

Häufig gestellte Fragen (FAQ)

FAQ 8: AUSKUNFTSRECHT

AUSKUNFTSRECHT

Personen müssen Zugang zu Daten haben, die eine Organisation über sie gespeichert hat, und diese Daten berichtigen, ergänzen oder löschen lassen können, wenn sie unrichtig sind. Der Zugang kann jedoch verwehrt werden, wenn seine Gewährung mit Kosten oder Arbeit verbunden ist, die im Einzelfall in keinem Verhältnis zum Nachteil für die Privatsphäre des Betroffenen stehen, oder wenn legitime Rechte Dritter verletzt würden.

F 1: Gibt es ein absolutes Auskunftsrecht?

A 1: Nein. Nach den Grundsätzen des „sicheren Hafens“ ist das Auskunftsrecht zwar grundlegend für den Schutz der Privatsphäre und ermöglicht es dem einzelnen, die Richtigkeit von Daten zu überprüfen, die über ihn gespeichert sind. Die Pflicht einer Organisation, Personen Zugang zu den sie betreffenden personenbezogenen Daten zu gewähren, hat jedoch Grenzen, die sich nach dem Grundsatz der Verhältnismäßigkeit und der Zumutbarkeit bestimmen, und muss in bestimmten Fällen abgemildert werden. In der Begründung zu den Datenschutzleitlinien der OECD von 1980 wird schon klar gesagt, dass das Auskunftsrecht nicht absolut ist. Die Organisation ist nicht verpflichtet, so gründlich zu recherchieren, wie es etwa im Rahmen einer gerichtlichen Untersuchung erforderlich wäre, und muss auch nicht Zugang zu allen von verschiedenen Speicherformen gewähren, in denen Daten über den Betroffenen gespeichert sind.

Verlangt jemand Zugang zu den über ihn gespeicherten Daten, sollte sich die angesprochene Organisation zunächst fragen, welche Gründe die Person dazu veranlassen. Ist beispielsweise eine Anfrage vage formuliert oder betrifft sie einen sehr weiten Bereich, so kann die Organisation mit der Person in Dialog treten, um die Gründe für die Anfrage besser zu verstehen und die gewünschten Daten zu ermitteln. Die Organisation kann sich danach erkundigen, mit welchen Teilen der Organisation die Person Kontakt hatte und/oder um welche Art von Daten (oder deren Nutzung) es geht. Wer Zugang zu den ihn betreffenden Daten verlangt, muss das allerdings nicht begründen.

Bei der Beurteilung der Zumutbarkeit sind die Kosten und die Arbeit zu berücksichtigen, die die Gewährung des Zugangs erfordert, sie sind aber nicht entscheidend. Bilden die Daten etwa die Grundlage für Entscheidungen, die für die Person von großer Tragweite sind (z. B. die Gewährung oder Versagung erheblicher Vorteile wie eine Versicherung, einen Kredit oder einen Arbeitsplatz), dann ist es der Organisation zumutbar, über diese Daten Auskunft zu geben, selbst wenn das einen relativ hohen Kosten- und Arbeitsaufwand erfordert.

Wenn die angeforderten Daten nicht sensibel sind oder nicht für Entscheidungen verwendet werden, die für die Person von großer Tragweite sind (z. B. nicht sensible Marketingdaten, nach

denen entschieden wird, ob die Person einen Katalog zugesandt bekommt), aber leicht zugänglich sind und kostengünstig zur Verfügung gestellt werden können, muss die Organisation Zugang zu den Daten gewähren, die sie über die Person speichert. Diese Daten können von der Person selbst erhoben, im Verlauf eines Geschäftsvorgangs gesammelt oder von anderen erlangt worden sein.

Wegen seines grundlegenden Charakters sollen Organisationen das Auskunftsrecht nie ohne Not beschränken. Müssen z. B. bestimmte Daten geschützt werden und lassen sie sich leicht von den Daten trennen, zu denen Zugang verlangt wird, sollte die Organisation die geschützten Daten unkenntlich machen und die übrigen zur Verfügung stellen. Beschließt eine Organisation in einem bestimmten Fall, keinen Zugang zu gewähren, sollte sie der Person, die um Zugang ersucht hat, ihre Entscheidung begründen und ihr eine Kontaktstelle nennen, die weitere Auskünfte erteilt.

F 2: Was sind vertrauliche Geschäftsdaten und dürfen Organisationen den Zugang zu personenbezogenen Daten verwehren, um vertrauliche Geschäftsdaten zu schützen?

A 2: Vertrauliche Geschäftsdaten (in den Federal Rules of Civil Procedure on discovery als „confidential commercial information“ bezeichnet) sind Daten, die ihr Inhaber durch besondere Vorkehrungen vor unbefugtem Zugriff geschützt hat, weil ihre Kenntnis Konkurrenten Vorteile verschaffen würde. Ein spezielles Rechnerprogramm, das eine Organisation verwendet, etwa ein Modellierungsprogramm, oder die Einzelheiten dieses Programms können vertrauliche Geschäftsdaten sein. Können vertrauliche Geschäftsdaten leicht von den Daten getrennt werden, zu denen Zugang verlangt wird, sollte die Organisation die vertraulichen Daten unkenntlich machen und die nichtvertraulichen zur Verfügung stellen. Eine Organisation kann den Zugang zu personenbezogenen Daten verwehren oder einschränken, wenn dadurch eigene vertrauliche Geschäftsdaten, wie z. B. von der Organisation erarbeitete Marketingkonzepte und Klassifikationen, offenbart würden oder aber Geschäftsdaten anderer, die einer vertraglichen Geheimhaltungspflicht unterliegen, sofern eine Geheimhaltungsverpflichtung in solchen Fällen üblich oder vorgeschrieben ist.

F 3: Kann eine Organisation, die personenbezogene Daten in ihren Datenbanken gespeichert hat, Personen lediglich mitteilen, welche Daten über sie gespeichert sind, oder muss sie ihnen Zugang zu den Datenbanken gewähren?

A 3: Es genügt eine Mitteilung über die gespeicherten Daten, der Person muss kein Zugang zu den Datenbanken der Organisation gewährt werden.

F 4: Muss eine Organisation ihre Datenbanken erforderlichenfalls umstrukturieren, um Auskunft gewähren zu können?

A 4: Die Organisation muss nur Auskunft über die von ihr gespeicherten personenbezogenen Daten geben. Das Auskunftsrecht begründet keine Pflicht, Dateien mit personenbezogenen Daten aufzubewahren, zu pflegen oder erforderlichenfalls umzustrukturieren.

F 5: Den vorstehenden Antworten ist zu entnehmen, dass Personen der Zugang zu sie betreffenden Daten in bestimmten Fällen verwehrt werden kann. In welchen anderen Fällen ist das noch möglich?

A 5: Das ist nur in wenigen Fällen möglich und muss in jedem Fall konkret begründet werden. Eine Organisation kann den Zugang zu personenbezogenen Daten insoweit verwehren, als ihre Bekanntgabe wesentliche öffentliche Belange gefährden würde wie die nationale Sicherheit, die Verteidigung oder die öffentliche Sicherheit. Außerdem kann der Zugang verwehrt werden, wenn personenbezogene Daten *ausschließlich* für wissenschaftliche oder statistische Zwecke verarbeitet werden sollen. Weitere Gründe für die Verweigerung oder Beschränkung des Zugangs sind:

- a) Beeinträchtigung von Rechtsvollzug oder Vollstreckung, einschließlich der Verhütung, Untersuchung oder Aufdeckung von Straftaten, oder des Rechts auf einen fairen Prozeß;
- b) Beeinträchtigung eines zivilrechtlichen Verfahrens, einschließlich der Abwehr, Untersuchung und Verfolgung von Rechtsansprüchen, oder des Rechts auf einen fairen Prozeß;
- c) die personenbezogenen Daten haben Bezüge zu anderen Personen, die nicht unkenntlich gemacht werden können;
- d) gesetzliche oder andere berufliche Rechte und Pflichten werden verletzt;
- e) es kommt zum Bruch der notwendigen Vertraulichkeit künftiger oder laufender Verhandlungen, z. B. über die Übernahme börsennotierter Organisationen;
- f) die Sicherheitsüberprüfung von Arbeitnehmern oder ein Beschwerdeverfahren wird beeinträchtigt;
- g) die Vertraulichkeit, die bei der Neubesetzung von Stellen oder bei der Umorganisation von Organisationen für eine gewisse Zeit gewahrt werden muss, wird gefährdet;
- h) die Vertraulichkeit ist gefährdet, die bei der Überwachung, bei der Prüfung und bei sonstigen gesetzlich vorgeschriebenen Ordnungsfunktionen im Zusammenhang mit der ordnungsgemäßen Wirtschaftsführung erforderlich ist;
- i) die Gewährung des Zugangs ist mit unverhältnismäßigen Kosten oder Arbeit verbunden, oder sie führt zur Beeinträchtigung der Rechte oder der berechtigten Interessen anderer.

Eine Organisation, die sich auf einen dieser Ausnahmefälle beruft, muss nachweisen, dass er tatsächlich vorliegt (was in der Regel der Fall ist). Wie bereits gesagt sollen der anfragenden Person die Gründe für eine Zugangsverweigerung oder -beschränkung mitgeteilt werden, und es soll ihr eine Anlaufstelle für weitere Fragen genannt werden.

F 6: Kann eine Organisation eine Gebühr erheben, um die Kosten für die Auskunftserteilung zu decken?

A 6: Ja, die OECD-Leitlinien gestehen Organisationen das Recht zu, eine Gebühr zu erheben. Sie darf aber nicht überhöht sein. Organisationen dürfen also eine angemessene Gebühr in Rechnung stellen. Eine Gebühr kann sinnvoll sein, um wiederholten oder belästigenden Anfragen vorzubeugen.

Organisationen, die öffentlich zugängliche Information gegen Entgelt anbieten, können ihre üblichen Gebühren erheben. Alternativ können Personen Zugang zu sie betreffenden Daten von der Organisation verlangen, die sie ursprünglich erhoben hat.

Der Zugang darf nicht aus Kostengründen verwehrt werden, wenn die Personen, die den Zugang verlangen, bereit sind, diese Kosten zu übernehmen.

F 7: Ist eine Organisation verpflichtet, Zugang zu personenbezogenen Daten zu gewähren, die sie aus öffentlichen Datenbeständen gewonnen hat?

A 7: Zunächst eine Begriffsklärung: öffentliche Datenbestände sind Datenbestände, die von Ämtern aller Ebenen geführt werden und der Öffentlichkeit zur Einsichtnahme offenstehen. Das Auskunftsrecht gilt für solche Daten nur, wenn sie mit anderen personenbezogenen Daten kombiniert sind. Das Auskunftsrecht gilt nicht, wenn lediglich kleine Mengen von Daten aus nichtöffentlichen Quellen verwendet wurden, um die öffentlichen Daten zu indexieren oder zu ordnen. Die Bestimmungen der einschlägigen Rechtsvorschriften über die Einsichtnahme in Datenbestände sind einzuhalten. Sind Daten aus öffentlichen Beständen mit anderen als den genannten Datenmengen aus nichtöffentlichen Quellen kombiniert, muss die Organisation Zugang zu allen personenbezogenen Daten gewähren, sofern nicht einer der genannten Ausnahmefälle vorliegt.

F 8: Gilt das Auskunftsrecht für öffentlich verfügbare personenbezogene Daten?

A 8: Wie bei Daten, die aus öffentlichen Beständen gewonnen wurden, (siehe F 7) ist das Auskunftsrecht nicht auf Daten anzuwenden, die bereits der Öffentlichkeit zur Verfügung stehen, sofern sie mit nicht öffentlich verfügbaren Daten kombiniert sind.

F 9: Wie kann sich eine Organisation vor wiederholten oder belästigenden Auskunftsbegehren schützen?

A 9: Eine Organisation muss solchen Auskunftsbegehren nicht entsprechen. Deshalb kann sie für Auskünfte eine angemessene Gebühr erheben oder die Zahl der Anfragen einer Person innerhalb eines bestimmten Zeitraums angemessen begrenzen. Bei der Festlegung dieser Grenze sind Faktoren zu berücksichtigen wie die Häufigkeit, mit der Daten aktualisiert werden, der Zweck, für den die Daten verwendet werden, und die Art der Daten.

F 10: Wie kann sich eine Organisation vor Auskunfterschleichung schützen?

A 10: Eine Organisation muss nur Auskunft erteilen, wenn die anfragende Person ihre Identität zweifelsfrei nachweist.

F 11: Gibt es eine Frist, innerhalb derer Auskunft erteilt werden muss?

A 11: Ja, eine Organisation soll ohne übermäßige Verzögerung und innerhalb angemessener Frist Auskunft erteilen. Wie in der Begründung der OECD-Datenschutzleitlinien von 1980 dargelegt wird, kann diese Forderung auf verschiedene Weise erfüllt werden. So kann eine Organisation, die Daten verarbeitet, von der Pflicht zur sofortigen Auskunftserteilung befreit werden, wenn es erfasste Personen regelmäßig informiert.