Whitepaper Datenschutz und Compliance

Stand: 02.06.2021

Mitwirkende:
Rudolf Schreiner, ObjectSecurity OSA GmbH
Uwe Stanislawski, CASKAN Networks
Lukas Wagner, HK2 Comtection GmbH

1. Einleitung

Nicht zuletzt aufgrund der Medienberichterstattung über spektakuläre IT-Sicherheitsvorfälle, wie der Trojaner-Befall beim Kammergericht Berlin oder die Datenschutz-Bußgelder in Rekordhöhe, die gegen den in Berlin ansässigen Immobilienkonzern Deutsche Wohnen verhängt wurden, sind die Themen IT-Sicherheit und Datenschutz im breiteren Bewusstsein der Öffentlichkeit der Hauptstadtregion angekommen. Dass man „da was tun muss“, weiß mittlerweile fast jeder; die beiden genannten Fälle zeigen aber wiederum, dass es meistens an der richtigen Umsetzung hapert. Diese stellt nach wie vor besonders für KMU eine besondere Herausforderung dar. Hier zumindest bei der IT-Sicherheit Abhilfe in Berlin und Brandenburg zu schaffen, ist ohnehin eines der gesetzten Ziele des it’s.BB e. V. IT-Sicherheit und Datenschutz liegen – nicht zuletzt aufgrund der technischen und organisatorischen Maßnahmen für ein angemessenes Schutzniveau – näher beieinander, als vielleicht gemeinhin vermutet wird, und bilden ineinandergreifende Bausteine für eine höhere IT-Compliance. Dieses Whitepaper stellt deshalb dar, wie das Netzwerk neben seinen bestehenden Angeboten für mehr IT-Sicherheit auch bei Datenschutz und Compliance unterstützen kann.

2. Ziele

Ziele des Engagements des it’s.BB e. V. in den Bereichen Datenschutz und Compliance sind die Stärkung des Bewusstseins für diese Themen in der Wirtschaft der Hauptstadtregion und der Abbau von Vorbehalten und Hemmnissen. Dazu sollen konkrete und niedrigschwellige Angebote erarbeitet werden, die KMU und vor allem auch innovative Startups aus der Hauptstadtregion bei Datenschutz und Compliance unterstützen. Perspektivisch sollen die Themen Datenschutz und Compliance im It’s.BB e. V. in einer eigenen Arbeitsgruppe etabliert werden.

3. Allgemeine Datenschutz-Anforderungen

Die Einhaltung des Datenschutzes ist eine gesetzliche Pflicht, die aus der europäischen Datenschutz-Grundverordnung ergibt. Die Verantwortlichen für die Verarbeitung personenbezogener Daten müssen die Datenverarbeitung so organisieren und durchführen, dass sie den Grundsätzen gem. Art. 5 DSGVO entsprechen. Diese sind im Einzelnen:

- Rechtmäßigkeit, Verarbeitung nach Treu und Glauben, Transparenz
- Zweckbindung

- Datenminimierung
- Richtigkeit
- Speicherbegrenzung
- Integrität und Vertraulichkeit
- Rechenschaft

Darüber hinaus sieht die DSGVO eine Reihe an Dokumentationspflichten vor, die insbesondere der Erfüllung der Rechenschaftspflicht dienen. Die datenschutzrelevanten Dokumentationen umfassen z. B ein detailliertes Verzeichnis von Verarbeitungstätigkeiten inkl. Löschfristen gem. Art. 30 DSGVO, eine Dokumentation technischer und organisatorischer Maßnahmen gem. Art. 32 DSGVO (s. u.), die Regelung des Datenzugriffes anhand eines Berechtigungskonzeptes, auf Grundlage des need-to-know-Prinzips, und die Teilnahme an Mitarbeiterschulungen.

Eine Reihe von Rechten und Pflichten definieren zudem das Verhältnis zwischen Verantwortlichen und Betroffenen. Bei Erhebung der Daten ist der Verantwortliche gem. Art. 13 und 14 DSGVO verpflichtet, den Betroffenen umfangreich u. a. über die Rechtsgrundlage, die Zwecke der Verarbeitung, Kategorien der zu verarbeitenden Daten, mögliche Empfänger in einem Drittland, die Dauer der Verarbeitung, und Rechte des Betroffenen zu informieren.

Mit der DSGVO genießen Betroffene – Kunden, Partner, Patienten, Beschäftigte etc. – weitreichende Rechte, die sie gegenüber den Verantwortlichen geltend machen können. Die Verantwortlichen müssen sich auf die Geltendmachung dieser Rechte technisch und organisatorisch einstellen, um diese adäquat erfüllen zu können. Hier müssen die entsprechenden Prozesse etabliert werden, möglichst bevor die ersten Ersuchen eingehen, denn nicht selten haben nicht rechtzeitig und/oder unvollständig bearbeitete Ersuchen zu einer Beschwerde bei der zuständigen Aufsichtsbehörde geführt und bergen deshalb ein erhebliches Bußgeldrisiko. Die Betroffenenrechte sind im Einzelnen:

- Auskunftsrecht gem. Art. 15 DSGVO
- Recht auf Berichtigung gem. Art. 16 DSGVO
- Recht auf Löschung ("Recht auf Vergessenwerden") gem. Art. 17 DSGVO
- Recht auf Einschränkung der Verarbeitung gem. Art. 18 DSGVO
- Recht auf Datenübertragbarkeit gem. Art. 20 DSGVO
- Widerspruchsrecht gem. Art. 21 DSGVO gegen die Verarbeitung auf Grundlage von Art. 6 Abs. 1 lit. e) oder f)

Berührungspunkte mit der Aufsichtsbehörde ergeben sich allerdings nicht nur im Falle einer Beschwerde seitens Betroffener, sondern auch formell aus verschiedenen Anforderungen der DSGVO: Gemäß Art. 37 Abs. 7 teilt der Verantwortliche der Aufsichtsbehörde die Kontaktdaten des Datenschutzbeauftragten mit. Dessen Aufgaben umfassen u. a. die Zusammenarbeit mit der Aufsichtsbehörde gem. Art. 39 Abs. 1 lit. d) und die Tätigkeit als Anlaufstelle für die Aufsichtsbehörde zu bestimmten Themen und Fragen gem. lit. e). Der Verantwortliche muss zudem gem. Art. 36 DSGVO die Aufsichtsbehörde ggf. im Zusammenhang mit Datenschutz-Folgeabschätzungen zu geplanten Verarbeitungsvorgängen, die ein hohes Risiko zur Folge hätten, konsultieren. Im Falle einer Datenpanne, die

it's.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net

häufig eine IT- und informationssicherheitsrelevante Dimension vorweisen, muss der Verantwortliche den Vorfall gem. Art. 33 DGSVO der Aufsichtsbehörde melden, wenn er voraussichtlich zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Die Nichteinhaltung der Anforderungen der DSGVO kann gem. Art. 83 DSGVO durch die zuständige Aufsichtsbehörde mit Bußgeldern von bis zu 20 Millionen Euro von bis zu 4 % des gesamten weltweit erzielten Jahresumsatzes geahndet werden. In der Hauptstadtregion wurden durch die Berliner Beauftragten für Datenschutz und Informationsfreiheit, nach bisherigen Informationen, mehrere Bußgelder zwischen 50.000 EUR und 14,5 Millionen Euro verhängt; aus Brandenburg sind noch keine Bußgelder auf Grundlage der DSGVO bekannt geworden.

4. Technischer Datenschutz, Datensicherheit

4.1. Technische und organisatorische Maßnahmen

Die bisher bekannt gewordenen bußgeldgeahndeten Fälle aus Berlin und anderen Regionen Deutschlands legen nahe, dass häufig die mangelnde Umsetzung technischer und organisatorischer Maßnahmen zum datenschutzwidrigen Umgang mit personenbezogenen Daten führte. Die Pflicht zur Ergreifung von technischen und organisatorischen Maßnahmen zur Gewährleistung eines dem Risiko angemessenes Schutzniveaus ergibt sich aus Art. 32 DSGVO. Die DSGVO führt hier auch mit der Pseudonymisierung, Verschlüsselung und Datensicherung einige Maßnahmen exemplarisch an, wodurch Artikel 32 DSGVO die wesentliche thematische Schnittstelle zur IT-Sicherheit bildet.

Noch deutlicher wird dieser Themenbezug im Standard-Datenschutzmodell 2.0 (SDM) der Datenschutz-Konferenz, dem Zusammenschluss aller deutschen Datenschutz-Aufsichtsbehörden, das als Praxisempfehlung der Aufsichtsbehörden angesehen werden kann. Teil D des SDM führt jeweils konkrete Maßnahmen zur Gewährleistung der Schutzziele Verfügbarkeit, Integrität, Vertraulichkeit, Nichtverkettung, Transparenz, Intervenierbarkeit und Datenminimierung an. Das SDM erklärt zu diesen Zielen:

> *In diesen Gewährleistungszielen finden sich die seit vielen Jahren in der Praxis bewährten Schutzziele der Informationssicherheit wieder. Die Ziele Verfügbarkeit, Integrität und Vertraulichkeit dienten bisher vorrangig der Gewährleistung der Informationssicherheit in Behörden und Unternehmen, also der Absicherung und dem Schutz der Daten einer Organisation*[1]*.*

4.2. Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen

Neben den technischen und organisatorischen Maßnahmen gem. Art. 32, mit denen der Verantwortliche die Verarbeitung personenbezogener Daten innerhalb seiner Organisation absichern sieht die

[1] *Das Standard-Datenschutzmodell. Eine Methode zur Datenschutzberatung und -prüfung auf der Basis einheitlicher Gewährleistungsziele.* Version 2.0 von der 98. Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder vom 5. bis 7. November 2019 in Trier beschlossen, S. 10, abgerufen am 10.12.2019 unter https://www.datenschutzkonferenz-online.de/media/ah/20191106_SDM-Methode_V2.0.pdf

it's.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net

DSGVO in Artikel 25 weitere technische Anforderungen für an eine datenschutzkonforme Verarbeitung vor. Diese betreffen neben der datenschutzkonformen Einrichtung von Organisationsprozessen auch die datenschutzfreundliche Ausgestaltung der eigenen Produkte, die von den Betroffenen erworben oder genutzt werden sollen. Dies soll bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung erfolgen. Erreicht werden soll dies durch Datenschutz durch Technikgestaltung gem. Art. 25 Abs. 1 DSGVO und Datenschutz durch datenschutzfreundliche Voreinstellungen gem. Art. 25 Abs. 2 DSGVO.

Mit dem Prinzip *Datenschutz durch Technikgestaltung* – auch bekannt unter dem Begriff *Privacy by Design* – bezweckt die DSGVO, dass bei der Entwicklung eines Produktes oder einer Dienstleistung die Einhaltung der Datenschutzgrundsätze gem. Art. 5 DSGVO von Anfang an mitgedacht und berücksichtigt wird. Das bedeutet, dass die Produktentwicklung in einer möglichst frühen Phase auch Datenschutz-Kompetenzen z. B. in Form des Datenschutzbeauftragten einbeziehen sollte. Eine Herausforderung ist hierbei, dass Entwickler und Datenschützer eine gemeinsame Sprache finden müssen, um Datenschutzanforderungen in entsprechende Produktspezifikationen übersetzen zu können. So kann z. B. ein datenschutzfreundliches Produktmerkmal eines Messenger-Dienstes die Ende-zu-Ende-Verschlüsselung der Nachrichten sein.

Das sprachlich etwas sperrigere Prinzip *Datenschutz durch datenschutzfreundliche Voreinstellungen* (*Privacy by Default*) sieht vor, dass durch die „werkseitigen“ Voreinstellungen eines Produktes oder einer Dienstleistung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Auch dieses Prinzip sollte idealerweise bereits bei der Entwicklung berücksichtigt werden, um bei der Einführung implementiert zu sein. Hier dürften sich ähnliche Herausforderungen bei der Übertragung von Datenschutzanforderung in Spezifikationen ergeben. Ein Beispiel für datenschutzfreundliche Voreinstellungen kann ein soziales Netzwerk sein, in dem Nutzerbeiträge zunächst nur für einen begrenzten Personenkreis (das eigene Netzwerk, „Freunde“) sichtbar sind und erst nach aktiver Änderung der Einstellungen durch den Nutzer öffentlich sichtbar werden.

5. Datenschutz bei der Verarbeitung von Applikationsdaten

In vielen Fällen ist eine datenschutzrechtliche Bewertung von Daten und Prozessen relativ einfach, beispielsweise bei einem einfachen Webshop. Kundendaten, Bestellungen, Zahlungsinformationen usw. werden in auch für den Laien nachvollziehbaren Prozessen verarbeitet. In anderen Fällen, beispielsweise in den Bereichen Cloud-Anwendungen, Internet of Things (IoT) und Telematic/Smart Cities, und vor allem bei Systemen, die auf Artificial Intelligence und Machine Learning basieren, kann vor allem die Umsetzung von Transparenz und der Schutz besonders sensitiver Daten sehr herausfordernd sein. Betrachten wir als einfaches Beispiel eine Cloud-basierte Temperatur- und Klimaregelung als Teil eines Smart Home. Dabei messen Sensoren mit hoher Genauigkeit Raumtemperatur und Luftfeuchtigkeit, und senden die Daten an einen Cloud-Server des Herstellers. Der Nutzer kann nun diese Daten über ein Smartphone abrufen, oder die Wunschtemperatur ändern. Auf den ersten Blick ist das alles in Bezug auf den Datenschutz recht harmlos. Bei genauer Betrachtung lassen sich aber allein aus diesen Daten, die in der Cloud gespeichert sind, sehr sensitive Informationen gewinnen, z.B. über das

it’s.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net

Sozialverhalten, sexuelles Verhalten oder die praktizierte Religion. Bei Kombination mit anderen Daten, die bei manchen Anbietern durchaus verfügbar sind, sind noch weit tiefere Einblicke in den persönlichen Lebensbereich möglich. Es sollte daher durch geeignete technische Maßnahmen sichergestellt werden, dass eine Auswertung der Daten durch den Anbieter nicht möglich ist.

Noch kritischer können Artificial Intelligence (AI) und Machine Learning (ML) basierte Anwendungen sein. Sie erfüllen meist nicht die datenschutzrechtliche Anforderung der Transparenz. Betrachten wir als einfaches Beispiel ein Kredit-Scoring-System. Bei einem klassischen regelbasierten System würde man z.B. definieren, dass ein Kredit nur dann erteilt wird, wenn die monatliche Rate verfügbar ist. Wird ein Kredit nach dieser Regel abgelehnt, kann man dies dem Antragssteller sehr einfach erklären, und somit der Anforderung der Transparenz nachkommen. Bei einem AI/ML basierten Scoring-System würde man nun nicht solche Regeln implementieren, sondern man würde das System mit Daten aus bestehenden Kreditverträgen und vor allem Daten über Kreditausfälle trainieren. Bei einem Kreditantrag entscheidet das System nach diesem Training, es kann aber im Normalfall nicht erklären, warum ein bestimmter Antrag abgelehnt wird, und erfüllt damit nicht die datenschutzrechtliche Anforderung der Transparenz. Beim Einsatz AI/ML basierter Systeme zur Unterstützung von Entscheidungen haben sich noch andere Probleme gezeigt. In den USA haben beispielsweise Systeme zur Abschätzung der Rückfallrate von Straftätern die Rasse in Betracht gezogen, sogar wenn die Rasse in den Trainingsdaten explizit nicht einbezogen war. Das System war so „intelligent“, dieses an sich nicht vorhandene Feature aus den vorhandenen Daten zu rekonstruieren, z.B. aus Wohnort und Namen. Es ist daher oft sehr schwer, solche Systeme so zu bauen, dass Diskriminierungen oder Vorurteilen nicht in die Entscheidungen miteinfließen.

Generell ist es, wie schon die einfachen Beispiele zeigen, eine Herausforderung rechtlich, vor allem datenschutzrechtlich, einwandfreie Anwendungen vor allem im Bereich IoT/AI/ML zu entwickeln. Die Implementierung von Datenschutz erfordert hier nicht nur den Willen zur korrekten Umsetzung der Richtlinien und rechtliche Kenntnisse, sondern vor allem auch Kenntnisse in Bereichen wie Analytics, AI und ML. Auch hier ist der schon genannte Grundsatz von Security and Privacy by Design anzuwenden.

6. IT-Compliance

Der Begriff „Compliance“ bei Unternehmen umfasst eine Reihe von Anforderungen an Maßnahmen und Verhaltensweisen, um mit Vorschriften und Richtlinien übereinzustimmen, die für ein Unternehmen gelten, weil es gesetzlich dazu angehalten ist oder weil die Unternehmensführung, Geschäftspartner, Kunden oder Lieferanten es verlangen.

Die IT-Compliance beschäftigt sich mit der anforderungskonformen Ausgestaltung der Datenverarbeitung im Unternehmen, also mit der Gestaltung der IT-Infrastruktur und mit Prozessen, die Daten elektronisch verarbeiten.

IT-Compliance

- stärkt die IT-Sicherheit im Unternehmen,

it’s.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net

- entdeckt und minimiert Risiken,
- verbessert die Transparenz,
- vereinfacht den Umgang mit schwierigen Situationen und Notfällen,
- steigert den Wert des Unternehmens und die Bonität

Für die Einführung und die Pflege der IT-Compliance in Unternehmen gibt es Compliance Management Systeme, Best Practices und Rahmenwerke. Der Umfang dieser Systeme überfordert in der Regel die Ressourcen, die kleine und mittlere Unternehmen zur Verfügung haben. Oft sind diese Umfänge für KMU auch gar nicht notwendig.

Deshalb möchte der it's.BB e.V. mit der Arbeitsgruppe „Datenschutz und Compliance" KMU eine Hilfestellung dabei bieten, IT-Compliance im benötigten Umfang zu erreichen und die Vorteile davon zu genießen.

7. Schritte zur Erreichung von IT-Compliance

Zur Erreichung von IT-Compliance kann ein Unternehmen die folgenden fünf Schritte durchführen und anschließend den Erfolg beurteilen. Die einzelnen Schritte sind dabei relativ simpel aufgebaut, benötigen aber ein gewisses Maß an Engagement, was die Umsetzung angeht.

1. IT-Sicherheitsstrategie definieren

Die Geschäftsführung eines Unternehmens definiert in der IT-Sicherheitsstrategie die grundlegenden Ziele der IT-Sicherheitspolitik ihres Unternehmens und gibt vor, was ihr die IT-Sicherheit wert ist. Daraus leiten sich alle weiteren Maßnahmen ab.

2. Ermitteln relevanter Anforderungen und Vorschriften

Es werden alle Anforderungen und Vorschriften ermittelt, die für das Unternehmen zutreffen und denen es genügen muss. Dazu gehören:

- gesetzliche Anforderungen (allgemeingültige, branchenspezifische und produktspezifische Vorschriften)
- Anforderungen der Kunden, Geschäftspartner, Lieferanten

3. Risiken ermitteln und bewerten

Die Risiken, denen das Unternehmen im Hinblick auf seine Datenverarbeitung ausgesetzt ist, werden ermittelt und bewertet.

Die Schritte dazu:

- Dokumentieren der Sachwerte und der immateriellen Werte
- Dokumentieren von Datenarten und Speicherorten (siehe Datenschutz)
- Ermitteln möglicher Störungen und Auswirkungen auf den Geschäftsbetrieb, die Daten und die Werte
- Ermitteln möglicher Kosten dieser Störungen

it's.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net

4. Gegenmaßnahmen ermitteln und bewerten

Die ermittelten und bewerteten Risiken werden mit Gegenmaßnahmen versehen. Die Gegenmaßnahmen werden bewertet (Kosten und Wirksamkeit) und es werden die Gegenmaßnahmen ausgewählt, die weniger Kosten verursachen als die Risiken wert sind, denen sie begegnen.

5. Gegenmaßnahmen anwenden, IT-Sicherheitskonzept erstellen

Die Gegenmaßnahmen werden dokumentiert und das IT-Sicherheitskonzept erstellt. Im IT-Sicherheitskonzept sollten bei kleinen und mittleren Firmen mindestens die folgenden Punkte enthalten sein:

- kurzer allgemeiner Überblick über die IT-Infrastruktur
- Technische und organisatorische Maßnahmen für Vertraulichkeit, Integrität und Verfügbarkeit der Daten
- Anweisungen für die regelmäßige Evaluation der Maßnahmen
- IT-Notfallplan
- Datensicherungskonzept
- andere Komponenten, je nach zutreffenden Anforderungen

Die IT-Sicherheitsstrategie wird an neue Gegebenheiten stets von der Geschäftsführung angepasst. Das IT-Sicherheitskonzept wird in regelmäßigen Abständen (mindestens 1x jährlich) überprüft, auf Aktualität und Anwendbarkeit überprüft und ggf. aktualisiert.

Es sollte ein System sein, das dem Unternehmen nutzt, seine Robustheit stärkt, seinen Marktwert erhöht und die gesamte Nutzererfahrung verbessert. So ist IT-Compliance ein echter Mehrwert für Unternehmen.

8. Kompetenzen im it’s.BB e. V.

Die Mitglieder des it’s.BB e. V. verfügen über zahlreiche sich ergänzende Kompetenzen in den Bereichen Compliance und Datenschutz. Dies beginnt bei der Beratung zu datenschutzrechtlichen Themen und der Stellung eines externen Datenschutzbeauftragten bis hin zur Konzeptionierung und Umsetzung von Compliance- und Informationssicherheitsmanagementsystemen. Ein Überblick über die spezifischen Kompetenzen der Mitglieder bietet die it’s.BB-Kompetenzmatrix.

it’s.BB e.V. (das IT-Sicherheitsnetzwerk Berlin-Brandenburg)
c/o NKMG mbH | Poßweg 45 | 14163 Berlin | www.itsbb.net | info@itsbb.net