Bitdefender Global Leader In Cybersecurity

Digitale Souveränität: **Haben Sie die Risiken Ihrer Technologieanbieter wirklich im Griff?**

LEGAL OPINION



Alle Rechte vorbehalten. © 2025 Bitdefender. Alle hier genannten Marken, Handelsnamen und Produkte sind Eigentum ihrer jeweiligen Inhaber. Die in diesem Dokument enthaltenen Informationen sind vertraulich und nur für den Gebrauch durch den vorgesehenen Empfänger bestimmt. Sie dürfen dieses Dokument nicht ohne vorherige Genehmigung durch Bitdefender veröffentlichen oder weiterverbreiten.

racine AVOCATS

In Zusammenarbeit mit der Anwaltskanzlei Racine erstelltes Dokument

Einleitung

In seinem Lagebericht für das Jahr 2025 erinnert das Bundesamt für Sicherheit in der Informationstechnik (BSI) eindringlich daran, dass „jede aus dem Internet erreichbare Institution oder Person prinzipiell bedroht ist“ und somit „jede und jeder ein interessantes Ziel“ der Cyberkriminellen darstellt.“[1] . Die Bedrohung der Cybersicherheit stellt heute kein isoliertes Risiko mehr dar, sondern ist zum Primärrisiko für sämtliche öffentlichen und privaten Einrichtungen geworden; maßgeblich hierfür sind die zunehmende Industrialisierung der Angriffsmethoden sowie die technologischen Abhängigkeiten innerhalb der Organisationsstrukturen.

Angesichts dieser Entwicklung verschärft der europäische Gesetzgeber schrittweise den Rechtsrahmen, um ein einheitliches und hohes Sicherheitsniveau durchzusetzen. Dies gilt für die DSGVO und die Verpflichtungen im Bereich der Sicherheit personenbezogener Daten, die Richtlinien NIS1 und NIS2 für wesentliche oder wichtige Einrichtungen, die DORA-Verordnung für den Banken-/Finanz-/Versicherungssektor oder auch die KI-Verordnung oder den Cyber Resilience Act für bestimmte Produkte oder Dienstleistungen.

Diese Texte verfolgen ein klares Ziel: die gesamte digitale Wertschöpfungskette, vom Kunden bis zum IT-Dienstleister, konsequent zur Verantwortung zu ziehen.

Daher ist die Frage der Souveränität von Lösungen zu einem wichtigen Thema geworden und untrennbar mit allen Überlegungen zu Compliance, Risikomanagement und digitaler Resilienz verbunden.

In einem Umfeld, in dem Cloud Computing zum Rückgrat vieler digitaler Dienste wird, erscheint es unerlässlich, die Konturen und Auswirkungen der digitalen Souveränität zu untersuchen, um die technologischen Entscheidungen von Organisationen zu beleuchten.
Tatsächlich werden Daten, die früher lokal gespeichert wurden, heute teilweise außerhalb der EU bei Anbietern gehostet, die möglicherweise ausländischen Rechtsordnungen unterliegen.

Die Abhängigkeit von diesen Akteuren setzt öffentliche oder private Unternehmen und Organisationen erhöhten Cybersicherheitsrisiken, rechtlichen Risiken im Zusammenhang mit der extraterritorialen Wirkung nicht-europäischer Gesetze, operativen Risiken im Zusammenhang mit der Konzentration von Anbietern und, im weiteren Sinne, einem Verlust der Kontrolle über ihre Daten und Informationssysteme aus.



[1] Bundesamt für Sicherheit in der Informationstechnik (BSI), Die Lage der IT-Sicherheit in Deutschland 2025, 11. November 2025, abrufbar unter: https://medien.bsi.bund.de/lagebericht/de/

Vom Grundsatz zur Verpflichtung...

Es gibt keine rechtliche Definition von „digitaler Souveränität" im deutschen oder europäischen Recht.

Derzeit gibt es keine Norm, die generell die Nutzung nationaler oder europäischer digitaler Dienstleistungslösungen vorschreibt.

Das Fehlen einer rechtlichen Definition hindert jedoch nicht daran, die Konturen dieser Begriffe oder Grundsätze zu skizzieren.

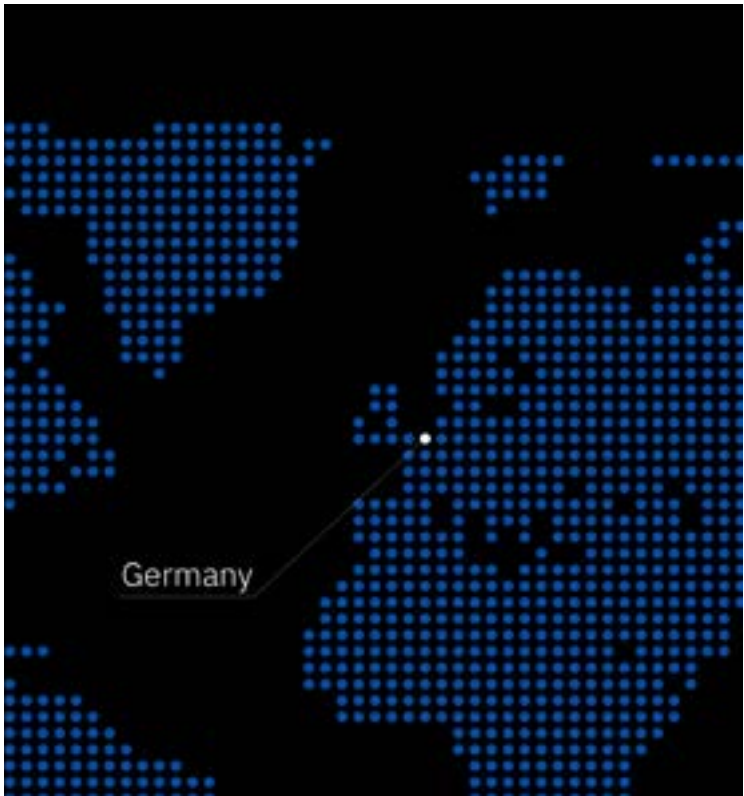
Technologische Souveränität könnte definiert werden als die Fähigkeit der Europäischen Union, Schlüsseltechnologien und wesentliche digitale Infrastrukturen zu konzipieren, zu entwickeln, zu produzieren und zu beherrschen, um die Sicherheit, Widerstandsfähigkeit und strategische Unabhängigkeit ihrer Systeme zu gewährleisten und gleichzeitig kritische Abhängigkeiten von Drittländern zu verringern.

Offene strategische Autonomie versteht sich als das Prinzip, wonach die Europäische Union bestrebt ist, ihre Handlungsfreiheit und ihre Fähigkeit zur Verteidigung ihrer grundlegenden Interessen in den Bereichen Wirtschaft, Industrie und Sicherheit zu wahren und gleichzeitig offen für internationale Zusammenarbeit und Handel unter Einhaltung multilateraler Regeln zu bleiben.

Darüber hinaus definiert das Bundesministerium für Digitales und Staatsmodernisierung im Rahmen der Strategie zur „Digitalen Souveränität in der öffentlichen Verwaltung" diese als „die Fähigkeiten und Möglichkeiten von Individuen und Institutionen, ihre Rolle(n) in der digitalen Welt selbstständig, selbstbestimmt und sicher ausüben zu können"[2].

Diese Begriffe, die lange Zeit im „politischen" Bereich verblieben sind, nehmen heute auf rechtlicher Ebene Gestalt an.

So kommt der Begriff der technologischen Souveränität in der Verordnung (EU) 2025/38 des Europäischen Parlaments und des Rates vom 19. Dezember 2024 über Maßnahmen zur Stärkung der Solidarität und der Kapazitäten in der Union für die Erkennung von, Vorsorge für und Bewältigung von Cyberbedrohungen und Sicherheitsvorfällen und zur Änderung der Verordnung (EU) 2021/694 (Cybersolidaritätsverordnung).[3]



[2]Bundesministerium für Digitales und Staatsmodernisierung (BMDS), Digitale Souveränität in der öffentlichen Verwaltung, abrufbar unter: Digitale Souveränität in der öffentlichen Verwaltung - Bundesministerium für Digitales und Staatsmodernisierung (abgerufen am 19. Februar 2026).

[3]Abrufbar unter: Verordnung - EU - 2025/38 - EN - EUR-Lex

Artikel 1 legt den Gegenstand und die Ziele der Verordnung fest und erinnert insbesondere daran, dass:

Artikel 1 – Gegenstand und Ziele:

(...)

(2) Mit dieser Verordnung werden die allgemeinen Ziele verfolgt, die Wettbewerbsposition von Industrie und Dienstleistungen der Digitalwirtschaft in der Union, einschließlich Kleinstunternehmen, kleiner und mittlerer Unternehmen sowie Start-up-Unternehmen, zu stärken und zur technologischen Souveränität und offenen strategischen Autonomie der Union im Bereich der Cybersicherheit beizutragen, unter anderem durch die Förderung von Innovationen im digitalen Binnenmarkt. Diese Ziele werden durch eine Stärkung der Solidarität auf Unionsebene, des Cybersicherheitsökosystems und der Cyberresilienz der Mitgliedstaaten sowie durch die Entwicklung der Fähigkeiten, des Fachwissens und der Kompetenzen von Fachkräften im Bereich der Cybersicherheit verfolgt.

Dieser Begriff der technologischen Souveränität wurde anlässlich der Empfehlung des Rates vom 6. Juni 2025 für einen EU-Konzeptentwurf für das Cyberkrisenmanagement erneut in den Vordergrund gerückt. [4]

Für Unternehmen und öffentliche Akteure bedeutet der Begriff der digitalen Souveränität somit ihre Fähigkeit, die für ihr reibungsloses Funktionieren erforderlichen Infrastrukturen, Technologien und Daten zu beherrschen und sicherzustellen, dass diese Mittel in einem abgegrenzten rechtlichen und territorialen Rahmen eingesetzt werden.



[4] Abrufbar unter: Empfehlung des Rates vom 6. Juni 2025 für einen EU-Konzeptentwurf für das Cyberkrisenmanagement

Trotz der Relevanz digitaler Souveränität ist eine entsprechende Einhaltungspflicht im positiven Recht nicht universell verankert; für kritische strategische Bereiche bestehen bereits spezifische, verschärfte Anforderungen.

Dies gilt insbesondere für Betreiber Kritischer Infrastrukturen (KRITIS), deren Tätigkeit für das Gemeinwesen und die öffentliche Sicherheit unerlässlich ist. Diese Akteure sind verpflichtet, branchenspezifische Sicherheitsstandards umzusetzen und ein wirksames Risikomanagement zu pflegen. Dies umfasst konkret die Erstellung und regelmäßige Aktualisierung von Notfall- und Krisenplänen, die kontinuierliche Schulung und Sensibilisierung der Beschäftigten sowie den Aufbau einer klaren Kommunikationsstruktur für den Krisenfall.

Eine solche Verpflichtung ist durch die Art der Tätigkeiten dieser Akteure gerechtfertigt, deren Ausfall oder Beeinträchtigung zu erheblichen Versorgungsengpässen oder zu Gefährdungen der öffentlichen Sicherheit führen würde.

Die gemäß dem KRITIS-Dachgesetz betroffenen Sektoren umfassen insbesondere die folgenden zehn Bereiche:

§ 4 KRITIS-Dachgesetz: Sektoren; Geltungsbereich; Verordnungsermächtigung

1) Dieses Gesetz gilt für Betreiber kritischer Anlagen in den folgenden Sektoren:

1. Energie,
2. Transport und Verkehr,
3. Finanzwesen,
4. Leistungen der Sozialversicherung sowie Grundsicherung für Arbeitsuchende,
5. Gesundheitswesen,
6. Wasser,
7. Ernährung,
8. Informationstechnik und Telekommunikation,
9. Weltraum und
10. Siedlungsabfallentsorgung

2) ...

Dieser klassische regulatorische Rahmen hat sich stetig ausgeweitet. Durch die NIS-2-Richtlinie (Richtlinie (EU) 2022/2555) ist der Kreis der betroffenen Akteure deutlich gewachsen, da nun zusätzliche Sektoren und neue Schwellenwerte gelten. Insbesondere durch die Unterscheidung in „Wesentliche“ und „Wichtige Einrichtungen“ fallen heute weit mehr Unternehmen unter die strengen Sicherheitspflichten als zuvor.

Dieser Wandel ist politisch gewollt, da die bisherige Regulierung laut EU-Gesetzgeber « *als Katalysator für den institutionellen und regulatorischen Ansatz im Bereich der Cybersicherheit in der Union gewirkt und den Weg für einen bedeutenden Wandel in der Mentalität geebnet hat* » [5].

In der Konsequenz bedeutet dies eine massive Zunahme der Compliance-Anforderungen für die deutsche Wirtschaft: Laut BSI sind seit dem 06.12.2025 rund 29.500 Unternehmen in Deutschland direkt von den neuen gesetzlichen IT-Sicherheitspflichten betroffen[6].

[5] Erwägungsgrund 2, Richtlinie (EU) 2022/2555 des Europäischen Parlaments und des Rates vom 14. Dezember 2022 über Maßnahmen für ein hohes gemeinsames Cybersicherheitsniveau in der Union (NIS-2-Richtlinie), abrufbar unter: Richtlinie - 2022/2555 - EN - EUR-Lex.

[6] Bundesamt für Sicherheit in der Informationstechnik (BSI), NIS-2-Starterpaket: Einleitung und Überblick, abrufbar unter: BSI - NIS-2-Starterpaket

Angesichts dieser hohen regulatorischen Vorgaben und der technischen Komplexität der Umsetzung greifen die zuständigen Verwaltungsbehörden auf nationaler und europäischer Ebene zunehmend steuernd ein.

In diesem Sinne verfolgt Deutschland mit der im Herbst 2020 verabschiedeten Deutschen Verwaltungscloud-Strategie (DVS) das Ziel, durch gemeinsame Standards und offene Schnittstellen eine souveräne, modulare Cloud-Infrastruktur für die öffentliche Verwaltung zu etablieren[7]. Diese Strategie soll die Abhängigkeit von einzelnen außereuropäischen Anbietern verringern und die staatliche Handlungsfähigkeit durch Interoperabilität sichern.

Parallel dazu hat das BSI mit dem Kriterienkatalog C5 (*Cloud Computing Compliance Criteria Catalogue*) einen Referenzrahmen für Cloud-Anbieter entwickelt, die ein hohes Maß an Informationssicherheit und Transparenz nachweisen möchten. Der Kriterienkatalog legt dabei besonderen Wert auf die Transparenz gegenüber ausländischen Zugriffsbefugnissen.

Dies bedeutet konkret, dass der Anbieter offenlegen muss, inwieweit er ausländischen Gesetzgebungen unterliegt, die den Zugriff auf gehostete Daten erlauben könnten (wie etwa der US Cloud Act). Ziel dieser Anforderungen ist es, sicherzustellen, dass potenzielle Rechtsrisiken durch kollidierende Jurisdiktionen identifiziert werden, was direkt zur Souveränität der Datenverarbeitung im Einklang mit europäischen Standards beiträgt.

BSI-Kriterienkatalog – Cloud Computing Compliance Criteria Catalogue – C5 :2020

BC-05 Angaben zum Umgang mit Ermittlungsanfragen staatlicher Stellen

Der Cloud-Anbieter macht in der Systembeschreibung nachvollziehbare und transparente Angaben zum Umgang mit Ermittlungsanfragen staatlicher Stellen für den Zugriff auf oder die Offenlegung von Daten der Cloud-Kunden.

Die Angaben umfassen folgende Aspekte:

↳ Verfahren zur Verifizierung der Rechtsgrundlage solcher Anfragen,
↳ Verfahren zur Information und Einbindung der betroffenen Cloud-Kunden bei Erhalt solcher Anfragen,
↳ Widerspruchsmöglichkeiten der betroffenen Cloud-Kunden,
↳ ob der Cloud-Anbieter bei verschlüsselten Daten der Cloud-Kunden im Falle solcher Anfragen die Möglichkeit zur Entschlüsselung hat und wie er diese für den Zugriff oder die Offenbarung anwendet

Die Europäische Union plant ihrerseits einen ähnlichen Ansatz mit dem European Union Cybersecurity Certification Scheme for Cloud Services (EUCS). Ziel dieses normativen Referenzrahmens ist es, den Markt zu harmonisieren, das Sicherheitsniveau von Cloud-Diensten zu erhöhen und die Entstehung eines europäischen Angebots zu fördern, das mit den größten Akteuren konkurrieren kann. Damit strebt die EU eine Verringerung der strategischen Abhängigkeit von außereuropäischen Akteuren an.

Auch wenn der Erhalt dieser Zertifizierungen die Partner beruhigen kann, sind sie weder obligatorisch noch rechtsverbindlich. Ihre Bedeutung ist daher im Wesentlichen anreizorientiert und strategisch.

[7] Bundesministerium des Innern und für Heimat (BMI), Deutsche Verwaltungscloud-Strategie (DVS), November 2020, abrufbar unter: BMI - Deutsche Verwaltungscloud-Strategie.

1.BESTEHT EIN RISIKO BEI DER INANSPRUCHNAHME DER DIENSTE EINES NICHT SOUVERÄNEN DIENSTLEISTERS?

Die Antwort ist klar. Ja, es besteht für jeden öffentlichen oder privaten Akteur ein Risiko, wenn er die Dienste eines ausländischen Anbieters in Anspruch nimmt, und zwar aus einem einfachen Grund: Dieser unterliegt nicht dem gleichen Rechtsrahmen wie ein deutscher oder europäischer Akteur und kann mehr oder weniger offiziell und offen Druck von seinen eigenen Behörden ausgesetzt sein.

Zunächst ist anzumerken, dass die „gewöhnlichen" Rechtsvorschriften innerhalb und außerhalb der EU nicht identisch sind.

Während das deutsche Recht weitreichende Haftungsausschlüsse in Standardverträgen untersagt oder stark einschränkt, herrscht im anglo-amerikanischen Rechtskreis eine weitreichendere Vertragsfreiheit. In diesen Jurisdiktionen und den darauf basierenden Vertragsmodellen sind Klauseln weitverbreitet und rechtlich wirksam, die die Haftung, Gewährleistung und Ersatzpflichten des Dienstleisters nahezu vollständig ausschließen können. Man muss nur die Verträge amerikanischer Verlage lesen, um Klauseln zu entdecken, deren Titel keinen Zweifel offen lässt: „NO WARRANTIES" (keine Gewährleistungen).

Über diese für sie recht vorteilhaften Vertragsregeln hinaus unterliegen Nicht-EU-Akteure jedoch auch lokalen Vorschriften, die ihnen manchmal den Zugriff auf die Daten ihrer Kunden ermöglichen, unabhängig von der Nationalität des Kunden.

Fast jeder hat schon einmal vom Cloud Act in den USA gehört, der Regelung, die es den amerikanischen Behörden ermöglicht, auf Daten zuzugreifen, die auf amerikanischem Territorium gehostet werden, unabhängig von der Nationalität des Unternehmens, das die Daten speichert. Diese Regelung gibt es in mehr oder weniger ähnlicher Form auch in vielen anderen Ländern, entweder indem diese Gesetze den Zugriff auf die in dem betreffenden Land gespeicherten Daten ermöglichen oder, schlimmer noch, indem sie vorschreiben, dass die Daten in dem betreffenden Land gespeichert werden müssen (insbesondere in China und Russland).

Darüber hinaus führt die Inanspruchnahme eines nicht europäischen Dienstleisters häufig dazu, dass das normalerweise geltende nationale oder europäische Recht durch einen ausländischen Rechtsrahmen ersetzt wird, mit dem die Unternehmen und ihre üblichen Berater nicht unbedingt vertraut sind. Dies bedeutet, dass bei rechtlichen Schwierigkeiten zusätzlich zu den Hindernissen, die sich aus der geografischen Entfernung zu den zuständigen Gerichten ergeben, weitere Mittel eingesetzt werden müssen.

Über die Rechtsvorschriften hinaus gibt es auch einige geopolitische Tatsachen, die niemand ignorieren kann. Die Sperrung der Geschäftskonten bestimmter Vertreter des Internationalen Strafgerichtshofs veranschaulicht diese Realität, auch wenn die Situation nicht ganz klar ist.

Schließlich können auch praktische Erwägungen ein Hindernis für die Inanspruchnahme außereuropäischer Dienstleister darstellen. Die schwierige Angleichung an die europäischen Cybersicherheitsstandards, die Undurchsichtigkeit der Unternehmensführung oder die Komplexität der Unterauftragsketten, die Audits erschweren, sind Beispiele für Probleme, mit denen Kunden häufig konfrontiert sind.



Digitale Souveränität: **Haben Sie die Risiken Ihrer Technologieanbieter wirklich im Griff?**

2. GIBT ES EINE MÖGLICHKEIT, DIESES RISIKO ZU BEGRENZEN?

Wenn es sich um einen politischen oder geopolitischen Ansatz handelt, lautet die Antwort nein.

Wenn es sich um ein rechtliches Risiko handelt, ist es möglich, dieses Risiko zu begrenzen, wie es die amerikanischen Vorschriften vorsehen.

Diese Texte sind in der Regel zielgerichtet und beziehen sich nur auf Verhaltensweisen, die den Interessen der betroffenen Länder schaden (z. B. Staatssicherheit, Kriminalität, Cyberkriminalität, Terrorismus usw.).

In Demokratien, die über solche Vorschriften verfügen, wird der Zugriff auf Daten ausländischer Unternehmen durch einen Richter kontrolliert.

Schließlich gibt es sehr oft verfahrensrechtliche Mittel für Dienstleister, die diesen Vorschriften unterliegen, um Maßnahmen, die einen solchen Zugriff anordnen, anzufechten.

Aber wie real und wirksam sind diese Beschränkungen? Niemand weiß es. Es ist fast unmöglich, Dienstleister zu zwingen, Maßnahmen anzufechten, die den Behörden den Zugriff auf Daten ermöglichen. Das Risiko für die Dienstleister ist oft größer, wenn sie sich weigern, als wenn sie zustimmen. Eine Weigerung könnte sie nach lokalem Recht strafrechtlich haftbar machen; eine Zustimmung würde sie letztlich nur einem vertraglichen Risiko gegenüber ihrem Kunden aussetzen.

Was die Klauseln betrifft, die den genannten Dienstleistern vorschreiben, ihre Kunden im Falle einer Zugangsanfrage einer lokalen Behörde zu informieren, so kommen diese, wenn sie angewendet werden, oft zu spät.

Kein Anbieter außerhalb der EU kann garantieren, dass er nicht per Gesetz oder durch eine zuständige Behörde dazu verpflichtet wird, Zugang zu den Daten eines Kunden zu gewähren, die auf seinen Servern gespeichert sind.

3. SOUVERÄNITÄT – FÜR WEN ? WIE?

Wie bereits erwähnt, muss zwischen Unternehmen oder öffentlichen oder privaten Einrichtungen, die verpflichtet sind, deutsche oder europäische Dienstleister in Anspruch zu nehmen (KRITIS/ wesentliche Einrichtungen), mit anderen unterschieden werden.

Die anderen Unternehmen oder Einrichtungen können ihre Strategie frei wählen, die im Wesentlichen von der Qualität ihrer Daten und dem Risiko abhängt, dass ein ausländischer Staat darauf zugreifen könnte.

In der Praxis gibt es also drei Arten von Akteuren:

TYP 1	Unterliegen der gesetzlichen Verpflichtung, deutsche oder europäische Dienstleister zu wählen
TYP 2	Entscheiden sich dafür, nur deutsche oder europäische Dienstleister auszuwählen oder diese Art von Dienstleistern zu bevorzugen
TYP 3	Keine spezifische Politik



Welche Kriterien würden bei Unternehmen des Typs 2 und 3 dazu führen, dass deutsche oder europäische IT-Dienstleister bevorzugt werden?

Das erste Kriterium betrifft die Art der Daten dieser Unternehmen.

Wenn diese Daten als „sensibel" gelten, werden diese Unternehmen Anbieter bevorzugen, bei denen das Risiko eines Zugriffs durch Dritte geringer ist.

Als sensibel gelten insbesondere :

- Daten von Industrieunternehmen, die internationale Verträge oder Ausschreibungen erfüllen, wenn deren Offenlegung einem ausländischen Betreiber einen Wettbewerbsvorteil verschaffen oder einer dritten Behörde ermöglichen könnte, den Wettbewerbsprozess zu beeinflussen;

- Daten in Bezug auf Forschung, Entwicklung, Innovation und Geschäftsgeheimnisse, darunter insbesondere technische Verfahren, Konstruktionspläne, Prototypen, proprietäre Algorithmen oder KI-Modelle, die auf internen Daten trainiert wurden;

- nicht öffentliche Finanz-, Geschäfts- oder Strategiedaten, wie Investitionsprognosen, Marktstudien, Preisstrategien, Informationen überlaufende Verhandlungen oder externe Wachstumsmaßnahmen;

- Daten zur Sicherheit oder zum internen Betrieb von Informationssystemen, einschließlich Architekturdiagrammen, Sicherheitsprotokollen (Logs), Netzwerkkonfigurationen, Identitätsreferenzsystemen (IAM) oder Kontinuitäts- und Notfallwiederherstellungsplänen;

- personenbezogene Daten, die im Falle eines unbefugten Zugriffs ein erhöhtes Risiko darstellen, wie sensible Daten im Sinne von Artikel 9 der DSGVO (Gesundheitsdaten, biometrische Daten, genetische Daten usw.) oder große Datenmengen, die die Erstellung detaillierter Profile von Kunden, Mitarbeitern, Nutzern oder Subunternehmern ermöglichen;

- Daten, die das Unternehmen verstärkten sektorspezifischen regulatorischen Verpflichtungen aussetzen, insbesondere in den Bereichen Gesundheit, Verkehr, Energie, Finanzen, Versicherungen oder Telekommunikation;

Diese Kriterien gelten für alle Arten von Unternehmen, unabhängig von ihrer Größe. Dies gilt auch für Start-ups, die sich aus finanziellen Gründen für den günstigsten Anbieter entscheiden, ohne sich um den Schutz ihrer Daten zu kümmern.

Über die Art der Daten hinaus kann die Wahl eines deutschen oder europäischen Dienstleisters durch die Notwendigkeit für das Unternehmen motiviert sein, ein hohes Maß an Kontrolle über seine Verarbeitungsprozesse und Infrastrukturen aufrechtzuerhalten. Dieses Kriterium umfasst insbesondere die Fähigkeit:

- die Kontinuität und Verfügbarkeit kritischer Dienste, beispielsweise für wesentliche Betriebssysteme (Produktion, Logistik, Finanzen, Personalwesen), sicherzustellen, um das Risiko von Unterbrechungen oder einer übermäßigen Abhängigkeit von einem außerhalb Europas ansässigen Dienstleister zu verringern;

- regelmäßige Audits durchzuführen und eine vollständige Rückverfolgbarkeit der Verarbeitungsvorgänge zu erreichen, um die Einhaltung gesetzlicher, behördlicher oder vertraglicher Verpflichtungen (DSGVO, NIS2, DORA, branchenspezifische Anforderungen) zu gewährleisten;

- Direkte Kontrolle über den physischen und logischen Zugriff auf Daten, einschließlich des Standorts der Server, der Kontrolle der Verschlüsselungsschlüssel und der Organisation der Support-Teams;

- Begrenzung der Risiken im Zusammenhang mit extraterritorialen Zugangsverpflichtungen, die von einem Drittstaat auferlegt werden, unter Beibehaltung der Fähigkeit, schnell und autonom auf die Infrastruktur und die Daten zuzugreifen.

Selbst wenn die Daten streng genommen nicht „sensibel" sind, ist das Maß an Überprüfbarkeit, Verfügbarkeit und Kontrolle ein entscheidendes Kriterium für die Bevorzugung eines lokalen oder europäischen Dienstleisters.

In der Praxis müssen Unternehmen die folgenden drei Kriterien sorgfältig abwägen:

- **Kriterium 1** – Müssen meine Daten geschützt werden?
- **Kriterium 2** – Wenn ja, gibt es in Deutschland oder Europa technische Lösungen, die diesen Anforderungen gerecht werden?
- **Kriterium 3** – Gibt es einen erheblichen Preisunterschied zwischen deutschen, europäischen und ausländischen Lösungen?

Um seine Interessen zu schützen, sollte ein Unternehmen manchmal eine souveräne Lösung wählen, die zwar teurer ist, aber dennoch alle benötigten Funktionen bietet.



4. GRAVITYZONE, DIE SOUVERÄNE SICHERHEITSPLATTFORM VON BITDEFENDER

In dem in diesem Rechtsgutachten beschriebenen Kontext, der durch die Risiken im Zusammenhang mit der Extraterritorialität bestimmter ausländischer Rechte und den verschärften Verpflichtungen aufgrund europäischer Vorschriften (DSGVO, NIS2, DORA, C5-Referenzsystem) gekennzeichnet ist, stellt die Plattform Bitdefender GravityZone ein Beispiel für eine Lösung dar, die den Souveränitätsanforderungen entspricht, die von Anbietern, die in der Europäischen Union tätig sind, erwartet werden.

Über das Hosting hinaus ist die Unternehmensführung des Herausgebers ein zentrales Bewertungskriterium. In dieser Hinsicht ist Bitdefender von der European Cyber Security Organisation (ECSO) zertifiziert, was bestätigt, dass:

- der tatsächliche Sitz in Europa liegt;
- kein Unternehmen außerhalb der Europäischen Union übt eine wesentliche Kontrolle aus;
- mehr als 50 % der FuE-Tätigkeiten finden in der Union statt;
- Die Lösungen entsprechen strikt den europäischen Anforderungen in Bezug auf Vertraulichkeit, Datenschutz und Integrität der Dienste.



Diese Anerkennung ermöglicht es, die Tätigkeit von Bitdefender als ein Souveränitätsmodell zu betrachten, das den europäischen Kriterien entspricht.

In diesem Zusammenhang erfüllt GravityZone die Erwartungen der europäischen und nationalen Behörden in Bezug auf Datenkontrolle, Cyber-Risikomanagement und Begrenzung strategischer Abhängigkeiten. Die Plattform ermöglicht:

- eine kontrollierte Lokalisierung der Daten;
- eine Verringerung des Risikos des Zugriffs durch eine ausländische Behörde;
- eine vollständige Rückverfolgbarkeit der Verarbeitungsvorgänge;
- eine zentralisierte Steuerung der Compliance und der Sicherheitslage;
- eine operative Anpassung an die Anforderungen der DSGVO, der NIS2, der DORA und der Referenzrahmen für Cyber-Resilienz.

Somit bieten die technische Architektur und die Governance von Bitdefender eine Cybersicherheitslösung, deren Merkmale den in diesem Rechtsgutachten identifizierten Souveränitätskriterien entsprechen, sowohl im Hinblick auf die außergemeinschaftlichen rechtlichen Risiken als auch auf die Kontroll- und Resilienz Verpflichtungen, die den in der Europäischen Union tätigen Wirtschaftsakteuren auferlegt sind.



Über Bitdefender

Bitdefender ist ein europäisches Cybersicherheitsunternehmen, das in Rumänien gegründet wurde, heute weltweit vertreten ist und als einer der wichtigsten Akteure der Branche anerkannt ist. Es hat seinen historischen Hauptsitz in Bukarest und verfügt über Niederlassungen in Europa, den Vereinigten Staaten, Australien und dem Nahen Osten und zählt mittlerweile Nutzer in mehr als 170 Ländern.

Bitdefender bietet eine einheitliche Plattform für umfassende Cybersicherheit. Vom traditionellen EPP-Schutz über EDR, XDR, E-Mail-Sicherheit, Threat Intelligence, Data Lake, Red Team- und Pen Test-Services bis hin zu rund um die Uhr verwalteten SOC-Services (MDR) sorgt Bitdefender für Prävention, Schutz, Erkennung, Reaktion und Untersuchung. Dieser einheitliche 360°-Ansatz ermöglicht es, die Abwehrmaßnahmen zu rationalisieren und zu verbessern und gleichzeitig die operative Belastung der Sicherheitsteams zu reduzieren.

Im Bereich der Prävention hat Bitdefender kürzlich neue Module für das Risikomanagement und die Risikominderung eingeführt. Diese Funktionen basieren auf der nahtlosen Integration fortschrittlicher Funktionen, die das Management von Benutzer- und Endgeräte-Risiken, die proaktive Reduzierung der Angriffsfläche (PHASR), das Management der externen Angriffsfläche (EASM), die Stärkung der Sicherheitslage in der Cloud (CSPM+) und das Compliance-Management abdecken. Das Ziel besteht darin, einen einheitlichen Echtzeit-Überblick über alle internen und externen Risiken zu bieten, indem Schwachstellen, Benutzerverhalten und Cloud-Konfigurationen kontinuierlich bewertet werden. Durch die Korrelation der Informationen aus diesen sich ergänzenden Bausteinen ermöglicht Bitdefender Unternehmen, Risiken zu antizipieren, zu priorisieren und zu behandeln, bevor sie sich verschlimmern, und gleichzeitig die Compliance zu rationalisieren und die kontinuierliche Cyber-Resilienz zu unterstützen – alles über eine einzige Schnittstelle.

Das Unternehmen entwickelt auch spezifische Lösungen zur Stärkung der Compliance und der internen Governance. Sein neues Angebot, Compliance Manager, bietet Echtzeit-Transparenz über den Compliance-Status, verfolgt dynamisch die regulatorischen Anforderungen und automatisiert einen Teil der internen Kontrollen. Es ist ein wesentlicher Vorteil für Unternehmen, die strengen Vorschriften wie NIS2, DORA oder der DSGVO unterliegen, und bietet ihnen eine zentralisierte und operative Steuerung.

Über die Autoren

Dieses White Paper wurde von Rechtsanwalt Eric BARBRY und Rechtsanwältin Gabrielle DENOIX DE SAINT MARC, Mitglieder der Anwaltskammer Paris und der Kanzlei Racine, verfasst.

https://www.racine.eu/membre/gabrielle-denoix-de-saint-marc/

Eric Barbry ist Mitleiter des Teams IP IT & Data der Kanzlei Racine Avocats, dass sich mit allen Fragen des geistigen Eigentums, des Rechts der Informationssysteme (Informatik/Internet/Telekommunikation) und des Rechts der personenbezogenen Daten befasst. Er begleitet Unternehmen bei ihren IT- und Digitalprojekten sowohl in beratender Funktion als auch bei Verträgen und Rechtsstreitigkeiten. Er befasst sich mit allen Fragen des Datenschutzrechts und insbesondere der DSGVO (Konformitätsprüfung, Konformitätsherstellung, ausgelagerter Datenschutzbeauftragter, Kontrolle und Rechtsstreitigkeiten vor den zuständigen Behörden, Unterstützung bei Sicherheitsverletzungen).

Eric ist ein anerkannter Experte auf dem Gebiet der Cybersicherheit, sowohl für Präventionsmaßnahmen (Verträge/Beratung/Charta) als auch für Maßnahmen als Reaktion auf Cyberangriffe.

https://www.racine.eu/membre/eric-barbry/

Gabrielle Denoix de Saint Marc arbeitet an der Seite von Éric in seinem IP/IT & Data-Team an strategischen Fragen im Zusammenhang mit Informationstechnologien, Informationssystemen und Datenschutzrecht. Sie ist auf Cyber-Regulierung und IT-Verträge spezialisiert, wodurch sie Unternehmen bei den rechtlichen Aspekten von Digital- und Cybersicherheitsprojekten unterstützen kann. Insbesondere unterstützt sie Kunden bei der Beratung, Ausarbeitung und Verhandlung von IT-Verträgen (Lizenzen, Wartung, SaaS, Outsourcing usw.), bei der Unterstützung im Bereich der Cyber-Regulierung, einschließlich Compliance, Audit, Prävention und Reaktion im Falle von Vorfällen, sowie bei der Einhaltung der DSGVO (ausgelagerter Datenschutzbeauftragter, Sicherheitsaudits und Rechtsstreitigkeiten vor den zuständigen Behörden).

Über das IP IT & Data-Team der Kanzlei Racine

Racine verfügt über ein Team von 12 Anwälten, die internationale Konzerne, Großunternehmen und mittelständische Unternehmen in Europa und Frankreich bei ihrer digitalen Transformation begleiten.

Sie arbeiten auch mit Akteuren aus dem Internetbereich (Online-Plattformen, digitale Dienstleistungsunternehmen) sowie Start-ups zusammen, die sich in der Welt der neuen Technologien und mobilen Anwendungen bewegen.

Die Anwälte dieses Teams sind in drei Kompetenzbereichen tätig:

- *Datenschutz, wo das Team im Bereich des Rechts der personenbezogenen Daten und der Umsetzung der Europäischen Datenschutz-Grundverordnung (DSGVO) tätig ist. Es begleitet seine Kunden auch im Bereich des allgemeinen Datenrechts mit Open Data, Daten von öffentlichem Interesse, vertraulichen Daten usw.*

- *IT, in allen Bereichen der Informatik, des Internets, der Telekommunikation, der Sicherung von Informationssystemen und der Digitalisierung: Das Team verfügt über anerkannte Fachkenntnisse in den Bereichen Digitalisierung (elektronische Signatur, Archivierung oder elektronische Abstimmung), Sicherheit von Informationssystemen, E-Commerce und Informatik (IT-Expertise und Lizenzprüfungen);*

- *IP, wo das Team am Schutz und der Valorisierung des immateriellen Vermögens von Unternehmen beteiligt ist: Das Team ist sowohl in der Beratung als auch in Rechtsstreitigkeiten zum Schutz von Konzepten, Algorithmen, IT- und mobilen Anwendungen, Marken, Domainnamen und Patenten sowie bei der Analyse und dem Schutz immaterieller Vermögenswerte und der Sicherung ihrer Nutzung tätig.*

Über die Kanzlei Racine

Racine ist eine unabhängige Wirtschaftskanzlei mit Schwerpunkt auf europäischem Recht und Hauptsitz in Paris und Brüssel. www.racine.eu

Dank ihrer Zugehörigkeit zum internationalen Netzwerk Multilaw und ihren engen Beziehungen zu ausländischen Kanzleien begleitet Racine europäische und internationale Unternehmen und Konzerne.

Sie beschäftigt rund 270 Anwälte und Juristen.

IP/IT & Data Protection
ebarbry@racine.eu

T: (+33) 6.13.28.91.28

Als führender Anbieter von Cybersecurity-Lösungen bietet Bitdefender hochwertige Lösungen bei der Prävention, Erkennung und Bereinigung von Bedrohungen. Millionen von Verbrauchern, Unternehmen und staatlichen Organisationen vertrauen auf das Expertenwissen von Bitdefender, wenn es um die Bekämpfung von Cybergefahren, den Schutz von Daten, digitale Identitäten und Privatsphäre und den Aufbau von Cyberresilienz geht. Bitdefenders umfangreiche Investitionen in Forschung und Entwicklung zahlen sich aus: So entdecken die Bitdefender Labs Hunderte neue Bedrohungen pro Minute und prüfen mehrere Milliarden Bedrohungsabfragen pro Tag. Bitdefender zeichnet für zahlreiche bahnbrechende Innovationen im Malware-Schutz, der IoT Sicherheit, bei Verhaltensanalysen und künstlicher Intelligenz verantwortlich, und die daraus resultierenden Technologien werden von über 200 der bekanntesten Tech-Unternehmen aus aller Welt eingesetzt. Bitdefender wurde 2001 gegründet, betreut Kunden in über 170 Ländern und ist weltweit mit Niederlassungen vertreten.

Romania HQ
Orhideea Towers
15A Orhideelor Road,
6th District,
Bucharest 060071

T: +40 21 4412452

GERMANY HQ
12 Lohbachstrasse,
58239
Schwerte

T: +49 2304 945 160