



---

INFORMATIONSKATALOG

# Microsoft PhotoDNA

## Was ist Microsoft PhotoDNA?

Informationskatalog: Wie wir PhotoDNA einsetzen, um Bildmaterial aus Erpressungsfällen technisch zu erkennen und an Plattformen zu melden



NivoSec verfügt über eine Lizenz zur Nutzung der Microsoft-PhotoDNA-Technologie.

# Microsoft PhotoDNA



Wie funktioniert die Bildererkennung mit PhotoDNA?

NivoSec nutzt Microsoft PhotoDNA, um aus Bildern, mit deren Veröffentlichung Betroffene erpresst oder bedroht werden, technische Vergleichswerte zu erzeugen. Für jedes ausgewählte Bild wird ein eigener technischer Vergleichswert erzeugt. Dieser technische Vergleichswert wird als PhotoDNA-Hash bezeichnet.

Der Hash ist vereinfacht gesagt ein digitaler Fingerabdruck des Bildes. Aus diesem Fingerabdruck lässt sich das ursprüngliche Bild nicht wiederherstellen. Die Plattform kann den Hash jedoch verwenden, um dasselbe oder ein sehr ähnliches Bild bei einem neuen Upload wiederzuerkennen.

Wir verwenden diese Technik, um technische Vergleichswerte für Erpressungsmaterial zu erzeugen und diese im Rahmen der Meldung an die zuständigen Plattformstellen zu übermitteln. Wird das registrierte Bild auf einer angebotenen Plattform erneut hochgeladen oder geteilt, kann es durch den Hash-Abgleich erkannt werden. Die Plattform kann anschließend die Weitergabe blockieren. Je nach Plattform können zusätzlich die verwendeten Konten eingeschränkt oder gesperrt werden.



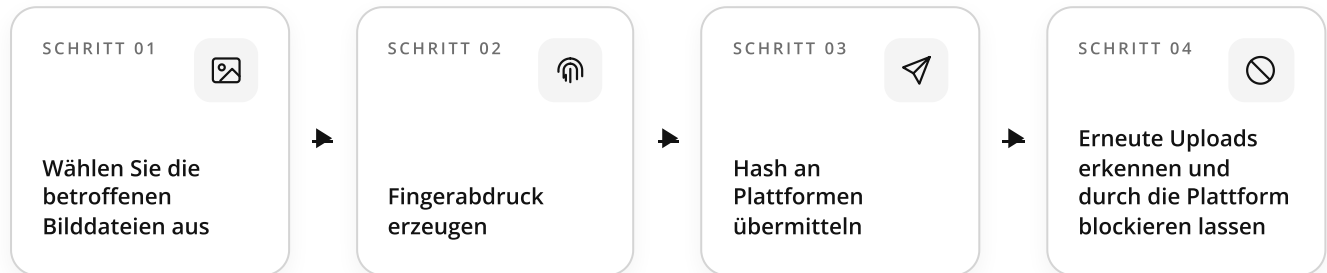
## ABLAUF

### Vom Bildmaterial zum Plattform-Abgleich



# Wie funktioniert PhotoDNA?

Vier Schritte vom Bild bis zum möglichen Plattform-Abgleich



## 01

### Wählen Sie die betroffenen Bilddateien aus

Sie wählen das Bild aus, mit dem Sie erpresst werden oder dessen Veröffentlichung angedroht wurde. Dieses Bild wird anschließend technisch verarbeitet, damit es von unterstützten Plattformen später wiedererkannt werden kann.

## 02

### Digitalen Fingerabdruck erzeugen

Aus dem ausgewählten Bild wird mit PhotoDNA ein digitaler Fingerabdruck erzeugt. Dabei entsteht keine Kopie des Bildes, sondern ein technischer Vergleichswert, mit dem das Bild später erkannt werden kann.

## 03

### Hash an Plattformen übermitteln

NivoSec übermittelt diesen digitalen Fingerabdruck zusammen mit den erforderlichen Informationen an die zuständigen Sicherheitsstellen der unterstützten Plattformen. Dort kann er für die Erkennung des betreffenden Bildmaterials hinterlegt werden.

## 04

### Erneute Uploads erkennen und durch die Plattform blockieren lassen

Versucht jemand anschließend, das registrierte Bild auf einer unterstützten Plattform hochzuladen oder erneut zu verbreiten, kann es durch den digitalen Fingerabdruck erkannt werden. Die Plattform kann den Upload blockieren und das betreffende Konto nach ihren eigenen Sicherheitsregeln einschränken oder sperren.

# Wofür nutzt NivoSec PhotoDNA?

Gezielter Einsatz bei Online-Erpressung und angedrohter Veröffentlichung

NivoSec verfügt über eine Lizenz zur Nutzung der Microsoft-PhotoDNA-Technologie. Wir setzen sie gezielt bei Bildern ein, die bei Online-Erpressung oder Sextortion als Druckmittel verwendet werden oder deren unerlaubte Veröffentlichung angedroht wird.



## DATEIAUSWAHL

Die betroffene Person wählt die Dateien selbst in unserem geschützten Verarbeitungsbereich aus. Aus jeder ausgewählten Bilddatei wird ein eigener technischer Hashwert erzeugt. Bei Videodateien verwenden wir – je nach Plattform – ein dafür vorgesehenes Video- oder Frame-Verfahren.



## VERGLEICHSWERT

Für die Meldung werden nur die Angaben verarbeitet, die für den jeweiligen Vorgang erforderlich sind. Für den späteren Abgleich wird nicht das Bild selbst, sondern der daraus erzeugte Hash als technischer Vergleichswert verwendet.



## PLATTFORM-ABGLEICH

Der Hash-Abgleich kann innerhalb der technischen Infrastruktur einer unterstützten Plattform erfolgen. Er ist nicht an das Smartphone, den Computer, die Telefonnummer oder das Benutzerkonto der Person gebunden, die das Bild verbreitet.

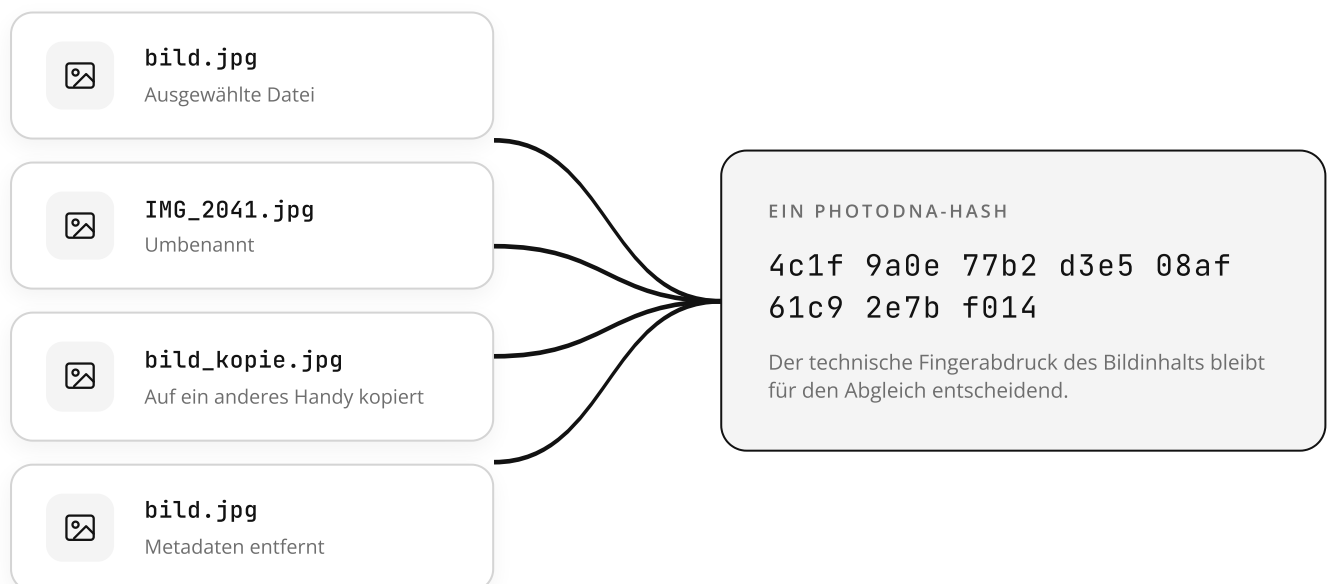
## DAS ZIEL

**Das Ziel ist einfach: Aus dem betreffenden Bild wird ein technischer Fingerabdruck erzeugt. Diesen übermitteln wir an die zuständigen Plattformstellen, damit das Bild bei einem späteren Upload erkannt und seine Weitergabe blockiert werden kann.**

# Warum ist der Hash wichtig?

Stellen Sie sich den Hash wie einen Fingerabdruck vor. Ein Bild kann umbenannt oder auf ein anderes Gerät kopiert werden, ohne dass sich sein Bildinhalt dadurch verändert. Der technische Fingerabdruck des Bildinhalts bleibt für den Abgleich jedoch entscheidend.

Dadurch kann eine Plattform ein bereits gemeldetes Bild wiedererkennen, ohne bei jedem neuen Versuch das ursprüngliche Bild manuell prüfen zu müssen. PhotoDNA wird eingesetzt, um registriertes Erpressungsmaterial bei einem erneuten Upload zu erkennen, damit die Plattform dessen Weitergabe blockieren kann.



EIN ANDERER DATEINAME, EIN ANDERES GERÄT ODER ENTFERNT METADATEN VERÄNDERN DEN BILDINHALT NICHT.

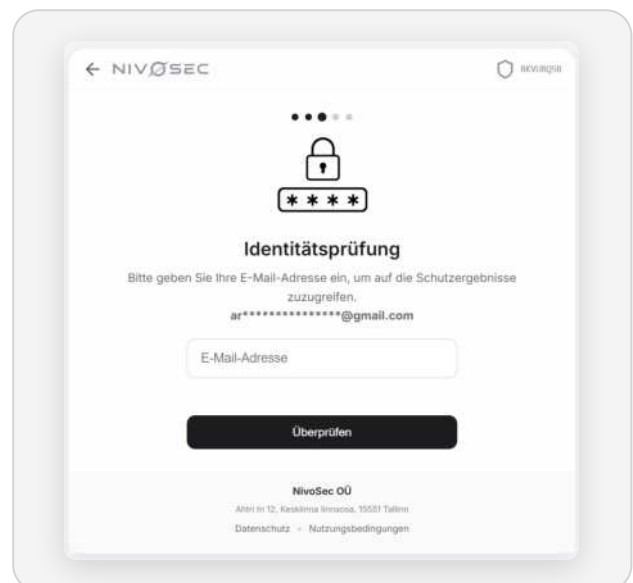
# So führen Sie die Meldung im NivoSec-Tool durch

Der Vorgang ist in wenige einfache Schritte unterteilt. Sie wählen Ihre Dateien selbst aus und sehen anschließend, welche Dateien verarbeitet und welche Meldungen übermittelt wurden.

## 01

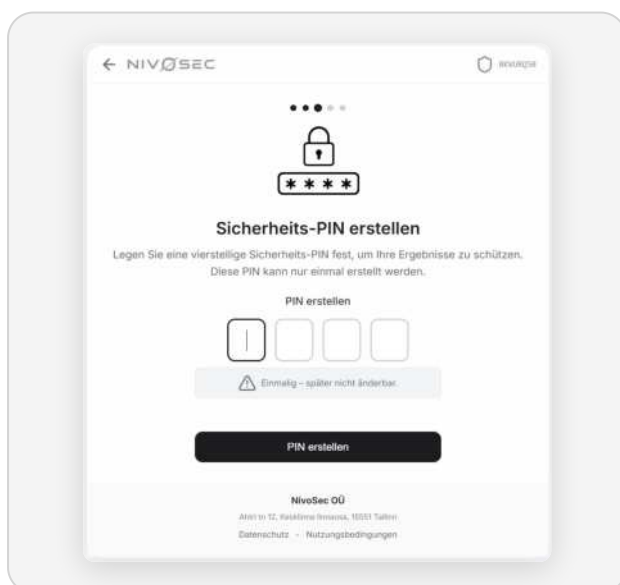
### E-Mail-Adresse eingeben

Geben Sie die E-Mail-Adresse ein, die Ihrem Vorgang zugeordnet ist. So wird geprüft, ob Sie Zugang zu diesem Vorgang haben.



ANSICHT 01

ZUGANGSPRÜFUNG



ANSICHT 02

SICHERHEITS-PIN ERSTELLEN

## 02

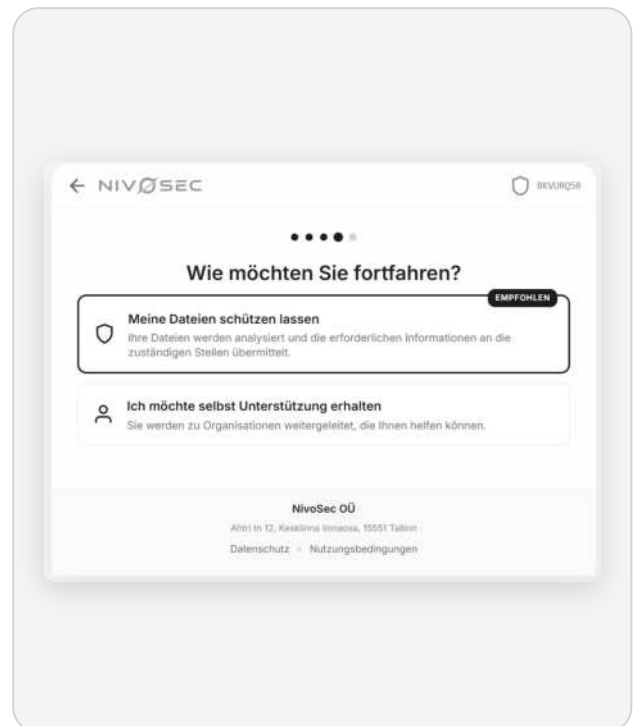
### Persönliche Sicherheits-PIN festlegen

Erstellen Sie eine vierstellige PIN. Diese PIN schützt den Zugang zu Ihrem Vorgang und Ihren Ergebnissen. Nach der Einrichtung kann die PIN nicht mehr geändert werden. Bewahren Sie sie daher sicher auf.

# 03

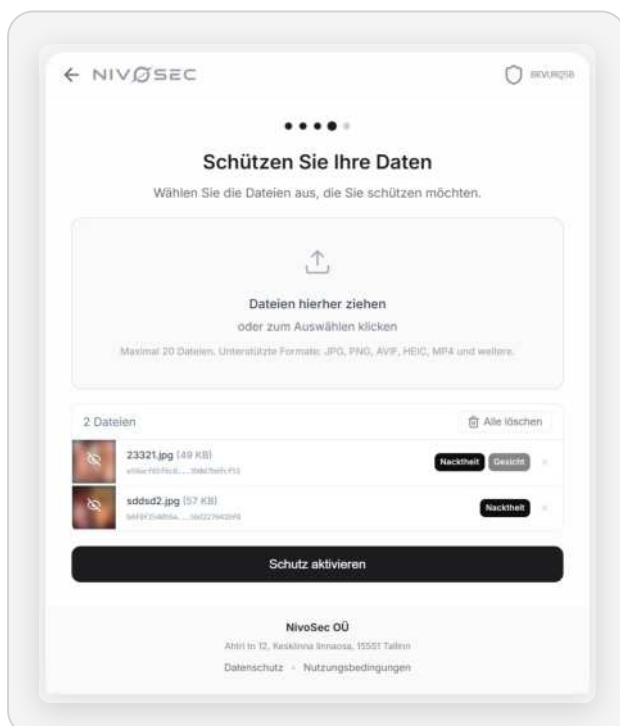
## „Meine Dateien schützen lassen“ auswählen

Wählen Sie „Meine Dateien schützen lassen“. Damit gelangen Sie zu dem Bereich, in dem Sie die Bilder auswählen können, mit denen Sie erpresst werden oder deren Veröffentlichung Sie verhindern möchten.



ANSICHT 03

WIE MÖCHTEN SIE FORTFAHREN?



ANSICHT 04

SCHÜTZEN SIE IHRE DATEN

# 04

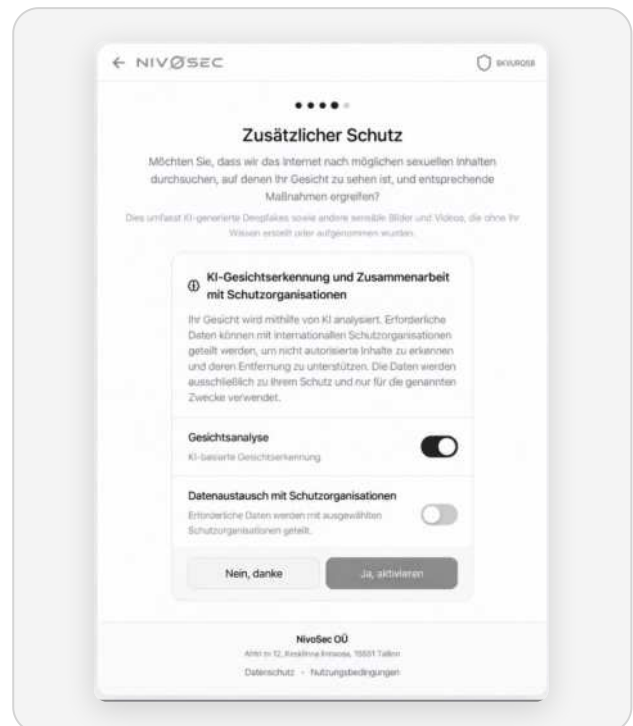
## Bilder oder Videos auswählen

Laden Sie die betroffenen Bilddateien sowie – je nach verfügbarem Verfahren – Videodateien hoch. Prüfen Sie die Auswahl und klicken Sie anschließend auf „Schutz aktivieren“.

# 05

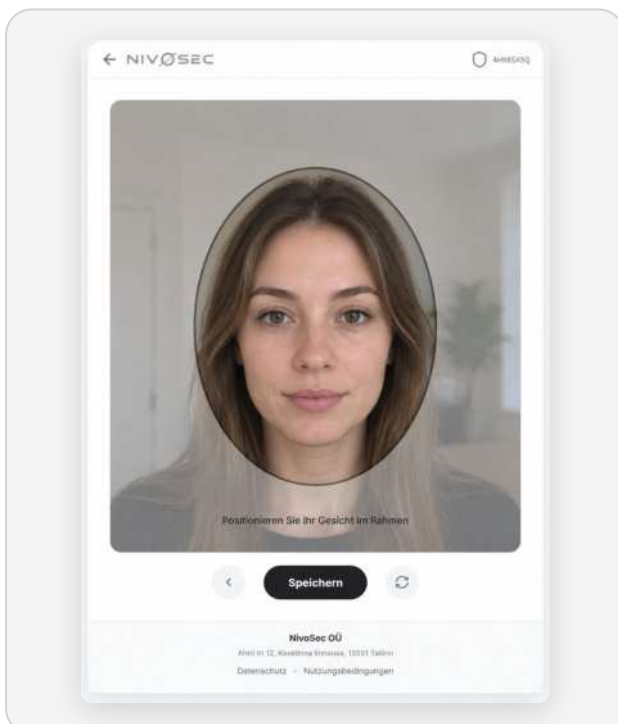
## Zusätzliche Funktionen auswählen

Falls neu erzeugte oder stark veränderte Inhalte zusätzlich geprüft werden sollen, können Funktionen wie die Gesichtsanalyse aktiviert werden. Diese Funktion ist getrennt von PhotoDNA. Erforderliche Falldaten werden nur weitergegeben, soweit dies für den gewählten Meldeweg notwendig ist.



ANSICHT 05

ZUSÄTZLICHER SCHUTZ



ANSICHT 06

GESICHTSERFASSUNG

# 06

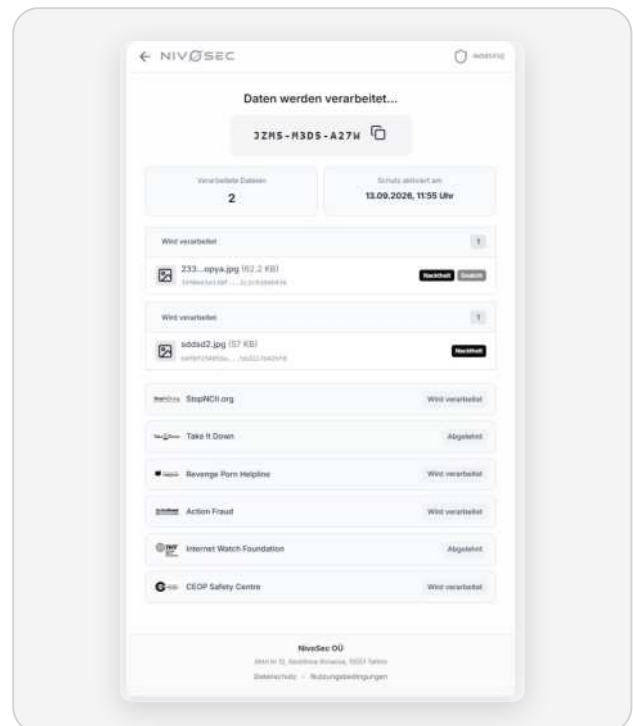
## Gesichtserfassung durchführen

Wenn Sie die zusätzliche Gesichtsanalyse aktiviert haben, positionieren Sie Ihr Gesicht im angezeigten Rahmen und drücken Sie anschließend auf „Speichern“. Diese Aufnahme gehört zur zusätzlichen Gesichtsanalyse und nicht zum PhotoDNA-Hash selbst.

## 07

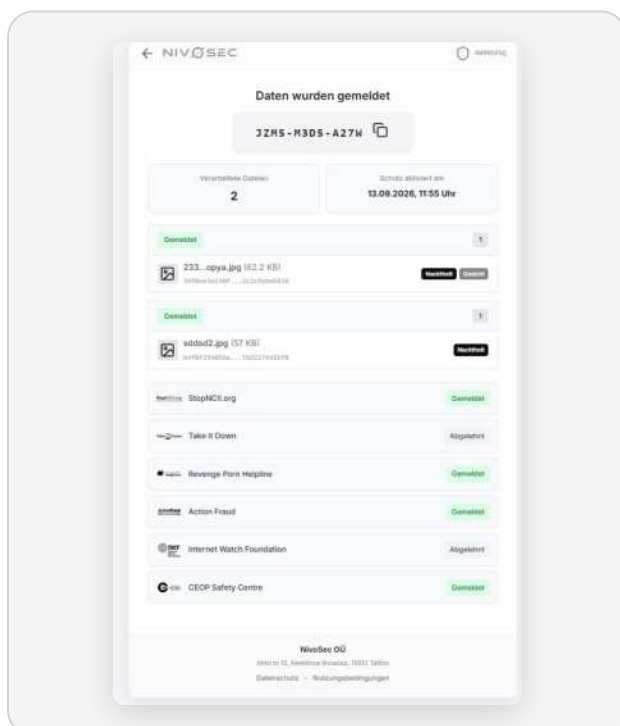
**Verarbeitung abwarten**

Nach dem Start erhalten Sie eine persönliche Vorgangs-ID. Auf der Seite sehen Sie, wie viele Dateien verarbeitet werden und an welche Stellen die Meldung gesendet wird. Der jeweilige Status wird direkt angezeigt.



ANSICHT 07

DATEN WERDEN VERARBEITET



ANSICHT 08

DATEN WURDEN GEMELDET

## 08

**Ergebnis und Meldestatus prüfen**

Nach Abschluss sehen Sie, welche Stellen die Meldung erhalten haben. Bewahren Sie Ihre Vorgangs-ID auf. Sie dient dazu, den Vorgang später eindeutig wiederzufinden. Der gemeldete Hash kann anschließend innerhalb der angebundenen Plattform- und Meldesysteme für den Abgleich verwendet werden.

# Häufige Fragen – einfach beantwortet

Geräte, Konten, Dateinamen und veränderte Kopien

F 01

## Was passiert, wenn die Person mein Bild über ein anderes Gerät hochlädt oder teilt?

Das ändert am Prinzip nichts. Der Abgleich ist nicht an ein bestimmtes Handy oder einen bestimmten Computer gebunden. Entscheidend ist das Bild selbst. Wird das registrierte Bild über ein anderes Gerät erneut hochgeladen, kann der Hash-Abgleich es wiedererkennen.

F 02

## Was passiert, wenn dafür ein neues oder anderes Konto benutzt wird?

Auch dann bleibt der für das Bild gemeldete Hash derselbe. Der Abgleich richtet sich nach dem Bildinhalt und nicht nach dem Benutzerkonto. Wird das Bild erkannt, kann die Plattform den Upload blockieren und gegen das verwendete Konto vorgehen.

F 03

## Funktioniert das nur bei privaten Nachrichten?

Nein. Je nach Plattform kann der Hash-Abgleich beispielsweise bei privaten Nachrichten, Beiträgen, Stories, Profilbildern oder anderen Uploads eingesetzt werden. Wird das Bild in einem solchen Bereich erkannt, kann die Weitergabe blockiert werden.

F 04

## Was passiert, wenn das Bild zugeschnitten oder komprimiert wird?

PhotoDNA wurde dafür entwickelt, bekannte Bilder auch nach bestimmten technischen Änderungen wiederzuerkennen. Dazu gehören zum Beispiel Größenänderungen, Komprimierung oder kleinere Bearbeitungen.

F 05

## Was passiert bei einem Screenshot?

Auch ein Screenshot kann dem ursprünglichen Bild weiterhin sehr ähnlich sein. PhotoDNA berücksichtigt den Dateinamen nicht, sondern vergleicht Merkmale des Bildinhalts. Deshalb kann auch eine veränderte Kopie beim Abgleich erkannt werden.

F 06

## Spielt der Dateiname eine Rolle?

Nein. Ein Umbenennen der Datei ändert den Bildinhalt nicht. Auch das Kopieren auf ein anderes Gerät verändert den Bildinhalt nicht. Entfernte Metadaten sind für den PhotoDNA-Abgleich nicht ausschlaggebend.

F 07

## Kann mein Bild aus dem Hash wiederhergestellt werden?

Nein. Aus einem PhotoDNA-Hash lässt sich das ursprüngliche Bild nicht wiederherstellen. Der Hash ist ein technischer Vergleichswert und keine Kopie des Bildes.

---

**04 / HÄUFIGE FRAGEN**

F 08

**Erkennt PhotoDNA mein Gesicht?**

Nein. PhotoDNA ist keine Gesichtserkennung. Es vergleicht Bilder anhand ihres technischen Fingerabdrucks. Eine Gesichtsanalyse im NivoSec-Tool ist eine separate Funktion.

F 09

**Wird mein Originalbild bei jedem späteren Abgleich erneut versendet?**

Nein. Für den späteren Abgleich wird der registrierte Hash verwendet. Eine unterstützte Plattform kann neue Uploads mit diesem technischen Referenzwert abgleichen.

F 10

**Wo wirkt die Bildsperre?**

Die Erkennung und mögliche Blockierung erfolgen auf den Plattformen und in den Systemen, an die der betreffende Hash übermittelt wurde und die einen entsprechenden Hash-Abgleich unterstützen. Deshalb übermitteln wir den Hash und die erforderlichen Falldaten gezielt an die jeweils zuständigen Plattformstellen.

F 11

**Was passiert, wenn das Bild bereits veröffentlicht wurde?**

Dann kann der bereits veröffentlichte Inhalt ebenfalls gemeldet werden. Der Hash dient gleichzeitig dazu, weitere Uploads und erneute Verbreitungsversuche des registrierten Bildes zu erkennen. Die Plattform kann erkannte Uploads anschließend blockieren.

F 12

**Was passiert mit dem Konto, über das das Bild verbreitet wird?**

Wird ein registrierter Inhalt erkannt, kann die Plattform nicht nur den Upload blockieren, sondern auch Maßnahmen gegen das verwendete Konto einleiten. Dazu gehören je nach internen Regeln Einschränkungen oder eine Sperrung des Kontos.

F 13

**Wie lange wird der Hash verwendet?**

Wie lange ein Hash für den Abgleich gespeichert oder verwendet wird, richtet sich nach dem Verfahren der jeweiligen Plattform oder Meldestelle.

F 14

**Können auch Videos gemeldet werden?**

Ja, je nach Plattform und verfügbarem Verfahren. Die Videoverarbeitung und der PhotoDNA-Abgleich für Einzelbilder sind technisch getrennte Verfahren.

F 15

**Was ist mit KI-generierten oder stark veränderten Bildern?**

Für neu erzeugte oder stark veränderte Inhalte können zusätzliche Prüfungen eingesetzt werden. Dazu gehört zum Beispiel die optionale Gesichtsanalyse im NivoSec-Tool. Sie ist eine zusätzliche, vom PhotoDNA-Hash-Abgleich getrennte Prüffunktion.

# Datenschutz und Vertraulichkeit

Hash für den Abgleich, PIN für  
den geschützten Zugang



## #

**TECHNISCHER HASH**

Für den PhotoDNA-Abgleich wird aus der ausgewählten Bilddatei ein technischer Hash erzeugt. Der Hash ist kein Bild und lässt sich nicht in das ursprüngliche Bild zurückverwandeln.

## 🔒

**GESICHERTER ZUGANG**

Der Zugang zu Ihrem NivoSec-Vorgang wird durch die Prüfung Ihrer E-Mail-Adresse und eine persönliche Sicherheits-PIN abgesichert. Jede ausgewählte Datei wird dem jeweiligen Vorgang eindeutig zugeordnet.

## 📄

**NUR ERFORDERLICHE ANGABEN**

An Plattformen oder andere zuständige Stellen werden nur die Informationen weitergegeben, die für die konkrete Meldung und Bearbeitung erforderlich sind.

**TECHNISCHER HINWEIS**

PhotoDNA erkennt bekannte Bilder über ihren technischen Hash. Der Hash enthält kein sichtbares Bild und kann nicht in das Original zurückverwandelt werden. NivoSec übermittelt diesen Hash an zuständige Plattformstellen, damit registriertes Bildmaterial aus Erpressungsfällen bei einer erneuten Weitergabe erkannt und durch die Plattform blockiert werden kann.

# Zusammenfassung

PhotoDNA wird eingesetzt, um aus Bildern, mit deren Veröffentlichung Menschen erpresst werden, technische Vergleichswerte zu erzeugen, anhand derer erneute Uploads auf unterstützten Plattformen erkannt werden können.

NivoSec erzeugt dafür aus dem betroffenen Bild einen technischen Hash, übermittelt diesen an die zuständigen Plattformstellen und begleitet den weiteren Meldeprozess. Dadurch kann ein bereits registriertes Bild bei einem erneuten Upload erkannt werden. Die Plattform kann den Upload anschließend blockieren. Wird ein Upload erkannt, kann die Plattform nach ihren eigenen Sicherheitsregeln Maßnahmen gegen das verwendete Konto einleiten.

