

DIGI TAL BUS IN ESS



Cybersecurity
IT-Recht
Datenschutz

DIGITAL BUSINESS

CYBERSECURITY

Cybersecurity

CYBERSECURITY COMPLIANCE

Cybersecurity compliance

4

NIS-2 COMPLIANCE FÜR UNTERNEHMEN

NIS-2 compliance for companies

6

CYBER RESILIENCE ACT

Cyber Resilience Act

8

DIGITAL OPERATIONAL RESILIENCE ACT

Digital Operational Resilience Act

10

IT-RECHT

IT law

VERTRAGSGESTALTUNG FÜR DIGITALE GESCHÄFTSMODELLE

Drafting contracts for digital business models

12

DIE KI-VERORDNUNG: RAHMENBEDINGUNGEN FÜR KI-SYSTEME

The AI Regulation: Framework conditions for AI systems

14

DATA ACT – DIE EU-DATENVERORDNUNG

Data Act – The EU Data Regulation

16

OPEN-SOURCE SOFTWARE

Open-source software

18

DATENSCHUTZ

Data protection

DATENSCHUTZ-FOLGENABSCHÄTZUNGEN ERFOLGREICH DURCHFÜHREN

Successfully performing data protection impact assessments

20

LÖSCHKONZEPTE

Erasure concepts

22

DATENSCHUTZ-COMPLIANCE BEI MICROSOFT 365

Data protection compliance with Microsoft 365

24

ACCESSIBILITY BY DESIGN: BARRIEREFREIHEIT VON PRODUKTEN

Accessibility by design: Accessibility of products

26

Cybersecurity, IT-Recht und Datenschutz stehen im Zentrum einer zunehmend vernetzten Unternehmenswelt. Neue gesetzliche Vorgaben wie die NIS-2-Richtlinie, der Cyber Resilience Act oder der Data Act stellen Unternehmen vor komplexe Compliance-Anforderungen. Diese Broschüre bietet Ihnen praxisnahe Einblicke und Lösungsansätze, wie Sie rechtliche Risiken minimieren, Schwachstellen beheben und Ihr Unternehmen zukunftssicher aufstellen – rechtlich fundiert und strategisch gedacht.

Cybersecurity, IT law and data protection are at the heart of an increasingly interconnected business world. New legal requirements such as the NIS-2 Directive, the Cyber Resilience Act and the Data Act present companies with complex compliance challenges. This brochure offers practical insight and solutions on how to minimise legal risks, eliminate vulnerabilities and future-proof your business – with a sound legal foundation and strategic thinking.

AUTOREN / Authors



Stefan Hessel, LL.M.

Rechtsanwalt, Salary Partner und Head of Digital Business bei reuschlaw in Saarbrücken

Attorney-at-law | LL.M.
Head of Digital Business
at reuschlaw in Saarbruecken



Christoph Callewaert

Rechtsanwalt und Senior Associate in der Digital Business Unit bei reuschlaw in Saarbrücken

Attorney-at-law | Senior Associate
in the Digital Business Unit
at reuschlaw in Saarbruecken



Christina Kiefer, LL.M.

Rechtsanwältin und Senior Associate in der Digital Business Unit bei reuschlaw in Saarbrücken

Attorney-at-law | LL.M.
Senior Associate in the Digital
Business Unit at reuschlaw
in Saarbruecken

INTRO

CYBERSECURITY COMPLIANCE

Cybersecurity compliance

Haftungsrisiken durch Verstöße gegen cybersicherheitsrechtliche Verpflichtungen wirksam vorbeugen.

Durch die Digitalisierung und Vernetzung von Unternehmen und Produkten steigt die Bedeutung von Cybersicherheit. Gesellschaftliche Erwartungen und zunehmende Cyberangriffe führen zu einer steigenden Zahl und Komplexität an unternehmens- und produktbezogenen rechtlichen Vorgaben zur Cybersicherheit wie etwa der NIS-2-Richtlinie, dem Entwurf für einen Cyber Resilience Act und zahlreichen weiteren branchenspezifischen Vorgaben.

UNTERNEHMENSBEZOGENE ANFORDERUNGEN

Die unternehmensbezogenen Anforderungen ergeben sich künftig insbesondere aus der NIS-2-Richtlinie. Die Vorgaben richten sich an sogenannte „wesentliche“ und „wichtige“ Einrichtungen aus insgesamt 18 Wirtschaftssektoren. Betroffen sind bereits Unternehmen ab 50 Beschäftigten mit einem Jahresumsatz von 10 Mio. Euro. In Deutschland werden nach diesen Kriterien ca. 30.000 bis 40.000 Unternehmen erfasst, von denen Schätzungen zufolge derzeit noch knapp 80 % nicht wissen, dass sie betroffen sind. Unternehmen werden künftig unter anderem zur Durchführung von umfassenden Risikobewertungs- und Risikomanagementmaßnahmen verpflichtet. Leitungsorgane müssen die getroffenen Maßnahmen zur Cybersicherheit genehmigen, überwachen und haften unmittelbar für Verstöße.

PRODUKTBEZOGENE ANFORDERUNGEN

Auch in Bezug auf Produkte mit digitalen Elementen ist eine Compliance mit den vielfältigen rechtlichen Anforderungen wichtiger denn je. Unter anderem sollen solche Produkte nach dem geplanten Cyber Resilience Act in der EU künftig nicht nur ohne bekannte Schwachstellen und mit einer sicheren Standardkonfiguration ausgeliefert werden, sondern im Falle von Sicherheitslücken auch über die erwartete Produktlebensdauer oder einen definierten Zeitraum mit Sicherheitsupdates versorgt werden.

How to effectively prevent liability risks from infringements of cybersecurity obligations

The digitalisation and networking of companies and products is raising the importance of cybersecurity. Societal expectations and increasing cyberattacks lead to an increasing number and complexity of company-related and product-related legal requirements for cybersecurity, such as the NIS-2 Directive, the draft for a Cyber Resilience Act and numerous other sector-specific requirements.

Company-related requirements

In the future, company-related requirements will in particular be defined by the NIS-2 Directive. The requirements address so-called 'essential' and 'important' entities from a total of 18 economic sectors. Companies are already addressed if they have as few as 50 employees and an annual turnover of 10 million euros. In Germany, approximately 30,000 to 40,000 companies are covered based on these criteria, of which, according to estimates, almost 80% are still unaware that they are addressees of the NIS-2 Directive. In the future, companies will be obliged, among other things, to implement comprehensive risk assessment and risk management measures. Management bodies must approve and monitor the cybersecurity measures taken and are directly liable for infringements.

Product-related requirements

Also for products with digital elements, compliance with the various legal requirements is more important than ever. Among other things, according to the planned Cyber Resilience Act, such products are not only to be delivered in the EU without known vulnerabilities and with a secure standard configuration in the future, but in the event of security vulnerabilities security updates are also to be provided over the expected product lifetime or a defined period of time.

UNSER ANGEBOT

Wir beraten umfassend zur Cybersecurity Compliance und unterstützen Sie insbesondere mit folgenden Maßnahmen:

- Einführung und Evaluation von Prozessen zum Cybersecurity Compliance Management
- Durchführung von Workshops zur Information über das Cybersicherheitsrecht
- Identifikation von konkreten Vorgaben in Bezug auf Technologie, Organisation und Unternehmensprozesse sowie damit verbundene Gap-Analysen
- Rechtliche Unterstützung bei der Durchführung und Dokumentation von Risikobewertungen sowie erforderlichen Abhilfemaßnahmen
- Präventive und reaktive Unterstützung bei IT-Sicherheitsvorfällen, inkl. Abwicklung von Versicherungsfällen und Regress
- Vorbereitung auf und Begleitung von Verfahren vor Aufsichtsbehörden und Gerichten

What we offer

We provide comprehensive advice on cybersecurity compliance and can particularly support you with the following measures:

- *Introduction and evaluation of processes for cybersecurity compliance management*
- *Conducting workshops to inform on cybersecurity law*
- *Identification of specific requirements in terms of technology, organisation and company processes as well as related gap analyses*
- *Legal support in carrying out and documenting risk assessments and necessary remedial measures*
- *Preventive and reactive support in the event of IT security incidents, including handling of insurance claims and recourse*
- *Preparation for and support in proceedings before supervisory authorities and courts*



NIS-2 COMPLIANCE FÜR UNTERNEHMEN

NIS-2 compliance for companies

Betroffenheit und notwendige Maßnahmen zur Compliance mit der neuen EU-weiten Richtlinie für Cybersicherheit.

Mit der Novelle der Network and Information Security Richtlinie (NIS-2-Richtlinie) wird der Kreis der betroffenen Unternehmen deutlich erweitert und die Vorgaben für Cybersicherheit deutlich verschärft. Spätestens ab dem 18. Oktober 2024 müssen die Vorgaben über nationale Gesetze in den Mitgliedstaaten der EU angewandt werden.

WER IST BETROFFEN?

Die NIS-2-Richtlinie richtet sich an sog. „wesentliche“ und „wichtige“ Einrichtungen. Dies sind Unternehmen und Einrichtungen in insgesamt 18 Wirtschaftssektoren wie dem Energiesektor, dem Transportsektor, der digitalen Infrastruktur oder der Herstellung von Produkten. Betroffen sind bereits Unternehmen ab 50 Beschäftigten mit einem Jahresumsatz von 10 Mio. Euro. Teilweise können Unternehmen auch aufgrund anderer Kriterien als wesentlich bzw. wichtig qualifiziert werden. In Deutschland werden nach diesen Kriterien ca. 30.000 bis 40.000 Unternehmen erfasst, von denen Schätzungen zufolge derzeit noch knapp 80 % nicht wissen, dass sie betroffen sind.

WAS IST UMZUSETZEN?

Die Vorgaben der NIS-2-Richtlinie lassen sich in drei Gruppen zusammenfassen. Die erste Gruppe betrifft den Bereich Governance & Awareness. Leitungsorgane müssen ergriffene Maßnahmen im Bereich der Cybersicherheit billigen und überwachen und haften für Verstöße.

Die zweite Gruppe betrifft die Durchführung von Risikomanagementmaßnahmen. Bei unternehmensbezogenen Entscheidungen und Maßnahmen sind stets die Risiken für die Netz- und Informationssysteme zu bewerten. Ermittelte Risiken müssen durch geeignete technische und organisatorische Maßnahmen beherrschbar gemacht werden.

Die dritte Gruppe von Vorgaben betrifft schließlich einzuhaltende Meldepflichten. Bei erheblichen Sicherheitsvorfällen müssen die zuständigen Aufsichtsbehörden unverzüglich, spätestens jedoch innerhalb von 24 Stunden nach dem Vorfall informiert werden.

Addressees and necessary measures to ensure compliance with the new EU-wide cybersecurity directive

With the amendment of the Network and Information Security Directive (NIS-2 Directive), the group of addressees is significantly expanded and the requirements for cybersecurity are significantly tightened. As of 18 October 2024 at the latest, the requirements must be applied through national laws in the EU member states.

Who is affected?

The NIS-2 Directive addresses so-called 'essential' and 'important' entities. These are companies and entities in a total of 18 economic sectors such as energy, transport, digital infrastructure or manufacturing of products. Companies are already addressed if they have as few as 50 employees and an annual turnover of 10 million euros. In some cases, companies may also be qualified as essential or important based on other criteria. In Germany, approximately 30,000 to 40,000 companies are covered based on these criteria, of which, according to estimates, almost 80% are still unaware that they are addressees of the NIS-2 Directive.

What has to be implemented?

The requirements of the NIS-2 Directive can be summarised in three groups. The first group concerns Governance & Awareness. Management bodies must approve and monitor cybersecurity measures taken and are liable for infringements.

The second group concerns the implementation of risk management measures. When making company-related decisions and taking measures, the risks to the network and information systems must always be assessed. Identified risks must be made manageable through appropriate technical and organisational measures.

Finally, the third group of requirements concerns reporting obligations to be complied with. In the event of significant security incidents, the competent supervisory authorities must be informed immediately, but at the latest within 24 hours of the incident.

WAS DROHT BEI VERSTÖSSEN?

Bei Verstößen drohen neben Bußgeldern auch Weisungen der Aufsichtsbehörde, die bis hin zu einer Untersagung der Wahrnehmung von Leitungsfunktionen durch die Leitungsorgane des jeweiligen Unternehmens reichen. Darüber hinaus sind öffentliche Warnungen möglich.

What are the penalties for infringements?

In addition to fines, infringements may also result in measures by the supervisory authority, which may go as far as prohibiting the management bodies of the respective company from performing management functions. Furthermore, public warnings may be issued.

What we offer

We support you in the implementation of the requirements of the NIS-2 Directive by providing, amongst others, the following services:

- *Legal assessment of whether your company is addressed by the Directive*
- *Identification of the specific requirements for your company*
- *Legal support in the implementation and documentation*
- *Introduction of cybersecurity compliance management*



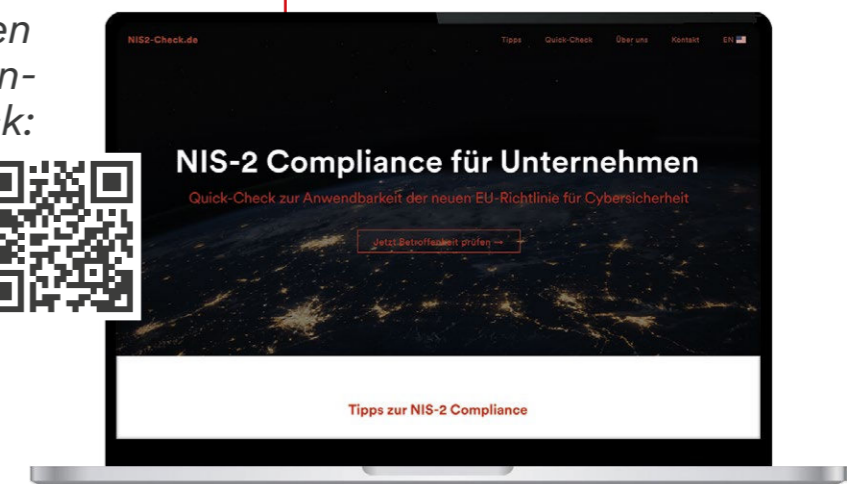
Find out if you are affected for free now: nis2-check.com

UNSER ANGEBOT

Wir unterstützen Sie bei der Umsetzung der Anforderungen der NIS-2-Richtlinie u.a. mit folgenden Leistungen:

- **Rechtliche Prüfung der Betroffenheit Ihres Unternehmens**
- **Ableitung der konkreten Vorgaben für Ihr Unternehmen**
- **Rechtliche Unterstützung bei der Umsetzung und Dokumentation**
- **Einführung eines Cybersecurity Compliance Managements**

Betroffenheit prüfen mit unserem kostenfreien Quick-Check: nis2-check.de



CYBER RESILIENCE ACT

Cyber Resilience Act

Betroffenheit und notwendige Maßnahmen zur Umsetzung der neuen EU-Verordnung zur Cybersicherheit von Produkten mit digitalen Elementen.

Mit dem Cyber Resilience Act (CRA) werden die Anforderungen an die Cybersicherheit für zahlreiche Produkte deutlich verschärft. Ziel des CRA ist die Schaffung eines einheitlichen Sicherheitsstandards für digitale Produkte auf dem Europäischen Markt. Die Verordnung soll ab dem Jahr 2027 unmittelbar in allen EU-Mitgliedstaaten gelten.

WER IST BETROFFEN?

Betroffen sind Hersteller, Einführer und Händler von Produkten mit digitalen Elementen. Produkte mit digitalen Elementen sind Software- oder Hardwareprodukte sowie deren Backend-systeme. Dazu gehören u.a.: Vernetzte Maschinen, IoT-Geräte, Apps, Wearables, Softwareprogramme, Festplatten, Firewalls, Passwort-Manager, Mikroprozessoren, uvm. Nur einige wenige Produktarten sind vom CRA ausgenommen.

WAS IST UMZUSETZEN?

Der CRA verpflichtet Hersteller von Produkten mit digitalen Elementen, bestimmte Anforderungen an die Cybersicherheit und das Schwachstellenmanagement zu erfüllen. Hersteller müssen Produkte mit digitalen Elementen so konzipieren und entwickeln, dass während des gesamten Produktlebenszyklus ein angemessenes Cybersicherheitsniveau gewährleistet ist.

Auf der Grundlage einer Bewertung der Cybersicherheitsrisiken müssen zahlreiche Maßnahmen ergriffen werden. Unter anderem dürfen die erfassten Produkte nur mit einer sicheren Standardkonfiguration und ohne bekannte ausnutzbare Schwachstellen auf den Markt gebracht werden. Darüber hinaus fordert der CRA zahlreiche technische und organisatorische Maßnahmen zur Resilienz der Produkte.

Hersteller von Produkten mit digitalen Elementen müssen außerdem weitreichende Anforderungen an die Behandlung von Schwachstellen erfüllen. Ausgehend von einer fortlaufenden Überwachung der Produkte müssen Hersteller bekannt gewordene Schwachstellen durch kostenlose Sicherheitsupdates beseitigen. Aktiv ausgenutzte Schwachstellen müssen an die Marktüberwachungsbehörde gemeldet werden.

Affected parties and necessary measures for the implementation of the new EU regulation on the cybersecurity of products with digital elements

The Cyber Resilience Act (CRA) significantly tightens the cyber security requirements for numerous products. The aim of the CRA is to create a uniform security standard for digital products on the European market. The regulation is to directly apply in all EU member states from 2027.

Who is affected?

Manufacturers, importers and distributors of products with digital elements are affected. Products with digital elements are software or hardware products and their backend systems. These include, among others: networked machines, IoT devices, apps, wearables, software programs, hard drives, firewalls, password managers, microprocessors and much more. Only a few product types are exempt from the CRA.

What needs to be implemented?

The CRA obliges manufacturers of products with digital elements to fulfil certain cybersecurity and vulnerability management requirements. Manufacturers must design and develop products with digital elements in such a way that an appropriate level of cyber security is guaranteed throughout the entire product life cycle.

Numerous measures must be taken on the basis of a cyber security risk assessment. Among other things, the products covered may only be placed on the market with a secure standard configuration and without known exploitable vulnerabilities. In addition, the CRA requires numerous technical and organisational measures for product resilience.

Manufacturers of products with digital elements must also fulfil far-reaching requirements for the handling of vulnerabilities. Based on continuous monitoring of the products, manufacturers must eliminate known vulnerabilities through free security updates. Actively exploited vulnerabilities must be reported to the market surveillance authority.

WAS DROHT BEI VERSTÖSSEN?

Die Marktüberwachungsbehörden verfügen über weitreichende Untersuchungs-, Abhilfe- und Sanktionsbefugnisse. Bei Verstößen gegen den CRA drohen unter anderem Produktwarnungen und Bußgelder bis zu 15 Millionen Euro oder 2,5 Prozent des weltweiten Jahresumsatzes.

What are the consequences of violations?

The market surveillance authorities have extensive powers to investigate, remedy and impose sanctions. Violations of the CRA can result in product warnings and fines of up to 15 million euros or 2.5 per cent of annual global turnover.

What we offer

We support your company in implementing the requirements of the Cyber Resilience Act with the following services, among others:

- Examination of the impact
- Requirements catalogue and gap analysis
- Drafting contracts with suppliers and service providers
- Cybersecurity compliance management

More information about the regulation:
cyber-resilience-act.com



Go directly to the Quick Check:
cra-check.com

UNSER ANGEBOT

Wir unterstützen Sie bei der Umsetzung der Anforderungen des Cyber Resilience Act u.a. mit folgenden Leistungen:

- Prüfung der Betroffenheit
- Anforderungskatalog und Gap-Analyse
- Vertragsgestaltung mit Lieferanten und Dienstleistern
- Cybersecurity Compliance Management

Mehr Infos zur Verordnung:
cyber-resilience-act.de

Direkt zum Quick-Check: cra-check.de



DIGITAL OPERATIONAL RESILIENCE ACT

Digital Operational Resilience Act

Betroffenheit und notwendige Maßnahmen zur Compliance mit der EU-weiten Cybersicherheitsverordnung für den Finanzsektor.

Mit dem Digital Operational Resilience Act (DORA) wird ein einheitlicher europäischer Rechtsrahmen für Cybersicherheitsanforderungen im Finanzsektor geschaffen. Ziel ist es, die operationelle Resilienz von Finanzunternehmen zu gewährleisten. Der DORA ist bereits in Kraft getreten und findet ab dem 17. Januar 2025 Anwendung.

WER IST BETROFFEN?

Der DORA richtet sich in erster Linie an Finanzunternehmen aus über 20 verschiedenen Branchen, darunter Kreditinstitute, Zahlungs- und Kontoinformationsdienstleister, Wertpapierfirmen, Versicherungs- und Rückversicherungsunternehmen sowie Einrichtungen der betrieblichen Altersversorgung. Darüber hinaus werden auch IKT-Drittdienstleister erfasst, die Finanzunternehmen mit IKT-Dienstleistungen unterstützen.

WAS IST UMZUSETZEN?

Die Anforderungen des DORA können in vier Hauptbereiche unterteilt werden. Der erste Bereich betrifft das IKT-Risikomanagement. Finanzunternehmen müssen einen internen Governance- und Kontrollrahmen einrichten, um IKT-Risiken effektiv zu identifizieren und darauf zu reagieren. Die Verantwortung für die Überwachung und Umsetzung liegt bei der Unternehmensleitung. Der zweite Bereich umfasst die Behandlung und Meldung von IKT-bezogenen Vorfällen. Unternehmen sind verpflichtet, ein Incident Management zu implementieren, das die Überwachung, Ursachenermittlung, Klassifizierung und Dokumentation von IKT-bezogenen Vorfällen umfasst. Der dritte Bereich betrifft Resilienztests. Die IKT-Resilienz muss regelmäßig durch umfassende Testverfahren wie Schwachstellenanalysen, Penetrationstests und Netzwerksicherheitsbewertungen sichergestellt werden. Der vierte Bereich regelt schließlich das Management von Drittanbieterisiken. Auch bei der Auslagerung an IKT-Drittdienstleister verbleibt die Verantwortung beim betroffenen Unternehmen. Es sind Risikoanalysen durchzuführen, ein Informationsregister zu führen und vertragliche Vereinbarungen mit vorgegebenen Mindestinhalten zu treffen. Für kleine Unternehmen gibt es teilweise Ausnahmen und Erleichterungen bei der Umsetzung einzelner Anforderungen.

Concerns and necessary measures for compliance with the EU-wide cybersecurity regulation for the financial sector

The Digital Operational Resilience Act (DORA) establishes a uniform European legal framework for cybersecurity requirements in the financial sector. The aim is to ensure the operational resilience of financial companies. The DORA has already entered into force and will apply from 17 January 2025.

Who is affected?

The DORA is primarily aimed at financial companies from over 20 different industries, including credit institutions, payment and account information service providers, investment firms, insurance and reinsurance companies, and institutions for occupational retirement provision. ICT third-party service providers that support financial companies with ICT services are additionally covered.

What needs to be implemented?

The requirements of the DORA can be divided into four main areas. The first area concerns ICT risk management. Financial firms need to establish an internal governance and control framework to effectively identify and respond to ICT risks. The responsibility for monitoring and implementation lies with the company's management. The second area covers the treatment and reporting of ICT-related incidents. Companies are required to implement incident management, which includes monitoring, root cause identification, classification and documentation of ICT-related incidents. The third area concerns resilience testing. ICT resilience must be ensured regularly through comprehensive testing procedures such as vulnerability assessments, penetration tests and network security assessments. Finally, the fourth area regulates the management of third-party risks. Even in the case of outsourcing to ICT third-party service providers, the responsibility remains with the concerned company. Risk analyses must be carried out, an information register must be maintained and contractual agreements with specified minimum content must be concluded. For small companies, there are some exceptions and facilitations in the implementation of individual requirements.

WAS DROHT BEI VERSTÖSSEN?

Aufsichtsbehörden wie die BaFin oder die EZB können Zwangsgelder verhängen, Weisungen erteilen und Verstöße öffentlich machen. Auch strafrechtliche Sanktionen sind möglich.

What are the consequences of violations?
Supervisory authorities such as BaFin or the ECB can impose penalty payments, issue instructions and make violations public. Criminal sanctions are also possible.

UNSER ANGEBOT

Wir unterstützen Sie bei der Umsetzung der Anforderungen des DORA u.a. mit folgenden Leistungen:

- **Rechtliche Prüfung der Betroffenheit Ihres Unternehmens**
- **Ableitung der konkreten Vorgaben für Ihr Unternehmen**
- **Rechtliche Unterstützung bei der Umsetzung und Dokumentation**
- **Einführung eines Cybersecurity Compliance Managements**

What we offer

We support you in implementing the requirements of the DORA with the following services, among others:

- **Legal review of the impact on your company**
- **Derivation of the concrete requirements for your company**
- **Legal support for implementation and documentation**
- **Introduction of cybersecurity compliance management**

VERTRAGSGESTALTUNG FÜR DIGITALE GESCHÄFTS- MODELLE

*Drafting contracts for digital
business models*

*Klare Regeln festlegen, Vertrauen sichern
und Haftungsrisiken minimieren.*

Bei digitalen Geschäftsmodellen wie Abo-, Pay-per-Use- oder Sharing-Modellen spielt die Vertragsgestaltung eine wichtige Rolle. Moderne Technologien und Innovationen bringen neue rechtliche Herausforderungen mit sich. Die verbindliche Festlegung von Rechten, Pflichten und Verantwortlichkeiten der Parteien erhöht die Transparenz, sichert das Vertrauen in die Leistungen und vermeidet gleichzeitig Haftungsrisiken.

IT-VERTRAGSRECHT

Grundlage jedes digitalen Geschäftsmodells sind Regelungen zur Überlassung und Nutzung der Produkte bzw. Dienstleistungen. Je nach Geschäftsmodell sind Regelungen aus dem Kauf-, Miet-, Werk- oder Dienstvertragsrecht zu beachten. Software-as-a-Service erfordert z.B. andere Regelungen als Platform- oder Infrastructure-as-a-Service. Insbesondere Gewährleistungs- und Haftungsklauseln sind auf ihre rechtliche Zulässigkeit zu prüfen. Eine besondere Herausforderung ist zudem der Einsatz von Open-Source Software (OSS) und die damit verbundene Prüfung und Auswahl der Lizenzbedingungen.

DATENSCHUTZ

Werden personenbezogene Daten verarbeitet, sind zunächst die datenschutzrechtlichen Verantwortlichkeiten zu prüfen. Darauf aufbauend sind ggf. Verträge über eine Auftragsverarbeitung oder eine gemeinsame Verantwortlichkeit zu prüfen und/oder zu erstellen. Dies kann aufgrund der strengen Anforderungen der Datenschutzaufsichtsbehörden eine Herausforderung darstellen. Insbesondere kritische Aspekte wie die Weisungs- und Kontrollrechte des Verantwortlichen oder die Löschung der Daten nach Auftragserledigung sind bei der datenschutzrechtlichen Vertragsgestaltung zu berücksichtigen.

*Establish clear rules, ensure trust
and minimise liability risks*

Contract design plays an important role in digital business models such as subscription, pay-per-use or sharing models. Modern technologies and innovations bring about new legal challenges. The binding definition of rights, obligations and responsibilities of the parties increases transparency, ensures trust in the services and at the same time avoids liability risks.

IT contract law

Every digital business model is based on regulations governing the provision and use of products and services. Depending on the business model, regulations from purchase, rental, work or service contract law must be observed. Software-as-a-Service, for example, requires different regulations than Platform- or Infrastructure-as-a-Service. Warranty and liability clauses in particular must be checked for their legal admissibility. Another particular challenge is the use of open-source software (OSS) and the associated review and selection of licence conditions.

Data protection

If personal data is processed, the responsibilities under data protection law must first be checked. Based on this, contracts for commissioned data processing or joint controllership may need to be reviewed and/or drawn up. This can pose a challenge due to the strict requirements imposed by the data protection supervisory authorities. In particular, critical aspects such as the controller's instruction and control rights or the deletion of data after the task has been completed must be taken into account when drafting contracts under data protection law.

CYBERSICHERHEIT

Mit dem neuen europäischen Cybersicherheitsrecht wird es zukünftig zahlreiche Vorgaben zur Cybersicherheit geben. Diese sind aufgrund der zunehmenden Cyberbedrohungen und Sicherheitsvorfälle insbesondere auch gegenüber Lieferanten und Dienstleistern durchzusetzen. Vertragliche Regelungen und die Weitergabe der Pflichten in der Lieferkette sind daher unerlässlich.

Cybersecurity

There will be numerous cybersecurity requirements in the future under the new European cybersecurity law. Due to the increasing cyber threats and security incidents, these requirements will also have to be enforced against suppliers and service providers in particular. Appropriate contractual regulations and the passing on of obligations in the supply chain are therefore essential and indispensable.

What we offer

We check and draft your contracts and render the following services to support you:

- *Determination and analysis of the facts*
- *Review and drafting of IT contracts*
- *Open-source in contract drafting*
- *Data protection compliance*
- *Contract drafting in the supply chain*
- *Contract management and strategic implementation*

UNSER ANGEBOT

Wir prüfen und erstellen Ihre Verträge und unterstützen Sie mit folgenden Leistungen:

- Sachverhaltsermittlung und Bestandsaufnahme
- Prüfung und Erstellung von IT-Verträgen
- Open-Source in der Vertragsgestaltung
- Datenschutz-Compliance
- Vertragsgestaltung in der Lieferkette
- Vertragsmanagement und strategische Umsetzung

DIE KI-VERORDNUNG: RAHMENBEDINGUNGEN FÜR KI-SYSTEME

The AI Regulation: Framework conditions for AI systems

Mit der KI-Verordnung (EU) 2024/1689 kommen auf Unternehmen umfangreiche rechtliche Anforderungen an den Einsatz von KI-Systemen zu.

Ziel der KI-VO, auch AI-Act genannt, ist ein einheitlicher Rechtsrahmen für die Entwicklung, das Inverkehrbringen, die Inbetriebnahme und die Verwendung von KI-Systemen auf dem Europäischen Binnenmarkt. Mit der KI-VO kommen umfangreiche Anforderungen auf Unternehmen zu. Erste Anforderungen müssen Unternehmen bereits ab dem 2. Februar 2025 erfüllen.

WER IST BETROFFEN?

Die KI-VO gilt sowohl für die Privatwirtschaft als auch für öffentliche Stellen innerhalb und außerhalb der EU, sofern KI-Systeme in der EU in Verkehr gebracht werden oder deren Nutzung Auswirkungen auf Menschen in der EU hat. Sie richtet sich in erster Linie an Anbieter und Betreiber von KI-Systemen, aber auch an Einführer, Händler und Produkthersteller.

RISIKOBASIERTER ANSATZ

Die KI-VO verfolgt einen risikobasierten Ansatz und unterscheidet zwischen verbotener KI, Hochrisiko-KI, General Purpose AI (GPAI) und KI mit geringem oder minimalem Risiko. Die Verbote für bestimmte Anwendungsfälle von KI gelten bereits ab dem 2. Februar 2025. Kernstück der KI-Verordnung sind die Regelungen für Hochrisiko-KI, die ab dem 2. August 2026 gelten. Die Regelungen für GPAI, zu denen auch Large Language Models (LLM) gehören, gelten ab dem 2. August 2025.

WAS IST UMZUSETZEN?

Anbieter von Hochrisiko-KI-Systemen müssen eine Risikobewertung durchführen und das System so gestalten, dass die Risiken für die Gesundheit, die Sicherheit und die Grundrechte minimiert werden. Zu den weiteren Pflichten der KI-VO gehören die Einführung von Qualitäts- und Risikomanagementsystemen, Transparenzpflichten, die Gewährleistung einer menschlichen Aufsicht sowie Dokumentations-, Informations- und Meldepflichten.

AI Regulation (EU) 2024/1689 imposes extensive legal requirements on companies for the use of AI systems

The aim of the AI Regulation, also known as the AI Act, is to create a uniform legal framework for the development, market placement, commissioning and use of AI systems on the European Single Market. The AI Regulation imposes extensive requirements on companies, which must meet the first requirements as early as 2 February 2025.

Who is affected?

The AI Regulation applies to both the private sector and public bodies inside and outside the EU, provided that AI systems are placed on the market in the EU or their use has an impact on people in the EU. It is primarily aimed at suppliers and operators of AI systems, but also at importers, distributors and product manufacturers.

Risk-based approach

The AI Regulation takes a risk-based approach and distinguishes between prohibited AI, high-risk AI, general purpose AI (GPAI) and low- or minimal-risk AI. The bans for certain use cases of AI will apply as early as 2 February 2025. At the heart of the AI Regulation are the regulations for high-risk AI, which will apply from 2 August 2026. The regulations for GPAI, which also include Large Language Models (LLM), will apply from 2 August 2025.

What needs to be implemented?

Providers of high-risk AI systems must carry out a risk assessment and design the system in such a way that the risks to health, safety and fundamental rights are minimised. Other obligations of the AI Regulation include the introduction of quality and risk management systems, transparency obligations, the guarantee of human supervision as well as documentation, information and reporting obligations.

WAS DROHT BEI VERSTÖSSEN?

Für die Überwachung und Durchsetzung der KI-VO sind die Marktüberwachungsbehörden der Mitgliedstaaten zuständig. Sie haben umfangreiche Befugnisse und können bei Verstößen empfindliche Geldbußen verhängen. Bei negativen Auswirkungen auf Verbraucher oder andere Personen drohen außerdem Schadenersatzansprüche.

What are the consequences of violations?
The market surveillance authorities of the member states are responsible for monitoring and enforcing the AI Regulation. They have extensive powers and can impose severe fines for violations. In the event of negative effects on consumers or other persons, there is also a risk of claims for damages.

What we offer

We support your company in implementing the requirements of the AI Regulation with the following services, among others:

- *Legal review of the impact of your applications*
- *Implementation of the requirements of the AI Regulation and best practices*
- *Data usage agreements and contractual frameworks for AI systems*
- *Conducting data protection and fundamental rights impact assessments*

UNSER ANGEBOT

Wir unterstützen Ihr Unternehmen bei der Umsetzung der Anforderungen an die KI-VO u.a. mit folgenden Leistungen:

- **Rechtliche Prüfung der Betroffenheit Ihrer Anwendungen**
- **Umsetzung der Anforderungen aus der KI-VO und Best Practices**
- **Datennutzungsverträge und Vertragsrahmenwerke für KI-Systeme**
- **Durchführung von Datenschutz- und Grundrechte-Folgenabschätzungen**

DATA ACT - DIE EU-DATEN- VERORDNUNG

Data Act – The EU Data Regulation

Der Data Act regelt den fairen Datenzugang und die Datennutzung in der EU – unabhängig davon, ob die Daten einen Personenbezug aufweisen. Anbieter von vernetzten Produkten und Diensten müssen von der Entwicklungsphase bis hin zur Datenweitergabe neue Pflichten beachten. Die Anforderungen der Verordnung gelten ab dem 12. September 2025.

DATENZUGANGSRECHTE

Ein wesentliches Element der **Verordnung (EU) 2023/2854** ist der Datenzugang für Nutzer. Nutzer können natürliche oder juristische Personen sein. Vernetzte Produkte und Dienste sind so zu konzipieren, dass Produkt- bzw. Dienstdaten für Nutzer zugänglich sind (Access by Design). Daten, auf die Nutzer nicht direkt zugreifen können, müssen auf andere Weise in Echtzeit zugänglich gemacht werden (Share by Request). Hierfür ist in der Regel eine Online-Plattform oder eine App erforderlich.

DATENNUTZUNG

Anbieter vernetzter Produkte und Dienste müssen bei der Nutzung von Daten, auch nicht-personenbezogener Daten, einen Datennutzungsvertrag mit ihren Nutzern abschließen. Folgende drei Regelungen sind daher nunmehr mindestens zu beachten:

- Hauptvertrag über das Produkt, d.h. Kauf-, Miet- oder Leasingvertrag
- Vertrag über die Nutzung nicht-personenbezogener Daten
- Rechtsgrundlage für die Verarbeitung personenbezogener Daten

Im B2B-Verhältnis gilt ein Verbot von missbräuchlichen Vertragsklauseln. Im B2C-Verhältnis gilt allgemeines Verbraucherrecht. Neben dem Datenzugang können Nutzer verlangen, dass ein Dateninhaber ihre Daten an Dritte weitergibt. Unternehmen müssen entsprechende Vertragswerke und Prozesse bereithalten. Auch Empfänger von Daten haben neue Pflichten zu beachten.

The Data Act regulates fair access to and use of data in the EU – regardless of whether the data is personal. Providers of networked products and services must comply with new obligations from the development phase to data sharing. The requirements of the regulation will apply from 12 September 2025.

Data access rights

A key element of Regulation (EU) 2023/2854 is access to data for users. Users can be natural or legal persons. Networked products and services must be designed in such a way that product or service data is accessible to users (access by design). Data that users cannot directly access must be made accessible in real time in another way (share by request). This usually requires an online platform or an app.

Data usage

Providers of networked products and services must conclude a data usage agreement with their users when using data, including non-personal data. The following three regulations must therefore now be observed as a minimum:

- *Main contract for the product, i.e., purchase, rental or leasing contract*
- *Contract for the use of non-personal data*
- *Legal basis for processing personal data*

In the B2B relationship, there is a ban on unfair contract terms. In the B2C relationship, general consumer law applies. In addition to data access, users can request that a data holder share their data with third parties. Companies must have appropriate contracts and processes in place. Recipients of data also have new obligations to observe.

INFORMATIONSPFLICHTEN UND SCHUTZMASSNAHMEN

Anbieter vernetzter Produkte und Dienste müssen vor Abschluss eines Kauf-, Miet- oder Leasingvertrages umfangreiche Informationen zur Datennutzung bereitstellen. Zudem können technische Schutzmaßnahmen gegen eine unbefugte Nutzung oder eine Offenlegung von Daten ergriffen werden. Diese dürfen die Rechte der Nutzer jedoch nicht beeinträchtigen.

Information obligations and protective measures

Providers of connected products and services must provide extensive information on data usage before concluding a purchase, rental or leasing contract. In addition, technical protection measures can be taken against unauthorised use or disclosure of data. However, they must not affect the rights of users.

What we offer

We are happy to support your company in the implementation of the Data Act with the following services, among others:

- *Check which of your products are affected and what data you need to provide*
- *Support in the fulfilment of information obligations*
- *Drafting of data usage and data transfer contracts*
- *Impact of the Data Act on existing contracts such as GTC*
- *Supply chain compliance*

UNSER ANGEBOT

Wir unterstützen Ihr Unternehmen bei der Umsetzung des Data Act gerne u.a. mit folgenden Leistungen:

- Prüfung, welche Ihrer Produkte betroffen sind und welche Daten Sie bereitstellen müssen
- Unterstützung bei der Erfüllung der Informationspflichten
- Erstellung von Datennutzungs- und Datenübertragungsverträgen
- Auswirkung des Data Act auf bestehende Vertragswerke wie z.B. AGB
- Compliance in der Lieferkette

OPEN-SOURCE SOFTWARE

Open-source software

Lizenzrechtliche Risiken im Unternehmen vermeiden.

Open-Source Software ist aus dem Alltag vieler Unternehmen nicht wegzudenken. In einer Bitkom-Umfrage aus dem Jahr 2021 gaben 87% der Unternehmen mit mehr als 2.000 Beschäftigten an, quelloffene Software im Unternehmen einzusetzen. Quelloffene Software ist jedoch nicht rechtsfrei. Aus der Verwendung bestimmter Open-Source Lizenzen kann sich beispielsweise die Pflicht zur Offenlegung des eigenen Programmcodes und damit von Geschäftsgeheimnissen ergeben.

JEDER KANN BETROFFEN SEIN

Die moderne Softwareentwicklung ist hochgradig modularisiert und in nahezu allen neueren Entwicklungsprojekten finden sich zumindest Spuren von Open-Source Code. Daher sind praktisch alle Anbieter und Entwickler digitaler Lösungen von den lizenzrechtlichen Herausforderungen von Open-Source Software betroffen – oftmals ohne, dass es ihnen bewusst ist.

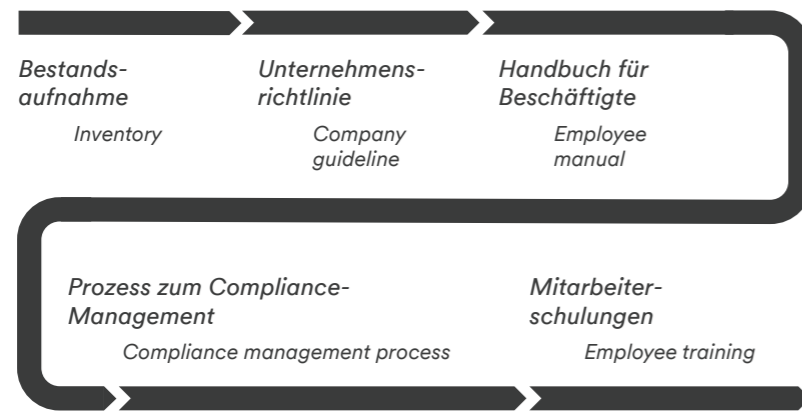


Abbildung / Figure: Open-Source Software Compliance
© reuschlaw, 2023

Eine genaue Prüfung erfordert der Einsatz von Open-Source Software in der Cloud oder in Embedded Systems: Es stellen sich vielfältige rechtliche Probleme, die unter anderem daraus resultieren, dass viele Lizenzbedingungen für Open-Source Software zu einer Zeit formuliert wurden, zu der ein Cloud-Einsatz nicht in Betracht kam.

Avoid licensing risks in the company

Open-source software has become an indispensable part of everyday life for many companies. In a Bitkom survey from 2021, 87% of companies with more than 2,000 employees stated that they use open-source software in their company. However, open-source software is not free of rights. Using certain open-source licences, for example, may result in the obligation to disclose one's own program code and thus business secrets.

Anyone can be affected

Modern software development is highly modularised. Almost all recent development projects contain at least traces of open-source code. As a result, virtually all providers and developers of digital solutions are confronted with the licensing challenges of open-source software – often without them being aware of it.

The use of open-source software in the cloud or in embedded systems requires close examination. Systems: A variety of legal problems can arise, resulting, among other things, from the fact that many licence conditions for open-source software were formulated at a time when cloud deployment was not an option.

OPEN-SOURCE SOFTWARE COMPLIANCE

Wir helfen Ihnen, die Vorteile und das Potenzial von Open-Source Software in ihrem Unternehmen zu nutzen und rechtliche Risiken zu minimieren. Unser Angebot deckt alle notwendigen Schritte zum Aufbau eines zuverlässigen Managementsystems für Open-Source Software Compliance ab. Dazu gehören:

- Die Bestandsaufnahme der verwendeten Open-Source Software und deren Lizenzbedingungen
- Unternehmensrichtlinien zum Einsatz von Open-Source Software
- Handbuch für Beschäftigte mit den wichtigsten Lizenzanforderungen und Handlungsempfehlungen
- Das Gestalten von Prozessen zur Einhaltung von Lizenzanforderungen, z.B. bei Neueinführung von Open-Source Software
- Mitarbeiterschulungen zur Sensibilisierung

Open-source software compliance

We will help you to use the advantages and potential of open-source software in your company and to minimise legal risks. Our offer covers all necessary steps to build a reliable management system for open-source software compliance. These include:

- The inventory of the open-source software used and its licensing conditions
- Corporate policies on the use of open-source software
- A manual for employees with the most important licensing requirements and recommended actions
- Design of processes to comply with licensing requirements, e.g., when introducing new open-source software
- Employee training to raise awareness

DATENSCHUTZ- FOLGENABSCHÄTZUNGEN ERFOLGREICH DURCHFÜHREN

So gelingt ein datenschutzkonformer Einsatz von neuen Technologien

Ob die Einführung von Microsoft 365 oder anderen Kollaborationstools, die Einrichtung digitaler Hinweisgebersysteme oder Videoüberwachung: Die Durchführung einer Datenschutz-Folgenabschätzung (kurz: DSFA) ist immer angezeigt, wenn eine Datenverarbeitung ein hohes Risiko für Betroffene darstellt. Eine DSFA macht häufig Aufwand, leistet jedoch einen wichtigen Beitrag zu einer datenschutzkonformen Einführung von neuen Technologien.

HOCHRISIKO-VERARBEITUNGEN

Die erste Hürde besteht darin, zu ermitteln, ob eine DSFA überhaupt erforderlich ist. Die Datenschutz-Grundverordnung (DSGVO) nennt zwar einige Beispiele für riskante Verarbeitungen, wie die umfangreiche Verarbeitung von sensiblen Daten oder die systematische und umfassende Bewertung natürlicher Personen, z.B. im Hinblick auf die Kreditwürdigkeit. In vielen Fällen ist der Verantwortliche jedoch auf sich selbst gestellt und muss mit einer Schwellwertanalyse eigenständig prüfen, ob hohe Risiken bestehen und eine DSFA erforderlich ist.

DIE DSFA IN DER PRAXIS

Klarer sind die rechtlichen Vorgaben, wie genau eine DSFA ausgestaltet sein muss. Diese muss mindestens vier Elemente enthalten:

- Beschreibung der geplanten Verarbeitungsvorgänge und Zwecke
- Bewertung der Notwendigkeit und Verhältnismäßigkeit der Verarbeitungsvorgänge
- Bewertung der Risiken für betroffene Personen
- Abhilfemaßnahmen, durch die der Schutz personenbezogener Daten sichergestellt wird

Successfully performing data protection impact assessments

Here's how to use new technologies in a way that complies with data protection laws

Whether implementing Microsoft 365 or other collaboration tools, setting up digital whistleblower systems or video surveillance: the performance of a data protection impact assessment is always indicated when a data processing operation poses a high risk for data subjects. A data protection impact assessment often isn't easy, but makes an important contribution to data-protection-compliant introduction of new technologies.

High-risk processing

The first hurdle is to determine whether a DSFA is even necessary. Although the General Data Protection Regulation (GDPR) provides some examples of risky processing, such as the extensive processing of sensitive data or the systematic and comprehensive assessment of natural persons (e.g. with regard to credit-worthiness), in many cases the data controller is on their own and must use a threshold analysis to independently check whether high risks exist and a data protection impact assessment is required.

Data protection impact assessment in practice

The legal requirements are clearer as to how exactly a data protection impact assessment must be structured. It must contain at least four elements:

- Description of the planned processing operations and purposes
- Assessment of the necessity and proportionality of the processing operations
- Assessment of the risks for data subjects
- Remedial measures ensuring the protection of personal data

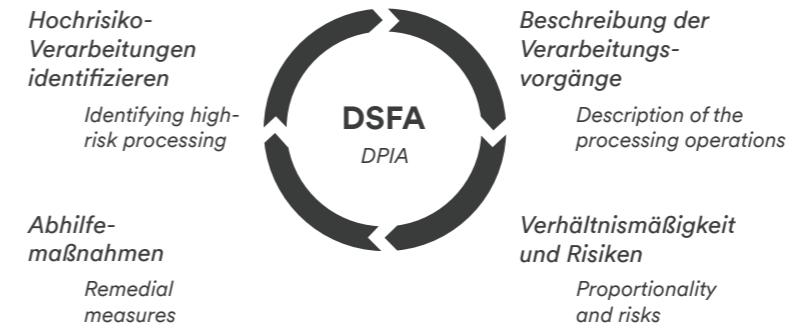


Abbildung / Figure:
DSFA / DPIA © reuschlaw, 2023

What we offer

We provide comprehensive advice on conducting data protection impact assessments and can particularly support you with the following measures:

- Identifying the processing operations, purposes and legal bases
- Conducting a threshold analysis and DSFA, incl. risk assessment and proposed remedial actions
- Involving all relevant stakeholders – from the specialist department through the data protection officer to management
- Ensuring documentation to prove compliance

UNSER ANGEBOT

Wir beraten umfassend zur Durchführung von Datenschutz-Folgenabschätzungen und können Sie insbesondere mit folgenden Maßnahmen unterstützen:

- Identifikation der Verarbeitungsvorgänge, Zwecke und Rechtsgrundlagen
- Durchführung von Schwellwertanalyse und DSFA, inkl. Risikobewertung und Vorschlägen für Abhilfemaßnahmen
- Einbeziehung aller relevanten Akteure – von der Fachabteilung über den Datenschutzbeauftragten bis hin zum Management
- Dokumentation zum Nachweis der Compliance

LÖSCHKONZEPTE

Erasure concepts

Das Löschen personenbezogener Daten erfordert planvolles Vorgehen. Schließlich sollen die richtigen Daten zur richtigen Zeit und am richtigen Ort gelöscht werden.

RISIKEN OHNE DATENSCHUTZ-KONFORMES LÖSCHEN

Das regelmäßige Löschen personenbezogener Daten gehört zu den Grundlagen datenschutzrechtlicher Compliance. Gerade für Unternehmen mit großem Datenbestand und einer über die Jahre gewachsenen IT-Infrastruktur ist datenschutzkonformes Löschen eine erhebliche Herausforderung. Es ist nicht damit getan, personenbezogene Daten auf Anfrage des Betroffenen zu löschen. Die DSGVO erfordert regelmäßiges Löschen. Wird nicht gelöscht, drohen empfindliche Bußgelder sowie Schadensersatzforderungen.

SCHRITTE ZUM DATENSCHUTZ-KONFORMEN LÖSCHEN

Das datenschutzkonforme Löschen von personenbezogenen Daten im Unternehmen bedarf sorgfältiger Analyse und Planung. Zentral ist ein Löschkonzept, das die wichtigen Punkte zur Löschung vorgibt. Rechtliche Anforderungen an das datenschutzkonforme Löschen, die Identifizierung relevanter Aufbewahrungsrechte und -pflichten sowie die Prozesse zum Löschen einschließlich eines Rollen- und Berechtigungskonzepts für Löschtscheidungen werden hier abgebildet. Ein Löschkonzept umfasst typischerweise strukturierte und unstrukturierte Daten sowie analoge Daten und Datenträger.

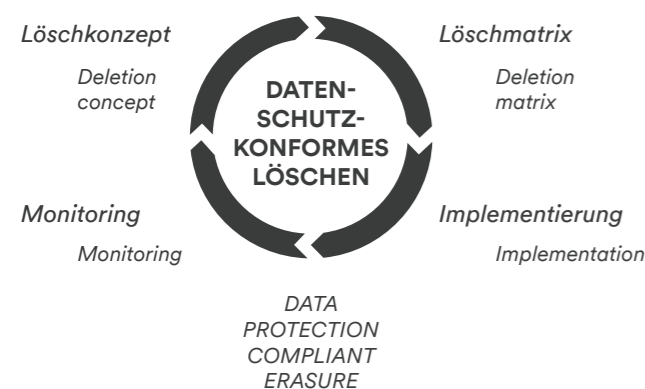


Abbildung / Figure:
Datenschutzkonformes Löschen /
Data protection compliant erasure © reuschlaw, 2023

Erasing personal data requires a planned approach. After all, the right data should be deleted at the right time and in the right place.

Risks without data protection compliant erasure

Regular erasure of personal data is one of the basics of data protection compliance. Particularly for companies with large data inventories and an IT infrastructure that has grown over the years, data protection compliant erasure is a considerable challenge. It is not enough to erase personal data at the request of the data subject. The GDPR requires regular erasure. Failure to erase data may result in severe fines and damage compensation claims.

Steps for data protection compliant erasure

The erasure of personal data in the company in compliance with data protection regulations requires careful analysis and planning. Key to this is an erasure concept that specifies the important points for erasure. Legal requirements for data protection-compliant erasure, the identification of relevant retention rights and obligations, and the processes for erasure including a role and authorisation concept for erasure decisions are mapped here. An erasure concept typically includes structured and unstructured data as well as analogue data and data carriers.

Konkretisiert wird das Löschkonzept mithilfe einer Löschematrix, die in unterschiedlicher Granularität erstellt werden kann. In dieser sind Datenarten Löschklassen zugeordnet und mit den jeweiligen Aufbewahrungs- und Löschfristen sowie den entsprechenden Startzeitpunkten versehen.

UNSER ANGEBOT

Wir bieten Ihnen vollumfängliche Beratung zum datenschutzkonformen Löschen in Ihrem Unternehmen. Insbesondere unterstützen wir Sie mit folgenden Maßnahmen:

- Erstellung eines Löschkonzeptes, das alle relevanten Löschfristen, Aufbewahrungsrechte und -pflichten sowie die Festlegung von Rollen und Verantwortlichkeiten und geeignete Löschverfahren enthält
- Konkretisierung des Konzeptes in einer Löschematrix
- Einbeziehung der Abhängigkeiten der gesamten IT-Infrastruktur (inklusive Data- und Dataflow-Mapping)
- Internationalisierung Ihres Löschkonzeptes
- Cybersecurity Compliance Management

The erasure concept is concretised with the help of an erasure matrix, which can be created in different granularities. Data types are assigned in the matrix to erasure classes and provided with the respective retention and erasure periods as well as the corresponding start times.

What we offer

We offer you comprehensive advice on data protection compliant erasure in your company. In particular, we support you with the following measures:

- *Creation of an erasure concept that includes all relevant erasure periods, retention rights and obligations, as well as definition of roles and responsibilities and suitable erasure procedures*
- *Concretisation of the concept in an erasure matrix*
- *Inclusion of the dependencies of the entire IT infrastructure (including data and dataflow mappings)*
- *Internationalisation of your erasure concept*

DATENSCHUTZ-COMPLIANCE

BEI MICROSOFT 365

Data protection compliance
with Microsoft 365

Ihr Weg zur datenschutzkonformen Nutzung.

Your way to data protection
compliant use

Legal risks when using Microsoft 365

The good news first: Based on our legal analysis, an intensive exchange with Microsoft and the data protection supervisory authorities, data protection-compliant use of Microsoft 365 is possible. However, untested or undocumented use of Microsoft 365 is a risk for companies and can result in fines and damage compensation claims.

Step-by-step to data protection compliance

In our experience from numerous implementation projects, data protection compliance with Microsoft 365 requires a multi-stage data protection process. This should be documented and include the following steps in particular:

- Determining the application scenarios
- Analysing the data protection requirements
- Implementing the specifications taking the technical configuration into account
- Continuous monitoring for future changes

RECHTLICHE RISIKEN BEIM EINSATZ VON MICROSOFT 365

Die gute Nachricht zuerst: Ausgehend von unserer rechtlichen Analyse, einem intensiven Austausch mit Microsoft und den Datenschutzaufsichtsbehörden ist ein datenschutzkonformer Einsatz von Microsoft 365 möglich. Der ungeprüfte oder undokumentierte Einsatz von Microsoft 365 ist jedoch ein Risiko für Unternehmen und kann Bußgelder und Schadensersatzklagen zur Folge haben.

STEP-BY-STEP ZUR DATENSCHUTZ-COMPLIANCE

Nach unserer Erfahrung aus zahlreichen Implementierungsprojekten zur Datenschutz-Compliance bei Microsoft 365 ist ein mehrstufiger Datenschutzprozess erforderlich. Dieser sollte dokumentiert werden und insbesondere folgende Schritte beinhalten:

- Ermittlung der Einsatzszenarien
- Analyse der datenschutzrechtlichen Vorgaben
- Umsetzung der Vorgaben unter Berücksichtigung der technischen Konfiguration
- Fortlaufendes Monitoring für zukünftige Änderungen

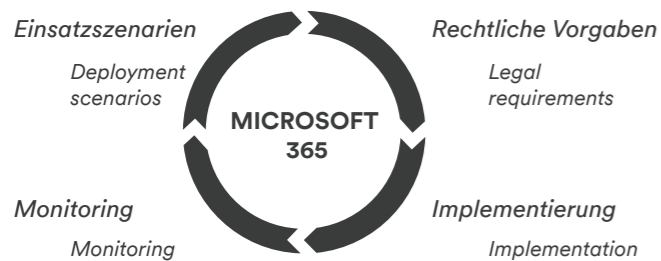


Abbildung / Figure:
Microsoft 365 © reuschlaw, 2023

UNSER ANGEBOT

Wir bieten Ihnen eine vollumfängliche und lückenlose datenschutzrechtliche Beratung bei der Einführung von Microsoft 365. Hierbei unterstützen wir Sie konkret insbesondere mit folgenden Maßnahmen:

- Datenschutzrechtliche Bewertung zum Einsatz von Microsoft 365 inklusive vollständiger Dokumentation und Datenschutzfolgenabschätzung
- Prüfung aller rechtlich relevanten Dokumente – von den Microsoft Verträgen bis zur Datenschutzinformation für Beschäftigte und Kunden
- Einbeziehung aller relevanten Stakeholder in den Prüfprozess – vom Datenschutzbeauftragten, über den Betriebsrat zur IT
- Empfehlungen oder Best-Practice Ansätze für die technische Umsetzung und den Betrieb

What we offer

We offer you comprehensive and complete data protection advice on how to introduce Microsoft 365. In this context, we will support you with the following measures:

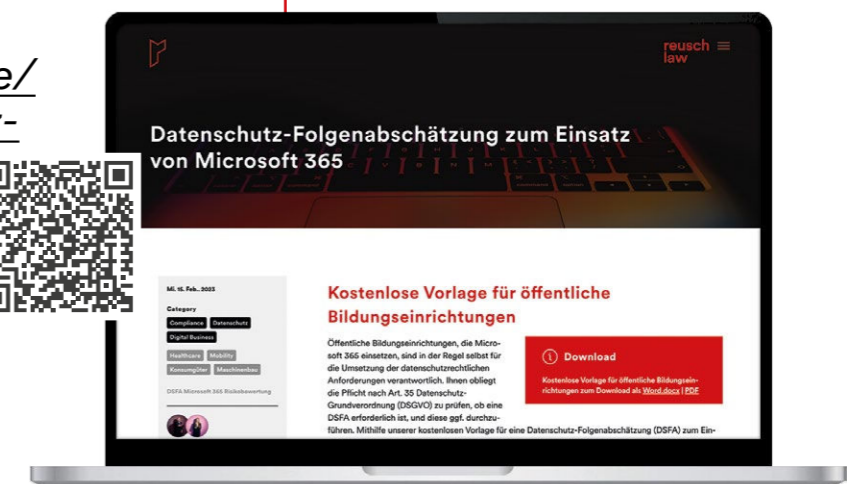
- *Data protection assessment of the use of Microsoft 365 including complete documentation and data protection impact assessment*
- *Review of all legally relevant documents – from Microsoft contracts to data protection information for employees and customers*
- *Involvement of all relevant stake-holders in the audit process – from the data protection officer, to the works council, to IT*
- *Recommendations or best-practice approaches for technical implementation and operation*

More information:

[www.reuschlaw.de/en/news/
data-protection-impact-assessment-for-the-use-of-microsoft-365](http://www.reuschlaw.de/en/news/data-protection-impact-assessment-for-the-use-of-microsoft-365)



Mehr Infos:
[www.reuschlaw.de/
news/datenschutz-
folgenab-
schaetzung-
zum-einsatz-
von-microsoft-
365](http://www.reuschlaw.de/news/datenschutz-folgenabschaetzung-zum-einsatz-von-microsoft-365)



ACCESSIBILITY BY DESIGN: BARRIEREFREIHEIT VON PRODUKTEN

*Accessibility by design:
Accessibility of products*

Es gibt viele gute Gründe auf barrierefreie Produkte und Dienstleistungen zu setzen. Informieren Sie sich jetzt über die neuen gesetzlichen Anforderungen und Wege zur effizienten Umsetzung.

Das Recht auf Barrierefreiheit ist in der UN-Behindertenrechtskonvention und im Grundgesetz verankert. Bisher wurden in erster Linie Behörden und andere öffentliche Stellen zur Sicherstellung der Barrierefreiheit verpflichtet. Mit dem Barrierefreiheitsstärkungsgesetz (BFSG) setzt der Gesetzgeber den European Accessibility Act um und macht Barrierefreiheit ab dem 28. Juni 2025 auch für Unternehmen zur Pflicht.

CHANCEN UND VORTEILE

Unabhängig von der gesetzlichen Verpflichtung bietet Barrierefreiheit zahlreiche Chancen für Unternehmen: Produkte werden nicht nur für neue Kundengruppen zugänglich, Unternehmen schaffen auch Vertrauen in ihr Produkt, reagieren auf die demografische Entwicklung und gewährleisten die Qualität, Sicherheit und Benutzerfreundlichkeit ihres Angebots. Wer sich bereits jetzt mit den Anforderungen des BFSG beschäftigt, verschafft sich frühzeitig einen Vorteil.

WER IST BETROFFEN?

Das BFSG betrifft mit wenigen Ausnahmen Hersteller, Händler und Importeure bestimmter Produkte sowie Erbringer von Dienstleistungen. Der Anwendungsbereich erstreckt sich über eine breite Palette von Produkten bis hin zu Dienstleistungen im Bankwesen oder im elektronischen Geschäftsverkehr. Im Produktbereich sind Selbstbedienungsterminals wie Check-in-Automaten und Verbraucherendgeräte mit interaktivem Leistungsumfang, die für Telekommunikationsdienste oder für den Zugang zu audiovisuellen Mediendiensten genutzt werden, umfasst. Beispiele sind Smartphones, Tablets und eBook-Reader.

There are many good reasons to focus on accessible products and services. Find out now about the new legal requirements and ways to implement them efficiently.

The right to accessibility is laid down in the UN Convention on the Rights of Persons with Disabilities and in the German Constitution. Until now it was primarily public authorities and other public bodies that were obliged to ensure accessibility. With the German Accessibility Reinforcement Act (Barrierefreiheitsstärkungsgesetz – BFSG), the German legislator is implementing the European Accessibility Act and makes accessibility mandatory also for companies from 28 June 2025.

Opportunities and benefits

Regardless of the legal requirements, accessibility brings numerous opportunities for companies: not only are products becoming accessible to new customer groups, companies are also building trust in their product, responding to demographic trends and ensuring the quality, security and user-friendliness of their offering. Companies that are now already addressing the requirements of the BFSG will gain an early advantage.

Who is affected?

The BFSG addresses, with only a few exceptions, manufacturers, distributors and importers of certain products as well as service providers. Its scope of application covers a wide range of products through to banking and e-commerce services. Among the products concerned are self-service terminals such as check-in machines and consumer terminals with interactive features that are used for telecommunications services or access to audiovisual media services. This includes, for example, smartphones, tablets and eBook readers.

ACCESSIBILITY BY DESIGN

Barrierefreiheit beinhaltet die vollumfängliche Einbeziehung von Menschen mit Behinderung. Produkte sind so zu gestalten, dass sie von allen Menschen gleichermaßen genutzt werden können. In Unternehmen sollten die vorgesehenen Übergangsfristen genutzt werden, um Barrierefreiheit im Produktdesign von Beginn an zu berücksichtigen. Hierbei müssen Unternehmen auch bedenken, dass die Nichterfüllung der gesetzlichen Vorgaben nach 2025 zu Markteinschränkungen und Bußgeldern führen kann.

UNSER ANGEBOT

Wir helfen Ihnen dabei, Ihre Produkte vollumfänglich an die neuen gesetzlichen Vorgaben anzupassen. Unsere Leistungen umfassen:

- Prüfung der Anwendbarkeit der Vorgaben des BFSG
- Best Practices für Accessibility by Design unter Einbeziehung der technischen Vorgaben und internationalen Standards
- Unterstützung bei der praktischen Umsetzung und Validierung der Ergebnisse

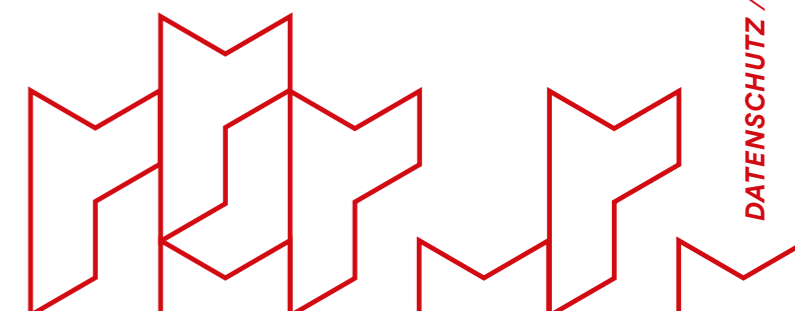
Accessibility by design

Accessibility means the full inclusion of people with disabilities. Products must be designed in such a way that they can be used equally by all people. Companies should utilise the transitional periods provided to take accessibility into account in product design right from the start. Companies must also bear in mind that failure to fulfil the legal requirements after 2025 can lead to market restrictions and fines.

What we offer

We help you to fully adapt your products to the new requirements. Our services include:

- *Checking whether the requirements of the BFSG are applicable*
- *Best practices for ensuring accessibility by design in consideration of technical specifications and international standards*
- *Support and assistance in the practical implementation and validation of the results*



**GET IN
TOUCH
WITH
US!**



www.reuschlaw.de