

Supplier Control Obligation (SCO)

ניבול פיקוח – דרישות

אבטחת מידע, אבטחת סייבר ואבטחה פיזית, טכנולוגיה, תכנון התאוששות,
פרטיות נתונים, ניהול נתונים ו-EUDA

MC 1.0 – פיקוח ואחריות

על הספק ליישם מסגרת מבוססת ועקבית בהתאם לתקני התעשייה עבור תחומי טכנולוגיית המידע (IT), אבטחת טכנולוגיית המידע, אבטחה פיזית, תכנון תהליכי התאוששות, ניהול נתונים וניהול מידע אישי (פרטיות נתונים/הגנה על נתונים), פיקוח (תקני NIST, ISO/IEC 27001, COBIT, BS10012, SSAE, ITIL, 18) או מסגרת תקנית דומה המדגימה את שיטות העבודה המומלצות בתעשייה, כדי להבטיח שאמצעי ההגנה או תהליכי ההתמודדות הנאותים המוטמעים בתהליכים, בטכנולוגיות ובסביבות הפיזיות שלו מתועדים ככאלה הפועלים באופן יעיל. עליו לוודא שתוכנית פיקוח מבוססת וכלל ארגונית מבטיחה שכל המסגרות בהקשר של זמינות, שלמות וסודיות נתמכות באופן מלא באמצעות יישום של אמצעי פיקוח הולמים. עליהם לצמצם או להפחית את רמות הסיכון לאובדן, הפרעה או השחתה של מידע. בנוסף, על הספק לוודא שכל אמצעי הפיקוח הנדרשים על ידי Barclays מיושמים ופועלים באופן יעיל כדי להגן על השירותים המסופקים ל-Barclays.

יש ליישם מסגרת פיקוח שחייבת לכלול אמצעי הגנה מנהליים, טכניים ופיזיים שמיועדים להגן על נכסים ומידע/נתונים מפני אובדן, חשיפה, שינוי או הרס מכוון ו/או מפי תאונה, גנבה, שימוש בלתי מורשה או בלתי הולם וכן מפני גישה, שימוש או חשיפה בלתי מורשים.

תוכנית הפיקוח והאחריות חייבת לכלול, אך אינה מוגבלת, את כל התחומים הבאים:

- כללי מדיניות פיקוח – סדרה של כללי מדיניות פיקוח שתוגדר ותאושר על-ידי ההנהלה, תפורסם ותימסר לעובדים של הספק ולכל צד רלוונטי ואף תישמר ותתעדכן מעת לעת.
 - כללי מדיניות, נהלים ותוכנית רגילה שיוצרים, מיישמים ומוודאים באופן רצוף ויעיל את רמת היעילות של המדיניות והתקנים המיושמים.
 - תוכנית פיקוח מקיפה שכוללת מבנה מנהיגות ברור, מפקחת על ידי ההנהלה הבכירה ונועדה להנחיל תרבות ארגונית שבבסיסה אחריות ומודעות.
 - תקשורת ומתן מידע רצוף אודות כללי מדיניות ונהלים מאושרים לכל עובדי הארגון.
 - התאמת הדרישות המשפטיות לכללי המדיניות ולשיטות העבודה, הגנה מוטמעת על נתונים ואמצעי פיקוח אחרים שמיועדים להבטיח שכללי המדיניות והתהליכים מיושמים באופן יעיל
- כללי המדיניות לכל תחומי הדומיין ייבחנו במרווחי זמן קבועים או במקרים של שינויים משמעותיים, כדי לוודא קיום של התאמה ויעילות רצופות.
 - על הספק לוודא כי כללי המדיניות והנהלים/התקנים נבדקים באופן שגרתי (לפחות פעם בשנה או במקרה של שינוי מהותי, המוקדם מביניהם).
 - על הספק למנות גורם (או גורמים) מנוסה ומוסמך/צוות שעמו Barclays יכולה לקיים קשר רציף לגבי דרישות SCO, כולל אבטחה פיזית ואבטחת מבנים, אבטחת מידע ואבטחת סייבר, כמו גם ניהול מידע אישי (פרטיות נתונים/הגנה על נתונים), תכנון תהליכי התאוששות, ניהול נתונים וקביעה מי אחראי על מה, הבטחה כי דרישות הפיקוח של Barclays או של הספק מיושמות ומנטרות באופן יעיל.
 - הספק חייב להתאים תפקידים ותחומי אחריות לעובדים שמיישמים, מנהלים ומפקחים על רמת היעילות של אמצעי הפיקוח על כוח האדם הארגוני וכן על קבלני משנה/מעבדי משנה.
- על הספק להטמיע תשתית מאובטחת ומסגרת פיקוח להתגונן כהלכה מפני כל איום (לרבות אבטחת סייבר)
- על הספק ליישם תוכנית ביקורת עצמאית כדי לבדוק אם אמצעי הפיקוח מיושמים, נשמרים ומתבצעים כהלכה פעם בשנה לפחות.

הנחיות עבור לקוח שירותי ענן (ספק)

מדיניות אבטחת מידע עבור מחשוב ענן צריכה להיות מוגדרת כמדיניות ספציפית העוסקת בלקוחות של שירותי הענן. מדיניות אבטחת המידע עבור לקוחות של שירותי הענן העוסקת במחשוב ענן צריכה להיות עקבית ובהתאם לרמות סיכוני האבטחה המקובלות בארגון בהקשר של המידע והנכסים האחרים שבבעלותו/ברשותו. בעת הגדרת מדיניות אבטחת המידע עבור מחשוב ענן, על לקוח של שירותי הענן לבחון את הנושאים הבאים:

- מידע המאוחסן בסביבת מחשוב ענן עשוי להיות כפוף לגישה ולניהול של ספק שירותי הענן.
- נכסים יכולים להישמר בסביבת מחשוב ענן, כגון אפליקציות.
- ניתן להפעיל תהליכים עבור שירותי ענן וירטואליים ומרובי דיירים.
- משתמשי שירותי הענן וההקשר שעל פיו הם משתמשים בשירותי הענן.
- מנהלי המערכת של שירותי הענן מקבלים גישה מועדפת ללקוח שירותי הענן.
- האתרים הגאוגרפיים של ספק שירותי הענן והמדינות שבהן הוא יכול לאחסן את נתוני הלקוחות של שירותי הענן (כולל אחסון זמני).

מדיניות האבטחה הרלוונטית של לקוח שירותי הענן צריכה לזהות את ספק שירותי הענן כסוג של ספק ולנהל אותו בהתאם למדיניות האבטחה. המטרה היא לצמצם את הסיכונים הנובעים מגישה וניהול של נתוני לקוחות שירותי ענן הקשורים לספק שירותי ענן.

על לקוח שירותי הענן לשקול ולבחון מהם החוקים והתקנות הרלוונטיים בתחומי שיפוט המסדירים את פעילותו של ספק שירותי הענן, בנוסף לאלה המסדירים את שימוש של הלקוח שירותי הענן. על לקוח שירותי הענן לקבל ראיות לכך שספק שירותי הענן עומד בכל התקנות והתקנים הרלוונטיים הנדרשים בהקשר של פעילותו העסקית של לקוח שירותי הענן. ראיות כגון אלה יכולות להיות גם עדויות/אישורים המופקים על ידי מבקרים חיצוניים שהם צדדים שלישיים.

על הספק להודיע ל-Barclays בכתב ומוקדם ככל האפשר מבחינה חוקית אם הוא נמצא בתהליך של מיזוג, רכישה או כל שינוי בעלות אחר.

MC 2.0 – ניהול סיכונים

על הספק לקיים תוכנית ניהול סיכונים שמבצעת הערכות, תיקונים וניטור של סיכונים באופן יעיל, בכל הסיביות שבשליטת הספק.

תוכנית ניהול הסיכונים חייבת לכלול, בין היתר, את התחומים הבאים:

- על הספק ליישם מסגרת ניהול סיכונים הולמת ומאושרת (כגון, מידע אישי, אם עיבוד נתוני PI, מידע, סייבר, פיזי, טכנולוגיה, תוכנית נתונים והתאוששות), תוך יכולת להדגים את שילובה במסגרת האסטרטגיה העסקית
- בהתאם למסגרת ניהול הסיכונים, יש לבצע הערכות סיכון רשמיות לפחות מדי שנה או במרווחי זמן מתוכננים, תוך שימוש בגישה מבוססת סיכונים או לוודא שהיא מופעלת על בסיס אירועים, למשל, בתגובה לאירוע או מקרי עבר שנלמדו, בשילוב עם כל שינוי שמתבצע במערכות המידע או במרחב הפיזי, כגון מבנים או חללי עבודה, כדי לקבוע מהן הסבירות וההשפעה של כל סיכון שזוהה, תוך שימוש בשיטות מבוססות איכות וכמות. הסבירות וההשפעות הכרוכות בסיכונים מובנים ושיוריים ייקבעו באופן עצמאי, בהתחשב בכל קטגוריות הסיכון (כגון תוצאות ביקורת, ניתוח איומים ונקודות חולשה, ציות לתקנות).
- קובעת ומתחזקת את קריטריוני הסיכון הכוללים:
 - קריטריון לקבלת סיכונים, וכן

- קריטריונים לביצוע הערכות סיכונים,
 - מזהה את הסיכונים:
 - החלת תהליך הערכת הסיכונים על מנת לזהות סיכונים בהקשר של אובדן סודיות, פגיעה ברמת היושרה ופגיעה בזמינות לקבלת מידע בהיקף של מסגרת הסיכון, וכן
 - זיהוי בעלי הסיכון,
 - מנתחת את הסיכונים:
 - הערכת ההשלכות הפוטנציאליות במקרה של זיהוי סיכונים,
 - הערכת הסבירות הראלית להתרחשות סיכונים שזוהו, וכן
 - קביעת רמת הסיכון
 - מעריכה את הסיכונים:
 - השוואת בין תוצאות ניתוח הסיכונים לקריטריוני הסיכונים שנקבעו, וכן
 - קביעת סדרי עדיפויות של הסיכונים המנותחים לצורכי טיפול בסיכונים
 - טיפול בסיכונים:
 - יש לבחור אפשרויות הולמות להתמודדות נאותה עם סיכונים, תוך התחשבות בתוצאות הערכת הסיכונים,
 - יש לקבוע את מהם אמצעי הפיקוח הדרושים ליישום אפשרות שנבחרה להתמודדות עם הסיכונים,
 - יש להפיק הצהרת יישום שכוללת את אמצעי הפיקוח הדרושים ואת ההצדקה להכלה, בין אם הם מיושמים ובין אם לאו
 - על הספק לוודא כי הסיכונים שזוהו ימזערו או יוסרו מהסביבה באמצעות תיעודף הסיכון ויישום אמצעי נגד. על הספק לנטר ללא הרף את אמצעי הנגד כדי לוודא שהם יעילים.
 - על הספק לבצע הערכת סיכונים לפחות פעם בשנה בהקשר של מידע, סייבר, אבטחה פיזית, ניהול מידע אישי (פרטיות נתונים/הגנה על נתונים) ותכנון התאוששות. בהתאם לסביבות ספציפיות עם איזמים קיימים ומתפתחים, על הספק לשקול מסגרת ביצוע הערכות תכופה יותר.
 - יש לבצע הערכה לפחות פעם בשנה באתרים קריטיים מבחינה תפעולית בהקשר של תהליכים/שירותים המסופקים ל-Barclays (לרבות מרכזי נתונים)
 - הארגון ישמור מידע מתועד אודות תהליך הערכת הסיכונים בהקשר של אבטחת מידע.
 - הערכות סיכונים הקשורות לדרישות הפיקוח על נתונים (לרבות מידע אישי, אם מתבצע עיבוד של נתוני PI) חייבות להתחשב בנושאים הבאים:
 - סיווג נתונים והגנה מפני שימוש, גישה, אובדן, הרס וזיוף בלתי מורשים.
 - מודעות לאחסון נתונים ורהעברתם בין יישומים, מסדי נתונים, שרתים ותשתיות רשת.
 - ציות לתקופות שמירה מוגדרות ולדרישות למחיקה בתום מחזור החיים.
 - על הספק לפעול כבקר או כמעבד נתונים ולהעריך את רמת הסיכון האפשרית לפרטיות בעת ביצוע עיבוד של כמויות גדולות או רגישות של נתונים של Barclays כדי לוודא שכל שינוי באופי הטיפול/העיבוד המתבצע בנתונים של Barclays אינו מהווה סיכון לפרטיות
 - על הספק לפתח וליישם את מבנה הפיקוח הארגוני כדי לאפשר הבנה רצופה של סדרי העדיפויות בארגון בהקשר של ניהול סיכונים עם מודעות לסיכוני פרטיות

MC 3.0 – תפקידים ותחומי אחריות

על הספק אחראי לוודא שכל עובדיו, לרבות, אך לא מוגבל לקבלנים, קבלני משנה, מעבדי משנה המעורבים במתן שירות ל-Barclays, מודעים לדרישות הפיקוח של Barclays ומצייתים להן. על הספק לוודא הקמה של צוות מומחים ו/או גורמים בעלי כישורים הולמים, תפקידים ותחומי אחריות מוגדרים לצורכי תמיכה ו/או לניהול דרישות הפיקוח של Barclays, שיפעל באופן יעיל כדי להגן על השירותים שמוענקים ל-Barclays.

על הספק להגדיר ולספק מידע לגבי תפקידים ותחומי אחריות כדי לספק תמיכה הולמת לדרישת הפיקוח של Barclays. יש לבדוק את התפקידים ותחומי האחריות באופן קבוע (ובכל מקרה, לא פחות מפעם ב-12 חודשים) ולאחר ביצוע כל שינוי מהותי במודל התפעולי או באופי הפעילות העסקית של הארגון.

הספק אחראי לוודא שעובדיו, הקבלנים, קבלני המשנה/מעבדי המשנה שהוא מעסיק מכירים את דרישות הפיקוח של Barclays ומצייתים לאמור בכללי המדיניות ובתקן ז. על הספק למנות גורם שתפקידו ליצור קשר עם Barclays במקרה של הסלמות הנובעות מאי ציות לדרישות הפיקוח. יש לשלוח דרישות חוזיות ספציפיות בכתב אל קבלני המשנה/מעבדי המשנה של הספק.

הנחיות עבור לקוח שירותי ענן (ספק)

על לקוח שירותי הענן להסכים עם ספק שירותי הענן על הקצאה הולמת של תפקידים ותחומי אחריות לצורכי אבטחת מידע ולאשר כי כל גורם כזה יכול לאיש את התפקיד ולקיים את תחומי האחריות שהוקצו לו. יש לציין את התפקידים ואת תחומי האחריות של שני הצדדים במסגרת הסכם. על לקוח שירותי הענן לזהות ולנהל את הקשר העסקי עם שירות הלקוחות ופונקציית הטיפול של ספק שירותי הענן.

על לקוח שירותי הענן להגדיר או להרחיב את המדיניות והנהלים הקיימים שלו, בהתאם לאופן השימוש בשירותי הענן ואף להדריך את משתמשי שירותי הענן בארגון שלו לגבי תפקידים ותחומי האחריות שלהם בעת שימוש בשירותי הענן.

MC 4.0 – הדרכה ומודעות

על הספק להפעיל תוכנית הכשרה להגברת המודעות באופן קבוע לכל עובדיו, לרבות קבלנים, שכירים המועסקים לטווח קצר ויועצים. על כל העובדים של הספק שעובדים בשביל השירותים של Barclays ו/או ניגשים לנתונים/למידע או לנכסים פיזיים אחרים לקבל הדרכה מתאימה ועדכונים שוטפים לגבי המדיניות, התהליכים והנהלים הארגוניים הקשורים לתפקוד המקצועי שלהם בארגון. על רמות ההכשרה והמודעות להכין את עובדי הספק כדי שיוכלו לבצע את תפקידיהם באופן מאובטח ולהבטיח כי הם מבינים את תחומי האחריות שלהם בעת גישה או עיבוד של נתוני Barclays, כולל מידע אישי. יש לתעד את רשומות התוכנית שמתבצעת בפלטפורמת ניהול למידה מתאימה או באופן ידני.

על הספק חייב לוודא שכל עובדיו ישלימו הכשרות חובה והדרכות בנושא אבטחה, אשר יכללו אבטחת סייבר, אבטחה פיזית, תכנון תהליכי התאוששות, ניהול מידע אישי (פרטיות נתונים/הגנה על נתונים), ניהול נתונים, IT, EUDA והגנה על נתוני Barclays, לא יאוחר מפרק זמן של **חודש אחד ממועד ההצטרפות** לארגון ו/או בעת הצטרפותם של עובדים כאלה למסגרות שעוסקות בשירותים המוענקים ל-Barclays. בנוסף להכשרת רענון מדי שנה, על הספק לוודא שעובדי הספק מבינים את אחריותם ומודעים לסיכונים שקשורים לנתונים של Barclays, לחוקים ולתקנות הרלוונטיים וכן לגורמים אחרים שעשויים להשפיע על הביצועים או לסכן את הבנק. יש לתעד כל הכשרה ומשודרת עבור כל עובדי הספק שעוסקים בשירותים המוענקים ל-Barclays לפי דרישה.

על הספק לוודא שתוכנית ההכשרה והמודעות כוללת מעקב אחר נושאי אבטחת סייבר – הנדסה חברתית ואיומים פנים ארגוניים, מומלץ שהספק יבצע בדיקות הדמיה של מתקפות הנדסה חברתית באמצעות טכניקות כגון בדיקות הדמיה של פעילויות דיג עבור כל עובדי הארגון, לרבות ניטור רצוף שנועד לוודא שאיום הגלום בסיכונים כגון אלה מובנים וכי בעיות שזוהו מטופלות ומתוקנות.

קבוצות בעלות סיכון גבוה, כגון כאלה עם גישה למערכות חסויות, עם גישה למרחב בסיכון גבוה או קריטי או עם גישה לפונקציות עסקיות רגישות (כולל משתמשים מורשים, לרבות מפתחים וגורמים המעניקים תמיכה, מנהלים בכירים, גורמי אבטחת מידע ובעלי עניין שהם צדדים שלישיים), נדרשות לעבור הכשרה בתחומי אבטחת ואבטחה פיזית, בהתאם לתפקידיהם ולתחומי האחריות שלהם.

כל העוסקים באבטחה פיזית, בין אם הם מועסקים על ידי הספק, בעלי נכסים או ספקים חיצוניים, מחייבים מסגרת חוזית, בין אם באמצעות קבלת אישורים, רישיונות של ספקי שירות מורשים בהתאם לחקיקה המקומית, וכשנדרש על פי סמכות שיפוטית, להחזיק ברישיון אישי המאפשר להם לעסוק במשימות אבטחה. גורמים העוסקים באבטחה פיזית נדרשים לעבור הכשרה בנושאי אבטחה, בהתאם לתפקידיהם ולתחומי אחריותם. יש לתעד כל הכשרה ולשתף את כל רשומות ההכשרה עם כל גורמי האבטחה ואף לאפשר בדיקה של Barclays, בהתאם לצורך.

על הספק לוודא שצוות העובדים המהווה צד שלישי ומקבל גישה לנתונים שמכילים מידע אישי כלשהו מודע לסיכונים פרטיות ומקיים את חובותיו ואת תחומי האחריות שלו, בהתאם למדיניות, לתהליכים, לנהלים, להסכמים ולערכי פרטיות ארגוניים קשורים. יש לתעד כל הכשרה ולשמור כל רשומה של הכשרה עבור כל צוות העובדים ואף לאפשר בדיקה של Barclays, בהתאם לצורך.

על הספק להכשיר עובדים לבצע את תפקידי ניהול הנתונים שלהם באופן יעיל (ניהול רכיבי נתונים קריטיים או יישומים המנוהלים על ידי צדדים שלישיים).

על ספק EUDA לזהות עובדים עם תחומי אחריות EUDA ולוודא שהם משלימים את ההכשרה והמודעות הדרושה למילוי תפקידם לפחות פעם בשנה ולהקפיד עד שמירת ראייה המוכיחה ציות לדרישות הפיקוח.

הנחיות עבור לקוח שירותי ענן (ספק)

על לקוח שירות הענן להוסיף את הפריטים הבאים לתוכנית המודעות, ההכשרה וההדרכה עבור מנהלי שירותי הענן, האחראים על שירותי הענן, משלבי המערכות של שירותי הענן ומשתמשי שירותי הענן, כולל עובדים וקבלנים רלוונטיים:

- תקנים ונהלים לשימוש בשירותי ענן.
- סיכונים אבטחת מידע הקשורים לשירותי הענן וכיצד יש לנהל סיכונים כאלה.
- סיכונים לסביבת המערכת ולסביבת הרשת בעת שימוש בשירותי ענן.
- שיקולים משפטיים ורגולטוריים רלוונטיים.

מודעות לאבטחת מידע, יש לספק תוכניות הכשרה והדרכה בנושא שירותי הענן למנהלים ולגורמים המפקחים, לרבות בעלי התפקידים האלה בכל היחידות העסקיות. מאמצים אלה מספקים תמיכה הולמת בתיאום יעיל של פעילויות אבטחת המידע.

MC 5.0 – ניהול תקריות

על הספק להחזיק מסגרת ניהול תקריות המנהלת, מכילה ומסירה/מפחיתה באופן יעיל תקריות ואת הסיבות שהובילו אליהן מסביבת הספק.

על הספק לקיים נוהל ניהול תקריות ומשברים הכולל את תהליך הסלמה של תקריות/משברים אל Barclays. על הספק לוודא כי צוותים ותהליכים שמיועדים לספק תגובה הולמת לתקריות/משברים נבדקים, לפחות פעם בשנה, כדי להוכיח כי הספק מסוגל להגיב לכל תקרית באופן יעיל ואפקטיבי. כמו כן, על הספק לבדוק את יכולתו לספק הודעה לגורמים הנוגעים לתקרית תוך מסגרת זמן מוגדרת מראש ולהדגים זאת ל-Barclays כשהוא מתבקש לעשות זאת.

על הספק לקיים תוכנית מתועדת היטב למתן תגובה לתקריות, שמגדירות תפקידים לעובדי הספק וכן שלבי ניהול תקריות ו/או טיפול בהן:

- אחריות ונהלים – על הספק ליצור תחומי אחריות ונהלים לטיפול על מנת להבטיח תגובה מהירה, יעילה ומסודרת במקרה של תקריות.
- דיווח על תקריות – תקריות חריגות ידווחו בערוצי הניהול המתאימים בהקדם האפשרי. כמו כן, על מנגנון הדיווח להיות קל ונגיש לכל העובדים והקבלנים של הספק.
- הערכת תקריות – על הספק להעריך תקריות על מנת לקבוע מהי רמת החומרה, מהו הסיווג ומהי התגובה הנדרשת.
 - סיווג תקריות – על הספק לקבוע סולם למיון תקריות ולהחליט אם יש לסווגן כתקריות. סיווג ותיעודן של תקריות יכולים לעזור לזהות את ההשפעה שלהן ואת היקפן.
- תגובה לתקריות – מקרים ייענו בהתאם לנהלים המתועדים לניהול תקריות שיצר הספק.
 - בלימה של תקריות – על הספק להפעיל עובדים, תהליכים ויכולות טכנולוגיות כדי לבלום במהירות וביעילות תקריות בסביבה העסקית שלו.
 - הסרת איומים/הגנה מפני איומים – על הספק להפעיל עובדים, תהליכים ויכולות טכנולוגיות כדי להסיר/למתן במהירות וביעילות איומי אבטחה ו/או את רכיביהם בסביבה העסקית שלו וממנה.
- הסקת מסקנות מתקריות – ידע שנרכש מניתוח ופתרון של תקריות ישמש להפחתת הסבירות או ההשפעה של תקריות בעתיד.
- איסוף ראיות – על הספק להגדיר וליישם נהלים לזיהוי, לאיסוף, לרכישה ולשימור של מידע, שיוכלו לשמש כראיות.

לאחר תקרית – בעקבות הפרעה לשירותים המסופקים ל-Barclays, יש לספק ל-Barclays דוח שלאחר התקרית לא יאוחר מארבעה שבועות קלנדריים מיום החזרת השירות לרמות תפעוליות רגילות. דרישות מינימליות של הדוח שלאחר תקרית:

- האירועים סביב המצב.
 - כיצד המשבר/התקרית נוהל.
 - ניתוח סיבת השורש למשבר/לתקרית.
 - אם התקרית מסווגת כ'אירוע סיכון' על-ידי הספק או Barclays (כלומר, היא נחשב משמעותית מספיק ולכן יש לדווח עליה/להעביר אותה לבעלי העניין הרלוונטיים, בהתאם למדיניות הרלוונטית שהספק מכיר).
 - אם מדובר ב'סיכון דפוס התנהגות' (למשל, אם הספק מטפל ישירות בלקוחות של Barclays).
 - כל תיקון הקשור ללקוחות של Barclays מוכר לספק,
 - שיפור מתמיד כדי למנוע התרחשות חוזרת, וכן
 - על הספק לנסות לקבוע כי פעילויות התגובה משופרות במידת האפשר באמצעות יישום לקחים שנלמדו מפעילויות הגילוי/התגובה הנוכחיות והקודמות.
- לצורכי תקשורת – על הספק למנות גורם שיעמוד בקשר עם Barclays במקרה של תקרית/משבר. על הספק לספק ל-Barclays את פרטי הקשר האישיים של הגורם הרלוונטי ועל כל שינוי בהם, כולל אמצעי קשר ומספרי טלפון מחוץ לשעות העבודה.

על הפרטים לכלול: שם, תחומי אחריות בארגון, תפקיד, כתובת דואר אלקטרוני ומספר טלפון

אם הספק מאשר במועד כלשהו שתקרית משפיעה על השירותים של Barclays, על המערכות של Barclays או על הנתונים של Barclays, על הספק להודיע על כך ל-Barclays באופן מיידי.

עם היוודע לספק על **תקרית סייבר**, לרבות באמצעות מתן הודעה מישות של Barclays, הספק יודיע על כך ל-Barclays באופן מיידי, אך בשום מקרה לא יאוחר מהנדרש על פי החוק החל או, אם אין דרישה כזו, לא יאוחר מ-**48 שעות** מרגע היוודע לראשונה אודות תקרית הסייבר באמצעות שליחת הודעה בדואר אלקטרוני אל הכתובת gcsojoc@barclays.com, לרבות כל המידע הרלוונטי, כולל, במידת האפשר (א) הקטגוריות והמספר המשוער של רשומות הנתונים של Barclays שהושפעו ואם רלוונטי, הקטגוריות והמספר המשוער של נשואי הנתונים המושפעים; (ב) ההשפעה וההשלכות האפשריות של תקרית הסייבר על Barclays ואם רלוונטי, על נשואי הנתונים המושפעים; וכן (ג) הפעולות המתקנות שננקטו או שיינקטו על ידי הספק.

במקרה של חשד לגנבה או גנבה בפועל, שימוש או חשיפה בלתי מורשים של **מידע אישי מוגן** כלשהו בשל כשל של אמצעי אבטחה אצל הספק (או מי מעובדי הספק) או גישה בלתי מורשית למידע אישי מוגן על ידי או דרך ספק (או מי מעובדי הספק) או אובדן, נזק או הרס של מידע אישי מוגן על ידי או דרך הספק או מי מעובדי הספק שמידע כגון זה שבפיקוחו או ברשותו, או כל עיבוד בלתי מורשה אחר של מידע אישי מוגן, הספק יודיע על כך ל-Barclays בהקדם האפשרי ובכל מקרה, עד **24 שעות** ממועד קבלת מידע לגבי התקרית הרלוונטית, באמצעות שליחת הודעה בדואר אלקטרוני אל הכתובת gcsojoc@barclays.com ואף לשתף פעולה ולעזור ל-Barclays באופן מלא ומקיף לפתרון תקרית כגון זו, כולל אספקת כל המידע הרלוונטי, לרבות נתונים, מועד התקרית, מיקום, סוג התקרית, רמת השפעתה, המצב הנוכחי ומידע לגבי הפעולות שננקטו לצמצום הסיכון.

אם הספק עושה שימוש בשירותים של קבלן/מעבד משנה כדי לספק את השירות והוא מחזיק נתונים, מידע או נכסים של Barclays או מעבד אותם, על הספק לקבל על כך אישור מראש ובכתב מ-Barclays. על הספק לקיים קשר חוזי עם קבלן/מעבד משנה ואף להבטיח שקבלן/מעבד המשנה מחזיקים בהסמכה הנדרשת עבור נהלי עבודה דומים בתעשייה ופועלים באופן יעיל כדי להגן על הנתונים/המידע של Barclays שהם מעבדים או מחזיקים. במקרה של תקרית אצל קבלן/מעבד משנה, יש לוודא שמתבצע דיווח על כל תקרית כגון זו, בהתאם למוסבר לעיל.

הנחיות עבור לקוח שירותי ענן (ספק)

על לקוח שירותי הענן לאמת את הקצאת תחומי האחריות לניהול תקריות ולוודא כי מציית לכל דרישות לקוח שירותי הענן. על לקוח שירותי הענן לבקש מידע מספק שירותי הענן על המנגנונים הבאים שמיועדים לאפשר:
ללקוח שירותי הענן לדווח על תקריות/תקריות שזוהו על ידו לספק שירותי הענן.
ללקוח שירותי הענן לקבל דיווחים על תקריות/תקריות שזוהו על ידו מספק שירותי הענן.
- ללקוח שירותי הענן לעקוב אחר מצבה של תקרית אבטחת המידע שעליה דיווח.

MC 6.0 – ניהול נכסי IT (חומרה ותוכנה)

על הספק ליישם תוכנית יעילה לניהול נכסים ולהפעיל אותה במשך כל מחזור חייהם של הנכסים. על תוכנית ניהול הנכסים לפקח על מחזור החיים של הנכסים, החל משלב הרכישה וכלה בשלב הוצאה משירות ו/או השלכה מאובטחת, תוך הבטחת נראות ויישום אמצעי אבטחה הולמים עבור כל סוגי הנכסים בסביבת המחשוב.

על הספק להחזיק ברשומות מלאי מלאות, מדויקות ועדכניות של נכסים קריטיים לפעילות העסקית שמופעלים בכל האתרים ו/או המיקומים הגאוגרפיים המשמשים לצורכי מתן שירות ל-Barclays, לרבות כל ציוד של Barclays המתארח אצל הספק, קבלני/מעבדי משנה המסופק על-ידי Barclays ולוודא שמתבצעת בדיקה פעם בשנה לפחות שנועדה לאמת שמלאי נכסי המידע הוא עדכני, מלא ומדויק ולהציג את התוצאות ל-Barclays, בהתאם לדרישה.

על תהליך ניהול הנכסים לכסות את התחומים הבאים:

- מלאי נכסים – נכסים הקשורים למתקנים שבהם מתבצע עיבוד מידע יזוהו ומלאי של נכסים אלה יירשם וישמר.
 - על הספק להחזיק ברשומת מלאי מדויקת ועדכנית המקיפה את כל נכסי חומרת ה-IT המאפשרים אחסון או עיבוד של מידע.
 - על הספק להחזיק ברשומת מלאי מדויקת ועדכנית של נכסי מידע עבור ציוד של Barclays המתארח בנכסי IT של הספק ו/או של Barclays המסופקים לספק.
 - על הספק עם רכיבים ברמה Tier1, Tier2 ו-Tier3 להחזיק ברשומת מלאי נכסים נוכחיים מלאה ומדויקת (לרבות מחשבים שולחניים, מחשבים ניידים, ציוד רשת, אסימוני RSA או כל נכס אחר שסופק על-ידי Barclays).
 - על הספק להתאים את כל הנכסים של Barclays (חומרה ותוכנה) מדי שנה, ולהודיע ל-Barclays (לצוות TPsecM במשרד סמנכ"ל האבטחה) על התוצאות.
 - על הספק להחזיק ברשומת מלאי עדכנית של כל מוצרי התוכנה המורשים שנפרסו, הדרושים לצורכי אספקת השירות ל-Barclays ולציית לתנאים וההתניות של הרישיונות המתאימים.
 - על מלאי הנכסים של לקוח שירותי הענן לכלול רשומות לגבי נכסים קשורים המאוחסנים בסביבת מחשוב הענן. על רשומות המלאי לציין היכן הנכסים נשמרים, למשל, זיהוי של שירות הענן.
 - שימוש מקובל בנכסים – יש לזהות, לתעד וליישם כללים לשימוש מקובל במידע ובנכסים שקשורים למידע ולמתקני עיבוד מידע.
 - יש לוודא שנכסים בלתי מורשים מוסרים מהרשת.
 - על הספק לוודא יישום של הליכים יעילים לצורך צמצום השימוש בטכנולוגיות בלתי נתמכות, להוצאה משירות בסוף מחזור החיים ולהשלכה מאובטחת של נכסים ונתונים כדי לחסל את הסיכון
 - יש לתייג תוכנות וחומרה שאינן נתמכות כבלתי נתמכות במערכת המלאי.
 - החזרת נכסים – על כל העובדים של הספקים וקבלני/מעבדי המשנה (בהיקף השירותים המסופקים ל-Barclays) להחזיר את כל הנכסים של Barclays שברשותם עם סיום העסקתם, סיום החוזה או סיום ההסכם.
 - יש לחקור כהלכה כל נכס של Barclays הנחשב 'אבוד או נגנב' ולדווח על כך ל-Barclays בהתאם לפיקוח על ניהול תקריות.
 - במקרים של נכס 'אבוד או נגנב' שמכיל מידע של Barclays, יש לדווח על כך ל-Barclays בהתאם לפיקוח על ניהול תקריות.
- על הספק להודיע ל-Barclays באופן מיידי על כל שינוי ידוע ביכולתו לספק תמיכה, בין אם באופן ישיר ובין אם באופן עקיף, בנכסי IT המשמשים למתן שירותים ל-Barclays, לרבות כשהמוצרים כוללים פגיעויות אבטחה. כמו כן, על הספק לוודא שדרוג או הוצאה משירות במועד של נכסי IT כגון אלה.

שינוע נכסים של חברת Barclays – על הספק לוודא שכל הנכסים והנתונים של Barclays מועברים/משונעים באופן מאובטח, תוך יישום אמצעי פיקוח הולמים, בהתאם לסיווג וערך הנכסים והנתונים המועברים/משונעים (הן מבחינת נזק פיננסי והן מבחינת מוניטין), בשילוב על ההשפעה של סביבת האיזמים שבה הם מועברים.

ניהול תמיכה (ספק)

על הספק להודיע ל-Barclays באופן מיידי על כל שינוי ידוע ביכולתו לספק תמיכה, בין אם באופן ישיר ובין אם באופן עקיף, בנכסי IT המשמשים למתן שירותים ל-Barclays, לרבות כשהמוצרים כוללים פגיעויות אבטחה. כמו כן, על הספק לוודא שדרוג או הוצאה משירות במועד של נכסי IT כגון אלה.

על הספק לוודא שכל שינוי אפשרי בהסדרי התמיכה העיקריים של צד שלישי כלשהו מזוהה ומועבר ל-Barclays תוך זיהוי הנכסים המושפעים, על מנת להבטיח שפרטי המוצר יישארו מעודכנים.

הנחיות עבור לקוח שירותי ענן (ספק)

על מלאי הנכסים של לקוח שירותי הענן צריך לכלול פירוט של המידע והנכסים הקשורים המאוחסנים בסביבת מחשוב הענן. על רשומות המלאי לציין היכן הנכסים נשמרים, למשל, זיהוי שירות הענן.

התקנת תוכנה מסחרית ברישיון בסביבת שירותי ענן עלולה להוות הפרה של תנאי רישיון התוכנה. על לקוח שירותי ענן ליישם תהליך לזיהוי דרישות רישוי ספציפיות לסביבת ענן לפני התקנת תוכנה ברישיון בסביבת שירותי ענן. יש להקפיד על מקרים שבהם שירותי הענן גמישים ומאפשרים הפעלה במערכות או בליבות מעבד רבות יותר מהמותר בהתאם לתנאי הרישיון.

MC 7.0 – השלכה/הריסה מאובטחת של נכסים פיזיים ושמירת נתונים של מידע אלקטרוני

על כל השמדה מחיקה מאובטחת של נכסי מידע של Barclays, כולל תמונות המשמשות לשירות, המאוחסנות בצורה פיזית ו/או אלקטרונית להתבצע בשיטה מאובטחת מתאימה ולוודא שנתוני Barclays אינם ניתנים לשחזור.

על הספק לקבוע נהלים עם תמיכה בתהליכים עסקיים ובאמצעים טכניים שמיועדים לאפשר השמדה ו/או השלכה מאובטחת באמצעות שיטות סניטציה מתאימות, כולל, בין היתר ניקוי, טיהור והרס לצורכי הסרה/מחיקה מאובטחת ושחזור של נתוני Barclays מכל אמצעי האחסון, כדי לוודא שנתוני Barclays אינם ניתנים לשחזור באמצעי מחשוב פורנזיים ידועים.

יש למחוק את נתוני Barclays המאוחסנים במדיה כדי להפוך אותם לבלתי ניתנים לשחזור, תוך שימוש בטכניקות מחיקת נתונים מתאימות, כגון מחיקה מאובטחת, טיהור, הסרת נתונים, השמדת נכסים או שיטה מבוססת תוכנה כדי להחליף את הנתונים או להשתמש במסגרת מקובלת בתעשייה להסרת נתונים (NIST). יש להשמיד כל ציוד (נכסי מידע) בסוף מחזור החיים ו/או החיים התפעוליים שלו (פגום, הוצא משירות או אינו נדרש עוד, שימוש לצורכי ניסויים או הוכחת רעיון, שימוש בשירותי מחיקת נתונים עבור ציוד שיש להשתמש בו שוב וכו').

הדרישות להשלכה חלות על קבלני/מעבדי משנה של ספקים המעניקים שירותים ל-Barclays.

יש לגרוס את עותקים קשיחים המכילים מידע בהתאם לתקן P4 DIN66399 (לכל הפחות) באמצעות שימוש במגרטת 'שתי וערב' (Crosscut), לרבות פרטים של כרטיס תשלום, או לשרוף אותם בהתאם לתקן BS EN15713:2009.

עבור Barclays, יש לשמור על ראיות לגבי השמדת הנתונים ולספק שובל ביקורת, ראיות ומעקב, החייבים לכלול:

- הוכחה להשמדה ו/או השלכה (כולל תאריך ושיטת הביצוע)
- יומני ביקורת של המערכת העוסקים במחיקה.
- אישורי השמדת נתונים.
- מי הגורם שביצע את ההשמדה (כולל כל שותף/צד שלישי או קבלן שעסק בתהליך ההשמדה)?
- יש להפיק דוח השמדה ואימות כדי לאשר את רמת ההצלחה או הכישלון של כל תהליך השמדה/מחיקה. (כלומר, תהליך המחיקה חייב לכלול דוח המפרט את כל הרכיבים שלא ניתן למחוק).

במהלך יציאה ממסגרת אספקת שירותים ל-Barclays, על הספק לוודא שהנתונים של Barclays יושמדו באופן מאובטח, תוך מתן הודעה וקבלת אישור מ-Barclays.

הנחיות עבור לקוח שירותי ענן (ספק)

על לקוח שירותי הענן לבקש אישור על כך שספק שירותי הענן מיישם מדיניות ונהלים להשמדה מאובטחת או שימוש חוזר במשאבים. על לקוח שירותי הענן לבקש תיאור מתועד של סיום תהליך השירות, המכסה את ההחזרה והסרה של נכסי לקוחות שירות הענן ולאחריו מחיקת כל העותקים של אותם נכסים מהמערכות של ספק שירותי הענן. על התיאור לכלול פירוט של כל הנכסים ותיעוד של לוח הזמנים לסיום השירות ועליו להיות מסופק תוך פרק זמן סביר.

MC 8.0 – סיווג מידע וטיפול בנתונים

על הספק להחזיק בתהליך סיווג מידע מבוסס ומתאים ובמסגרת/תוכנית הולמת לטיפול בנתונים (בהתאם לדרישות Good Industry ו/או Barclays) המכסים את הרכיבים הבאים:

- סיווג מידע – המידע יסווג במונחים של קריטריונים ורמות רגישות לחשיפה או שינוי בלתי מורשים.
- סימון מידע – מערכת מתאימה ליישום נהלים לסימון מידע תפוח ותיושם בהתאם לתוכנית סיווג המידע שאומצה על ידי הספק.
- טיפול בנכסים – הליכי הטיפול בנכסים יפותחו ויושמו בהתאם לתוכנית סיווג המידע שאומצה על ידי הספק.

הספק גם נדרש לוודא שכל צוות העובדים מודע לדרישות של הספק/Barclays לשימוש בתוויות וטיפול וכיצד יש החיל ככהלכה את סיווג המידע הנכון.

על הספק להתייחס לסכימת תוויות המידע של Barclays ולדרישות הטיפול (**נוסח A, הטבלאות A1 ו-A2**) או לתוכנית חלופית כדי להבטיח שהספק מגן על המידע המוחזק ו/או המעובד ומאבטח אותו. דרישה זו חלה על כל נכסי המידע של Barclays המוחזקים או מעובדים בשמה של Barclays, כולל על ידי קבלני/מעבדי משנה.

הנחיות עבור לקוח שירותי ענן (ספק)

על לקוח שירותי הענן לתייג מידע ונכסים קשורים המתוחזקים בסביבת מחשוב הענן, בהתאם להליכים שאומצו על ידי הלקוח לצורכי תיוג. כשהדבר רלוונטי, ניתן לאמץ פונקציונליות המסופקת על-ידי ספק שירותי הענן התומכת בתיוג.

MC 9.0 – מידע/גיבוי נתונים

על הספק ליישם תהליך מבוסס של גיבוי נתונים כדי להבטיח שהתשתית מגובה באופן קבוע ומדויק, על מנת למנוע אובדן נתונים. מידע המאוחסן בטופס אלקטרוני מגובה כדי להבטיח שנותר מאובטח במקרה של כשל מערכת, אסונות או תקריות. יש לפתח, לבדוק וליישם תוכניות גיבוי כדי ליישם בהצלחה מדיניות ספציפית לנושא גיבוי.

בעת יישום תוכנית גיבוי, יש להתחשב הרכיבים הבאים:

- קביעת דרישות לגיבוי – יש להקפיד על הגדרה ותיעוד ברורים ומוסכמים של דרישות הגיבוי, בהתאם לפעילות העסקית
 - הפקת רשומות מדויקות ומלאות של עותקי הגיבוי והליכי השחזור המתועדים.
 - תדירות הגיבוי (למשל, גיבוי מלא או דיפרנציאלי)
 - אחסון בטוח של גיבויים
 - אחסון הגיבויים במיקום מרוחק בטוח ומאובטח, במרחק מספק כדי להימנע מנזקים שעשויים להיגרם לנתונים שמאוחסנים באתר הראשי.
 - בדיקה שגרתית של מדיות הגיבוי כדי להבטיח שיהיו תקינות ושימוש במקרה חירום ובעת הצורך. בדיקת היכולת לשחזר נתונים מגובים באמצעות שימוש במערכת בדיקה, לא בהחלפת אמצעי האחסון המקוריים במקרה שתהליך הגיבוי או השחזור נכשל וגרם לנזק או לאובדן בלתי הפיך לנתונים.
 - יש לוודא שאובדן נתונים לא מכונן מזהה לפני ביצוע הגיבוי.
 - יש לוודא שהגיבוי תואם למטרה
- יש לוודא שהגיבויים מוגנים כהלכה באמצעות יישום אבטחה פיזית ו/או הצפנה כשהנתונים מאוחסנים וכן בעת העברתם ברשת/בין מיקומים שונים. הדבר כולל גיבויים מרוחק ושירותי ענן.
- יש לוודא שכל הנתונים של Barclays מגובים באופן קבוע ובהתאם לדרישת השירות.
- כשספק שירותי הענן מספק יכולת גיבוי כחלק משירותי הענן, על לקוח שירותי הענן לבקש את מפרטי יכולת הגיבוי מספק שירותי הענן. בנוסף, על לקוח שירותי הענן גם לוודא שספק שירותי הענן מציית לדרישות הגיבוי שלהם. לקוח שירותי הענן אחראי להטמעת יכולות גיבוי כשספק שירותי הענן אינו מספק אותן.
- על הספק להבטיח כי כל מערכות ה-IT והשירותים המשמשים לצורך אספקת השירותים ל-Barclays יכללו תהליכי גיבוי ושחזור הולמים, הפועלים בהתאם לצרכיה העסקיים של Barclays ונבדקים מעת לעת כדי לוודא שהם הולמים ויעילים.
- על הספק לוודא שכל אמצעי הגיבוי הקשורים לאספקת שירותים ל-Barclays, בשילוב עם הסדרים לטיפול ואחסון באמצעות רכיבי המדיה האלה, ייוותרו מאובטחים ואמינים בכל עת

MC 10.0 – ניהול תצורה

על הספק להגדיר וליישם תהליכים וכלים כדי לאכוף את התצורות המוגדרות (לרבות תצורות אבטחה) עבור חומרה, תוכנה, שירותים (לרבות שירותי ענן) ורשתות, עבור מערכות שהותקנו לאחרונה וכן עבור מערכות תפעוליות לאורך כל מחזור חייהן.

ניהול תצורות – על הספק להחזיק ערכת תצורות שנבדקה ואושרה עבור רכיבי חומרה, תוכנה ורשתות. יש לתעד את התצורות הללו ולהחזיק ביומן שמכיל תיעוד של כל שינויי התצורה. יש להקפיד על אחסון מאובטח של הרשומות הללו. ניתן לבצע זאת במגוון דרכים, כגון מסד נתונים של תצורות או תבניות תצורה.

ניטור תצורות – יש לפקח על התצורות באמצעות שימוש בערכה מקיפה של כלי ניהול מערכת (כגון כלי תחזוקה, תמיכה מרחוק, כלי ניהול ארגוניים, תוכנה לגיבוי ושחזור), ולבדוק אותן על בסיס קבוע כדי לאמת את הגדרות התצורה, להעריך את עוצמת הסיסמאות ולבצע הערכה של פעילויות שבוצעו. ניתן להשוות תצורות בפועל לתבניות היעד המוגדרות. יש לטפל בכל סטייה, בין אם באמצעות יישום אכיפה אוטומטית של תצורת היעד המוגדרת ובין אם באמצעות ביצוע ניתוח ידני של הסטייה ויישום של פעולות מתקנות.

רישום ותחזוקה של פריטי תצורה – על הספק להחזיק ברישום מלא ומדויק של כל היקף פריטי התצורה המשמשים לצורכי אספקת שירותים ל-Barclays (כולל בעלות ותלות/מפויים במעלה ובמורד הזרם). על הספק ליישם אמצעי פיקוח שמבטיחים תחזוקה שוטפת ואת רמת הדיוק והשלמות של הנתונים.

בידוד סביבת הייצור – על הספק לוודא כי שירותי הייצור המסופקים ל-Barclays אינם תלויים ברכיבים שאינם רכיבי ייצור, כדי שניתן יהיה להימנע מאספקת שירות באופן שאינו מאובטח או מהימן.

הגדרת תצורה מאובטחת – על הספק להחזיק מסגרת מוגדרת כדי לוודא שהגדרות התצורה של כל המערכות ו/או ציוד הרשת מאובטחות בהתאם לתקני התעשייה המומלצים (כגון CIS, SANS, NIST).

- תקנים אלה קובעים כללי מדיניות, נהלים/אמצעים ארגוניים וכלים המאפשרים ליישם את תקני תצורת האבטחה הטובים ביותר בתעשייה עבור כל התקני הרשת המורשים וכן עבור מערכות ההפעלה, האפליקציות והשרתים.
- ביצוע בדיקות אכיפה רגילות (לפחות פעם בשנה) כדי להבטיח שאי התאמה לתקני האבטחה הבסיסיים מוסדרת באופן מיידי. ביצוע בדיקות ובקרה הולמות על מנת להבטיח את שלמות רכיבי הבנייה או ההתקנים.
- הגדרת התצורה של מערכות והתקני רשת מאפשרות לפעול בהתאם לעקרונות אבטחה (כגון תפיסת מגבלות השליטה על יציאות, פרוטוקולים ושירותים, מניעת שימוש בתוכנות בלתי מורשות, הסרה והשבתה של חשבונות משתמש מיותרים, שינוי סיסמאות ברירת מחדל, הסרת תוכנות מיותרות וכו').
- בצע ביקורת תצורה תקופתית (לפחות פעם בשנה) כדי להבטיח שסביבת הייצור בפועל אינה מכילה תצורה בלתי מורשית.
- יש לוודא שניהול התצורה מפקח על תקני הגדרות תצורה מאובטחים בכל הרמות ומזהה, מתריע ומגיב באופן פעיל לכל שינוי או סטייה בהקשר של הגדרות התצורה.

הנחיות עבור לקוח שירותי ענן (ספק) המשמשים לצורכי אספקת שירותים ל-Barclays

על לקוח שירותי הענן (CSC) לוודא יישום של אמצעי פיקוח מאובטחים על הגדרות תצורה על מנת לאבטח את השירותים המסופקים ל-Barclays –

- בעת קביעת הגדרות התצורה של מחשבים וירטואליים, על לקוחות שירותי ענן לוודא הקשחה של היבטים רלוונטיים (כגון, רק היציאות האלה, רק הפרוטוקולים והשירותים הדרושים) וכי האמצעים הטכניים המתאימים נפרסו (כגון כלים להתמודדות עם תוכנות זדוניות, רישום כניסות) עבור כל מחשב וירטואלי שבו נעשה שימוש.

MC 11.0 – דרישות אבטחה לבינה מלאכותית (AI)

על הספק להתייעץ עם Barclays (צוות TPSecM במשרד סמנכ"ל האבטחה externalcyberassurance@barclayscorp.com), אם הוא משתמש בכלי בינה מלאכותית בכל חלק של מחזור החיים של שירותים ו/או עיבוד נתונים של Barclays.

כשהספק משתמש בבינה מלאכותית בכל חלק של מחזור החיים של שירותים ו/או עיבוד נתונים של Barclays, עליו להפעיל מערכת לניהול בינה מלאכותית. מערכת ניהול זו צריכה לכל הפחות לתעד תהליכים/נהלים סביב הנקודות הבאות:

- פיקוח באמצעות בינה מלאכותית – על הספק להגדיר ולהקים מסגרת פיקוח לשימוש בכלי בינה מלאכותית (כולל כלי בינה מלאכותית של צד שלישי). על מסגרת הפיקוח לוודא שכלי בינה מלאכותית מתוכננים/נפרסים או משולבים בתהליכים קיימים באופן שמגן מפני אובדן נתונים, נזק למערכת, הפרעות בשירות והשלכות רגולטוריות. יש לוודא שתוכנית פיקוח מבוססת מודאגת שכל המסגרות בהקשר של זמינות, שלמות וסודיות נתמכות באופן מלא באמצעות יישום של אמצעי פיקוח מתאימים. יש לתכנן את אמצעי הפיקוח כדי להפחית או לצמצם את הסיכונים לאובדן, לשיבוש או להשחתה של מידע באמצעות מערכת הבינה המלאכותית, ועל הספק לוודא שאמצעי הפיקוח על האבטחה מיושמים ופועלים ביעילות כדי להגן על הנתונים והשירותים של Barclays הניתנים ל-Barclays היכן שהם מקיימים אינטראקציה עם מערכת בינה מלאכותית כזו.

- אבטחה באמצעות בינה מלאכותית – על הספק להגדיר ולבסס מסגרת אבטחה באמצעות בינה מלאכותית שצריכה לכלול, בין היתר, את התחומים הבאים:

- מדיניות שקשורה לבינה מלאכותית – על הספק לתעד מדיניות של בינה מלאכותית שמפרטת את הדרישות לשימוש בטוח ואחראי או לפיתוח של מערכות בינה מלאכותית
- ארגון פנימי - הספק צריך להבטיח לבסס אחריות בתוך הארגון על מנת לקיים את גישתו האחראית ליישום, תפעול וניהול של מערכות בינה מלאכותית.
- משאבים למערכות בינה מלאכותית – על הספק לוודא שהארגון אחראי על המשאבים (כולל רכיבים ונכסים של מערכת הבינה המלאכותית) של מערכת הבינה המלאכותית, כדי להבין את הסיכונים וההשפעות ולטפל בהם באופן מלא.
- נתונים למערכות בינה מלאכותית – על הספק לוודא שהארגון מבין את התפקיד ואת ההשפעות של נתונים (כולל נתוני Barclays) במערכות בינה מלאכותית ביישום ובפיתוח, באספקה, או בשימוש במערכות בינה מלאכותית במשך כל מחזור החיים שלהם.
- מידע לבעלי עניין במערכות בינה מלאכותית – על הספק להבטיח שכל בעל עניין רלוונטי (כולל Barclays) יש המידע הדרוש כדי להבין ולהעריך את הסיכונים של מערכת הבינה המלאכותית ואת ההשפעות שלה (חיוביות ושליליות).
- יחסי צד שלישי ולקוחות – על הספק לוודא שהארגון מבין את אחריותו ונשאר אחראי על מערכת הבינה המלאכותית והסיכונים מחולקים כראוי כשצדדים שלישיים מעורבים בשלבי מחזור החיים של מערכת הבינה המלאכותית.

EUDA – כשירותי ספקים או יכולות מוצר או פונקציונליות של ספקים שמועברות ל-Barclays משתמשים באפליקציות EUDA, ובינה מלאכותית מיושמת או נפרסת כדי ליישם את אותן אפליקציות EUDA או לתמוך בהן, על הספק ליידע את Barclays ולוודא שהשימוש בבינה מלאכותית אינו מתנגש עם דרישות EUDA של Barclays.

הערה: דרישת הפיקוח על האבטחה אינה חלה רק על בינה מלאכותית (AI), אלא גם על למידת מכונה (ML), כיוון שבינה מלאכותית ולמידת מכונה קשורות ומחוברות מאוד. על הספק ליישם את כל דרישות הבקרה לשימוש בכלי למידה מלאכותית בכל חלק של מחזור החיים של שירותים ו/או בעיבוד נתונים של Barclays.

הגדרת בינה מלאכותית/למידת מכונה: בינה מלאכותית היא מערכת שמבוססת על מכונה שנועדה לפעול ברמה של אוטונומיה ומסוגלת לייצר פלט כגון תחזיות, המלצות או החלטות שמשפיעות על סביבות פיזיות או וירטואליות לקבוצה נתונה של מטרות. למידת מכונה היא קבוצת משנה של בינה מלאכותית, שקשורה ליכולת של מכונה לשפר את הביצועים שלה מניסיון באמצעות איטרציות, ללא תכנות מפורש עם כללים.

שיטה/אפליקציה/כלי שמתאימים להגדרה לעיל נחשבים כבינה מלאכותית/למידת מכונה אם הם מדגימים מאפיינים של בינה מלאכותית/למידת מכונה¹ או משתמשים באלגוריתם רשום של בינה מלאכותית/למידת מכונה².

1. לשיטה/אפליקציה/כלי יש מאפיינים של בינה מלאכותית/למידת מכונה אם הם כוללים פרמטרים שהוכשרו באמצעות נתונים, ומומחה לנושא לא יכול להעריך את ההתאמה של הפרמטרים בנפרד. הסיבה לכך יכולה להיות המספר הגבוה של פרמטרים, המורכבות של החישוב, או התדירות שבה הם מתעדכנים. למטרות ההגדרה, 'פרמטרים' הם משתנים מספריים באלגוריתם שניתן לשנות אותם כדי להשפיע על הפלט שלו; 'התאמה' היא הפלט של המודל שמתאים למטרה בהתאם לשימוש בו; ו'מומחה לנושא' הוא בעל מודל או מפתח מודל (אם משמש כנציג לפיתוח מודל).

2. אלגוריתמים של בינה מלאכותית/למידת מכונה כוללים 'צירוף' (יער אקראי וכו'), 'הגברה' (XGBoost, GBM וכו'), 'חלוקה לצברים' (DBSCAN, K-Means וכו'), למידה עמוקה/רשת עצבית, למידה מבוססת מופעים (KNN וכו'), רגרסיה מוסדרת (למשל Ridge, Lasso), למידת חיזוק, מכונת וקטורים תומכים.

הזכות לבדיקה

על הספק לאפשר ל-Barclays, לאחר מתן הודעה בכתב עד עשרה (10) ימי עסקים מראש, לערוך בדיקת אבטחה של כל אתר או טכנולוגיה המשמשים את הספק או את קבלני/מעבדי המשנה שלו לצורכי פיתוח, בדיקה, שיפור, תחזוקה או הפעלה של מערכות המשמשות לספק את השירותים, כדי לבחון את רמת הציות של הספק להתחייבויותיו כלפי Barclays. כמו כן, על הספק לאפשר ל-Barclays לבצע בדיקה על בסיס שנתי לפחות ו/או מיד לאחר תקרית אבטחה.

כל אי התאמה לבקרות שזוהתה על ידי Barclays במהלך ביצוע הבדיקה חייב להיות סיכון שהוערך על ידי Barclays ו-Barclays חייבת לציין מסגרת זמן לביצוע התיקון הנדרש. לאחר מכן, על הספק להשלים כל תיקון נדרש במסגרת זמן זו.

הספק חייב לספק את כל הסיוע המבוקש באופן סביר על ידי Barclays ביחס לכל בדיקה ותיעוד שנמסרו לו במהלך ביצוע הבדיקה. יש להשלים את התיעוד ולהחזיר אותו מיד ל-Barclays. הספק גם חייב לספק תמיכה ל-Barclays ולמלא את שאלון ההערכה שיכלול את כל הראיות הנדרשות במהלך כל ביצוע של הערכה. על כל צד לשאת בעלויות משלו בהתאם לבדיקות/לביקורות/להערכות.

נספח א': דרישות סימון מידע ודרישות הטיפול בתכונים של Barclays

טבלה A1: סכימת הסימון והמידע של Barclays

תווית	הגדרה	דוגמאות
סוד	<p>יש להעניק למידע את הסיווג Secret, אם לחשיפה הבלתי מורשית של מידע כגון זה תהיה השפעה שלילית על Barclays, אם במסגרת הערכה מסוג 'מסגרת ניהול סיכונים ארגונית' (ERMF) Enterprise Risk Management Framework)) היא נקבעת כ'קריטית' (הן מבחינה פיננסית והן מבחינה שאינה פיננסית).</p> <p>מידע זה מוגבל לקהל יעד מסוים ואין להפיצו הלאה ללא אישור היוצר. הקהל היעד עשוי לכלול נמענים חיצוניים, לאחר קבלת אישור מפורש מבעלי המידע.</p>	<ul style="list-style-type: none"> • מידע אודות מיזוגים או רכישות פוטנציאליים • תכנון אסטרטגי – מידע עסקי וארגוני • מידע מסוים אודות תצורת אבטחת המידע • דוחות וממצאי ביקורת מסוימים • סיכום דיוני מועצת המנהלים • אימות או זיהוי ואישור (ID&V) פרטים – לקוח/לקוח ועמית • כמויות מידע גדולות של מחזיק הכרטיס • תחזיות רווח או דוחות פיננסיים שנתיים (לפני פרסומם לציבור) • כל הפריטים המכוסים במסגרת הסכם סודיות (NDA) רשמי
מוגבל – פנימי	<p>יש לסווג את המידע כמוגבל – פנימי, אם הנמענים הצפויים הם עובדים מאומתים של Barclays וספקי שירות מנוהלים של Barclays (MSP) בלבד הפועלים במסגרת חוזה פעיל וכשהמידע מוגבל לקהל יעד מסוים.</p> <p>לחשיפה בלתי מורשית תהיה השפעה שלילית על Barclays, שהערכתה במסגרת ERMF היא 'מהותית' או 'מוגבלת' (הן מבחינה פיננסית והן מבחינה שאינה פיננסית).</p> <p>מידע כגון זה אינו מיועד להפצה כללית, אך ייתכן שיועבר לנמענים או ישותף על ידם בהתאם לעקרונות הצורך לדעת.</p>	<ul style="list-style-type: none"> • אסטרטגיות ותקציבים • הערכות ביצועים • שכר עובדים ומידע אישיים • הערכת נקודות חולשה
מוגבל – חיצוני	<p>יש לסווג את המידע כמוגבל – חיצוני אם הנמענים הצפויים הם עובדים מאומתים של Barclays ו-ספקי שירות מנוהלים של Barclays (MSP) בלבד הפועלים במסגרת חוזה פעיל וכשהמידע מוגבל לקהל מסוים או לצדדים חיצוניים שקיבלו הרשאה של בעלי המידע.</p> <p>לחשיפה בלתי מורשית תהיה השפעה שלילית על Barclays, שהערכתה במסגרת ERMF היא 'מהותית' או 'מוגבלת' (הן מבחינה פיננסית והן מבחינה שאינה פיננסית).</p> <p>מידע כגון זה אינו מיועד להפצה כללית, אך ייתכן שיועבר לנמענים או ישותף על ידם בהתאם לעקרונות הצורך לדעת.</p>	<ul style="list-style-type: none"> • תוכניות מוצר חדשות • חוזים עם לקוחות • חוזים משפטיים • לקוחות בודדים/לקוחות בהיקף עסקי נמוך/פרטי • לקוחות למשלוח לגורמים חיצוניים • לקוחות/תקשורת עם לקוחות. • הצעות חדשות (למשל, תשקיף, מזכר הצעה) • מסמכי מחקר סופיים • מידע שאינו בבעלות Barclays ואינו מהווה מידע ציבורי (MNPI) • דוחות מחקר מכול סוג • חומרי שיווק מסוימים • פרשנות השוק

ביקורת	וממצאי	• דוחות	
		<ul style="list-style-type: none"> • חומרי שיווק • פרסומים • הודעות לציבור • פרסומות בנושא העסקה • מידע שאין לו כל השפעה על Barclays 	<p>יש לסווג את המידע כבלתי מוגבל, אם הפצתו היא כללית או אם לחשיפתו לא תהיה השפעה שלילית על הארגון.</p>

טבלה A2: סכמת תיוג מידע של Barclays – דרישות לטיפול בנתונים

*** מידע אודות תצורת אבטחת מערכות, ממצאי ביקורת ורשומות אישיות עשויים לקבל סיווג 'מוגבל – פנימי' או 'סודי', בהתאם לרמת ההשפעה של חשיפה בלתי מורשית על הארגון

שלב מחזור חיים	סוד	מוגבל – פנימי	מוגבל – חיצוני
יצירה והצגה		<ul style="list-style-type: none"> • יש להקצות נכסים לבעלי המידע. 	<ul style="list-style-type: none"> • יש להקצות נכסים לבעלי המידע.
אחסון	<ul style="list-style-type: none"> • אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) במקום שבו גורמים בלתי מורשים עשויים לקבל גישה או להציג נתונים כגון אלה. • יש להגן על נכסים אלקטרוניים מאוחסנים באמצעות יישום הצפנה או אמצעי שיפוי הולמים אם קיים סיכון מהותי שגורמים בלתי מורשים יוכלו לקבל גישה לנתונים. • על כל המפתחות הפרטיים המשמשים להגנה על נתונים, על זהות ו/או על המוניטין של Barclays להיות מוגנים באמצעות יישום מודולי אבטחת חומרה מאושרים (HSM) מסוג FIPS 140-2 Level 3. 	<ul style="list-style-type: none"> • אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) באזורים ציבוריים (לרבות אזורים ציבוריים במתחמים שבהם תיתכן גישה של מבקרים ללא פיקוח הולם). • אין להשאיר מידע באזורים ציבוריים במתחמים שבהם תיתכן גישה של מבקרים ללא פיקוח הולם. 	<ul style="list-style-type: none"> • אין לאחסן נכסים (בין אם פיזיים ובין אם אלקטרוניים) במקום שבו גורמים בלתי מורשים עשויים לקבל גישה או להציג נתונים כגון אלה. • יש להגן על נכסים אלקטרוניים מאוחסנים באמצעות יישום הצפנה או אמצעי שיפוי הולמים אם קיים סיכון מהותי שגורמים בלתי מורשים יוכלו לקבל גישה לנתונים.
גישה ושימוש	<ul style="list-style-type: none"> • אין לעבוד על נכסים (פיזיים או אלקטרוניים) או להשאיר אותם ללא השגחה במקום שבו גורמים בלתי מורשים יוכלו להציג אותם או לקבל גישה אליהם. יש לעבוד על נכסים רק לאחר יישום אמצעי פיקוח נאותים (כגון מסכי פרטיות). • יש להדפיס נכסים רק באמצעות מדפסות מאובטחות. • יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים 	<ul style="list-style-type: none"> • אין להשאיר נכסים (פיזיים או אלקטרוניים) באזורים ציבוריים מחוץ למתחם. • אין להשאיר נכסים (פיזיים או אלקטרוניים) באזורים ציבוריים, במקומות שבהם מבקרים יוכלו לקבל גישה לנכסים ללא כל פיקוח. • יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים, במידת הצורך 	<ul style="list-style-type: none"> • אין לעבוד על נכסים (פיזיים או אלקטרוניים) או להשאיר אותם ללא השגחה במקום שבו גורמים בלתי מורשים יוכלו להציג אותם או לקבל גישה אליהם. יש לעבוד על נכסים רק לאחר יישום אמצעי פיקוח נאותים (כגון מסכי פרטיות). • לאחר הדפסת נכס כלשהו, יש לקחת את פלט ההדפסה באופן מידי מהמדפסת. אם הדבר אינו אפשרי, יש להשתמש במדפסת מאובטחת. • יש להגן על נכסים אלקטרוניים באמצעות יישום אמצעי ניהול גישה לוגיים הולמים.

שיתוף	<ul style="list-style-type: none"> יש להוסיף תווית מידע גלויה לכל עמוד בעותק קשיח של נכס. יש להוסיף תוויות מידע גלויות למעטפות המכילות עותקים קשיחים של נכסים ולחתום אותן באמצעות חותם מובהק. לפני הפצתם, יש להניחם בתוך מעטפה משנית שאינה כוללת תווית כלשהי. יש להוסיף תווית מידע גלויה וברורה לעותקים של נכסים אלקטרוניים. יש להוסיף תווית מידע גלויה לכל עמוד של עותק אלקטרוני של מסמך מרובה עמודים. יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי. יש להפיץ נכסים רק לגורמים שקיבלו הרשאה מפורשת מבעלי המידע לקבל נכסים כגון אלה. אין לשלוח נכסים בפקס. יש להצפין נכסים אלקטרוניים באמצעות שימוש במנגנון הגנה קריפטוגרפי מאושר כשהם במעבר מחוץ לרשת הפנים ארגונית. יש להקפיד על שרשרת המשמורת על נכסים אלקטרוניים. 	<ul style="list-style-type: none"> יש להוסיף תווית מידע גלויה לעותק קשיח של נכס. יש להצמיד את התווית לעמוד הכותרת לכל הפחות. יש להוסיף תווית מידע גלויה וברורה לעותקים של נכסים אלקטרוניים. יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי. נכסים חייבים להיות מחולקים רק לגורמים שלהם צורך עסקי לקבלם. אין לשלוח עותקי נכסים בפקס, אלא אם השולח אישר שהנמענים מוכנים ויכולים לקבל את עותקי הנכסים באופן מיידי. יש להצפין נכסים אלקטרוניים באמצעות שימוש במנגנון הגנה קריפטוגרפי מאושר כשהם במעבר מחוץ לרשת הפנים ארגונית. 	<ul style="list-style-type: none"> יש להוסיף תווית מידע גלויה לעותק קשיח של נכס. יש להצמיד את התווית לעמוד הכותרת לכל הפחות. מעטפות יש להוסיף תווית מידע גלויה לחזית מעטפות המכילות עותקים קשיחים של נכסים יש להוסיף תווית מידע גלויה וברורה לעותקים של נכסים אלקטרוניים. יש להוסיף תווית מידע גלויה לכל עמוד של עותק אלקטרוני של מסמך מרובה עמודים. יש להפיץ נכסים רק באמצעות מערכות, שיטות או ספקים שאושרו על ידי הארגון. נכסים חייבים להיות מופצים רק לגורמים המועסקים על ידי הארגון או כאלה שפועלים במסגרת חוזית מתאימה או כחלק מצרך עסקי מוכר בבירור, כגון משא ומתן חוזי. נכסים חייבים להיות מחולקים רק לגורמים שלהם צורך עסקי לקבלם. אין לשלוח עותקי נכסים בפקס, אלא אם השולח אישר שהנמענים מוכנים ויכולים לקבל את עותקי הנכסים באופן מיידי. יש להצפין נכסים אלקטרוניים באמצעות שימוש במנגנון הגנה קריפטוגרפי מאושר כשהם במעבר מחוץ לרשת הפנים ארגונית.
אחסון בארכיון והשלכה	<ul style="list-style-type: none"> יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד. התקן מדיה שבה אוחסנו נכסים אלקטרוניים סודיים חייב לעבור תהליך סניטציה הולם לפני או במהלך השלכה. 	<ul style="list-style-type: none"> יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד. 	<ul style="list-style-type: none"> יש להשליך עותקים קשיחים של נכסים באמצעות שירות פסולת חסוי. עותקים של נכסים אלקטרוניים חייבים להימחק גם מ'פחי המיחזור' של המערכת או התקנים דומים במועד.

נספח ב': הגדרות

מידע סודי של Barclays הוא מידע שמתקבל על-ידי הספק או עובדיו (או כל גורם בעל גישה), בקשר לתנאים הכלליים ו/או לחוזים שמתייחסים לפעילויות עסקיות בעבר, בהווה או בעתיד (1) לפעילות עסקית, מוצר ו/או פיתוח של כל ישות בבעלות Barclays ו/או (2) כל עובד, לקוח, צד שלישי/ספק ו/או קבלן של כל חברה בבעלות Barclays (למעט ישויות ספקים), לרבות כל קניין רוחני בבעלות כל ישות של Barclays (לרבות בכפוף לאמור בכל חוזה) או כל ספק/קבלן שהוא צד שלישי כאמור, מידע אישי מוגן, תנאים כלליים אלה, כל מודול וכל חוזה וכן רשומות הנשמרות במסגרת כל חוזה וכל מידע הקשור לתוכניות, תמחור, מתודולוגיות, תהליכים, נתונים פיננסיים, זכויות קניין רוחני, מחקר, מערכות, תוכנית ו/או טכנולוגיית מידע;

הנתונים של Barclays משמעם כל הנתונים, המידע, הטקסט, האיורים וחומרים אחרים המגולמים בכל מדיום, כולל כל מדיה אלקטרונית, אופטית, מגנטית או מוחשית (I) הנגישה לספק בהקשר לכל חוזה, (II) הנמסרים לספק על ידי כל ישות של Barclays או (III) שהספק מייצר, אוסף, מעבד, מאחסן או משדר בהקשר לכל חוזה, למעט חומרים של הספק עצמו.

המערכות של Barclays הן מערכות מידע אלקטרוניות שכוללות רכיבי חומרה, ציוד, תוכנה, ציוד היקפי ורשתות תקשורת בבעלות, בפיקוח, מופעלות ו/או בשימוש של ישויות מטעם Barclays.

תקריט סייבר משמעה כל אירוע, בין אם התרחש הלכה למעשה או אם הספק או Barclays סבורים כי התרחש (על בסיס איום, מודיעין וכו' מהימנים), עם פוטנציאל להוות גורם סיכון (I) לסודיות, לשלמות או לזמינות מלאה של נתוני Barclays או (II) לסודיות, לשלמות או לזמינות מלאה ולפעולה רגילה של מערכת הספק או המערכת של Barclays.

תקריט טכנולוגיות משמען הפרעה לא מתוכננת לשירות IT או פגיעה באיכות שירות ה-IT, כולל, אך אינה מוגבלת לכשל של פריט תצורה שעדיין לא השפיע על שירות. **תקריט מהותית** – תקריט המהווה גורם סיכון/גורם בעל השפעה מהותיים על Barclays, ועלולה להוביל לתוצאות חמורות, כולל אובדן מהותי של פרודוקטיביות, פגיעה במוניטין, נזק רגולטורי והשפעה על תהליכים עסקיים, אמצעי פיקוח או מערכות עיקריים.

הערכת ההשפעה של הגנת נתונים משמעה הערכה של השפעת פעולות העיבוד החזויות על ההגנה על מידע אישי, כנדרש במסגרת החקיקה להגנת הנתונים.

חקיקה להגנת נתונים משמעה, במידה החלה על ביצוע כל אחת מהתחייבויות הספקים, בהתאם לכל חוזה: (I) החוק EU Directive on Privacy and Electronic Communications 2002/58/EC של האיחוד האירופי (העשוי לכלול עדכונים ושינויים שיבוצעו מעת לעת), (II) התקנה הכללית EU General Data Protection Regulation 2016/679 של האיחוד האירופי (תקנות **GDPR**), החלטות והנחיות של הנציבות האירופית וכל חקיקה לאומית ליישום, (III) תקנות GDPR בבריטניה, (IV) החוק Health Insurance Portability and Accountability Act 1996, (V) החוק Gram–Leach–Bliley Act Provisions relating to non-public personal information, (VI) כל החוקים, התקנות וההנחיות הרגולטוריות החלים בנוגע להגנה על נתונים ופרטיות (א) בכל תחום שיפוט שבו פועלת הישות הרלוונטית של Barclays והספק מקיים בה את התחייבויותיו וכן (ב) בכל תחום שיפוט שבו הספק מקיים את התחייבויותיו בהתאם לאמור בכל חוזה;

חובות בקרת פרטיות נתונים משמען כל מסגרת פרטיות נתונים המהווה חלק מסעיף 7 (חובת פיקוח על ספקים חיצוניים).

נשוא נתונים יהיה בעל המשמעות שהוענקה לו במסגרת החקיקה להגנת נתונים. כשמונח זה אינו מוגדר במסגרת החקיקה להגנת נתונים, משמעו אדם מזוהה או אדם שניתן לזהו, הן במישרין והן בעקיפין, במיוחד באמצעות הפניה לאמצעים מזהים כגון שם, מספר מזהה, פרטי מיקום, מזהה מקוון או הפניה לגורם אחד או יותר הספציפיים לנתונים פיזיים, פיזיולוגיים, גנטיים, נפשיים, כלכליים, תרבותיים או חברתיים של אותו אדם.

התנהלות עסקית טובה משמעה, ביחס לכל התחייבות ובכל נסיבות, מימוש ברמה הגבוהה ביותר של מיומנות, חריצות, זהירות וראיית הנולד, שלהן ניתן לצפות באופן סביר מאדם מיומן ומנוסה מאוד הנושא תפקיד מאותו סוג בנסיבות זהות או דומות.

מידע אישי נושא את המשמעות שהוענקה לו במסגרת החקיקה להגנת נתונים. כשמונח זה אינו מוגדר במסגרת החקיקה להגנת נתונים, משמעו הוא כל מידע הקשור, הן באופן ישיר והן בעקיפין, לנשוא הנתונים.

פריצה למידע אישי נוסאת את המשמעות שהוענקה לה במסגרת החקיקה להגנת נתונים. כשהמונח אינו מוגדר במסגרת החקיקה להגנת נתונים, משמעו כל הפרה של אבטחה המובילה להרס, לאובדן, לשינוי, לגילוי או לגישה בלתי מכוונת או בלתי חוקיים לנתונים אישיים שמועברים, מאוחסנים או מעובדים בכל דרך אחרת.

עיבוד נושא את המשמעות שהוענקה לו במסגרת החקיקה להגנת נתונים. כשמונח זה אינו מוגדר במסגרת החקיקה להגנת נתונים, משמעו כל פעולה או קבוצת פעולות המבוצעת על מידע אישי, בין אם באמצעים אוטומטיים, כגון (ללא הגבלה) איסוף, הקלטה, ארגון, אחסון, התאמה או שינוי, אחזור, ייעוץ, שימוש, גילוי באמצעות שידור, הפצה או כל אמצעי אחר לצורכי הנגשה, התאמה או שילוב, חסימה, מחיקה או הרס, המונחים **עיבוד ומעובד** יישאו את המשמעויות המתאימות;

קבלן משנה משמעו כל צד שלישי המספק מעת לעת טובין ו/או שירותים בהקשר של: (א) אספקת מוצרים, שירותים ו/או תוצרים; ו/או (ב) עיבוד או שימוש אחר בכל מידע אישי מוגן, בהתאם למותר במסגרת החוזה.

צוות עובדים של ספק/צד שלישי משמעו כל האנשים ו/או הגורמים שנוטלים חלק כלשהו ביישום או אספקת השירותים או מוצרים כלשהם במסגרת כל חוזה ובכלל זה עובדים, קבלני משנה ו/או נציגים של הספק או של כל אחד מקבלני המשנה שלו.

מערכות של ספק/צד שלישי משמעותן מערכות מידע אלקטרוניות מכל סוג, העשויות לכלול חומרה, ציוד, תוכנה, ציוד היקפי ורשתות תקשורת (או חלק מהן), אשר: (I) משמשות לצורכי אספקת מוצרים או שירותים כלשהם לכל גורם הקשור ל-Barclays בהקשר לחוזה כלשהו; או (II) מוחזקות, מנהלות, מנטרות או בשליטה של ספק או קבלן משנה בהקשר לחוזה כלשהו.

מערכת היא מערכת מידע אלקטרונית (שעשויה לכלול חומרה, ציוד, תוכנה, ציוד היקפי ורשתות תקשורת) מכל סוג (או חלק מהם), ומשמשת לצורכי אספקת טובין או שירותים כלשהם לכל גורם הקשור ל-Barclays בהקשר לחוזה כלשהו.