

המחויבות של Canon לפרטיות: אמצעים טכניים וארגוניים (TOMS)

הגנת מידע ופרטיות



אמצעים טכניים וארגוניים אלה עוזרים להבטיח את התאימות של Canon לחובות הגנת המידע.

אמצעים ארגוניים

מדיניות

מסגרת האחריות על פרטיות של Canon כוללת סדרה של הצהרות מדיניות שמשקפות את ההיבטים השונים של הגנת מידע ותאימות לחוקי הפרטיות.



פיקוח

מבנה פיקוח מקיף שכולל רשת של DPOs ו-Privacy Champions, עם תפקידים ותחומי אחריות שמוגדרים באופן ברור, משמשים להטבעת מסגרת האחריות ברחבי אירופה, המזרח התיכון ואפריקה (EMEA).



ניהול סיכונים

מספר גישות לניהול סיכונים המשמשות לנטרול הסיכונים המאיימים על הגנת הנתונים כוללות הערכות של ההשפעה על הפרטיות, הערכת ההשפעה על הגנת מידע, שאלונים בנושא אמצעים טכניים וארגוניים וכן נהלים מקיפים של בדיקת נאותות של ספקים.



סודיות

הגישה לנתוני לקוחות מורשית רק במידת הצורך כדי לשרת את מטרת עיבוד הנתונים הרלוונטיות, וכל העובדים שיש להם גישה לנתוני הלקוחות כפופים לחובות שמירה על סודיות.



חינוך ומודעות

חינוך ומודעות מחזקים את מסגרת האחריות, וכל העובדים שיש להם גישה לעיבוד נתונים אישיים או אחראים לעיבוד זה נדרשים לעבור הדרכה הולמת באמצעות Canon's Development Hub.



בדיקת נאותות של ספקים

חברות של צד שלישי עוברות בדיקות נאותות ויכולות לעבד נתונים רק בהתאם להסדרים חוזיים שנערכו עמם.



אמצעים ארגוניים (המשך 9)

אפטרופסות



Canon מחויבת לטפל באופן בטוח בנתונים האישיים שאנו מעבדים בשם הלקוחות שלנו, ואנו עובדים באופן הדוק עם השותפים שלנו כדי להבטיח שהם יצייתו לתקנות הפרטיות.

העברת נתונים



Canon לא מעבירה נתונים מחוץ לסמכות שיפוט מסוימת ללא הגנות מתאימות, לדוגמה, סעיפים חוזיים סטנדרטיים, במקרה של EEA.

הודעה ושקיפות



הודעת הפרטיות של Canon משקפת את האופן שבו הקבוצה מנהל נתונים אישיים. שקיפות ואמון הם עקרונות מרכזיים בעת עיבוד נתונים.

פרטיות מובנית



נושא הפרטיות מוטבע בכל המוצרים, הפתרונות והשירותים לאורך מחזור החיים של הנתונים.

קוד התנהגות



Canon מצייתת לקוד ההתנהגות של הקבוצה, שמציין כי ההנהלה והעובדים של הקבוצה צריכים לנהל בקפידה את כל צורות המידע האישי ולציית לכל החוקים והתקנות החלקים ולנהל החברה שנקבעו מראש.

אחריות



Canon מפגינה אחריות בכך שהיא מנהלת רשומות פנימיות מקיפות ש כל פעילויות עיבוד הנתונים האישיים, בקשות זכויות המידע, הפרות נתונים ותהליכי הערכת סיכונים. אנחנו עוזרים גם ללקוחות לעמוד בחובות האחריות שלהם.

ניהול מקרים ורציפות עסקית



Canon מנהלת תהליכים לזיהוי, דיווח, ניהול פתרון הפרות של נתונים אישיים וכן להתאוששות ממקרים כאלה.

המחויבות של Canon לפרטיות: אמצעים טכניים וארגוניים (TOMS)

Canon

הגנת מידע ופרטיות

מדיניות גישה

מדיניות ותהליכים של בקרת גישה, המבוססים על דרישות העסק ועל דרישות אבטחת המידע, תועדו ויושמו באופן רשמי, והם נבדקים מעת לעת. קווי מדיניות ותהליכים אלה מטפלים בגישה מורשית של המשתמשים ובהסדרי עבודה מהבית/במכשירים ניידים.



בקרת גישה של המשתמש

יושמו בקרות גישה לוגיות. בקרות משתמש ייחודיות מוקצות רק לאנשים מורשים, ומוגדרות לספק גישה מינימלית למידע. בקרות סיסמאות נאכפות.



אבטחה פיזית

אזורים מאובטחים מוגנים על-ידי בקרות כניסה הולמות כדי להבטיח שרק עובדים מורשים יורשו לגשת לאזורים שמכילים מידע עסקי רגיש או קריטי ולמתקני עיבוד מידע.



אמצעים טכניים

אישורים

כאשר הדבר נדרש למוצר/פתרון/שירות מסוים, Canon מחזיקה באישורים רלוונטיים כמו ISO/IEC 27001.



ביטול זיהוי ומחיקה

שיטות לביטול הזיהוי מובעות במוצרים ובפתרונות שלנו ועשויים לכלול הפיכת נתונים לאנונימיים, מניעת גישה לפרטים מזהים ומחיקה ללא גרימת נזק לשלמות ההקשרים.



אבטחת מסמכים

Canon מגנה על הנתונים האישיים שנמצאים במעבר בסביבות ייצור ובסביבות אחרות באמצעות בקרות הצפנה הולמות. בעת הצורך, מתבצעת "הקשה" של התצורה כדי להבטיח את אבטחת המכשיר.



המחויבות של Canon לפרטיות: אמצעים טכניים וארגוניים (TOMS)

Canon

הגנת מידע ופרטיות

השלכה מאובטחת או שימוש חוזר בציוד

קיימים תהליכי השלכה מאובטחים לכל סוגי המדיה ולכל פריטי הציוד שמכילים מדיה אחסון, שעברו בדיקות כדי להבטיח שכל הנתונים האישיים הוסרו או נדרסו בבטחה על-פי תקן הולם לפני ההשלכה או השימוש החוזר.



יומן פעילות

הפתרון או השירות יכולים לאחסן יומני פעילות (לדוגמה, ניתוק גישת משתמש ומנהל מערכת, וכן הזנה, שינוי ומחיקה של נתונים).



ניטור

פעילות המשתמש ופעילות המערכת מנוטרת כדי לזהות ולעזור למנוע הפרות נתונים.



זמינות

קיימות בקורות שמטרתן להבטיח את מהימנות השירות ולהפחית את מספר התקלות.



שילוב של חומרה ותוכנה

פתרונות מסמכים בבעלותה של Canon, כמו uniFLOW ו-IRIS מאפשרים לנו להסתגל במהירות רבה יותר לצרכי האבטחה שמתעוררים ולצמצם את הפוטנציאל להפרות מערכת.



אמצעים טכניים (המשך)

סביבה מבודדת

כאשר פתרון מתארח, מתבצעת אכיפה של הפרדה לוגית של הלקוח.



מדיה נשלפת

נקבעו בקורות לניהול השימוש במדיה נשלפת כדי למנוע חשיפה, שינוי, הסרה או השמדה בלתי מורשים של הנתונים המאוחסנים במדיה זו.

