28 בפברואר, 2016

לכבוד
משרד ראש הממשלה – מטה הסיבר הלאומי
משרד הביטחון- אגף הפיקוח על היצוא הביטחוני

שלום רב,

הנדון: <u>בקשה לגניזת טיוטת צו הפיקוח על הסייבר</u>
<u>-התייחסות של ארגון Cyber Together</u>

1. במהלך חודש ינואר 2016 פרסם אגף הפיקוח על הייצוא הבטחוני (אפ"י) ביחד עם מטה הסייבר הלאומי את טיוטת צו הפיקוח על הסייבר. הטיוטא מבקשת להרחיב את הפיקוח על יצוא הסייבר מזה הקיים כבר כיום על פי אמנת ואסנר. אפ"י ומטה הסייבר איפשרו להגיש תגובות לטיוטת הצו עד לתאריך 7 בפברואר 2016 – נציין כי ככל הנראה בטווח זמנים זה הטיוטא לא הועברה לכלל התעשייה אלא לגורמים מצומצמים בלבד. לאחר מכן ניתנה הארכה נוספת למתן תגובות והטיוטא הועברה להערותיה של כלל התעשייה, ונכון להיום המועד הקובע למתן תגובות הוא ה-3 למרס, 2016, בשעה 16:00.
2. **בשבועות האחרונים התקיימו מספר כינוסים ומפגשים שונים בקשר לטיוטת צו הפיקוח שפורסמה. הטענות הנשמעות מצד החברות השונות בקשר לטיוטא הן רבות ומגוונות (חלקן טענות כלליות על הפרוצדורה ועל הסבירות של המהלך, וחלקן נקודתיות), ואולם הטענה העיקרית הנשמעת על ידי רוב רובן של החברות, בשלב זה, היא שדרוש זמן נוסף, מעבר למועד שנקבע למתן התגובות, על מנת שהחברות השונות יוכלו להגיש את תגובותיהם לטיוטת הצו בצורה מסודרת ומלאה.**
3. **לאור האמור להלן, אנו מבקשים בזאת שהצו המוצע על ידי אפ"י ועל ידי מטה הסייבר הלאומי ייגנז, ובו זמנית, ייקבע תהליך עבודה מובנה אשר יכלול בין היתר הקמת ועדה משותפת שתכלול את נציגי אפ"י ואת מטה הסייבר הלאומי וכן את התעשיה. עבודת הועדה תכלול שיתוף של מומחים מתחומי הכלכלה, המשפט, התעשיה והייצוא על מנת לגבש תכנית מסודרת יותר וברורה יותר שמצד אחד תגן על האינטרסים של מדינת ישראל ללא כל פשרה, ומצד שני, לא תפגע בצורה כה גורפת בתעשית הסייבר הישראלית ותגרום לנזקים ארוכי טווח, שאחר כך יהיה קשה לתקן.**
4. **בכל מקרה יש להדגיש שהתאריך שנקבע להגשת התגובות לטיוטת הצו (3.3.2016) אינו ראוי מן הטעם שדוקא בתקופה זו מתקיימים האירועים הבינלאומיים החשובים והגדולים ביותר בתעשיית הסייבר, ביניהם כנס סייברטק 2016, כנס קספרסקי וכנס RSA, ובשל כך, רבות מהחברות (יותר מוגש בקרב החברות הקטנות והבינוניות) עסוקות בהתארגנות ובהשתתפות בכנסים אלו והאירועים שמסביבם, דבר שמשפיע על יכולתם של החברות להשקיע את המשאבים והזמן הראוי ללמידת הטיוטא ולשקול את המשמעויות שלה ולהגיב עליה.**
5. כפי שהנכם בוודאי יודעים, בעקבות פרסום טיוטת צו הפיקוח על הסייבר נוצרה בקרב תעשית הסייבר הישראלית בכלל, ובקרב החברות השונות, המולה רבה וניכר שנוצר בלבול רב בכל הקשור לצו הפיקוח המוצע ולתחולתו, וקיימת חוסר בהירות מוחלטת בנוגע להשלכות שיהיו במקרה שטיוטת צו הפיקוח על הסייבר אכן תאושר בועדת החוץ והבטחון של הכנסת, ותכנס לתוקף.
6. באופן כללי ניתן לציין את הטענות הבאות שנשמעו מקרב החברות השונות:

א. **הכוונה טובה אך הדרך להשיג אותה אינה נכונה-** מיותר לציין שכל החברות מדגישות שוב ושוב ובאופן גורף כי הן תומכות ללא עוררין בצורך להגן על האינטרסים של מדינת ישראל, אלא שהשאלה היא מהי הדרך היותר סבירה והיותר נכונה להשיג את אותה המטרה.

ב. **אי מתן זמן הולם לתגובה-** לחברות השונות דרוש זמן על מנת לבחון את טיוטת הצו ולהתייחס בהתאם. לרוב מדובר בחברות שיש להם משקיעים, וראוי שיתאפשר להם לקיים דיונים הפנימיים על מנת להבין את ההשלכות שיהיו להחלה של הצו, דבר המצריך יותר זמן.

ג. **הרגולציה על יצוא סייבר הקיימת זה מכבר בישראל מספיקה ועונה על האינטרסים השונים שהרגולטור מבקש לפקח** – במצב הקיים, ככל הנראה, מדינת ישראל הינה המדינה היחידה בעולם המאמצת לתוך חוקיה באופן ישיר ו as is, את הסדר וואסנר, המסדיר את הפיקוח על העברתם של אמצעי לחימה קונבנציונלים, טובין וטכנולוגיות דו-שימושיים. בואסנר חברים 41 מדינות, ביניהם: בריטניה, צרפת, גרמניה, ארה"ב, אוסטרליה, יפן ורוסיה. מטרת ואסנר הינו לתרום לביטחון הלאומי והבינלאומי של מדינות העולם והיציבות העולמית וכן למנוע רכישת פריטים אלו על ידי טרוריסטים[1].

לאור אינטרסים אלו, בשנים האחרונות, הוסיפו המדינות לוואסנר, פיקוח על מוצרים ידע ושירותי סייבר בשני תחומים עיקריים: תשתיות תוכנת חדירה ו Deep pocket inspection (ניתור תעבורה מעמיקה DPL). לאחר דיונים עמוקים בנושא בשיתוף גורמים רבים (ביניהם ארגונים לשמירה על זכויות אדם), נקבע, כי הפיקוח בנוגע לתוכנות חדירה יצומצם ל- 2 תנאים מצטברים: לרכיבים בתוכנה (כגון כאלו היכולים לזהות, להבין, ליצור ולנצל חולשות, להתחמק ולאכוף אמצעי הגנה כדוגמת אנטיוירוסים, אימות זהות ועוד, היכולים לאסוף מידע לשנותו ולהעבירו, להתקין אוטומאטית תוכנות הפעלת מערכת ולאכוף הרשאות מנהל, לתקשר עם תוכנות זדוניות אחרות וכד') היוצרים את ההתנהגות הזדונית (כגון שיבוש, מניעה וביזוי של המידע או פגיעה ברשת ובמכשירים).[2]

בהקשר לזה הודגש כי אין הכוונה לפקח על תוכנת החדירה כשלעצמה הואיל: וכל בעל מכשיר שעליו מותקנת תוכנת חדירה (אף ללא ידיעתו) היה יוצא מחוץ לגבולות המדינה, היה הלכה למעשה נתון בסיכון לעבירת יצוא ללא רשיון; וכן מבדיקה שנערכה על ידי המדינות עולה, כי כלים, פלטפורמות ותוכנות רבות המספקים שירותים טכנולוגיים בסיסיים, נמכרות ומופצות כחוק ולהן שימושים לגיטימיים, מהווים תוכנות חדירה לכל דבר על כן אין כל כוונה לפקח עליהם.[3] **הוספת "תוכנת חדירה" לפיקוח בטיוטת הצו מרחיבה יתר על המידה את הרגולציה הנדרשת וכן חוטאת לעיקר.**

ד. **הפיקוח על "חולשות", "פורנזיקה בעל רכיב פיזי", ו"מוצרי הגנה שפותחו במיוחד לשימוש במערכות אסרטגיות ולמטרות ביון" הינו מבחינת עודף רגולציה אשר אינו משיג כל מטרה, אינו הכלי המתאים לכך ופוגע בחוסנה של מדינת ישראל-** בבוא המדינות בהסדר ואסנר להסדיר את הפיקוח על יצוא סייבר בחרו הם להתמקד בשני התחומים של תשתיות תוכנת חדירה וניתור תעבורה מעמיקה (DPL) הואיל ומדובר בתחומים המרכזים בתוכם את היכולות הטכנולוגיות אשר מאפשרות את הפגיעה ממנה רוצים הם להימנע, ומהווים האיזון הראוי שבין האינטרס בשמירה על ביטחון המדינות והעולם לזכויות חוקתיות ופגיעה מינימלית בהתחדשות הטכנולוגית.

בעניין פיקוח על חולשות, הגיעו המדינות למסקנה, כי ידע על קיום חולשה כשלעצמה אינה רלוונטית עד שעושים בה שימוש. על כן, בתיקון שנעשה לואסנר כאמור, ההתמודדות עם חולשות נעשה על ידי ההגדרה של תוכנת חדירה כשם שמופיעה בואסנר כלוקחת בחשבון כלים העושים בחולשות שימוש או היוצרים את החולשות. על כן, אין כל יתרון בלבצע פיקוח על חולשות כשלעצמן.

זאת ועוד, הדרישה לפיקוח על יצוא חולשות אינו מגן כלל על האינטרסים של מדינת ישראל ואף פוגע בה, הואיל ובראייה עולמית, החולשות הקיימות היום בעולם עולים במספרם, מספר רב של מונים, מהחולשות הקיימות בארץ, כך שבעוד ובארץ תהיה הגבלה בסחר בהן, העולם ימשיך לנהוג כמנהגו. הגבלה זו תימנע מהיזמנים והחברות לעסוק באיתור ולמידת חולשות חדשות ולמעשה יעמיד את ישראל בנחיתות טכנולוגית וסכנה ממשית.

אף באם יימצא הצדקה כלשהי לפיקוח על חולשות כשלעצמן, כלי הפיקוח המוצע אינו מתאים כלל בעניין זה. עולם החולשות בסייבר הינו דינאמי, ובעל קצב השתנות מהיר, ברמה של דקות עד שעות. הליך קבלת

---

[1] ראה הסבר מפורט על הסדר ואסנר באתר http://www.wassenaar.org/

[2] ראה לעניין זה את הדיווחים הבאים בתקשורת בזמנו http://www.techweekeurope.co.uk/workspace/surveillance-malware-privacy-133780 ; http://www.ft.com/intl/cms/s/0/2903d504-5c18-11e3-931e-00144feabdc0.html#axzz4167PQVNQ

[3] תוספת זו לוואסנר הייתה יוזמה במקור של ממשלת בריטניה. בביקור רשמי בישראל בשנת 2015 של נציגים ממדינות החברות בואסנאר נמסרה עמדה זו על ידי John King, Head of UK delegation to the Wassenaar Arrangemen במצגת סקירה שהעביר בנושא. כמו כן ראה לעניין זה, בנוסף, מאמר שפורסם באתר ממשלת בריטניה – The Department for Business, Innovation & Skills (BIS) http://blogs.bis.gov.uk/exportcontrol/files/2015/08/Intrusion-Software-Tools-and-Export-Control1.pdf עמוד 5 והלאה.

הרישיון כשם שקבוע בחוקים השונים הינו הליך מורכב הדורש זמן רב. כבר כיום, אפ״י מתקשה לעמוד במספר הבקשות אשר מוגשות לה ונצפו מקרים רבים שהעיסקה בסופו של דבר לא יצאה לפועל הואיל והרישיון לא ניתן בזמן. ייעול הפרוצדורה המתבקשת דורשת בחובה, העלאת כוח האדם וכן משאבים לקליטת הבקשות ועיבודן דבר אשר ישית עלויות רבות על האזרחים. עלויות אלה אינן מוצדקות לאור העובדה כי הפיקוח אינו נדרש כלל.

בכל הנוגע למוצרי פורנזיקה, הפיקוח המוצע הינו נרחב דיו ולא משיג כלל את האינטרס שרגולטור מבקש להגן עליו (כשם שהוצג על ידי נציג אפ״י, בע״פ באחד הכינוסים בנושא). כל שכן יש לבחון האם אינטרס זה גובר על הפגיעה בחופש העיסוק, ביכולת החדשנות וההובלה של מדינת ישראל וביכולת ההגנה שלה. נראה כי לא נעשה דיון מעמיק בנושא. כמו כן, נראה כי יש פער טכנולוגי בהבנה של מוצרי הפורנזיקה למיניהם שרבים מהם כלל לא מסכנים את האינטרס של הרגולטור בנושא. באם הרגולטור יכול להצביע על אינטרס הגנה ספציפי וייחודי (כשם שעשה בפועל) ראוי שיתאים את הפיקוח המתבקש, למוצרי ידע והשירותים הרלוונטיים – לצורך כך עליו לעשות סקרי שוק והבנה של הכלים, היכולות והטכנולוגיה הקיימת זה מכבר בשוק. נראה כי צעד זה לא נעשה כלל על ידו.

בנוגע לפיקוח על מוצרי הגנה שפותחו במיוחד לשימוש במערכות אסרטגיות ולמטרות ביון, מתעלם הרגולטור מהעובדה כי עבודה למול כוחות הביטחון הינה מפוקחת זה מכבר על ידי חוקים שונים ורגולטורים שונים והן על ידי סטנדרטים מחייבים ומקובלים בתחום. כבר כיום נשמע לא אחת הטענה כי הרגולציה הקיימת זה מכבר בנושא מונעת מחברות רבות מלעסוק בתחום. כמו כן, אף מבחינה עיסקית כוחות הביטחון דואגות לשמירה על האינטרסים של המדינה, על ידי הגבלות שימוש, ייצור ומכירה של המוצרים שעושות בהן שימוש לצד ג׳. על כן הרחבת הרגולציה המוצעת על מוצרים אלה הינה הכבדה יתרה ואינה רלוונטית הואיל והאינטרס המדינתי נשמר באמצעים אחרים קיימים זה מכבר.

בהקשר לזה נציין כי הפיקוח בואסנר על DPL עונה לדרישות הרגולטור בנושא שכן אמצעי זה אומץ על מנת לפקח על ריגול תעשייתי המוני.

ה. **הרחבת הפיקוח על יצוא סייבר והאופן שבו היא מבוצעת, מנוגדת להחלטות ממשלה מחייבות קודמות בנושא-** החלטת ממשלה מספר 2118[4] (״**ההחלטה**״) קובעת, זה מכבר, כי יש להפחית את הנטל הרגולטורי ומטילה על על כל משרד ממשלתי להכין תוכנית חומש להפחתת הנטל[5]. הרחבת הרגולציה בטיוטת הצו כאמור מנוגדת להחלטת ממשלה מחייבת זו.

בנוסף, ההחלטה קובעת, כי התוכנית תגובש לאחר קיום שיח עם המגזר העיסקי והמגזר השלישי[6]. כאמור בהרחבה בהמשך, לא נעשתה התייעצות אמיתית וכנה עם כלל המגזר העיסקי בתחום הסייבר.

כמו כן, קובעת ההחלטה כי בבוא הרגולטור לקבוע רגולציה חדשה לשקול גם בחירה בחלופה המפחיתה את הנטל הרגולטורי וכן להגדיר תכלית ברורה לרגולציה, להגדיר את הצורך להתערבות רגולטורית להשגת תכלית זו ולהגדיר את הערכת התועלות הצפויות מהחלת הרגולציה[7]. אפ״י ומטה הסייבר נמנעו מלציין את האינטרסים שמבקשים הם להסדיר בטיוטא, אינם מגדירים את הצורך להרחבת ההתערבות ביצוא סייבר ואינם מסבירים את התועלת הצפויה מקבלת הרגולציה. כל שעשו בעניין זה הוא לצרף לטיוטת הצו הסבר על השינויים המוצעים, דבר המנוגד להחלטה כאמור וכן מונע מהתעשייה ליתן התייחסותה באופן מעמיק, אמיתי וכן.

בנוסף, קובעת ההחלטה כי על הרגולטור לחשב את הנטל הרגולטורי הצפוי מהרגולציה בהתחשב במידע שבפניו.[8] נראה כי טרם הוצאת הטיוטא לא נעשה כל בדיקה אמפירית על הנעשה בעולם בנושא והמשמעויות של המהלך מבחינה עולמית, לא נעשה בדיקה אמפירית בשטח על משמעויות הרגולציה ו/או הצורך בה וכן לא נעשו סקרים בנושא על מספר החברות שבפועל אמורות להיות מפוקחות.

---

[4] החלטת ממשלה מספר 2118 מיום 22.10.2014
[5] סעיף 1 א׳ להחלטה
[6] סעיף 1 ה׳ לחהלטה
[7] סעיף 3 א׳ להחלטה
[8] סעיף 3 ג׳ להחלטה

זאת ועוד, נקבע בהחלטה, כי על הרגולטור ליצור בהירות, ודאות ועקביות למפוקחים בכל הנוגע להוראות הרגולציה, אופני הפיקוח על קיום הוראותיה ודרכי אכיפתה, תוך הנגשת מידע זה[9]. טיוטת הצו שפורסמה אינה מסבירה את המכלול הנורמטיבי אשר בגדרה פועלת: מכוח איזה חוקים היא פועלת, מי הרגולטור הרלוונטי, מהם אופני הפיקוח (כדוגמת הוצאת רישיון) ועוד. כל אלה נעדרים מדברי ההסבר שהתלוו להצעה ולמעשה מונעת מהתעשייה ליתן התייחסותה כראוי ונוגדת את ההחלטה.

ו. **נדרשת עבודת הכנה נוספת -** נראה שחברות הסייבר, על תחומי פעילותן השונים והיקפי הפעילות שלהם והמחזורים העסקיים לא נכללו בצורה מסודרת בגיבוש טיוטת הצו. קיימת תחושה, גם אם היא לא מדוייקת, שהעבודה שנעשתה על ידי משרד הבטחון ומטה הסייבר הלאומי בוצעה כמעין "הנחתה" על תעשית הסייבר כולה. רבים שואלים מדוע החברות השונות מהתחום, כאלה שמייצגות את התעשיה כולה, על מורכבויותיה (גודל חברה, היקפי פעילות, וותק בתחום), לא שותפו בדיונים שנמשכו במשך שנתיים או שלוש, ומדוע לא בוצע שיתוף פעולה מלא יותר עם ארגונים כמו מכון הייצוא והתאחדות התעשיינים.
נדרש, כי תיעשה בחינה מחודשת של אסדרת הפיקוח על מוצרי סייבר בשיתוף נציגים וארגונים: מכלל הסקטורים (ביטוח, פיננסים, תשתיות קריטיות, בריאות, יצוא אזרחי, יצוא ביטחוני, מוצרי תקיפה, מוצרי הגנה וכד') ומכלל סוגי החברות (יזמים, סטארטאפים, חברות קטנות, חברות גדולות, משקיעים וכד').

ז. **נזק תדמיתי לכל תעשיית הסייבר הישראלית-** קיים חשש שלא נבחנו המשמעויות התדמיתיות שיהיו להחלה של הצו על תעשיית הסייבר הישראלית כתעשיה ישראלית ועולמית מובילה, ומה תהיה ההשפעה שלו על הרצון של חברות אזרחיות גלובליות להמשיך ולרכוש מוצרי ושירותי סייבר ישראליים, או להשקיע במחקר משותף בתחום. קיים חשש כבד שלהחלה של הצו יהיו השלכות רוחביות חמורות, ועלולים להגרם נזקים עצומים לתעשית הסייבר הישראלית, ולהובלה של החברות הישראליות בתחום הסייבר בעולם.

ח. **היבטים נוספים שלא נלקחו בחשבון-** התחושה היא שהדגש שניתן לנושא "הבטחון", דחק לקרן הפינה את שאר השיקולים שהיה ראוי לתת להם משקל כבד יותר (ההיבטיים משפטיים והחוקתיים, כלכליים (מיקרו ומקרו) , תחרות עסקית אל חברות אחרות מהעולם, תקינות ההליך סבירותו וחיוניותו, המידתיות של המהלך המוצע, השוואה אל שאר מדינות העולם, יכולת יישום בשטח ואכיפה). השיקול הבטחוני הוא חשוב, אך יש לשקול עוד שיקול ביחס למטרותיהם של אויבי ישראל. אם המטרה של אויבי ישראל היא להחליש את מדינת ישראל, יש סיכוי שההחלה של הצו, תביא לפגיעה בתעשית הסייבר הישראלית ובמשך ההתפתחות שלה וההשקעות בה, וכן תביא לפגיעה כלכלית וביכולת של ישראל להוביל את תחום הסייבר בעולם. בנוסף, הצו עלול לגרום לחברות סייבר ישראליות לא למכור את מוצריהן לגופי הבטחון הישראליים, בגלל כל הבירוקרטיה והסיכונים הכרוכים הכך.

ט. **חוסר הכוונה מראש ואי פרסום הנחיות-** לא נמסרה לתעשיה כל הכוונה מראש בנוגע לבעיות שאותם מנסה משרד הביטחון לפתור, או בנוגע לתחומים הספציפיים שהצו מנסה לכסות, ולא פורסמו כל הנחיות בענין כעבודה מקדימה להחלה של צו. לא ברור מה הם הבעיות שיש במצב החוקי הקיים, ומדוע יש צורך לשנות אותו (כי כבר היום יש פיקוח על הייצוא של טכנולוגיה).

י. **הצו מנוסח בצורה לא בהירה ועלולות להיות לכך משמעויות פליליות-** הצו מנוסח בצורה לא ברורה דבר שמקבל משמעות מיוחדת בשל ההשלכות הפלילות עלולות להיות להחלה של הצו (וזאת למרות שגם מר לביא, ראש אפ"י הודה בכנס שנערך במשרד עורכי הדין HFN, שככל הנראה הצו לא יחול על 90% מהחברות הישראליות). אם הצו לא אמור לחול על 90% מהחברות, אז מדוע ולמה הוחלט להכניס לתזזית שכזו את כל התעשיה כולה?

יא. **עצירת השקעות זרות-** קיים חשש כבד שההחלה של הצו תביע לעצירה של השקעות מתוכננות בתחום על ידי משקיעים זרים ולבריחה של משקיעים. מתן יכולת כה גורפת למשרד הביטחון, עלולה להתפרש כהתערבות של משרד הבטחון הישראלי בפעילות העסקית, מה שיפגע ביכולת לעבודה עם לקוחות גדולים, ויפגע באטרקטיביות של החברות הישראליות בתחום האזרחי. נציין בהקשר הזה כי כבר כיום נשמעת

[9] סעיף 3 ו' להחלטה

מחברות גלובליות התמיהה על כך שענייני היצוא בישראל מפוקחים על ידי משרד הביטחון בעוד שבמדינות רבות בעולם העניין מפוקח על ידי משרד החוץ או הסחר או הכלכלה כשם שראוי שיעשה. תמיהה זו מרימה לא פעם קשיים ומסבכת את העיסקאות בנושא היצוא במדינות שונות בעולם.

יב. **פגיעה בתחרות אל מול מתחרים עסקיים מהעולם** – יש חשש כבד שההחלה של הצו תביא לפגיעה ביכולת של החברות הישראליות להתחרות בצורה הוגנת מול המתחרים עסקיים בעולם שלא נתונים לצוים שכאלה. ניתן לומר שיש סיכוי שדווקא המתחריים של החברות הישראליות מאוד שמחים על פרסום טיוטת הצו. דוגמת ארה"ב.

יג. **פגיעה אנושה בחברות צעירות ובמשקיעים-** מדובר פה בפגיעה כלכלית ישירה, בודאות העסקית, ובקביעת עובדות בשטח על ידי גוף ממשלתי, חשוב ככל שיהיה, מבלי שבוצעה עבודת הכנה מתאימה. ההשפעה על עתידן של חברות צעירות יכולה להיות מוחלטת (בעוד שהגדולות, ימצאו את הדרך להתמודד, ויש להם יותר משאבים לכך).

יד. **בחינת אלטרנטיבות-** רבים שואלים האם משרד הבטחון ואפ"י הם הגוף המתאים לביצוע הפיקוח? האם ראוי להחיל את חוק הפיקוח על הייצוא הבטחוני שבמקור נועד לטפל בתחומים מאוד ספציפיים, על תחום הסייבר, שהוא מורכב יותר, טכנולוגי יותר, אשר עיקר התפוצה שלו היא דווקא בשוק האזרחי ולא הבטחוני? האם נבחנו אלטרנטיבות? האם לא ראוי שדווקא משרד הכלכלה יהיה אחראי על "ההגבלות החדשות על הייצוא", אם בכלל הן נדרשות. בהקשר לזה נציין כי ההליך במשרד הכלכלה אמור להיות קצר יחסית, ויעיל יותר תוך חיסכון בעלויות רבות: הגשת הבקשה הינה דיגיטלית הניתנת לעשייה אף מבית הלקוח או מכל מקום אחר ובכל שעה; אישור הבקשה ומתן הרישיון נעשה בתוך 5 ימים מיום הגשת הבקשה ובאופן דיגיטלי.

7. **בשל כל האמור לעיל אנו מבקשים בזאת שהצו המוצע על ידי אפ"י ועל ידי מטה הסייבר הלאומי ייגנז, ווישתוקם הועדה המשותפת לרגולטור ולתעשיה ושתגובש תכנית מסודרת יותר וברורה יותר, אשר ד תגן על האינטרסים של מדינת ישראל ללא כל פשרה, ומבלי שהמשך התפתחותה של תעשית הסייבר הישראלית וההובלה שלה תפגע. .**

בכבוד רב,

שם חברה _____

מנכ"ל _____

מסמך זה חובר על ידי ובשיתוף חברים ב-Cyber Together (בינהם: נציגי חברות סייבר, ועורכי דין), ונערך בשיתוף עם <u>עו"ד אדמית אבגי</u>, בעלת משרד עורכי-דין, AI-LAW, מתמחה במשפט טכנולוגיה, סייבר ומידע וחוקרת במרכז מינרבה ובסדנת יובל נאמן באוניברסיטת תל- אביב שמחקריה מתמקדים ברגולציה ותקינה, לאומית ובינאלומית בתחום הסייבר.