

Schatten-IT:

Risiken erkennen und richtig handeln

ungeprüfter
Nebenpfad

geprüfte
Datenroute



AI GENERATED

SCHATTEN-IT: WENN ANWENDUNGEN IM UNTERNEHMEN UNTER DEM RADAR LAUFEN

SELBSTTEST

Wo lauert Schatten-IT in Ihrem Unternehmen? 4–5

ALARMZEICHEN ERKENNEN

Warnsignale: Wann Sie genauer hinschauen sollten 8



Onlinebereich:
<https://www.privacyxperts.de>



Live-Talk:
<https://t1p.de/live-talk>



E-Mail-Beratung:
<https://t1p.de/anna-mauch>



PRIVACYXPERTS



Mehr Transparenz statt Verbote

Liebe Leserin, lieber Leser,

Schatten-IT gibt es in fast jedem Unternehmen – auf dem Schirm haben sie jedoch längst nicht alle. Cloud-Dienste, KI-Anwendungen und Online-tools sind schnell eingesetzt, oft ohne Wissen von IT oder Datenschutz.

Für Sie als Datenschutzbeauftragten gilt es, Transparenz zu schaffen und Risiken frühzeitig zu erkennen. Dieses Themenheft zeigt, wie Sie Schatten-IT identifizieren, bewerten und gemeinsam mit IT und Fachbereichen datenschutzkonforme Lösungen entwickeln.

Viele Grüße

Dr. Anna-Kathrin Mauch,
Rechtsanwältin und Redakteurin

Ihre Expertin für Datenschutz

Dr. Anna-Kathrin Mauch ist Rechtsanwältin und Europajuristin mit Erfahrung im Vertrags- und Datenschutzrecht. Sie bringt Datenschutz verständlich und praxisnah auf den Punkt.

Inhalt

Durchblick schaffen

Schatten-IT verstehen:
Wie und warum sie im Unternehmen entsteht

Seiten 1–2

Risiken erkennen

Unter dem Radar: Risiken und Folgen von Schatten-IT erkennen

Seite 3

Selbst einschätzen

Selbsttest: Wo lauert Schatten-IT in Ihrem Unternehmen?

Seiten 4–5

Gezielt vorgehen

Schatten-IT angehen:
Ihr Schritt-für-Schritt-Leitfaden

Seiten 6–7

Alarmzeichen erkennen

Warnsignale: Wann Sie genauer hinschauen sollten

Seite 8



Zu Ihrem Onlinebereich:
<https://www.privacyxperts.de>



Live-Talk:
<https://t1p.de/live-talk>



E-Mail-Beratung:
<https://t1p.de/anna-mauch>

Impressum



ein Unternehmensbereich des
VNR Verlags für die Deutsche Wirtschaft AG
Theodor-Heuss-Str. 2–4, 53095 Bonn
Telefon: 02 28 / 9 55 01 60
Fax: 02 28 / 3 69 64 80
ISSN: 1614 – 5674

Vorstand: Richard Rentrop, Michael Schrader, Bonn
V.i.S.d.P.: Michael Jodda (Adresse s. oben)
Produktmanagement: Franziska Rohrbach, Bonn

Autorin:
Dr. Anna-Kathrin Mauch, Rottweil
Design: Kreativ Konzept Agentur für Werbung, Bonn
Satz: Schmelzer Medien GmbH, Siegen
Druck: Warlich Druck Meckenheim GmbH,
Am Hambuch 5, 53340 Meckenheim
Bildnachweise: Titel: Adobe Stock | privacy_KI generiert; Seite 1:
Adobe Stock | tippapatt
Erscheinungsweise: 36-mal pro Jahr
E-Mail: kundendienst@privacyxperts.de
Internet: www.privacyxperts.de
(bei Rückfragen bitte Kundennummer angeben)

Alle Angaben wurden mit äußerster Sorgfalt ermittelt und überprüft. Sie basieren jedoch auf der Richtigkeit uns erteilter Auskünfte und unterliegen Veränderungen. Eine Gewähr kann deshalb nicht übernommen werden.

Im Interesse der Lesbarkeit verzichten wir in unseren Beiträgen auf geschlechtsbezogene Formulierungen. Selbstverständlich sind immer alle Geschlechterformen gemeint, auch wenn explizit nur eines der Geschlechter angesprochen wird.

Dieses Produkt besteht aus FSC®-zertifiziertem Papier.

© 2026 by VNR Verlag für die Deutsche Wirtschaft AG, Bonn, Berlin, Bukarest, Jacksonville, Manchester, Passau, Warschau



Wenn Mitarbeiter Anwendungen im Unternehmen einsetzen, die der IT nicht bekannt sind, kann das Risiken auslösen.

Schatten-IT: Wie und warum sie im Unternehmen entsteht

Digitale Anwendungen sind heute nur wenige Klicks entfernt. Cloud-Dienste, KI-Assistenten und spezialisierte Onlinetools lassen sich schnell in den Arbeitsalltag integrieren. Dabei entstehen leicht Datenverarbeitungen außerhalb der bekannten und kontrollierten IT-Landschaft – die sogenannte Schatten-IT. Für Datenschutzbeauftragte ist das eine praktische Herausforderung: Denn nur bekannte Datenverarbeitungen und IT-Systeme lassen sich datenschutzrechtlich bewerten und wirksam steuern. Bleiben Anwendungen unentdeckt, können Risiken für Datenschutz und Informationssicherheit lange unbemerkt bleiben.

Was ist Schatten-IT?

Von Schatten-IT spricht man, wenn Beschäftigte digitale Anwendungen oder IT-Dienste nutzen, ohne dass diese zuvor von der IT-Abteilung oder dem Arbeitgeber freigegeben wurden. Dazu gehören beispielsweise KI-Anwendungen, Cloud-Speicher, Messenger-Dienste, Projektmanagement-Tools oder selbst erstellte Datenbanken.

Entscheidend ist nicht, welche Anwendung genutzt wird, sondern wie sie im Unternehmen eingeführt wurde. Erfolgt der Einsatz außerhalb der etablierten IT-, Beschaffungs- oder Datenschutzprozesse, fehlt häufig die Prüfung. Dadurch bleibt etwa unklar,

- › ob personenbezogene Daten verarbeitet werden,
- › ob ein Vertrag zur Auftragsverarbeitung erforderlich ist,
- › ob Daten in Drittländer übermittelt werden,
- › welche technischen und organisatorischen Maßnahmen zum Schutz der Daten bestehen oder
- › wer auf die Daten zugreifen kann.

Schatten-IT beschränkt sich längst nicht mehr auf selbst installierte Programme oder den sprichwörtlichen „Server unter dem Schreibtisch“. Cloud Computing, Software-as-a-Service (SaaS) und generative KI haben die Einstiegshürden erheblich gesenkt: Neue Anwendungen sind innerhalb weniger Minuten verfügbar und teilweise kostenlos. Dadurch kann Schatten-IT heute leichter entstehen und sich im Unternehmen verbreiten.

Wie entsteht Schatten-IT im Unternehmen?

Schatten-IT entsteht meist schleichend. Was mit der Suche nach einer schnellen Lösung für ein konkretes Problem beginnt, kann sich im Arbeitsalltag etablieren, ohne jemals die vorgesehenen Freigabe- und Prüfprozesse durchlaufen zu haben. IT und Datenschutz erfahren dann mitunter erst durch eine interne Prüfung, einen Sicherheitsvorfall oder eine Betroffenenanfrage von der Anwendung.

Typischer Weg zur Schatten-IT

Fachbereich benötigt kurzfristig eine Lösung.



Unternehmenslösung erfüllt den Bedarf nicht, ist nicht bekannt oder der Freigabeprozess dauert zu lange.



Cloud-Dienst, KI-Anwendung oder Onlinetool wird ohne Abstimmung genutzt.



Personenbezogene Daten werden verarbeitet.



IT und Datenschutz erfahren häufig erst durch einen Zufall, einen Sicherheitsvorfall oder eine Betroffenenanfrage von der Nutzung.



Praxistipp

Wenn Sie auf Schatten-IT im Unternehmen aufmerksam werden, bedeutet das nicht, dass Sie die Anwendung automatisch verbieten müssen. Entscheidend ist, warum sie genutzt wird und welche Risiken damit verbunden sind. Oft lässt sich eine passende datenschutzkonforme Lösung finden, die den tatsächlichen Bedarf der Beschäftigten berücksichtigt. Einfache und zügige Freigabeprozesse helfen zusätzlich dabei zu verhindern, dass Beschäftigte auf eigene Lösungen ausweichen.

Eigene Datenbanken	Excel- oder Access-Dateien	Fachbereiche verwalten personenbezogene Daten in selbst erstellten Datenbanken außerhalb zentraler Systeme.
Browser-Erweiterungen	KI-Plug-ins, Übersetzungsdienste	Erweiterungen erhalten Zugriff auf Inhalte von Webseiten, Dokumenten oder E-Mails.
Fachanwendungen	CRM-, HR- oder Recruiting-Software	Fachabteilungen beschaffen und nutzen Software eigenständig, ohne die vorgesehenen Freigabeprozesse einzuhalten.

Typische Erscheinungsformen von Schatten-IT

Schatten-IT umfasst keine fest definierten Anwendungen oder Dienste. Grundsätzlich kann nahezu jede digitale Anwendung zur Schatten-IT werden, wenn sie ohne die erforderliche Freigabe oder außerhalb der vorgesehenen IT- und Datenschutzprozesse eingesetzt wird.

Entscheidend ist daher nicht die Art der Anwendung für Schatten-IT, sondern die Art ihrer Einführung und konkreten Nutzung im Unternehmen.

In der Praxis treten bestimmte Anwendungsgruppen besonders häufig auf. Die folgende Übersicht zeigt typische Beispiele und erläutert, wann daraus Schatten-IT wird.

Übersicht: Erscheinungsformen der Schatten-IT

Anwendungsgruppe	Typische Beispiele	Wann wird daraus Schatten-IT?
KI-Anwendungen und KI-Agenten	ChatGPT, Claude, Gemini, Copilot; selbst erstellte KI-Agenten und automatisierte KI-Workflows	Beschäftigte nutzen KI-Anwendungen oder erstellen KI-Agenten und -Workflows ohne Freigabe – auch durch die Kombination bereits freigegebener Tools.
Cloud-Speicher	Dropbox, Google Drive, OneDrive, iCloud	Dateien werden außerhalb der freigegebenen Unternehmensspeicher gespeichert oder mit Dritten geteilt.
Messenger-Dienste	WhatsApp, Signal, Telegram	Kunden-, Beschäftigten- oder Unternehmensdaten werden über private Messenger ausgetauscht.
Projektmanagement	Trello, Notion, Asana, Monday	Projekt-, Kunden- oder Beschäftigtendaten werden ohne Freigabe in externen Tools verarbeitet.
Dateiaustausch	WeTransfer, Smash, Filemail	Personenbezogene oder vertrauliche Dateien werden über nicht freigegebene Dienste versendet.
Umfrage- und Formulartools	SurveyMonkey, Typeform, Google Forms	Personenbezogene Daten werden ohne datenschutzrechtliche Prüfung oder Freigabe erhoben.
Grafik- und Marketingtools	Canva, Adobe Express	Mitarbeiter-, Kunden- oder Produktdaten werden in externe Cloud-Dienste hochgeladen.

Warum nutzen Beschäftigte Schatten-IT?

Wer Schatten-IT reduzieren möchte, sollte verstehen, warum Beschäftigte auf nicht freigegebene Anwendungen zurückgreifen. Dahinter steckt meist weder mangelndes Datenschutzbewusstsein noch die Absicht, interne Vorgaben zu umgehen. Vielmehr möchten Mitarbeitende ihre Aufgaben schneller, einfacher oder effizienter erledigen – häufig aus praktischer Notwendigkeit.

Für Sie als Datenschutzbeauftragten ist es wichtig, diese Ursachen zu kennen, um passende und praxistaugliche Maßnahmen entwickeln zu können.

Gründe für Einsatz von Schatten-IT und Beispiele

Beweggrund	Typisches Praxisbeispiel	Mögliche Auswirkungen
Beschaffungsprozesse dauern zu lange.	Ein Projekt startet kurzfristig und die Fachabteilung beschafft eigenständig ein Onlinetool.	Die Anwendung wird ohne Datenschutz- und IT-Prüfung eingesetzt.
Unternehmenssoftware bietet benötigte Funktionen nicht.	Das Marketing nutzt Canva, weil die vorhandene Software bestimmte Funktionen nicht bietet.	Personenbezogene oder vertrauliche Unternehmensdaten werden in einem externen Dienst verarbeitet.
KI spart Zeit.	Verträge, Bewerbungen oder E-Mails werden von einem KI-Assistenten zusammengefasst oder analysiert.	Vertrauliche oder personenbezogene Daten gelangen an den Anbieter.
Einfache Bedienung	Die Registrierung ist in wenigen Minuten abgeschlossen und die Anwendung sofort einsatzbereit.	Die Nutzung erfolgt ohne Beteiligung der IT oder des Datenschutzes.
Zusammenarbeit mit Externen	Dateien werden über private Cloud-Speicher oder Dateiaustauschdienste geteilt.	Unternehmen verlieren die Kontrolle über Speicherorte und Datenflüsse.
Mobile Arbeit und Homeoffice	Beschäftigte greifen auf private Geräte oder Anwendungen zurück.	Geschäftliche und private Daten werden miteinander vermischt.
Fehlendes Risikobewusstsein	Beschäftigte erkennen die datenschutzrechtliche Relevanz einer Anwendung nicht.	Risiken bleiben lange unentdeckt und werden häufig erst später erkannt.
Empfehlungen von Kollegen	Neue Anwendungen werden innerhalb des Teams weiterempfohlen und übernommen.	Nicht freigegebene Anwendungen verbreiten sich schrittweise im Unternehmen.

Unter dem Radar: Risiken und Folgen von Schatten-IT erkennen

Nicht jede nicht freigegebene Anwendung führt automatisch zu einem Datenschutzverstoß. Das eigentliche Risiko liegt vielmehr darin, dass Datenverarbeitungen außerhalb der bekannten IT- und Datenschutzprozesse stattfinden. Dadurch fehlen häufig Transparenz, Kontrolle und eine datenschutzrechtliche Bewertung.

Wenn Schatten-IT zum Datenschutzproblem wird

Eine Vertriebsmitarbeiterin nutzt einen privaten Cloud-Speicher, um Kundendokumente mit einem externen Dienstleister auszutauschen. Der Dienst beschleunigt die Zusammenarbeit, ist IT und Datenschutz jedoch nicht bekannt. Erst als ein Kunde Auskunft nach Art. 15 DSGVO verlangt, stellt sich heraus, dass ein Teil seiner personenbezogenen Daten ausschließlich in diesem Cloud-Speicher liegt.

Nun müssen kurzfristig zahlreiche Fragen geklärt werden: Wo werden die Daten gespeichert? Wer hatte Zugriff? Wurde ein Vertrag zur Auftragsverarbeitung geschlossen? Ist eine Übermittlung in ein Drittland erfolgt?

Die wichtigsten Risiken im Überblick

Welche datenschutzrechtlichen Risiken mit Schatten-IT verbunden sind, hängt von der jeweiligen Anwendung und ihrer konkreten Nutzung ab. Für Sie als Datenschutzbeauftragten kommt es deshalb darauf an, genau hinzusehen: Welche Daten werden verarbeitet? Wer erhält Zugriff auf die Daten? Und welche Vorgaben sind zu beachten?

Darüber hinaus kann der Einsatz nicht freigegebener IT-Lösungen weitere rechtliche Anforderungen berühren, etwa die IT-Sicherheit, das Geschäftsgeheimnis-, Urheber- und Arbeitsrecht sowie die betriebliche Mitbestimmung. Auch diese Bereiche sollten Sie bei Ihrer Bewertung im Blick behalten.

Übersicht: Rechtliche Risiken durch Schatten-IT



Risiko	Was bedeutet das in der Praxis?	Rechtliche Relevanz
Fehlende Transparenz	Es ist nicht bekannt, welche Anwendungen Beschäftigte tatsächlich nutzen.	Unbekannte Verarbeitungen können weder geprüft noch dokumentiert werden.
Unzulässige Datenübermittlungen	Personenbezogene Daten werden an externe Anbieter oder in Drittländer übermittelt.	Rechtsgrundlage, Drittlandtransfer und ggf. Auftragsverarbeitung müssen geprüft werden.
Unzureichende Datensicherheit	Anwendungen entsprechen möglicherweise nicht den Sicherheitsanforderungen des Unternehmens.	Anforderungen der Datenschutz-Grundverordnung (DSGVO) und ggf. des IT-Sicherheitsrechts können betroffen sein; zudem steigt das Risiko von Sicherheitsvorfällen.
Fehlende Verträge	Erforderliche Verträge, etwa zur Auftragsverarbeitung, wurden nicht abgeschlossen.	Die datenschutzkonforme Einbindung des Dienstleisters ist nicht gewährleistet.
Unkontrollierte Zugriffe	Berechtigungen und Nutzerkreise sind nicht bekannt oder nicht geregelt.	Vertraulichkeit und Integrität personenbezogener Daten sowie Geschäftsgeheimnisse können gefährdet sein.
Fehlende Dokumentation	Verarbeitungen erscheinen nicht im Verzeichnis der Verarbeitungstätigkeiten oder anderen erforderlichen Dokumentationen.	Gesetzliche Nachweis- und Dokumentationspflichten können nicht erfüllt werden; Audits werden erschwert.
Erschwerte Betroffenenrechte	Daten befinden sich in unbekannten Systemen.	Auskunfts-, Lösungs- oder Berichtigungsansprüche lassen sich nur schwer erfüllen.
Dateninkonsistenzen	Daten werden parallel in verschiedenen Anwendungen gespeichert und gepflegt.	Unterschiedliche Datenbestände erschweren eine rechtmäßige und einheitliche Verarbeitung.
Erhöhte Angriffsfläche	Unbekannte Anwendungen verfügen möglicherweise über unzureichende Sicherheitsmechanismen oder Schnittstellen.	Das Risiko von Cyberangriffen und Datenschutzverletzungen steigt; auch Anforderungen des IT-Sicherheitsrechts können betroffen sein.
Gefährdung von Geschäftsgeheimnissen	Vertrauliche Unternehmensinformationen werden in nicht freigegebenen Anwendungen verarbeitet oder an externe Anbieter übermittelt.	Der angemessene Schutz von Geschäftsgeheimnissen kann beeinträchtigt sein.
Urheberrechtliche Risiken	Geschützte Inhalte werden über nicht freigegebene Anwendungen genutzt, verarbeitet oder weitergegeben.	Urheber- und Nutzungsrechte können verletzt werden.
Arbeitsrechtliche Risiken	Beschäftigte nutzen Anwendungen entgegen internen Vorgaben oder ohne erforderliche Freigabe.	Arbeitsvertragliche Pflichten und betriebliche Regelungen können betroffen sein.
Fehlende Betriebsratseinbindung	Anwendungen werden eingeführt oder genutzt, ohne erforderliche Beteiligungsprozesse zu durchlaufen.	Beteiligungs- und Mitbestimmungsrechte des Betriebsrats können tangiert sein.



Selbsttest: Wo lauert Schatten-IT in Ihrem Unternehmen?

Wie gut ist Ihr Unternehmen beim Thema Schatten-IT aufgestellt? Mit dem folgenden Selbsttest können Sie schnell einschätzen, wo bereits gute Strukturen bestehen und wo noch Handlungsbedarf besteht. Beantworten Sie die Fragen so, wie die Abläufe in Ihrem Unternehmen tatsächlich gelebt werden. Die Auswertung gibt Ihnen eine erste Orientierung für die nächsten Schritte.

Anleitung

Bewerten Sie die folgenden Aussagen anhand Ihrer aktuellen Unternehmenssituation.

- ☐ Ja = 0 Punkte
- ☐ Teilweise = 1 Punkt
- ☐ Nein = 2 Punkte

Je höher die Gesamtpunktzahl, desto größer ist das Risiko, dass Schatten-IT im Unternehmen entsteht oder unentdeckt bleibt.

Selbsttest an Ihr Unternehmen anpassen

Der Selbsttest bietet eine erste, bewusst vereinfachte Orientierung, da alle Fragen in der Auswertung gleich gewichtet werden. Passen Sie den Fragenkatalog daher an die Besonderheiten Ihres Unternehmens an: Ergänzen Sie unternehmensspezifische Risikofaktoren und gewichten Sie besonders relevante Fragen stärker. So erhalten Sie eine aussagekräftigere Einschätzung Ihres individuellen Schatten-IT-Risikos.

Schatten-IT auf der Spur: Der Unternehmens-Check



Bereich / Frage	Ja	Teilweise	Nein
A. Transparenz und Überblick			
Ist bekannt, welche Cloud- und SaaS-Dienste in den einzelnen Fachbereichen tatsächlich genutzt werden?	☐	☐	☐
Existiert ein aktuelles und möglichst vollständiges Verzeichnis der eingesetzten Software und Anwendungen?	☐	☐	☐
Werden neue Anwendungen und Onlinedienste zentral erfasst?	☐	☐	☐
Kennen IT und Sie als Datenschutzbeauftragter die KI-Anwendungen, die im Unternehmen dienstlich genutzt werden?	☐	☐	☐
Werden Browser-Erweiterungen und Plug-ins zentral erfasst oder verwaltet?	☐	☐	☐
Ist bekannt, welche privaten Geräte für dienstliche Zwecke genutzt werden?	☐	☐	☐
Wird regelmäßig überprüft, ob neben den bekannten Anwendungen weitere, bislang nicht erfasste Dienste genutzt werden?	☐	☐	☐
B. Beschaffung und Freigabe			
Gibt es einen klar geregelten und dokumentierten Freigabeprozess für neue Software und Onlinedienste?	☐	☐	☐
Können Fachbereiche neue Anwendungen unkompliziert und mit vertretbarem Zeitaufwand beantragen?	☐	☐	☐
Werden IT und Sie als Datenschutzbeauftragter bei der Einführung neuer Anwendungen frühzeitig eingebunden?	☐	☐	☐
Werden auch kostenlose Onlinedienste sowie Test- und Pilotanwendungen in die Freigabeprozesse einbezogen?	☐	☐	☐
Gibt es definierte Kriterien, anhand derer über die Freigabe neuer Anwendungen entschieden wird?	☐	☐	☐
Ist für die Beschäftigten klar erkennbar, welche Anwendungen bereits freigegeben sind und welche nicht?	☐	☐	☐
Ist geregelt, wie mit Anwendungen umzugehen ist, die bereits ohne vorherige Freigabe eingesetzt werden?	☐	☐	☐
C. KI und Cloud-Dienste			
Gibt es verbindliche Vorgaben für den dienstlichen Einsatz von KI-Anwendungen?	☐	☐	☐
Ist geregelt, welche personenbezogenen oder vertraulichen Daten in KI-Systeme eingegeben werden dürfen?	☐	☐	☐
Werden auch selbst erstellte KI-Agenten und KI-Workflows, die auf bereits vorhandenen IT-Tools basieren, von den Freigabeprozessen erfasst?	☐	☐	☐
Sind private Cloud-Speicher für dienstliche Daten untersagt oder technisch eingeschränkt?	☐	☐	☐
Stehen geeignete und freigegebene Lösungen für Dateiaustausch, Zusammenarbeit und andere typische Anwendungsfälle zur Verfügung?	☐	☐	☐
Werden KI-Funktionen in Browsern, Office-Anwendungen und anderen bereits eingesetzten Programmen bei den internen Vorgaben berücksichtigt?	☐	☐	☐
Ist geregelt, ob und unter welchen Voraussetzungen Beschäftigte eigene Accounts bei KI- und Cloud-Diensten für dienstliche Zwecke anlegen dürfen?	☐	☐	☐

D. Organisation und Sensibilisierung

Werden Beschäftigte regelmäßig über Schatten-IT und die damit verbundenen Datenschutzrisiken informiert?	☐	☐	☐
Wissen Beschäftigte, an wen sie sich wenden können, wenn sie eine neue Anwendung benötigen oder einsetzen möchten?	☐	☐	☐
Werden Fachbereiche regelmäßig danach gefragt, welche neuen Anwendungen oder Onlinedienste sie tatsächlich nutzen?	☐	☐	☐
Ist Schatten-IT Bestandteil interner Audits oder vergleichbarer Kontroll- und Überprüfungsprozesse?	☐	☐	☐
Werden neue Beschäftigte bereits im Rahmen der Einarbeitung über Vorgaben zur Nutzung von Software, Cloud-Diensten und KI informiert?	☐	☐	☐
Werden festgestellte Fälle von Schatten-IT ausgewertet, um deren Ursachen zu erkennen und Prozesse anschließend zu verbessern?	☐	☐	☐
Können Beschäftigte mögliche Fälle von Schatten-IT unkompliziert und ohne unnötige Hürden melden?	☐	☐	☐

E. Datenschutz

Werden neue Anwendungen vor ihrer Freigabe systematisch auf datenschutzrechtliche Risiken geprüft?	☐	☐	☐
Wird bei externen Dienstleistern geprüft, ob eine Auftragsverarbeitung vorliegt und ein entsprechender Vertrag erforderlich ist?	☐	☐	☐
Werden mögliche Drittlandübermittlungen einschließlich der hierfür geltenden date	☐	☐	☐
Werden neue Verarbeitungstätigkeiten nach der Einführung einer Anwendung in die erforderliche Datenschutzdokumentation aufgenommen?	☐	☐	☐
Wird geprüft, ob Betroffenenrechte und Löschpflichten auch bei externen Diensten zuverlässig erfüllt werden können?	☐	☐	☐
Werden die technischen und organisatorischen Maßnahmen externer Anbieter vor der Freigabe angemessen bewertet?	☐	☐	☐
Wird vor der Freigabe geprüft, welche personenbezogenen Daten eine Anwendung tatsächlich verarbeitet und auf welcher Rechtsgrundlage dies erfolgt?	☐	☐	☐

Auswertung

Addieren Sie die Punkte aller 35 Fragen. Insgesamt können maximal 70 Punkte erreicht werden.

0–12 Punkte: niedriges Risiko

Ihr Unternehmen verfügt bereits über gute organisatorische und datenschutzrechtliche Strukturen, um Schatten-IT vorzubeugen und nicht freigegebene Anwendungen zu erkennen. Prüfen Sie dennoch regelmäßig, ob neue Technologien und veränderte Arbeitsweisen zusätzliche Risiken schaffen. Denn auch gut etablierte Strukturen bieten nur dann Sicherheit, wenn sie mit der tatsächlichen Entwicklung im Unternehmen Schritt halten.

13–29 Punkte: mittleres Risiko

Wichtige Strukturen sind vorhanden, werden jedoch noch nicht durchgängig umgesetzt. Dadurch können einzelne Anwendungen außerhalb der vorgesehenen Prozesse genutzt werden. Prüfen Sie insbesondere die Bereiche, in denen Sie mehrfach „Teilweise“ oder „Nein“ angekreuzt haben, und schließen Sie bestehende Lücken gezielt.

30–47 Punkte: erhöhtes Risiko

Es bestehen deutliche Anhaltspunkte dafür, dass Schatten-IT entstehen oder längere Zeit unentdeckt bleiben kann. Verschaffen Sie sich zunächst einen Überblick über die tatsächlich eingesetzten Anwendungen und überprüfen Sie insbesondere Freigabeprozesse, Verantwortlichkeiten und die Einbindung von IT und Datenschutz.

48–70 Punkte: hohes Risiko

Die Wahrscheinlichkeit unerkannter Schatten-IT ist hoch. Priorität sollte darauf liegen, tatsächlich genutzte Anwendungen sichtbar zu machen und risikoreiche Datenverarbeitungen zu identifizieren. Anschließend sollten klare Freigabeprozesse, Zuständigkeiten und praktikable Alternativen für die Fachbereiche geschaffen werden.

**Praxistipp**

Ein niedriger Punktestand bedeutet nicht automatisch, dass keine Schatten-IT vorhanden ist. Beschäftigte nutzen nicht freigegebene Anwendungen häufig aus praktischen Gründen und sprechen darüber oft nicht von sich aus. Ergänzen Sie den Selbsttest deshalb regelmäßig durch Gespräche mit den Fachbereichen, interne Audits sowie technische Analysen der tatsächlich genutzten Anwendungen. So lassen sich Risiken frühzeitig erkennen und geeignete Maßnahmen gezielt umsetzen.

Ihre nächsten Schritte

Schauen Sie sich zunächst die Fragen genauer an, die Sie mit „Teilweise“ oder „Nein“ beantwortet haben. Häufen sich die Antworten in einem bestimmten Bereich, sollten Sie dort zuerst ansetzen. Besondere Aufmerksamkeit verdienen Anwendungen, mit denen personenbezogene oder vertrauliche Daten verarbeitet werden oder die ohne vorherige Prüfung und Freigabe genutzt werden.

Überlegen Sie anschließend, welche Lücken besonders dringend geschlossen werden sollten. Halten Sie für die wichtigsten Punkte fest, was zu tun ist, wer sich darum kümmert und bis wann die Maßnahme umgesetzt werden soll.

Wichtig: Schatten-IT lässt sich nicht allein durch Verbote verhindern. Fragen Sie deshalb auch nach den Gründen für die Nutzung nicht freigegebener Anwendungen. Fehlt eine geeignete Alternative? Ist der Freigabeprozess zu aufwendig oder den Beschäftigten gar nicht bekannt? Solche Hinweise helfen Ihnen, Lösungen zu schaffen, die im Arbeitsalltag tatsächlich funktionieren. Prüfen Sie nach einiger Zeit, ob die vereinbarten Maßnahmen umgesetzt wurden und Wirkung zeigen.



Schatten-IT angehen: Ihr Schritt-für-Schritt-Leitfaden

Stoßen Verantwortliche im Unternehmen auf Anzeichen für Schatten-IT oder stellen sie deren Nutzung fest, sollten sie nicht vorschnell mit Verboten reagieren. Ein Verbot beseitigt weder den tatsächlichen Bedarf der Beschäftigten noch bereits vorhandene Datenbestände. Häufig führt es lediglich dazu, dass die Beschäftigten die betreffenden Anwendungen künftig besser verbergen.

Schrittweise zum Ziel

Zielführender ist ein strukturiertes Vorgehen: Damit machen Sie zunächst unbekannte Anwendungen sichtbar, bewerten anschließend ihre datenschutzrechtlichen Risiken und legen geeignete Maßnahmen fest. Dabei arbeiten Sie als Datenschutzbeauftragter eng mit IT, Informationssicherheit sowie den betroffenen Fachbereichen zusammen.

Wichtig: Sie als Datenschutzbeauftragter sind nicht dafür verantwortlich, sämtliche Anwendungen selbst zu ermitteln oder technisch zu prüfen. Ihre Aufgabe besteht darin, Datenschutzrisiken zu bewerten, zu beraten und auf geeignete organisatorische Prozesse hinzuwirken.

Schritt 1: Zuständigkeiten festlegen

Bevor die Bestandsaufnahme beginnt, sollten die Verantwortlichen Ziel, Umfang und Zuständigkeiten festlegen. So können sie die Untersuchung einheitlich durchführen und die Ergebnisse nachvollziehbar dokumentieren.

Klären Sie vor allem,

- › welche Unternehmensbereiche einbezogen werden,
- › welche Anwendungen betrachtet werden sollen,
- › wer die Bestandsaufnahme koordiniert und
- › wie festgestellte Anwendungen bewertet werden und
- › wer über das weitere Vorgehen entscheidet.

Übersicht: Sinnvolle Beteiligte

Beteiligte Stelle	Typische Aufgabe
IT-Abteilung	technische Ermittlung, Systembewertung und Umsetzung technischer Maßnahmen
Datenschutzbeauftragter	Prüfung datenschutzrechtlicher Risiken und Beratung zu erforderlichen Maßnahmen
Informationssicherheit	Bewertung von Sicherheitsrisiken, Schnittstellen und Zugriffsmöglichkeiten
Einkauf oder Beschaffung	Prüfung bestehender Verträge, Lizenzen und Beschaffungswege
Fachbereiche	Erläuterung des tatsächlichen Nutzungszwecks und des betrieblichen Bedarfs
Compliance oder Recht	Prüfung weiterer rechtlicher und regulatorischer Anforderungen
Geschäftsleitung	Entscheidung bei erheblichen Risiken oder bereichsübergreifenden Maßnahmen

Schritt 2: Schatten-IT sichtbar machen

Eine erfolgreiche Bestandsaufnahme kombiniert organisatorische und technische Maßnahmen. Während technische Analysen Hinweise auf eingesetzte Anwendungen liefern, zeigen Gespräche mit den Fachbereichen häufig, welche Onlinedienste oder KI-Anwendungen tatsächlich im Arbeitsalltag genutzt werden.

Organisatorische Erkenntnisquellen

- › Gespräche mit Fachbereichen
- › Workshops oder Befragungen
- › Software- und Lizenzlisten
- › Beschaffungsunterlagen und Verträge
- › Verzeichnis von Verarbeitungstätigkeiten

Technische Erkenntnisquellen

- › Netzwerk- und Proxy-Protokolle
- › Cloud-Nutzungsberichte
- › installierte Programme
- › Browser-Erweiterungen
- › Single-Sign-on-Systeme

Offen statt direkt fragen: Fragen Sie nicht nach „verbotener Software“. Offene Fragen wie „Welche Onlinedienste nutzen Sie für Ihre tägliche Arbeit?“ oder „Welche Anwendung würden Sie ungern wieder aufgeben?“ liefern häufig deutlich bessere Ergebnisse als die direkte Frage nach nicht freigegebenen Programmen. andere überschreibt

Schritt 3: Anwendungen erfassen

Dokumentieren Sie jede identifizierte Anwendung anhand einheitlicher Kriterien. Bereits wenige Angaben schaffen eine gute Grundlage für die anschließende datenschutzrechtliche Bewertung.

Das sollten Sie erfassen: Name und Anbieter · Bereich · Nutzungszweck · betroffene Personen und Daten · besondere Datenkategorien · Kontenart · Speicherort · vertragliche Grundlage · Zugriffsrechte · freigegebene Alternative

Die Dokumentation muss zu diesem Zeitpunkt noch nicht vollständig sein. Kennzeichnen Sie offene Punkte und verfolgen Sie diese im weiteren Prüfprozess nach. Ziel ist zunächst eine belastbare Grundlage für die anschließende Bewertung.

Schritt 4: Datenschutzrisiken bewerten

Nicht jede Schattenanwendung ist gleich ein Risiko. Entscheidend sind insbesondere die Art der verarbeiteten Daten, der Anbieter

sowie die technischen und organisatorischen Rahmenbedingungen. Prüfen Sie vor allem,

- › welche personenbezogenen Daten verarbeitet werden,
- › ob eine Rechtsgrundlage und ggf. eine Auftragsverarbeitung vorliegen,
- › wo die Daten gespeichert werden,
- › welche Sicherheitsmaßnahmen der Anbieter durchführt,
- › ob Betroffenenrechte und Löschpflichten erfüllt werden können und
- › ob zusätzliche Dokumentationspflichten bestehen.

Für die erste Priorisierung kann eine einfache Ampelbewertung sinnvoll sein. Auf Grundlage dieser Informationen lässt sich das Risiko einer Anwendung zunächst grob einschätzen und priorisieren.

Risikomatrix: Wie dringend müssen Sie handeln?

Risikostufe	Typische Merkmale	Reaktion
Grün – geringes Risiko	keine oder nur wenige unkritische personenbezogene Daten; begrenzter Nutzerkreis; Anbieter und Datenstandort bekannt	Nutzung dokumentieren und reguläre Freigabeproofung durchführen
Gelb – mittleres Risiko	regelmäßige Verarbeitung personenbezogener Daten; offene Vertrags- oder Sicherheitsfragen; mehrere Nutzer	Nutzung vorläufig einschränken und zeitnah vollständig prüfen
Rot – hohes Risiko	besondere Datenkategorien, große Datenmengen, sensible Unternehmensinformationen, unbekannter Datenstandort oder erhebliche Sicherheitsmängel	Nutzung aussetzen, Daten sichern und unverzüglich Maßnahmen einleiten

Schritt 5: Geeignete Maßnahmen festlegen

Nach der datenschutzrechtlichen Bewertung sollte für jede Anwendung eine nachvollziehbare Entscheidung getroffen werden. Welche Maßnahme geeignet ist, hängt insbesondere von der Art der verarbeiteten Daten, dem festgestellten Risiko und dem betrieblichen Bedarf ab. Häufig lassen sich Risiken bereits durch organisatorische oder technische Maßnahmen ausreichend reduzieren.

Nicht automatisch verbieten: Eine entdeckte Schattenanwendung muss nicht zwangsläufig abgeschaltet werden. Entscheidend ist, warum sie genutzt wird, welches Risiko tatsächlich besteht und ob sich dieses ausreichend reduzieren lässt.

Erkennen → Bedarf verstehen → Risiko bewerten → passende Lösung finden

Grundsätzlich kommen vier Handlungsoptionen in Betracht:

- › Anwendung freigeben, wenn die datenschutzrechtlichen und technischen Anforderungen erfüllt werden können.
- › Nutzung einschränken, beispielsweise auf bestimmte Datenarten, Nutzergruppen oder Anwendungsfälle.
- › Durch eine freigegebene Alternative ersetzen, wenn bereits eine geeignete Unternehmenslösung vorhanden ist.
- › Nutzung untersagen, wenn erhebliche Datenschutz- oder Sicherheitsrisiken bestehen und diese nicht angemessen reduziert werden können.

Unabhängig von der gewählten Maßnahme sollte den Beschäftigten möglichst eine praktikable und datenschutzkonforme Alternati-

ve zur Verfügung stehen. Verbote allein führen häufig dazu, dass der betriebliche Bedarf auf andere, ebenfalls nicht freigegebene Anwendungen verlagert wird.

Schritt 6: Entscheidungen dokumentieren

Jede Entscheidung sollten die Verantwortlichen nachvollziehbar dokumentieren. Dies erleichtert nicht nur die spätere Nachvollziehbarkeit gegenüber der Geschäftsleitung oder Aufsichtsbehörden, sondern unterstützt auch interne Audits und die regelmäßige Überprüfung getroffener Maßnahmen. Dokumentieren Sie mindestens:

- › betroffene Anwendung,
- › betroffenen Fachbereich,
- › festgestellte Datenschutzrisiken,
- › beschlossene Maßnahmen,
- › verantwortliche Personen,
- › Umsetzungsfrist,
- › Freigabeentscheidung sowie
- › Termin für eine erneute Überprüfung.

Übersicht: Maßnahmenübersicht

Feststellung	Maßnahme	Verantwortlich	Frist	Status
Privater Cloud-Speicher im Vertrieb	Daten auf Unternehmensspeicher übertragen und privates Konto löschen	Vertrieb und IT	14 Tage	offen
KI-Tool im Personalbereich	Nutzung aussetzen und Anbieter prüfen	HR, IT und DSB	7 Tage	in Prüfung
Nicht freigegebenes Umfragetool	Unternehmensvertrag abschließen und VVT ergänzen	Marketing und Einkauf	30 Tage	offen
Private Messenger-Gruppe	freigegebenen Kommunikationsdienst bereitstellen	IT	21 Tage	geplant

Schritt 7: Wiederholungen verhindern

Die Bearbeitung einzelner Anwendungen reicht nicht aus. Unternehmen sollten aus jedem festgestellten Fall ableiten, weshalb die Schattenlösung entstanden ist und welche strukturellen Änderungen erforderlich sind. Prüfen Sie daher:

- › War der Beschaffungsprozess zu langsam?
- › War die bestehende Software ungeeignet?
- › War eine freigegebene Alternative unbekannt?
- › Fehlten klare Regeln?
- › War die Antragstellung zu kompliziert?
- › Gab es keine zentrale Ansprechperson?
- › Haben Beschäftigte die Datenschutzrisiken unterschätzt?
- › War mobile Arbeit oder Zusammenarbeit mit Externen nicht ausreichend berücksichtigt?

Aus den Antworten sollten konkrete Verbesserungen folgen. Denkbar sind ein vereinfachter Freigabeprozess, ein zentraler Softwarekatalog, klare KI-Vorgaben, regelmäßige Befragungen der Fachbereiche und verbindliche Regeln für Cloud-Dienste, Messenger und private Geräte.

Warnsignale: Wann Sie genauer hinschauen sollten

Schatten-IT wird häufig erst entdeckt, wenn bereits ein Datenschutzvorfall, eine Betroffenenanfrage oder ein Audit einen Anlass für eine genauere Prüfung bietet. Dabei gibt es oft schon im Vorfeld Anzeichen dafür, dass Anwendungen außerhalb der vorgesehenen IT- und Datenschutzprozesse genutzt werden. Einzelne Hinweise müssen zwar nicht zwangsläufig auf Schatten-IT hindeuten. Häufen sich jedoch mehrere Warnsignale, empfiehlt sich eine genauere Betrachtung gemeinsam mit IT und den betroffenen Fachbereichen.

Übersicht: Wenn die Alarmglocken läuten: So reagieren Sie



Warnsignal	Empfohlene erste Maßnahme
Fachbereiche beschaffen Software eigenständig oder schließen Onlineabonnements selbst ab.	Suchen Sie zunächst das Gespräch mit dem Fachbereich: Welche Anwendungen wurden beschafft und warum lief die Beschaffung nicht über den vorgesehenen Weg? Prüfen Sie dabei auch, ob personenbezogene Daten verarbeitet werden. Zeigt sich, dass Freigabeprozesse zu aufwendig oder zu langsam sind, sollten Sie gemeinsam mit IT und Einkauf nach einer praktikablen Lösung suchen.
Beschäftigte nutzen private KI-Konten oder sprechen regelmäßig über neue KI-Anwendungen.	Verschaffen Sie sich zunächst einen Überblick: Welche KI-Tools werden tatsächlich genutzt und wofür? Besonders wichtig ist, ob Beschäftigte personenbezogene oder vertrauliche Daten eingeben. Klären Sie anschließend mit der IT, ob bereits freigegebene KI-Lösungen zur Verfügung stehen oder ob klare Vorgaben für die Nutzung erforderlich sind.
Dateien werden regelmäßig über private Cloud-Speicher oder Dateiaustauschdienste versendet.	Fragen Sie nach, warum Beschäftigte auf diese Dienste ausweichen. Fehlt eine geeignete Unternehmenslösung oder ist die vorhandene Lösung zu umständlich? Prüfen Sie anschließend, welche Daten über die Dienste ausgetauscht werden und ob eine freigegebene Alternative bereitgestellt oder besser kommuniziert werden sollte. Achten Sie vor allem darauf, ob sensible oder besonders schützenswerte Daten betroffen sind.
Private Messenger oder private E-Mail-Konten werden dienstlich genutzt.	Klären Sie zunächst, wofür private Kommunikationswege genutzt werden und welche Informationen darüber ausgetauscht werden. Häufig liegt die Ursache darin, dass freigegebene Lösungen fehlen, im Arbeitsalltag unpraktisch sind oder nicht ausreichend bekannt sind. Hier sollten Sie ansetzen und gemeinsam mit der IT eine praktikable Alternative schaffen. Machen Sie den Beschäftigten zugleich deutlich, welche Kommunikationswege dienstlich genutzt werden dürfen.
In Fachbereichen existieren zahlreiche Excel- oder Access-Dateien mit personenbezogenen Daten.	Fragen Sie im Fachbereich nach: Welche Daten werden dort gespeichert, wofür werden die Dateien benötigt und wer hat Zugriff? Prüfen Sie anschließend, ob die Daten besser in einer zentralen Anwendung verarbeitet werden können. Ist das nicht möglich, sollten zumindest Zugriffsrechte, Speicherort und Löschung eindeutig geregelt sein. Nehmen Sie besonders Dateien in den Blick, die über Jahre gewachsen sind oder von mehreren Personen gepflegt werden.
Betroffenenanfragen oder Löschersuchen lassen sich nur mit hohem Aufwand bearbeiten.	Nehmen Sie den hohen Suchaufwand als Warnsignal. Prüfen Sie, in welchen Anwendungen und Dateien die betreffenden Daten gespeichert sind und ob dabei bislang unbekannte Datenbestände auftauchen. Dokumentieren Sie diese direkt – so erleichtern Sie sich zugleich die Bearbeitung künftiger Anfragen. Prüfen Sie anschließend, ob die neu entdeckten Datenbestände auch in bestehenden Datenschutzdokumentationen berücksichtigt sind.
Bei Audits oder Sicherheitsvorfällen werden bislang unbekannte Anwendungen entdeckt.	Prüfen Sie nicht nur die entdeckte Anwendung selbst. Fragen Sie auch, wie sie unbemerkt eingesetzt werden konnte: War der Freigabeprozess unbekannt, zu kompliziert oder gab es keinen passenden Prozess? Nutzen Sie die Erkenntnisse, um genau diese Lücke für die Zukunft zu schließen. Prüfen Sie außerdem, ob vergleichbare Anwendungen auch in anderen Fachbereichen eingesetzt werden.
Niemand kann zuverlässig sagen, welche Cloud-, SaaS- oder KI-Dienste tatsächlich genutzt werden.	Starten Sie gemeinsam mit IT und Fachbereichen eine strukturierte Bestandsaufnahme. Fragen Sie ausdrücklich auch nach kostenlosen Tools, Testzugängen und selbst angelegten Accounts – gerade diese geraten schnell aus dem Blick. Erfassen Sie die gefundenen Anwendungen zentral und legen Sie fest, welche davon näher geprüft werden müssen. Wiederholen Sie die Bestandsaufnahme regelmäßig, damit die Übersicht nicht schon nach kurzer Zeit wieder veraltet ist.



Praxistipp:

Warten Sie nicht, bis Schatten-IT zum Problem wird. Achten Sie frühzeitig auf Warnsignale und suchen Sie den Austausch mit IT und Fachbereichen. Fragen Sie konkret nach, welche Anwendungen im Arbeitsalltag genutzt werden und warum Beschäftigte auf nicht freigegebene Lösungen ausweichen. So erkennen Sie nicht nur Risiken, sondern auch Lücken in bestehenden Prozessen und Angeboten.

Datenschutz aktuell Live Talk:

Gratis-Webinar

**Austausch, Aktualität, fachliche Tiefe
für alle mit Aufgaben im Datenschutz**



**am letzten
Freitag
jeden Monats**



**um
16:30 Uhr
60 Minuten**

**Moderator & Fachexperte
Andreas Würtz**



Warum am Live Talk teilnehmen?

Neue Leitlinien, geplante Gesetzesänderungen, behördliche Anforderungen und praxisnahe Umsetzungsfragen stellen Datenschutzverantwortliche regelmäßig vor neue Herausforderungen. Oft bleiben dabei konkrete Fragen offen – oder es fehlt die Gelegenheit, Themen direkt mit einem Experten zu besprechen.

Der **Datenschutz aktuell Live Talk** ist aufgrund seines digitalen Formats bequem von überall erreichbar. Im Mittelpunkt steht ein **vertraulicher**,

fachlicher Austausch zu aktuellen Schwerpunktthemen aus Datenschutzrecht und Datenschutzpraxis.

Die Veranstaltung wird **nicht aufgezeichnet**. So entsteht ein geschützter Rahmen, in dem auch sensible Fragestellungen offen angesprochen werden können. Sie entscheiden selbst, wie aktiv Sie teilnehmen möchten: **Bringen Sie Ihre Fragen ein oder hören Sie einfach zu** – ganz nach Ihrem Bedarf und ganz wie Sie mögen.

Der Live Talk ist bewusst kein klassisches Webinar mit Frontalvortrag, sondern ein dialogorientiertes Format, das auf Austausch, Aktualität und fachliche Tiefe setzt.

Ich freue mich auf Ihre Teilnahme!

Ihr Moderator & Fachexperte Andreas Würtz

Rechtsanwalt | Datenschutzexperte

Chefredakteur des Fachratgebers „Datenschutz aktuell“

**Jetzt zum
nächsten
Live-Talk
anmelden:**



 t1p.de/live-talk



Telefon: 02 28 95 50 150

Fax: 02 28 36 96 480

E-Mail: kundendienst@privacyxperts.de

Internet: www.privacyxperts.de

**Ein Unternehmensbereich des VNR Verlags
für die Deutsche Wirtschaft AG
Theodor-Heuss-Straße 2–4
53177 Bonn**