



HERZOG FOX & NEEMAN
LAW OFFICE



Life Sciences Compliance Forum II

אתגרים והזדמנויות לתעשיית מדעי החיים
לאור ההתפתחויות ברגולציות הפרטיות בעולם

אריאל יוספי, שותף
ראש מחלקת הטכנולוגיה והרגולציה

דצמבר 2018

עידן המידע ו"אובדן הפרטיות"

החשיבות והרלוונטיות של דיני פרטיות המידע

- 90% מכל המידע הרשום בעולם נוצר בשנתיים האחרונות
- 2.5 קווינטיליון (2,500,000,000,000,000,000) – מספר הבייטים של מידע שאנו מייצרים בכל יום
- גודל המידע שנוצר משחר ההיסטוריה ועד 2003 = המידע שאנו מייצרים בכל יום
- אנו משתמשים יותר באינטרנט, באמצעות יותר ממשקים, עבור יותר מטרות

PINTEREST
USERS PIN

3,472
images.

YOUTUBE
USERS UPLOAD
72 HRS.
OF NEW
VIDEO.

EMAIL
USERS SEND
204,000,000
MESSAGES.

Google
RECEIVES OVER
4,000,000
SEARCH
QUERIES.

FACEBOOK
USERS SHARE
2,460,000
PIECES OF CONTENT.

TINDER
USERS SWIPE
416,667
TIMES.

WHATSAPP
— USERS SHARE —
347,222
PHOTOS.

TWITTER USERS
TWEET
277,000
TIMES.

INSTAGRAM
USERS »
POST
216,000
NEW PHOTOS.

AMAZON
MAKES
\$83,000
IN ONLINE SALES.

PANDORA
USERS LISTEN TO
61,141
HOURS OF
music.

APPLE USERS
DOWNLOAD
48,000
apps.

YELP USERS
POST
26,380
REVIEWS.

SKYPE
USERS
CONNECT FOR
23,300 HOURS.

VINE
USERS
SHARE
8,333
VIDEOS.

EVERY
MINUTE
OF THE
DAY



על מה הדרמה?

מקרי אכיפה משמעותיים

מידע = כסף

איבוד מידע = איבוד כסף

על מה הדרמה?

מקרי אכיפה משמעותיים

דלף מידע רפואי רגיש בקנה מידה משמעותי [ארה"ב, 10.2018]

- בשורה של מתקפות סייבר על חברת הביטוח Anthem בין דצמבר 2014 וינואר 2015, נפרצו מערכות החברה ודלפו רשומות רפואיות של כמעט **79 מליון מבוטחים**
- נמצא כי החברה לא עמדה כראוי בדרישות הגנת המידע הרפואי על פי ה-HIPAA
- התוצאה: הסכם פשרה בגובה שיא של **\$16,000,000 קנס** ותכנית לתיקון הכשלים
- [\[קישור\]](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

דלף מידע רפואי רגיש בקנה מידה רחב [ארה"ב, 8.2016]

- 4 מחשבים ניידים נגנבו מבנייני בית-חולים, וגרמו לדליפת **מידע רפואי רגיש של 4 מיליון מטופלים** בקירוב
- לאחר-מכן - 2 אירועים נוספים שגרמו לדליפת מידע רפואי רגיש של אלפי מטופלים נוספים
- התוצאה: **\$5,550,000 קנס** ותכנית לתיקון הכשלים
- [\[קישור\]](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

חשיבות כלי שליטה ובקרה על הגישה למידע בתוך הארגון [ארה"ב,
2.2017]

- עובדים של רשת בתי-חולים ניגשו בצורה בלתי-מורשית, באמצעות **שם משתמש וסיסמה של עובד לשעבר** ממכון רפואי אחר ברשת, למידע רפואי של למעלה מ-**110,000 מטופלים**
- המידע אף נחשף באופן בלתי-מורשה בפני **צוות עובדים של מכון רפואי אחר ברשת**
- התוצאה: **\$5,500,000 קנס** ותכנית לתיקון הכשלים
- [\[קישור\]](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

זמינות מידע רפואי אלקטרוני במנועי חיפוש, והעדר אמצעי אבטחה
הולמים [ארה"ב, 5.2014]

- רופא המועסק באוניברסיטה ומפתח עבודה ועבור בית-חולים יישומים, ניסה להשבית שרת מחשב אישי בו נמצא מידע רפואי של מטופלי בית-החולים

- עקב העדר אמצעי אבטחה טכניים לשרת, ההשבתה גרמה **למידע הרפואי של 6,800 מטופלים** להיות נגיש במנועי החיפוש באינטרנט

- התוצאה: **\$4,800,000 קנס** ותכנית לתיקון הכשלים

- [קישור](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

דלף מידע רפואי בעקבות גניבת מחשב נייד, ונהלי אבטחת מידע לקויים [ארה"ב, 3.2016]

- מחשב נייד של מכון מחקר רפואי, בו **מידע רפואי אלקטרוני על 13,000 מטופלים ומשתתפים במחקר**, נגנב מרכב של עובד

- **נהלי האבטחה של החברה היו לקויים**. למשל: נוהל גישה למידע רפואי על-ידי עובדי המכון, ונוהל הכנסת והוצאת מחשבים ניידים המכילים מידע רפואי מן המתקנים של מכון המחקר

- **לא הותקנו מנגנוני הגנה על ציוד אלקטרוני** אשר נרכש לא בהליך הסטנדרטי

- התוצאה: **\$3,900,000 קנס** ותכנית לתיקון הכשלים

- [קישור](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

אי-נקיטת צעדים לתיקון כשלים, ושימוש בסיסמאות פשוטות
[ארה"ב, 7.2016]

- אוניברסיטה היתה מודעת לסיכונים ונקודות התורפה במערכות שלה שנים רבות, אולם לא נקטה פעילות משמעותית לניהול סיכונים במשך אותו זמן

- פעלה רק לאחר אירוע דלף מידע שפגע ב-10,000 יחידים בקירוב

- היתה אפשרות לגישה בלתי-מורשית לכונן רשת שהכיל מידע רפואי רגיש דרך הרשת האלחוטית באוניברסיטה, היות שנעשה שימוש בשם משתמש וסיסמה גנריים

- התוצאה: **\$2,750,000 קנס** ותכנית לתיקון הכשלים

- [קישור](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

העדר בקרות בנוגע לניהול מידע, מינוי קצין ציوت, וקבלת הסכמה מנושאי המידע [גרמניה, 12.2014]

- נציגי מכירות בחברת ביטוח השיגו מידע (כתובת מגורים) באופן לא מורשה אודות עובדים אשר עתידים להיקלט במגזר הציבורי, במטרה לשווק להם מוצרי ביטוח לאחר שייקלטו

- הבקרות והנהלים הפנימיים של החברה בנוגע לניהול ואבטחת מידע היו לקויים

- התוצאה: € 1,300,000 קנס וחובת מינוי קציני ציוט

- [קישור](#)

על מה הדרמה?

מקרי אכיפה משמעותיים

חשיפת כתובות דואר אלקטרוני ושמות של מטופלים דרך הפצת עדכוני לקוחות [אנגליה, 5.2016]

- בית-חולים שלח עדכון לקוחות בדואר אלקטרוני לכ-700 מטופלים המקבלים טיפול ל-HIV. העדכון נשלח כאשר כתובות הדואר האלקטרוני והשמות של כל המטופלים הוזנו בטעות בשדה "אל" (ולא בצורה מוסתרת) באופן שהיו חשופים לכל הנמענים להודעה

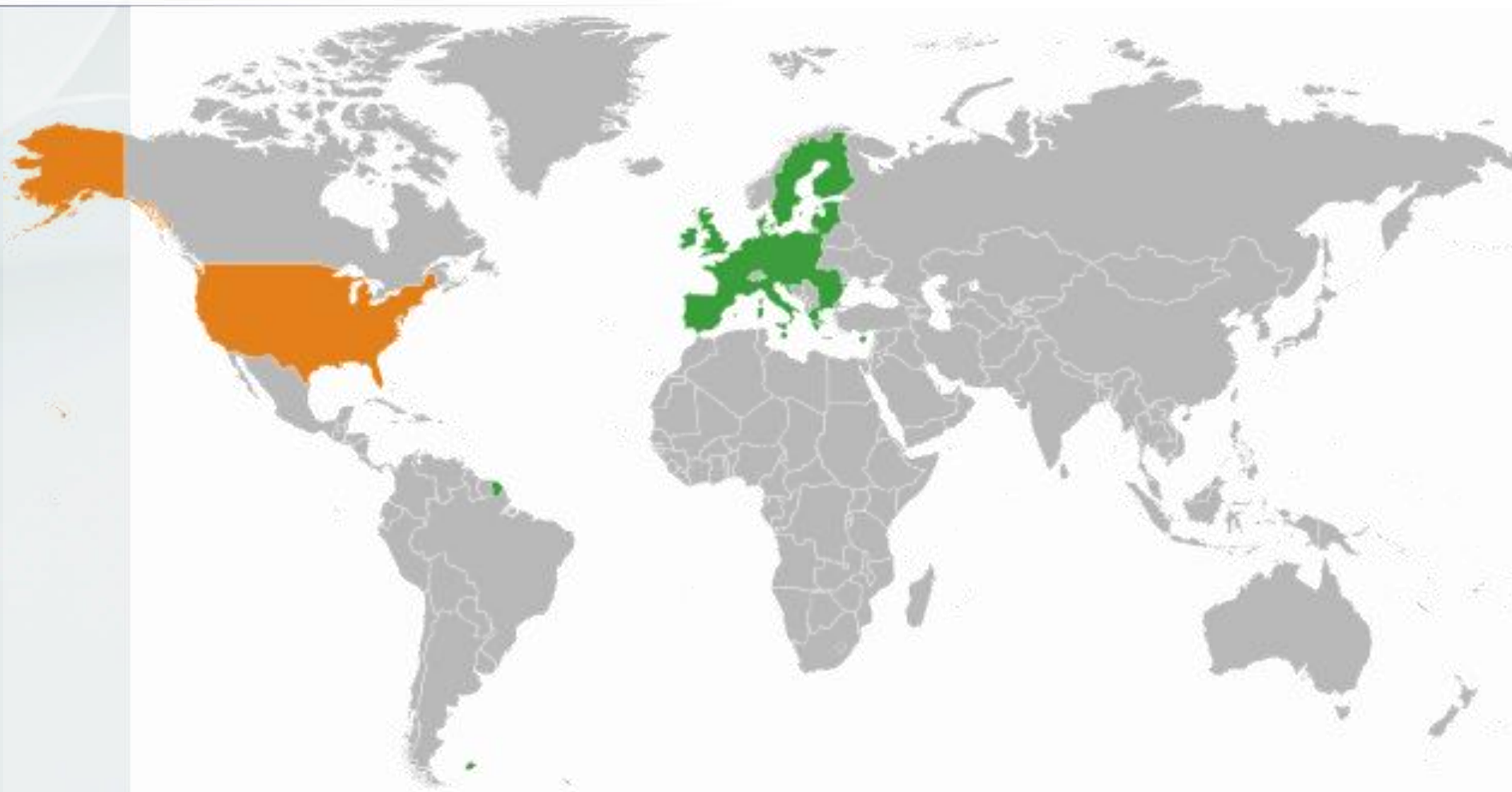
- בית-החולים לא עדכן את המטופלים בנוגע לאפשרות כי ייעשה שימוש בכתובות הדואר האלקטרוני שלהם לשליחת עדכוני לקוחות בתפוצה רחבה

- התוצאה: **£ 180,000 קנס**

- [\[קישור\]](#)

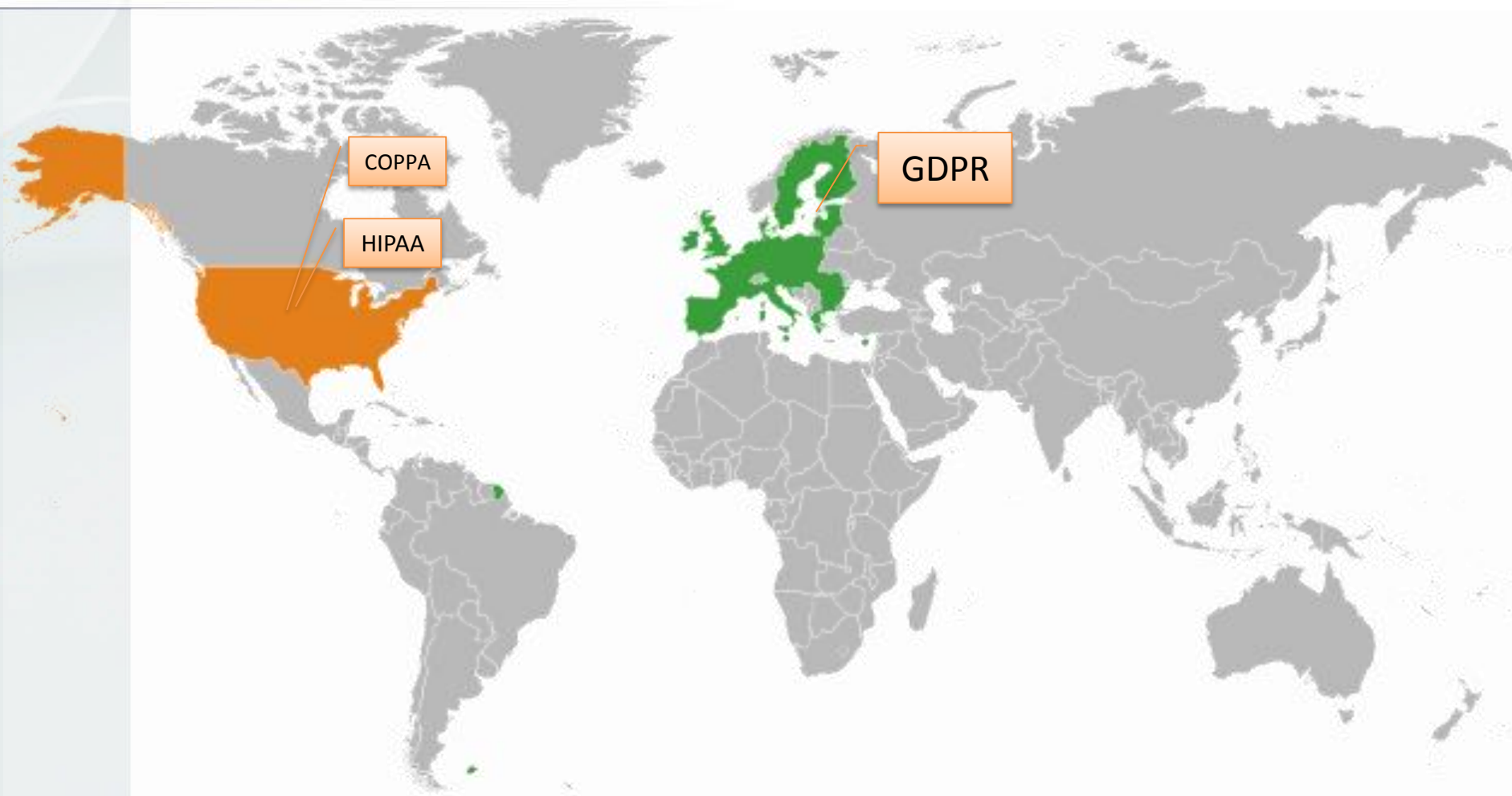
פקעת רגולטורית

שינויים רגולטוריים ברחבי העולם



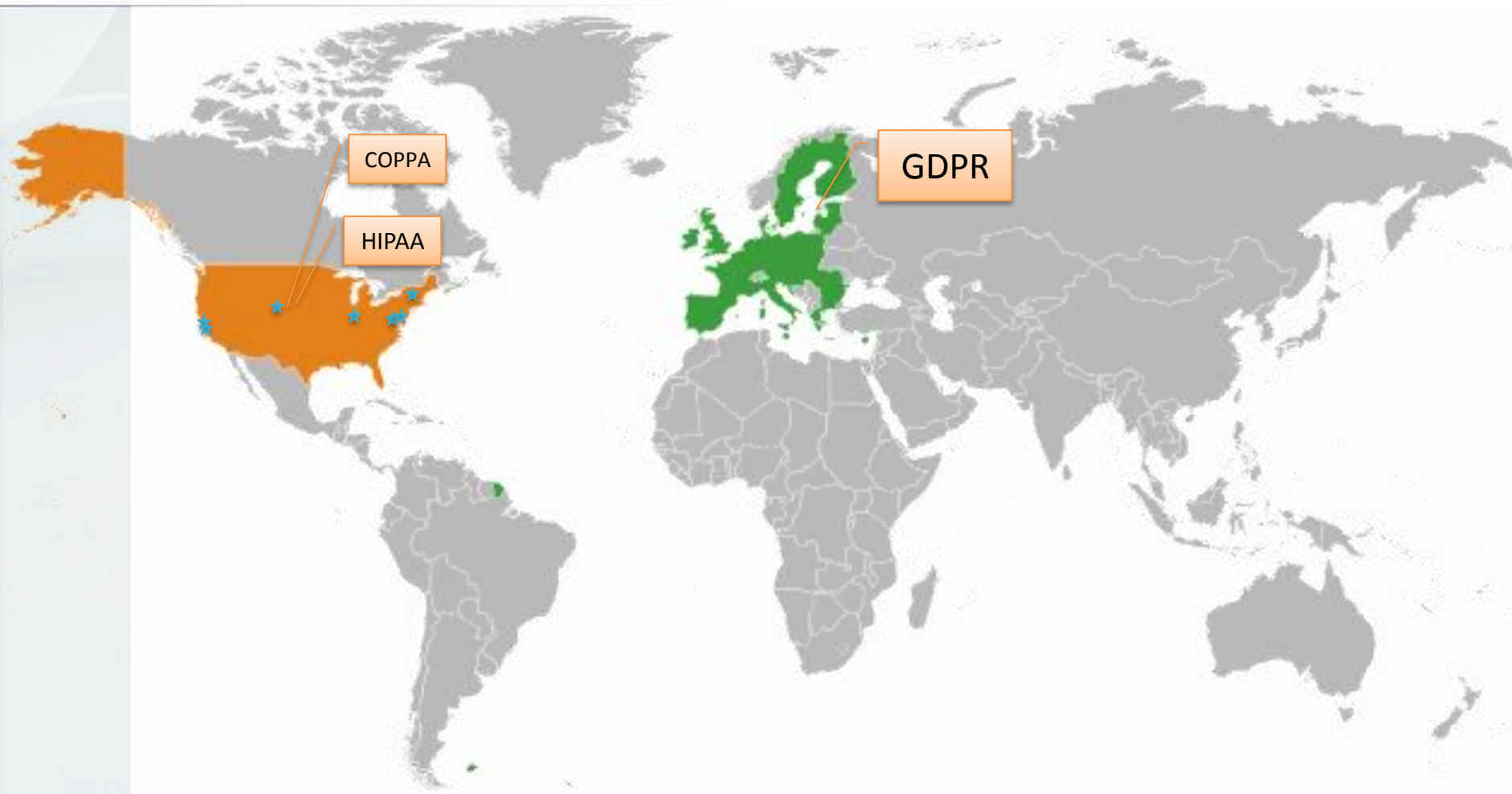
פקעת רגולטורית

שינויים רגולטוריים ברחבי העולם



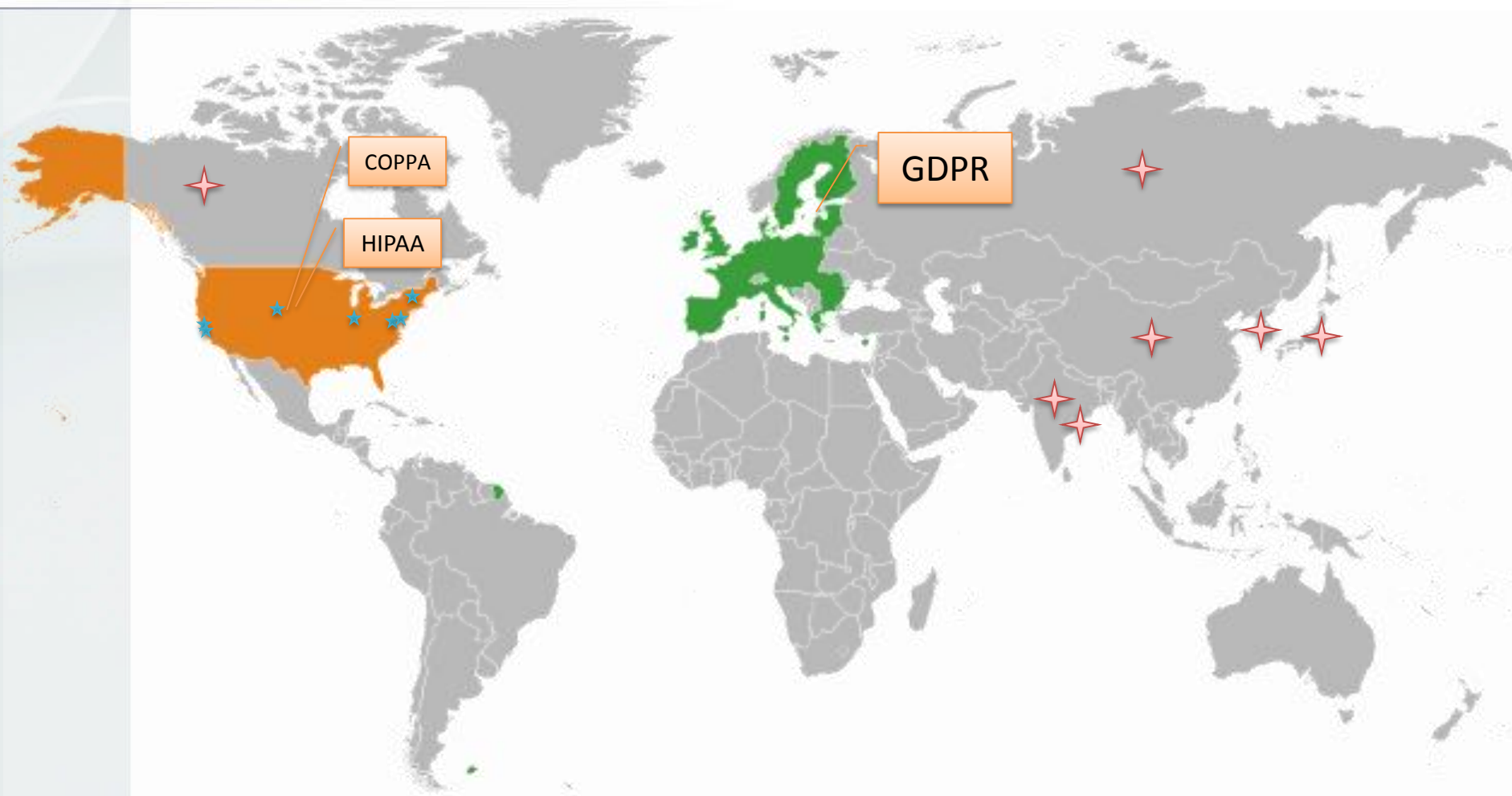
פקעת רגולטורית

שינויים רגולטוריים ברחבי העולם



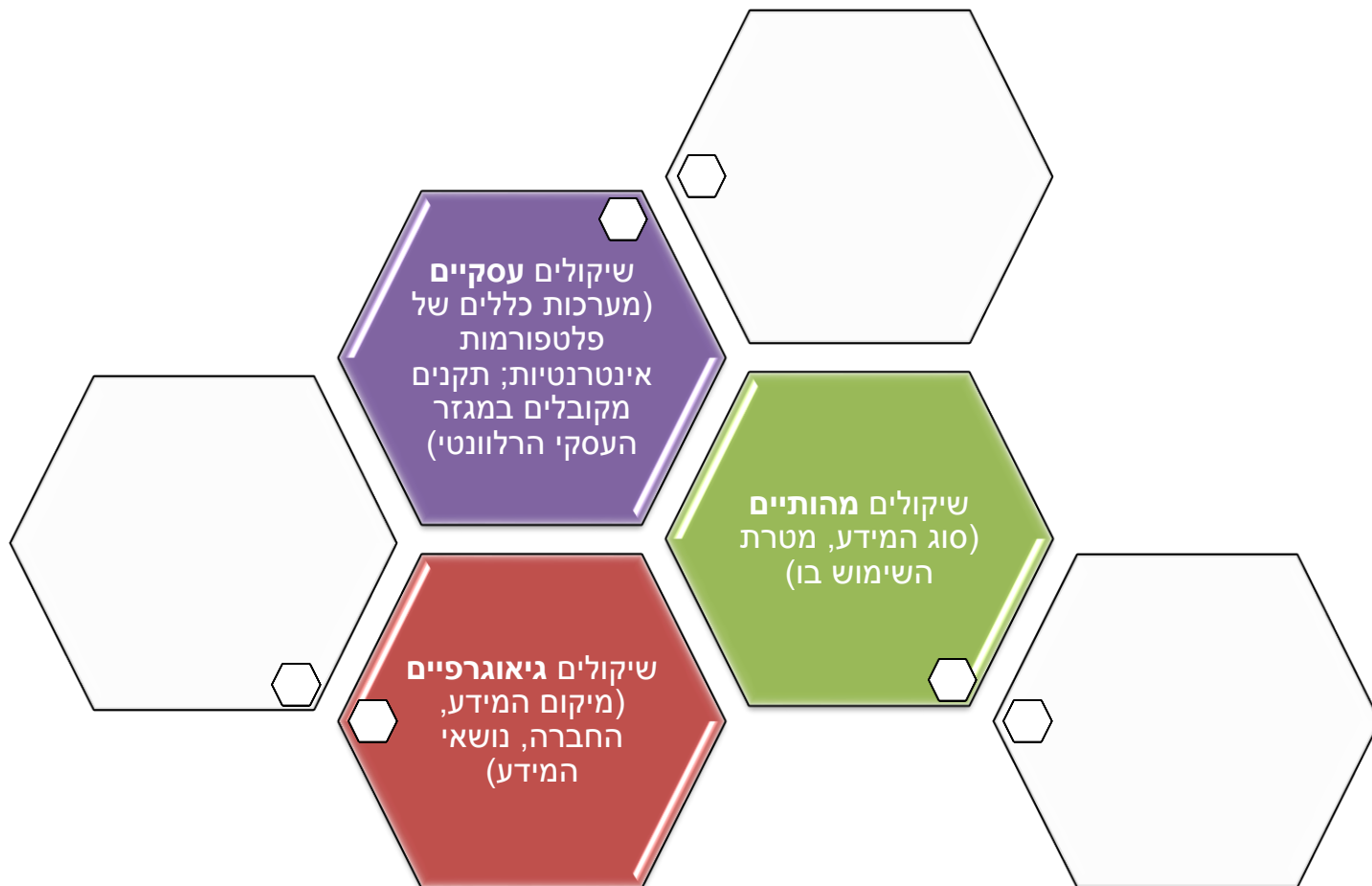
פקעת רגולטורית

שינויים רגולטוריים ברחבי העולם



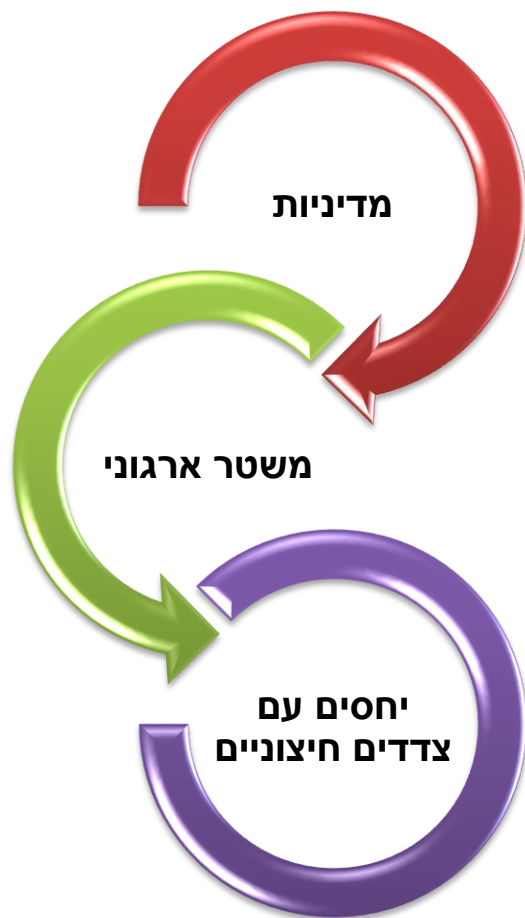
פקעת רגולטורית

מערכת השיקולים לא מוגבלת להיבטים הטריטוריאליים



להתיר את הפקעת

דרישות מפתח עיקריות



- לגיטימיות איסוף המידע
- מדיניות הטיפול במידע
- שמירה על המידע

- אחריות מרוכזת
- פיקוח
- ביקורת ובקרה

- הנחיות והתחייבויות חוזיות
- ממשקים מול נושאי המידע (שקיפות)
- העברה למדינות אחרות

להתיר את הפקעת

מדיניות שמירת פרטיות

לגיטימציה לאיסוף המידע

- הסכמה
- הצדקה אחרת (חוזית, מהותית)

הגבלות על שימוש והעברה

- הגבלת השימוש במידע למטרות שהצדיקו את איסופו
- הגבלת זמן שמירת המידע למטרות הנדרשות ולאילוצים חוקיים אחרים
- העברה לגורמים שלישיים בצמידות למטרות האיסוף ותוך שמירה על רמת הגנת המידע

שמירה על המידע ואיכותו

- איכות, דיוק, נכונות, אמיתות ורלוונטיות המידע
- אבטחת המידע (אמצעים מנהליים, פיסיים וטכנולוגיים)
- מדיניות במקרה של דליפת מידע

זכויות נושאי המידע

- הגבלה על שימוש
- עיון, עדכון ומחיקה

להתיר את הפקעת

משטר ארגוני



להתיר את הפקעת

יחסים עם צדדים חיצוניים

