PRODATIS®

The eBusiness Solution Company.

Auskunftsverlangen der Polizei

Auskunftsverlangen der Polizei

Die Polizei, die Staatsanwaltschaft oder andere Behörden stellen aus den unterschiedlichsten Gründen Auskunftsbegehren an ein Unternehmen: Hier soll z.B. im Rahmen eines eingeleiteten Ermittlungsverfahrens ein Diebstahl, ein Betrug oder eine Sachbeschädigung aufgeklärt werden, dort ein Straßenverkehrsdelikt.

Dazu ist es erforderlich, Informationen über den Sachverhalt und die beteiligten Personen einzuholen. Nur so können die Behörden einem Verdacht nachgehen und die erforderlichen Beweise erheben.

Üblicherweise handelt es sich dabei um Auskünfte, die personenbezogene Daten zum Gegenstand haben, z.B. Namen, IP-Adressen, Video-, Bild- und Audiodateien oder Standortdaten. Video-, Bild- und Audiodateien werden zudem häufig als biometrische Daten einzuordnen sein (siehe Art. 4 Nr. 14 Datenschutz-Grundverordnung (DSGVO)). Sie gelten daher als besondere Kategorien personenbezogener Daten.

DSGVO überhaupt anwendbar?

Bevor Verantwortliche Überlegungen zum datenschutzrechtlich zulässigen Umgang mit den Daten anstellen, ist zu prüfen, welche Rechtsgrundlagen überhaupt anwendbar sind.

Laut Art. 2 Abs. 2 Buchst. d DGSVO findet die DSGVO nämlich keine Anwendung auf Verarbeitungen von personenbezogenen Daten, die durch „die zuständigen Behörden zum Zwecke der Verhütung, Ermittlung, Aufdeckung oder Verfolgung von Straftaten oder der Strafvollstreckung, einschließlich des Schutzes vor und der Abwehr von Gefahren für die öffentliche Sicherheit“ verarbeitet werden. Stattdessen gelten u.a. die §§ 45 ff. des neuen Bundesdatenschutzgesetzes (BDSG), die die Anforderungen der JI RL (EU) 2016/680 umsetzen.

Allerdings betreffen letztere Regelungen ausschließlich den Umgang mit den Daten durch die Behörde selbst (in ihrer Funktion als eigener Verantwortlicher).

Sie regeln nicht, ob und wie ein Unternehmen in diesem Zusammenhang Daten verarbeiten darf. Hier bleibt das Un-

ternehmen selbst Verantwortlicher im Sinne von Art. 4 Nr. 7 DSGVO.

Daher ist der Anwendungsbereich der DSGVO eröffnet.

1. Schritt: Behörde und Anfragenden identifizieren
Bevor es an die Prüfung geht, ob die Herausgabe der Daten zulässig ist, heißt es, den Anfragenden eindeutig zu identifizieren.

Auch wenn die DSGVO nicht zwingend eine solche Identifizierung verlangt, liegt dies im Eigeninteresse jedes Verantwortlichen. Denn eine unzulässige Übermittlung führt zu einem Datenschutzverstoß.

Daher müssen die Mitarbeiter wissen, dass sie immer eine schriftliche Anfrage der Behörde einfordern sollten (Brief oder Fax), aus der sich eindeutig die verantwortliche Behörde und die Stammdaten des Anfragenden ergeben (z.B. Kontakt und Faxnummer).

Telefonische Auskunftsverlangen sollten sie ablehnen. Kommt die Anfrage per E-Mail, sollten die Mitarbeiter überprüfen, ob die E-Mail-Adresse korrekt ist und die Nachricht tatsächlich vom Absender stammt.

Jegliche Kommunikation ist zu dokumentieren, um im Zweifelsfall nachzuweisen, dass keine Daten an einen unberechtigten Empfänger gingen.

Schritt 2: Herausgabeverlangen prüfen
Der Verantwortliche muss zunächst prüfen, ob die Behörde die Daten überhaupt herausverlangen darf. Grundlage des Herausgabeverlangens kann z.B. ein richterlicher Beschluss oder ein – unterzeichnetes – Auskunftsersuchen der Staatsanwaltschaft bzw. der Polizei sein. Es sollte u.a. ein Aktenzeichen, die Rechtsgrundlage des Verlangens (z.B. §§ 160 ff. Strafprozessordnung (StPO)) und eine Begründung bzw. eine kurze Darstellung des Sachverhalts enthalten.

Eine weitergehende vertiefte Prüfung durch den Empfänger wird wohl nicht erforderlich sein. Denn dies würde den Verantwortlichen vor unverhältnismäßige Anforderungen stellen.

Es empfiehlt sich, bereits hier – neben den üblicherweise zuständigen Stellen wie Rechtsabteilung oder Interne Revision – den Datenschutzbeauftragten einzubinden, damit er eventuelle Risiken identifizieren kann.

Schritt 3: Rechtsgrundlage für die Weitergabe prüfen
Die DSGVO sieht in Art. 5 vor, dass eine Verarbeitung von Daten nur dann erfolgen darf, wenn eine Rechtsgrundlage dies erlaubt. Im Gegensatz zum alten BDSG (seinerzeit § 28 Abs. 2 Nr. 2 Buchst. b BDSG a.F.) enthält die DSGVO allerdings keine eigenständige Rechtsgrundlage mehr für die Herausgabe von Daten für die Zwecke der Strafverfolgung.

Insofern muss die Weitergabe über Art. 6 DSGVO bzw. Art. 9 für besondere personenbezogene Daten gerechtfertigt werden. In Betracht kommen beispielsweise Art. 6 Abs. 1 Buchst. c oder f DSGVO.

Rechtliche Verpflichtung (Art. 6 Abs. 1 Buchst. c DSGVO)
Gemäß Art. 6 Abs. 1 Buchst. c DSGVO darf ein Verantwortlicher Daten übermitteln, wenn er die Daten aufgrund einer rechtlichen Verpflichtung verarbeitet, der er unterliegt.

Sofern die Polizei daher auf Grundlage der Strafprozessordnung (§§ 160, 161, 161a oder auch 163 StPO) als Ermittlungsperson der Staatsanwaltschaft oder in eigener Sache bei Gefahr in Verzug tätig wird, ist das Unternehmen grundsätzlich rechtlich verpflichtet, in den Grenzen der StPO Auskunft zu erteilen.

Hier ist zu berücksichtigen, dass das Unternehmen – wird es z.B. als Zeuge gemäß §§ 48 ff. StPO herangezogen – ggf. keine Verpflichtung zur Aussage trifft, sondern dass die Auskunft gegenüber der Polizei auf freiwilliger Basis erfolgen kann oder Zeugnisverweigerungsrechte bestehen können.

Überwiegende berechtigte Interessen (Art. 6 Abs. 1 Buchst. f DSGVO)

Daneben lässt sich die Übermittlung auch über Art. 6 Abs. 1 Buchst. f DSGVO rechtfertigen.

So erkennt der Gesetzgeber die Weitergabe von Daten im Rahmen der Strafverfolgung in Erwägungsgrund 50 der Datenschutz-Grundverordnung als berechtigtes Interesse des Verantwortlichen an:

„Der Hinweis des Verantwortlichen auf mögliche Straftaten oder Bedrohungen der öffentlichen Sicherheit und die Übermittlung der maßgeblichen personenbezogenen Daten … an eine zuständige Behörde sollten als berechtigtes Interesse des Verantwortlichen gelten."

Die schutzwürdigen Interessen des Betroffenen werden hier regelmäßig hinter den berechtigten Interessen des Verantwortlichen zurücktreten.

Denn die Mitwirkung an der Aufklärung ist – wie oben beschrieben – eine gesetzliche Verpflichtung. Zudem besteht auch beim Betroffenen in der Regel ein Interesse, den Tathergang korrekt aufzuklären.

Und wie steht es mit besonderen personenbezogenen Daten?

Grundsätzlich ist auf die Verarbeitung von besonderen personenbezogenen Daten Art. 9 DSGVO anwendbar.

Dieser Artikel sieht allerdings über Abs. 2 Buchst. g in Verbindung mit Abs. 4 der Grundverordnung eine Öffnungsklausel für den nationalen Gesetzgeber vor, der damit eigene Regelungen treffen kann.

Der deutsche Gesetzgeber hat davon u.a. im Bereich der Videoüberwachung von öffentlich zugänglichen Räumen Gebrauch gemacht. Er hat mit § 4 Abs. 3 BDSG eine Regelung eingeführt, die insbesondere die Verarbeitung für Zwecke der Gefahrenabwehr oder Strafverfolgung erlaubt. Damit dürfen Verantwortliche beispielsweise Daten, die von Videoüberwachungskameras in Kaufhäusern, an Geldautomaten oder im öffentlich zugänglichen Gelände erhoben werden, für diese Zwecke herausgeben.

Das öffentliche Interesse, das im Rahmen von Art. 9 Abs. 2 Buchst. g DSGVO erforderlich ist, lässt sich aus der Verpflichtung des Unternehmens, nach der StPO mit den Behörden zusammenzuarbeiten, ableiten.

Sofern es sich um eine Videoüberwachung handelt, die nicht in den Anwendungsbereich von § 4 BDSG fällt – z.B. eine Überwachung von Produktionshallen, zu denen nur das Personal Zutritt hat –, ist auf den ersten Blick kein Erlaubnistatbestand ersichtlich, der die Weitergabe von besonderen personenbezogenen Daten legitimieren würde: Weder Art. 9 DSGVO noch § 22 BDSG treffen dazu ausdrückliche Regelungen.

Teilweise lässt sich hier argumentieren, dass sich letztlich über die Verpflichtung des Unternehmens, nach StPO z.B. als Zeuge an einem Ermittlungsverfahren mitzuwirken, in Verbindung mit Art. 9 Abs. 2 Buchst. g DSGVO eine entsprechende Rechtsgrundlage ableiten lasse.

Das ist durchaus vertretbar. Im Einzelfall sollte das allerdings der Datenschutzbeauftragte noch einmal kritisch prüfen.

Wie umgehen mit Zweckänderungen?

Verantwortliche müssen bereits bei der Erhebung von Daten den Zweck bestimmen, dem die jeweilige Verarbeitung dient. Im Rahmen der Videoüberwachung werden die Zwecke wie z.B. Strafverfolgung und Prävention regelmäßig bereits vor Erhebung festgelegt. Die Betroffenen müssen darüber nach Art. 13 DSGVO informiert werden.

Anders stellt sich die Lage dar, wenn Verantwortliche die Daten z.B. im Rahmen eines vertraglichen Verhältnisses und für die Erfüllung vertraglicher Zwecke erheben. Dann ist die Verarbeitung – d.h. die Weitergabe an die Polizei – eine Verarbeitung für andere Zwecke und damit eine Zweckänderung im Sinne von Art. 6 Abs. 4 DSGVO. Diesen DSGVO-Artikel konkretisiert § 24 BDSG.

Nach § 24 Abs. 1 Nr. 1 BDSG ist eine Zweckänderung bei der Verarbeitung von personenbezogenen u.a. dann zulässig, wenn „sie zur Abwehr von Gefahren für die öffentliche Sicherheit oder zur Verfolgung von Straftaten erforderlich ist".

Insofern lässt sich argumentierten, dass Verantwortliche die Daten auch für diese Zwecke weitergeben dürfen.

24 Abs. 2 BDSG regelt Zweckänderungen bei der Verarbeitung von besonderen personenbezogenen Daten. Diese ist ebenfalls für die in § 24 Abs. 1 Nr. 1 BDSG aufgeführten Zwecke zulässig – vorausgesetzt, ein Ausnahmetatbestand von Art. 9 Abs. 2 DSGVO oder von § 22 BDSG erlaubt die Verarbeitung.

Insofern lässt sich wohl entsprechend der obigen Argumentation davon ausgehen, dass jedenfalls die Daten der Videoüberwachung öffentlich zugänglicher Räume für geänderte Zwecke genutzt werden dürfen – sofern hier überhaupt eine Zweckänderung erfolgt.

Die Weitergabe anderer Videoüberwachungen müssen Verantwortliche zumindest kritisch daraufhin prüfen, ob Art. 9 Abs. 2 Buchst. g DSGVO in Verbindung mit der StPO eine Rechtsgrundlage bilden kann.

Schritt 4: Daten herausgeben und Prozess dokumentieren

Gibt ein Verantwortlicher die Daten weiter, muss er sicherstellen, dass er dabei den Grundsatz der Datenminimierung einhält. Das bedeutet, nur die Daten herauszugeben, die für die Ermittlung tatsächlich erforderlich sind und nicht z.B. das komplette Videomaterial. Weiterhin sind technisch-organisatorische Maßnahmen zum Schutz der Daten umzusetzen. Konkret heißt das, z.B. Verschlüsselungstechniken einzusetzen oder die Daten per Kurier und besser schriftlich als elektronisch zu übermitteln.

Achten Sie darauf, dass der gesamte Vorgang zum Nachweis seiner Rechtmäßigkeit (siehe Art. 5 DSGVO) dokumentiert ist. Das beginnt mit Schritt 1 und endet mit Schritt 4. Insbesondere ist die Rechtmäßigkeitsprüfung in Schritt 3 – die ggf. eine Interessenabwägung erfordert – nachvollziehbar zu dokumentieren. Hierzu kann Ihnen die Checkliste: Wie umgehen mit Auskunftsverlangen der Polizei? weiterhelfen.

Sonstige Überlegungen

Es kann sich empfehlen, die Vorgehensweise im Verfahrensverzeichnis nach Art. 30 DSGVO zu dokumentieren. Sehr sinnvoll sind auch Anweisungen an die Mitarbeiter, denen zu entnehmen ist, wie sie vorzugehen haben.

Zudem müssen Verantwortliche sicherstellen, dass die Betroffenen nach Art. 13 ff. DSGVO ordnungsgemäß belehrt werden; dies gilt insbesondere, wenn eine Zweckänderung erfolgt.

Weiterhin ist zu bedenken, ob und inwieweit ein Auskunftsverlangen nach Art. 15 DSGVO auch solche Daten umfassen könnte – bzw. wie sich etwaige Risiken für Dritte, die sich daraus ergeben könnten, abmildern lassen (Schwärzung von gespeicherten Daten o.Ä.).

Fazit: einheitliche Spielregeln schaffen

Das polizeiliche Auskunftsverlangen und den ordnungsgemäßen Umgang damit sollten Verantwortliche als Teil des unternehmensinternen Datenschutzmanagements dokumentieren und leben.

Da es – je nach Branche – zu Anfragen von Jugendämtern, Sozialämtern oder anderen Behörden kommen kann, sollten auch für diese Fälle einheitliche Spielregeln vorhanden sein.

Das stellt die datenschutzrechtliche Compliance sicher und erleichtert den Mitarbeitern die Arbeit.

Quelle:
www.datenschutz-praxis.de