות סייבר ולאשר באופן מפורש את תוכניות ההגנה הארגוניות. במידה ויתרחש אירוע סייבר ויימצא כי החברה לא השקיעה את המשאבים הנדרשים המשמעות עשוי להיות עיצומים כספיים אישיים על חברי הדירקטוריון והמנהלים, ואף השעיה מתפקידם. תזכיר החוק הישראלי אף הרחיב את היריעה: חברות פיתוח תוכנה, אחסון ענן וניהול מערכות IT המעסיקות מעל 50 עובדים או בעלות מחזור הגבוה מ-40 מיליון ש"ח, יסווגו כ"ארגון חיוני" הכפוף לפיקוח ישיר של מערך הסייבר ולאכיפה מחמירה.

כך, בעידן הרגולטורי של 2026 אבטחת סייבר חדלה מלהיות סוגיה טכנולוגית גרידא והפכה לאירוע ליבה של ניהול סיכונים משפטיים, שבו ייעוץ משפטי מומחה בשילוב עם ייעוץ סייבר מהווה את קו ההגנה הראשון של הארגון[5]. מעבר לצורך האקוטי בליווי משפטי צמוד שיאפשר בניית "חומות הגנה" סביב הדירקטוריון ונושאי המשרה וימנע חשיפה לתביעות ואחריות אישית, חשוב להיערך מראש עם בדיקת נאותות סייבר של הארגון. בסופו של יום, השילוב בין מומחיות טכנולוגית להבנה משפטית מעמיקה הוא הדרך היחידה להקנות לארגון חזקת תקינות משפטית ולספק שקט נפשי למנהלים אל מול הרגולטור והשוק הגלובלי כאחד. יתרה מכך, חברה שלא תעשה זאת עלולה לגלות שאינה יכולה לעבוד מול חברות אירופאיות.

---

* **עו"ד עדי מרכוס** הינה עורכת דין במשרד אפיק ושות' (www.afiklaw.com), שהינו חלק מרשת המשרדים BOKS International (www.boks-international.com) ומתמקדת במשפט מסחרי ודיני חברות, זכויות יוצרים, דיני תקשורת ואומנים ועסקאות בינלאומיות. עו"ד מרכוס הינה בוגרת הפקולטה למשפטים ובעלת תואר שני בתקשורת באוניברסיטת תל אביב ותואר שני במנהל עסקים בינלאומי מאוניברסיטת בר אילן. היא התמחתה במשרד המשפטית אצל המשנה ליועץ המשפטי לממשלה בתחום הדין האזרחי וזכויות היוצרים, לאחר מכן עבדה כ18 חודש במשרד שלמה כהן בתחום הקניין הרוחני, כ-11 שנה במחלקה המשפטית בגוף התקשורת "רשת נגה בע"מ"(ערוץ 2 של הטלוויזיה), כאשר תפקידה האחרון בטרם מיזוג החברה עם ערוץ 10, כראש תחום במחלקה המשפטית ולאחר כן, טרם הצטרפותה למשרד, כיועצת המשפטית הפנימית של קנלר ייצוג אמנים, בכל נושא היעוץ המשפט של אמנים ואנשי תרבות, בין בישראל ובין במישור הבינלאומי. **מר גבריאל מרקוס** הינו ארכיטקט סייבר בכיר, המייעץ לחברות בתחום הסייבר ופועל בשיתוף פעולה עם משרד אפיק ושות' לביצועי סקרי סיכוני סייבר וטיפול בבעיות בנושא. 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] תזכיר חוק הגנת הסייבר הלאומית, התשפ"ו-2026. פורסם להערות הציבור ב-22 בינואר 2026

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

[4] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and administrative relief for small mid-caps (הוגש בינואר 2026).

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

NIS1 NIS2 – NIS who?/Adi Marcus, Adv., Mr. Gabriel Marcus*

In the business world of 2026, information security is no longer merely a technical issue under the exclusive responsibility of development and IT personnel. With the entry into force of the latest amendments to the European NIS2 Directive and the enactment of the Israeli National Cyber Defense Law Memorandum, 2026[1], the legal responsibility for cyber incidents has shifted from the server room directly to the boardroom table.

Over the past decade, global cyber regulation has undergone an accelerated maturation process. For Israeli companies operating in the international arena, understanding the regulatory timeline is no longer a matter of "technical compliance," but a prerequisite for business and legal survival. The process began in 2016 with the adoption of the European NIS1 Directive.[2] This directive focused on "operators of essential services" (national infrastructures) and was largely voluntary for the broader business sector.

However, a dramatic turning point occurred in 2024 with the entry into force of the NIS2 Directive,[3] which expanded the scope of regulation to 18 different sectors - including manufacturing, food, waste management, and digital services. It imposed strict reporting obligations and established that company management bears direct responsibility for adopting adequate protection measures. Despite being a European legislation, its impact on the Israeli economy is critical: any Israeli company providing services to the EU, operating within its territory, or acting as a link in the supply chain of a European entity, is obligated to meet these standards.

In January 2026, the European Union introduced significant changes (the "Cyber Package 2026"[4]) designed to address geopolitical risks and ransomware attacks. Concurrently, in Israel, the 2026 Cyber Defense Law Memorandum imposes similar obligations on entities defined as "digital service providers" and "essential infrastructures," seeking to require companies to conduct Cyber Due Diligence for every supplier in their supply chain. As long as a company operates as a software or IT provider, it is highly likely that its clients will demand proof of compliance with NIS2 standards as a precondition for contractual engagement.

The updated regulation also requires reporting any significant cyber incident within 24 hours, including details on ransomware attacks, leading to extensive exposure of the company's activities during a crisis. Furthermore, responsibility can no longer be exclusively delegated to the Chief Information Security Officer (CISO); senior executives are now required to undergo cyber training and explicitly approve organizational defense plans. If a cyber incident occurs and it is found that the company did not invest the necessary resources, the implications could include personal financial sanctions against board members and executives, and even suspension from their positions.

The Israeli law memorandum has broadened the scope even further: software development, cloud storage, and IT system management companies employing over 50 workers or with a turnover exceeding ILS 40 million will be classified as an "essential organization," subject to direct supervision by the National Cyber Directorate and strict enforcement.

Thus, in the regulatory era of 2026, cybersecurity has ceased to be a purely technological issue and has become a core element of legal risk management, where expert legal counsel combined with cyber consulting constitutes the organization's first line of defense[5]. Beyond the acute need for close legal guidance to build "defensive walls" around the board of directors and officers to prevent exposure to lawsuits and personal liability, it is crucial to prepare in advance with an organizational cyber due diligence process. Ultimately, the integration of technological expertise with deep legal understanding is the only way to provide the organization with a presumption of legal propriety and offer peace of mind to executives facing both the regulator and the global market. Moreover, a company that fails to do so may find itself unable to conduct business with European companies.

---

* **Adi Marcus, Adv.** is an attorney in the office of Afik & Co. (www.afiklaw.com), which is part of BOKS International (www.boks-international.com) and who focuses primarily on commercial and corporate law, copyrights, media law and international transactions. Advocate Marcus holds a major in law, an M.A in communication from Tel Aviv University and an international MBA from Bar Ilan University. She completed her internship at the Ministry of justice under the Deputy Attorney General focusing civil law and copyright law, then worked for about 18 months in the office of Shlomo Cohen in the field of intellectual property, about 11 years in the legal department of the communications network "Noga Network" (Channel 2 of TV), with her last position before the company merged with Channel 10, was head of department in the legal department and then, before joining the firm, as Kneller Artists Representation's internal legal advisor, representing in all matters of legal advice to artists and cultural figures, both in Israel and internationally. **Mr. Gabriel Marcus** is a senior cyber architect who advises companies in the cyber field and works in collaboration with Afik & Co. to perform cyber risk surveys and address issues related to the subject. Nothing herein should be treated as a legal advice and all issues must be reviewed on a case-by-case basis. For additional details: +972-3-6093609 or at the e-mail: afiklaw@afiklaw.com.

[1] National Cyber Defense Law Memorandum, 2026, Published in Israel for public comments on January 22, 2026.

[2] Directive (EU) 2016/1148 of the European Parliament and of the Council of 6 July 2016 concerning measures for a high common level of security of network and information systems across the Union.

[3] Directive (EU) 2022/2555 of the European Parliament and of the Council of 14 December 2022 on measures for a high common level of cybersecurity across the Union.

[4] Proposal for a Directive of the European Parliament and of the Council amending Directive (EU) 2022/2555 as regards simplification measures and administrative relief for small mid-caps (Submitted in January 2026).

[5] 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://he.afiklaw.com/articles/a424

NIS1 NIS2 – ¿NIS quién?/Adi Marcus, Abogada, señor Gabriel Marcus*

En el mundo empresarial de 2026, la seguridad de la información ya no es meramente un problema técnico bajo la responsabilidad exclusiva del personal de desarrollo y TI. Con la entrada en vigor de las últimas enmiendas a la Directiva europea NIS2 y la promulgación del Memorando de la Ley Nacional de Defensa Cibernética de Israel de 2026[1], la responsabilidad legal por los incidentes cibernéticos se ha trasladado de la sala de servidores directamente a la mesa de la junta directiva.

Durante la última década, la regulación cibernética global ha experimentado un proceso de maduración acelerado. Para las empresas israelíes que operan en el ámbito internacional, comprender la línea de tiempo regulatoria ya no es una cuestión de "cumplimiento técnico", sino un requisito previo para la supervivencia comercial y legal. El proceso comenzó en 2016 con la adopción de la Directiva europea NIS1.[2] Esta directiva se centró en los "operadores de servicios esenciales" (infraestructuras nacionales) y fue en gran medida voluntaria para el sector empresarial en general.

Sin embargo, en 2024 se produjo un punto de inflexión dramático con la entrada en vigor de la Directiva NIS2,[3] que amplió el alcance de la regulación a 18 sectores diferentes, incluidos la manufactura, la alimentación, la gestión de residuos y los servicios digitales. Impuso estrictas obligaciones de presentación de informes y estableció que la dirección de la empresa tiene la responsabilidad directa de adoptar medidas de protección adecuadas. A pesar de ser una legislación europea, su impacto en la economía israelí es crítico: cualquier empresa israelí que preste servicios a la UE, opere dentro de su territorio o actúe como un eslabón en la cadena de suministro de una entidad europea, está obligada a cumplir con estos estándares.

En enero de 2026, la Unión Europea introdujo cambios significativos (el "Paquete Cibernético 2026"[4]) diseñados para abordar los riesgos geopolíticos y los ataques de ransomware. Paralelamente, en Israel, el Memorando de la Ley de Defensa Cibernética de 2026 impone obligaciones similares a las entidades definidas como "proveedores de servicios digitales" e "infraestructuras esenciales", buscando exigir a las empresas que realicen una Debida Diligencia Cibernética (Cyber Due Diligence) para cada proveedor en su cadena de suministro. Mientras una empresa opere como proveedora de software o TI, es muy probable que sus clientes exijan pruebas de cumplimiento con los estándares NIS2 como condición previa para la contratación comercial.

La regulación actualizada también requiere informar cualquier incidente cibernético significativo dentro de las 24 horas, incluyendo detalles sobre ataques de ransomware, lo que lleva a una amplia exposición de las actividades de la empresa durante una crisis. Además, la responsabilidad ya no puede delegarse exclusivamente en el Director de Seguridad de la Información (CISO); ahora se requiere que los altos ejecutivos reciban capacitación cibernética y aprueben explícitamente los planes de defensa organizacional. Si ocurre un incidente cibernético y se determina que la empresa no invirtió los recursos necesarios, las implicaciones podrían incluir sanciones económicas personales contra los miembros de la junta y los ejecutivos, e incluso la suspensión de sus cargos.

El memorando de la ley israelí ha ampliado aún más el alcance: las empresas de desarrollo de software, almacenamiento en la nube y gestión de sistemas de TI que empleen a más de 50 trabajadores o con una facturación superior a 40 millones de ILS serán clasificadas como una "organización esencial", sujeta a la supervisión directa de la Dirección Nacional de Cibernética y a una aplicación estricta.

Por lo tanto, en la era regulatoria de 2026, la ciberseguridad ha dejado de ser un problema puramente tecnológico y se ha convertido en un elemento central de la gestión de riesgos legales, donde el asesoramiento legal experto combinado con la consultoría cibernética constituye la primera línea de defensa de la organización[5]. Más allá de la necesidad imperiosa de contar con una estrecha orientación legal para construir "muros defensivos" alrededor de la junta directiva y los funcionarios para evitar la exposición a demandas y responsabilidades personales, es crucial prepararse con anticipación mediante un proceso de debida diligencia cibernética organizacional. En última instancia, la integración de la experiencia tecnológica con una profunda comprensión legal es la única forma de proporcionar a la organización una presunción de corrección legal y ofrecer tranquilidad a los ejecutivos frente al regulador y al mercado global. Además, una empresa que no lo haga puede verse imposibilitada de hacer negocios con empresas europeas.

---

* **Adi Marcus, abogada** es abogado en la oficina de Afik & Co. (www.afiklaw.com), que forma parte de BOKS International (www.boks-international.com) y se centra principalmente en derecho mercantil y corporativo, derechos de autor, derecho de medios y transacciones internacionales. El abogado Marcus tiene una licenciatura en Derecho, un máster en comunicación por la Universidad de Tel Aviv y un MBA internacional por la Universidad Bar Ilan. Realizó sus prácticas en el Ministerio de Justicia bajo la supervisión del Subfiscal General, centrada en derecho civil y derecho de autor, y luego trabajó unos 18 meses en la oficina de Shlomo Cohen en el ámbito de la propiedad intelectual, unos 11 años en el departamento legal de la red de comunicaciones "Noga Network" (Canal 2 de la televisión), ocupando su último puesto antes de que la empresa se fusionara con Channel 10, fue jefe de departamento en el departamento jurídico y luego, antes de incorporarse al despacho, asesor jurídico interno de Kneller Artists Representation, representando en todos los asuntos de asesoramiento legal a artistas y figuras culturales, tanto en Israel como internacionalmente. **El Sr. Gabriel Marcus** es arquitecto senior de ciberseguridad que asesora a empresas en el ámbito cibernético y colabora con Afik & Co. para realizar encuestas de riesgos cibernéticos y abordar cuestiones relacionadas con el tema. Nada de lo aquí contenido debe considerarse asesoramiento legal y todos los asuntos deben revisarse caso por caso. Para más detalles: +972-3-6093609 o en el correo electrónico: afiklaw@afiklaw.com.

[1] Memorando de la Ley Nacional de Defensa Cibernética, 2026, publicado en Israel para comentarios del público el 22 de enero de 2026.

[2] Directiva (UE) 2016/1148 del Parlamento Europeo y del Consejo, de 6 de julio de 2016, relativa a las medidas para garantizar un elevado nivel común de seguridad de las redes y sistemas de información en la Unión.

[3] Directiva (UE) 2022/2555 del Parlamento Europeo y del Consejo, de 14 de diciembre de 2022, relativa a las medidas para garantizar un elevado nivel común de ciberseguridad en toda la Unión

[4] Propuesta de Directiva del Parlamento Europeo y del Consejo por la que se modifica la Directiva (UE) 2022/2555 en lo que respecta a las medidas de simplificación y el alivio administrativo para las pequeñas empresas de mediana capitalización (Presentada en enero de 2026)

[5] 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

NIS1 NIS2 – NIS qui ?/Adi Marcus, avocat, M. Gabriel Marcus*

Dans le monde des affaires de 2026, la sécurité de l'information n'est plus seulement un problème technique relevant de la responsabilité exclusive du personnel de développement et de l'informatique. Avec l'entrée en vigueur des derniers amendements à la directive européenne NIS2 et la promulgation du mémorandum de la loi nationale israélienne sur la cyberdéfense de 2026[1], la responsabilité juridique des cyberincidents est passée de la salle des serveurs directement à la table du conseil d'administration.

Au cours de la dernière décennie, la réglementation mondiale en matière de cybersécurité a connu un processus de maturation accéléré. Pour les entreprises israéliennes opérant sur la scène internationale, comprendre le calendrier réglementaire n'est plus une question de « conformité technique », mais une condition préalable à la survie commerciale et juridique. Le processus a commencé en 2016 avec l'adoption de la directive européenne NIS1.[2] Cette directive se concentrait sur les « opérateurs de services essentiels » (infrastructures nationales) et était largement volontaire pour le secteur des entreprises au sens large.

Cependant, un tournant dramatique s'est produit en 2024 avec l'entrée en vigueur de la directive NIS2,[3] qui a élargi le champ d'application de la réglementation à 18 secteurs différents - y compris la fabrication, l'alimentation, la gestion des déchets et les services numériques. Elle a imposé des obligations de déclaration strictes et établi que la direction de l'entreprise porte la responsabilité directe de l'adoption de mesures de protection adéquates. Bien qu'il s'agisse d'une législation européenne, son impact sur l'économie israélienne est critique : toute entreprise israélienne fournissant des services à l'UE, opérant sur son territoire ou agissant comme un maillon de la chaîne d'approvisionnement d'une entité européenne, est tenue de respecter ces normes.

En janvier 2026, l'Union européenne a introduit des changements significatifs (le « Paquet Cyber 2026 »[4]) conçus pour faire face aux risques géopolitiques et aux attaques par ransomware. Parallèlement, en Israël, le mémorandum de la loi sur la cyberdéfense de 2026 impose des obligations similaires aux entités définies comme « fournisseurs de services numériques » et « infrastructures essentielles », cherchant à exiger des entreprises qu'elles fassent preuve de diligence raisonnable en matière de cybersécurité (Cyber Due Diligence) pour chaque fournisseur de leur chaîne d'approvisionnement. Tant qu'une entreprise opère en tant que fournisseur de logiciels ou d'informatique, il est fort probable que ses clients exigent une preuve de conformité aux normes NIS2 comme condition préalable à un engagement contractuel. conçus pour faire face aux risques géopolitiques et aux attaques par ransomware. Parallèlement, en Israël, le mémorandum de la loi sur la cyberdéfense de 2026 impose des obligations similaires aux entités définies comme « fournisseurs de services numériques » et « infrastructures essentielles », cherchant à exiger des entreprises qu'elles fassent preuve de diligence raisonnable en matière de cybersécurité (Cyber Due Diligence) pour chaque fournisseur de leur chaîne d'approvisionnement. Tant qu'une entreprise opère en tant que fournisseur de logiciels ou d'informatique, il est fort probable que ses clients exigent une preuve de conformité aux normes NIS2 comme condition préalable à un engagement contractuel.

La réglementation mise à jour exige également de signaler tout cyberincident significatif dans les 24 heures, y compris des détails sur les attaques par ransomware, ce qui conduit à une exposition importante des activités de l'entreprise en temps de crise. De plus, la responsabilité ne peut plus être exclusivement déléguée au responsable de la sécurité des systèmes d'information (RSSI/CISO) ; les cadres dirigeants sont désormais tenus de suivre une formation en cybersécurité et d'approuver explicitement les plans de défense organisationnels. Si un cyberincident se produit et qu'il est avéré que l'entreprise n'a pas investi les ressources nécessaires, les implications pourraient inclure des sanctions financières personnelles à l'encontre des membres du conseil d'administration et des dirigeants, voire une suspension de leurs fonctions.

Le mémorandum de la loi israélienne a encore élargi la portée : les entreprises de développement de logiciels, de stockage cloud et de gestion de systèmes informatiques employant plus de 50 travailleurs ou ayant un chiffre d'affaires dépassant les 40 millions d'ILS seront classées comme « organisation essentielle », soumises à la supervision directe de la Direction nationale de la cybersécurité et à une application stricte de la loi.
Ainsi, dans l'ère réglementaire de 2026, la cybersécurité a cessé d'être un problème purement technologique et est devenue un élément central de la gestion des risques juridiques, où le conseil juridique expert combiné au conseil en cybersécurité constitue la première ligne de défense de l'organisation[5]. Au-delà du besoin urgent d'un accompagnement juridique étroit pour construire des « murs défensifs » autour du conseil d'administration et des dirigeants afin d'éviter l'exposition aux poursuites et à la responsabilité personnelle, il est crucial de se préparer à l'avance avec un processus de diligence raisonnable en matière de cybersécurité organisationnelle. En fin de compte, l'intégration de l'expertise technologique à une compréhension juridique approfondie est le seul moyen de fournir à l'organisation une présomption de régularité juridique et d'offrir une tranquillité d'esprit aux dirigeants face au régulateur et au marché mondial. De plus, une entreprise qui ne le fait pas pourrait se retrouver dans l'incapacité de faire des affaires avec des entreprises européennes.

---

* **Adi Marcus, avocate,** est avocate au sein du cabinet Afik & Co. (www.afiklaw.com), qui fait partie de BOKS International (www.boks-international.com) et se concentre principalement sur le droit commercial et des sociétés, le droit d'auteur, le droit des médias et les transactions internationales. L'avocat Marcus est titulaire d'un diplôme de droit, d'un master en communication de l'Université de Tel Aviv, et d'un MBA international de l'Université Bar Ilan. Elle a effectué un stage au ministère de la Justice sous la supervision du procureur général adjoint, se concentrant sur le droit civil et le droit d'auteur, puis a travaillé pendant environ 18 mois au bureau de Shlomo Cohen dans le domaine de la propriété intellectuelle, environ 11 ans au département juridique du réseau de communication « Noga Network » (chaîne 2 télévision). dans son dernier poste avant la fusion de la société avec Channel 10, il était chef de département juridique puis, avant de rejoindre le cabinet, conseiller juridique interne pour Kneller Artists Representation, représentant artistes et figures culturelles dans tous les domaines de conseil juridique, tant en Israël qu'à l'international. **M. Gabriel Marcus** est architecte principal en cybersécurité, conseille des entreprises dans le domaine du cyber et collabore avec Afik & Co. pour mener des enquêtes sur les risques cybernétiques et traiter les questions liées aux risques cybernétiques. Rien de ce contenu ne doit être considéré comme un conseil juridique et toutes les questions doivent être examinées au cas par cas. Pour plus de détails : +972-3-6093609 ou par email : afiklaw@afiklaw.com.

[1] Mémorandum de la loi nationale sur la cyberdéfense, 2026, publié en Israël pour commentaires publics le 22 janvier 2026.

[2] Directive (UE) 2016/1148 du Parlement européen et du Conseil du 6 juillet 2016 concernant des mesures destinées à assurer un niveau élevé commun de sécurité des réseaux et des systèmes d'information dans l'Union.

[3] Directive (UE) 2022/2555 du Parlement européen et du Conseil du 14 décembre 2022 concernant des mesures destinées à assurer un niveau élevé commun de cybersécurité dans l'ensemble de l'Union.

[4] Proposition de directive du Parlement européen et du Conseil modifiant la directive (UE) 2022/2555 en ce qui concerne les mesures de simplification et l'allègement administratif pour les petites entreprises de taille intermédiaire (Soumise en janvier 2026).

[5] Voir : Quand un directeur « entre en état d'Atraf » (devient frénétique) à cause d'une fuite de données / Osnat Nitay, Avocate, publié dans Afik News 424, 16.10.2024 - https://fr.afiklaw.com/articles/a424

NIS1 NIS2 – NIS quem?/Adi Marcus, Advogada, Sr. Gabriel Marcus*

No mundo dos negócios de 2026, a segurança da informação não é mais meramente uma questão técnica sob responsabilidade exclusiva da equipe de desenvolvimento e TI. Com a entrada em vigor das últimas emendas à Diretiva Europeia NIS2 e a promulgação do Memorando da Lei Nacional de Defesa Cibernética de Israel de 2026[1], a responsabilidade legal por incidentes cibernéticos mudou da sala de servidores diretamente para a mesa da diretoria.

Na última década, a regulamentação cibernética global passou por um processo de amadurecimento acelerado. Para as empresas israelenses que operam na arena internacional, entender a linha do tempo regulatória não é mais uma questão de "conformidade técnica", mas um pré-requisito para a sobrevivência comercial e jurídica. O processo começou em 2016 com a adoção da Diretiva Europeia NIS1.[2] Esta diretiva focava nos "operadores de serviços essenciais" (infraestruturas nacionais) e era amplamente voluntária para o setor empresarial em geral.

No entanto, um ponto de virada dramático ocorreu em 2024 com a entrada em vigor da Diretiva NIS2,[3] que expandiu o escopo da regulamentação para 18 setores diferentes - incluindo manufatura, alimentos, gestão de resíduos e serviços digitais. Ela impôs obrigações rigorosas de relatórios e estabeleceu que a administração da empresa tem responsabilidade direta pela adoção de medidas de proteção adequadas. Apesar de ser uma legislação europeia, seu impacto na economia israelense é crítico: qualquer empresa israelense que preste serviços à UE, opere em seu território ou atue como um elo na cadeia de suprimentos de uma entidade europeia é obrigada a atender a esses padrões.

Em janeiro de 2026, a União Europeia introduziu mudanças significativas (o "Pacote Cibernético 2026"[4]) projetadas para lidar com riscos geopolíticos e ataques de ransomware. Paralelamente, em Israel, o Memorando da Lei de Defesa Cibernética de 2026 impõe obrigações semelhantes a entidades definidas como "provedores de serviços digitais" e "infraestruturas essenciais", buscando exigir que as empresas conduzam uma *Due Diligence* Cibernética para cada fornecedor em sua cadeia de suprimentos. Contanto que uma empresa opere como fornecedora de software ou TI, é altamente provável que seus clientes exijam provas de conformidade com os padrões NIS2 como pré-condição para o engajamento contratual.

A regulamentação atualizada também exige relatar qualquer incidente cibernético significativo dentro de 24 horas, incluindo detalhes sobre ataques de ransomware, levando a uma ampla exposição das atividades da empresa durante uma crise. Além disso, a responsabilidade não pode mais ser delegada exclusivamente ao Diretor de Segurança da Informação (CISO); altos executivos agora são obrigados a passar por treinamento cibernético e aprovar explicitamente planos de defesa organizacional. Se ocorrer um incidente cibernético e for constatado que a empresa não investiu os recursos necessários, as implicações podem incluir sanções financeiras pessoais contra membros do conselho e executivos, e até mesmo a suspensão de seus cargos.

O memorando da lei israelense ampliou o escopo ainda mais: empresas de desenvolvimento de software, armazenamento em nuvem e gestão de sistemas de TI que empregam mais de 50 funcionários ou com faturamento superior a 40 milhões de ILS serão classificadas como uma "organização essencial", sujeitas à supervisão direta da Diretoria Nacional de Cibernética e a uma fiscalização rigorosa.

Assim, na era regulatória de 2026, a segurança cibernética deixou de ser uma questão puramente tecnológica e se tornou um elemento central da gestão de riscos jurídicos, onde o aconselhamento jurídico especializado combinado com a consultoria cibernética constitui a primeira linha de defesa da organização.[5] Além da necessidade aguda de orientação jurídica próxima para construir "muros defensivos" em torno do conselho de administração e dos diretores para evitar a exposição a processos judiciais e responsabilidade pessoal, é crucial preparar-se antecipadamente com um processo de *due diligence* cibernética organizacional. Em última análise, a integração da expertise tecnológica com uma profunda compreensão jurídica é a única maneira de fornecer à organização uma presunção de propriedade legal e oferecer tranquilidade aos executivos que enfrentam tanto o regulador quanto o mercado global. Além disso, uma empresa que não o fizer pode se ver impossibilitada de realizar negócios com empresas europeias.

---

* **Adi Marcus, advogada,** é advogada no escritório da Afik & Co. (www.afiklaw.com), que faz parte da BOKS International (www.boks-international.com) e foca principalmente em direito comercial e corporativo, direitos autorais, direito de mídia e transações internacionais. O advogado Marcus possui diploma em direito, mestrado em comunicação pela Universidade de Tel Aviv e MBA internacional pela Universidade Bar Ilan. Ela estagiou no Ministério da Justiça sob supervisão do Vice-Procurador-Geral, com foco em direito civil e direitos autorais, e depois trabalhou por cerca de 18 meses no escritório de Shlomo Cohen na área de propriedade intelectual, cerca de 11 anos no departamento jurídico da rede de comunicações "Noga Network" (televisão Canal 2). em sua última posição antes da fusão da empresa com o Channel 10, foi chefe do departamento jurídico e, antes de ingressar no escritório, assessor jurídico interno da Kneller Artists Representation, representando artistas e figuras culturais em todos os assuntos de consultoria jurídica, tanto em Israel quanto internacionalmente. **O Sr. Gabriel Marcus** é arquiteto sênior de cibersegurança que assessora empresas na área cibernética e colabora com a Afik & Co. para conduzir pesquisas de risco cibernético e abordar questões relacionadas ao risco. Nada aqui contido deve ser considerado aconselhamento jurídico e todos os assuntos devem ser revisados caso a caso. Para mais detalhes: +972-3-6093609 ou e-mail: afiklaw@afiklaw.com.

[1] Memorando da Lei Nacional de Defesa Cibernética, 2026, publicado em Israel para comentários públicos em 22 de janeiro de 2026.

[2] Diretiva (UE) 2016/1148 do Parlamento Europeu e do Conselho, de 6 de julho de 2016, relativa a medidas destinadas a garantir um elevado nível comum de segurança das redes e da informação em toda a União.

[3] Diretiva (UE) 2022/2555 do Parlamento Europeu e do Conselho, de 14 de dezembro de 2022, sobre medidas para um elevado nível comum de cibersegurança em toda a União

[4] Proposta de Diretiva do Parlamento Europeu e do Conselho que altera a Diretiva (UE) 2022/2555 no que diz respeito a medidas de simplificação e alívio administrativo para pequenas empresas de média capitalização (Apresentada em janeiro de 2026).

[5] Ver: Quando um diretor "entra em estado de Atraf" (fica frenético) devido a um vazamento de dados / Osnat Nitay, Advogada, publicado na Afik News 424, 16.10.2024 - https://pt.afiklaw.com/articles/a424