European SharePoint Office 365 & Azure Community

EBOOK

DSGVO / GDPR Field Guide für Office 365 & Azure

Written by Nicki Borell

DSGVO / GDPR Field Guide for Office 365 & Azure

Ab dem 25.05.2018 gilt die EU-Datenschutzgrundverordnung (DSGVO oder auch GDPR abgekürzt) und wird damit geltendes Recht für alle Unternehmen, egal wie groß sie sind.

Dem IT Verantwortlichen wird das Thema schnell zu theoretisch und vor allem viel zu juristisch. Der Datenschutzbeauftragte und der Compliance Officer sind meist etwas überfordert, wenn es um die DSGVO geht. Die Geschäftsleitung und der Betriebsrat machen Druck und wollen wissen, ob man bei dem Thema gut aufgestellt sei.

In aller Regel ist das die Situation, die sich zum Thema DSGVO in Unternehmen findet.

Erfahren Sie in diesem Whitepaper, wie Sie mit dem Thema hier und heute schon souverän umgehen und zum Stichtag 25. Mai 2018 bestens gerüstet sind.

Inhalte

In aller Regel wird das Thema DSGVO entweder aus juristischer Sicht oder aus der technischen Perspektive angegangen. In beiden Fällen ist leider schnell ein Punkt erreicht, an dem es kein substantielles Weiterkommen mehr gibt. Dem Juristen stellen sich bald konkrete technische Fragen, die er nicht (alleine) beantworten kann. Wird das Thema aus der IT getrieben, stößt man alsbald auf juristische oder organisatorische Fragestellungen.

Dieses Whitepaper beantwortet die wichtigsten Fragestellungen rund um das Thema DSGVO im Kontext von Office 365 & Azure aus Sicht der IT - allerding mit dem Fokus auf die juristischen Ausprägungen.

Sie erhalten eine Übersicht und klare Empfehlungen, welche Services und Dienste des Microsoft Stacks für Sie sinnvoll eingesetzt werden, Ihnen fachliche und organisatorische Vorteile bringen können und wie eine Strategie im unternehmerischen Sinne für Sie aussehen kann. Microsoft stellt Kunden und Partnern Tools, Konzepte und Unterstützung zur Verfügung, um ihr Business fit für die DSGVO zu machen. Erfahren Sie hier welche das sind und wie sie effektiv eingesetzt werden können.

Inhalt

Die rechtlichen Aspekte

Die DSGVO definiert viele neue Regeln und Vorgaben. Nicht alle davon sind im Kontext von Office 365 & Azure relevant. Gleiches gilt für das Datenschutz-Anpassungs-und-Umsetzungsgesetz, das unter anderem das neue Bundesdatenschutzgesetz im Hinblick auf die kommende DSGVO beinhaltet.

Grundsätzlich

- Die Gesetze definieren Vorgaben bezüglich des Umgangs mit personenbezogenen Daten.
- Sensitive Daten, Daten zur ordnungsgemäßen Buchführung oder ähnliches sind davon nicht betroffen, es sei denn sie beinhalten ebenfalls personenbezogene Informationen. (Maßnahmen die ergriffen werden, um personenbezogene Daten zu schützen, können allerdings oft analog auch zum Schutz sensibler Unternehmensdaten genutzt werden.)
- Es gilt die Rechenschaftspflicht des Verantwortlichen.
- Es gibt keine Mindestgröße ab der die DSGVO für ein Unternehmen gilt. Die DSGVO trifft jedes Unternehmen. Es gibt allerdings Erleichterungen für Unternehmen mit weniger als 250 Mitarbeitern hinsichtlich des Führens von Verarbeitungsverzeichnissen. Vgl. Artikel 30 Absatz 5 DSGVO

Die Vorgaben im Kontext von Office 365 & Azure

Der folgende Abschnitt beschreibt die wesentlichen und direkten Auswirkungen der DSGVO in Bezug auf die Microsoft Online Dienste Office 365 & Azure. Welche ggf. nur mittelbaren Berührungspunkte darüber hinaus im Detail bestehen, sowie eine generelle Bewertung, welche der folgenden Aspekte im konkreten Einzelfall zutreffen, muss juristisch belastbar geprüft werden. Die folgenden Abschnitte stellen eine Orientierungshilfe dar.

Mit Inkrafttreten der DSGVO werden bisher bestehende nationale Regelungen, wie z.B. das Bundesdatenschutzgesetz, komplett abgelöst und ein neues BDSG erlassen. Die DSGVO benennt allerdings explizit einzelne Bereiche, wie z.B. der Beschäftigtendatenschutz, wo nach wie vor nationale Regelungen eigenständig getroffen werden können.

Die DSGVO betrifft alle Unternehmen mit einer Niederlassung in der EU, unabhängig von ihrer Größe, die zum Beispiel folgende Kriterien erfüllen:

- Austausch von Daten mit anderen Unternehmen
- Daten bei einem Cloud Anbieter speichern
- Ihre Datenverarbeitung an einen Dienstleister teilweise oder ganz ausgelagert haben

Daneben betrifft die DSGVO auch Unternehmen, die außerhalb der EU niedergelassen sind, wenn sie Waren und Dienstleistungen in der EU anbieten oder das Verhalten von Personen innerhalb der EU beobachten.

Dies gilt allerdings nur, wenn es sich bei den Daten um personenbezogene Daten natürlicher Personen handelt (Artikel 4 Nummer 1 DSGVO). Da als personenbezogenes Datum z.B. der Name, die Adresse oder auch die E-Mail-Adresse einer Person gilt, ist dies fast immer der Fall. Darüber hinaus gelten z.B. auch schon Informationen über Hobbies, Login-Daten, IP Adressen oder Standortdaten als personenbezogene Daten. Eine IT gestützte Datenverarbeitung im unternehmerischen Umfeld ist daher de facto immer auch mit personenbezogenen Daten verbunden.

Mittels der Klassifikations-Funktion, welche die aktuellste Version des Microsoft Azure Information Protection Clients mit sich bringt, können Unternehmen ihre Daten dahingehend prüfen. Basierend auf vorkonfigurierten Regeln prüft der Scanner ob Daten, die z.B. auf einem Fileserver oder in

SharePoint abgelegt sind, personenbezogene Inhalte haben. Der Report, den der Scanner erzeugt, zeigt im Detail auf, welche Daten / Dateien betroffen sind.

Rechtsgrundlage für die Verarbeitung von Daten nach DSGVO

Um Daten mit personenbezogenem Inhalt verarbeiten zu dürfen, muss ganz allgemein eine gesetzliche Legitimation vorliegen. Das war auch schon im Bundesdatenschutzgesetz so geregelt. Eine Legitimation kann immer dann vorliegen, wenn das berechtigte Interesse des Unternehmens die Daten zu verarbeiten, die schutzwürdigen Interessen des Betroffenen überwiegt.

Ob diese Voraussetzungen erfüllt sind, welche Vorgaben genau gelten (kleiner Konzern-Privileg) etc. oder ob ggf. weitere Erlaubnistatbestände wie z.B. die Einwilligung greifen, muss juristisch belastbar geklärt werden.

Da Daten, auch mit personenbezogenem Inhalt, Bestandteil von jedem Geschäftsprozess sind, sollte stets eine Legitimation zur Datenverarbeitung hergeleitet werden.

Auftragsdatenverarbeitung durch Microsoft

Bisher regelte § 11 Bundesdatenschutzgesetz die sogenannte Auftragsdatenverarbeitung, also das Verarbeiten von personenbezogenen Daten durch Dritte. Zukünftig wird dieser Sachverhalt generell in Kapitel 4 bzw. Artikel 28 der DSGVO beschrieben.

Artikel 4 Nummer 8 der DSGVO legt zudem fest, dass derjenige als Auftragsverarbeiter gilt, der Daten im Auftrag eines Anderen verarbeitet. Microsoft ist mit seinen Services Office 365 & Azure also ganz klar ein Auftragsverarbeiter im Sinne des Artikel 4 Nummer 8 DSGVO.

Insofern gelten folgende Vorgaben:

Pflichten des Auftraggebers (des Unternehmen)

Artikel 28 Absatz 1 der DSGVO verpflichtet den Auftraggeber zu einer sorgfältigen Auswahl des Auftragsverarbeiters. Darunter fällt z.B. die Prüfung, ob der Auftragsverarbeiter geeignete technische und organisatorische Maßnahmen implementiert hat, um einen ordnungsgemäßen, sicheren und reibungslosen Betrieb zu garantieren.

Die diesbezüglich in Artikel 5 Absatz 2 DSGVO geforderte Rechenschaftspflicht kann im Falle der Microsoft Online Dienste zumindest dem Grunde nach durch die Zertifizierungen der Plattformen erfüllt werden. Details dazu siehe: Trust Center, Compliance Berichte (Anmeldung an Office 365 erforderlich) und Trust Center - Microsoft Azure.

Pflichten des Auftragsverarbeiters (Microsoft)

Artikel 30 Absatz 2 DSGVO verlangt auch vom Auftragsverarbeiter ein sogenanntes Verzeichnis von Verarbeitungstätigkeiten, ehemals Verfahrensverzeichnis genannt.

Microsoft listet sowohl für Office 365 als auch für Azure im Detail die angebotenen Services auf. Details dazu siehe:

- **Office 365 Service Descriptions**
- **Microsoft Azure & Microsoft Azure Legal Information**
- **Licensing Terms and Documentation**

Informationen dazu, wie interne Verfahren ablaufen, wie der Support Prozess aussieht, welche Subunternehmen ggf. beteiligt sind und welche Rechte und Pflichten beide Seiten haben, wird in den Licensing Terms and Documentation beschrieben. Damit erfüllen die Microsoft Cloud Dienste Office 365 & Azure auch folgende Anforderungen:

- **Nachweis der Einhaltung hinreichender Garantien zur Durchführung von geeigneten technischen und organisatorischen Maßnahmen - Artikel 28 Absatz 1, 4, 5 & Artikel 40, 42 DSGVO**
- **Regelungen zu Unterstützungsleistungen - Artikel 28**
- **Absatz 3:**
    - **Umsetzung der technischen und organisatorischen Maßnahmen - Artikel 32 DSGVO**
    - **Meldung von Datenpannen an die Aufsichtsbehörden und die betroffenen Personen - Artikel 33, 34 DSGVO**
    - **Durchführung von Datenschutzfolgeabschätzungen - Artikel 35 DSGVO**
- **Einsatz von Subunternehmern und wenn ja, welche - Artikel 28 Absatz 2,3,4**
- **Verschwiegenheit - Artikel 28 Absatz 3**
- **Rückgabe oder Vernichtung der Daten - Artikel 28 Absatz 3**

Artikel 32 Absatz 1 DSGVO verpflichtet den Auftragsverarbeiter dazu, eigenverantwortlich technische und organisatorische Maßnahmen zu implementieren, welche die Datensicherheit gewährleisten.

Auch hier stellen die oben bereits erwähnten Quellen Trust Center, Compliance Berichte (Anmeldung an Office 365 erforderlich) und Trust Center - Microsoft Azure eine gute Übersicht dar, welche Maßnahmen Microsoft hier implementiert hat.

Die Zurverfügungstellung aller Informationen zur Durchführung von Kontrollen durch den Auftraggeber, wie in Artikel 28 Absatz 3 der DSGVO beschrieben, wird ebenfalls durch die oben erwähnten Webseiten bedient.

Die hier aufgeführten Punkte werden in Anhang 1 Licensing Terms and Documentation seit September 2017 pflichtgemäß aufgeführt und sind somit Teil der Lizensierung.

Sperrung & Löschung von Daten

Sperrung

Der Artikel 18 DSGVO regelt das Recht auf Einschränkung der Verarbeitung. Diese Regelung ist nicht deckungsgleich mit dem bekannten Recht auf Sperrung, sondern in diesem Fall ein subjektives Recht des Betroffenen auf die Sperrung der Daten.

Voraussetzungen für die Einschränkung der Verarbeitung:

- Bestreiten der Richtigkeit
- Einschränkungsverlangen
- Geltendmachung, Ausübung oder Verteidigung von Rechtsansprüchen
- Widerspruch

Ob eine Voraussetzung gegeben ist, muss selbstverständlich juristisch geprüft werden. Für den Fall, dass dem so ist, stehen in Office 365 & Azure Funktionen zur Verfügung, um die dann notwendige Kennzeichnungspflicht umzusetzen. Üblicherweise stehen die betroffenen Daten dann nur noch eingeschränkt zur Verfügung.

Die im Erwägungsgrund 67 DSGVO aufgeführten Aspekte lassen sich wie folgt mit Office 365 & Azure umsetzen:

- **Mit einem Sperrvermerk, der einen Zugriff auf die Daten für bestimmte Zwecke unmöglich macht:**
    - → **Labels in Azure Information Protection**
    - → **Retention Policies in Office 365**
- **Über eine separate Speicherung der Daten:**

→ Export von Inhalten im Office 365 Security & Compliance Center
→ Optionen für den Download von Date aus Office 365 heraus

Löschung

Unter Löschung versteht man die generelle Unkenntlichmachung oder Vernichtung von Daten. Die DSGVO unterscheidet dabei das normale Recht auf Löschung nach Artikel 17 Absatz 1 DSGVO und dem Recht auf Vergessenwerden nach Artikel 17 Absatz 2 DSGVO.

Artikel 17 DSGVO definiert folgende Fälle:

- Zweckfortfall
- Widerruf der Einwilligung
- Widerspruch
- Unrechtmäßige Verarbeitung
- Erfüllung einer rechtlichen Verpflichtung
- Daten von Minderjährigen

Zum Thema Löschung sind in den oben bereits erwähnten Licensing Terms and Documentation detaillierte Regelungen beschrieben. Allgemein obliegt dem Kunden alleine die Verantwortung für das Löschen von Daten. Wird ein kompletter Office 365 Tenant gelöscht, greift folgende Regelung: Zitat: *„Nach Ablauf des Aufbewahrungszeitraums von 90 Tagen wird Microsoft das Konto des Kunden deaktivieren und die Kundendaten löschen.“*

Das Bundesdatenschutzgesetz regelt ergänzend, dass Daten dann nicht zu löschen sind, wenn Archivierungspflichten bestehen. Das BDSG-neu ergänzt den Artikel 17 Absatz 3 DSGVO. Dort heißt es, dass eine Löschung auch dann nicht erfolgen muss, wenn sie einen unverhältnismäßigen Aufwand bedeutet und nur ein geringes Interesse des Betroffenen an der Löschung vorliegt. Weitere Gründe können sein: Beeinträchtigung der schutzwürdigen Interessen Betroffener durch die Löschung sowie satzungsgemäße oder vertragliche Aufbewahrungsfristen. Trifft einer dieser Fälle zu, kann eine Sperrung der Daten ausreichen. Dies muss begründet werden und die Betroffenen sind zu informieren.

Artikel 13 Absatz 3 (Zweckänderung)

Der Artikel 13 Absatz 3 DSGVO sieht vor, dass bei Zweckänderung (Art. 6 Absatz 4 DSGVO) der Verarbeitung personenbezogener Daten die betroffene Person darüber zu informieren ist. Dies kann auch dann der Fall sein, wenn Daten von BigData Anwendungen, Auswertetools wie PowerBI oder Machine Learning Algorithmen wie dem Office Graph in Office 365 verarbeitet werden.

Ob dies im Einzelfall gegeben ist, muss individuell geprüft werden. Ggf. kann hier schon das Inkludieren der betreffenden Services (BigData Anwendungen, Auswertetools wie PowerBI oder Machine Learning Algorithmen wie dem Office Graph in Office 365) in das Verfahrensverzeichnis eine Lösung sein.

Auch schränkt § 32 BDSG-neu den Artikel 13 DSGVO dahingehend ein, dass eine Pflicht zur Information bei Zweckänderungen unter bestimmten Umständen (u.a. Zwecke sind vereinbar) entfallen kann.

Artikel 15 DSGVO (Auskunftsrecht)

Nach Artikel 15 DSGVO haben Personen das Recht auf Auskunft darüber, ob von ihnen personenbezogene Daten verarbeitet werden. Ist das der Fall, ergibt sich daraus das Recht auf Auskunft über Art, Umfang, Speicherung und Speicherdauer, Verarbeitungszwecke und welche personenbezogenen Daten genau von ihnen verarbeitet werden.

Es handelt sich hier also um ein zweistufiges Recht.

1. Auskunftsrecht, ob personenbezogene Daten verarbeitet werden.

Um zu analysierend, ob in einem bestimmten Bereich oder von einer bestimmten Person personenbezogene Daten in Office 365 verarbeitet werden, können folgende Services genutzt werden:

- **DLP Policies. Mithilfe einer Richtlinie zur Verhinderung von Datenverlust (Data Loss Prevention, DLP) im Office 365 Security & Compliance Center können Sie vertrauliche Informationen in Office 365 identifizieren, überwachen und automatisch schützen.**
- **Mittels der Klassifikations-Funktion, welche die aktuellste Version des Microsoft Azure Information Protection Clients mit sich bringt, können Unternehmen ihre Daten auf personenbezogene Inhalte automatisch prüfen.**

2. Werden personenbezogenen Daten verarbeitet, besteht grundsätzlich ein Recht auf Auskunft.

Sofern nichts anderes gefordert ist, können die Daten in einem gängigen elektronischen Format zur Verfügung gestellt werden. Hier kommen also wieder die bereits weiter oben erwähnten Lösungen „Export von Inhalten“ und „Download von Inhalten“ zum Einsatz:

- **Export von Inhalten im Office 365 Security & Compliance Center**
- **Optionen für den Download von Daten aus Office 365 heraus**

Anmerkung: Artikel 15 Absatz 4 DSGVO schränkt das Recht auf Erhalt einer Kopie einer Datenkategorie dann ein, wenn dadurch die Rechte und Freiheiten anderer Personen beeinträchtigt werden. Das ist bei der Erstellung von Reports zu beachten. §§ 29, 34 BDSG-neu ergänzen Artikel 15 DSGVO zusätzlich wie folgt:

- Keine Pflicht zur Auskunft besteht unter anderem dann, wenn:
  - Geheimhaltungspflicht besteht
  - die Speicherung für Zwecke der Datensicherheit und der Datenschutzkontrolle erfolgt und die Auskunft einen unverhältnismäßigen Aufwand erfordern würde sowie eine Verarbeitung zu anderen Zwecken durch geeignete technische und organisatorische Maßnahmen ausgeschlossen ist
  - die Daten deshalb gespeichert sind, weil sie aufgrund gesetzlicher oder satzungsgemäßer Aufbewahrungsvorschriften nicht gelöscht werden dürfen

Diese Punkte machen gerade die praktische technische Implementierung der Auskunftspflicht ggf. sehr viel einfacher für die verantwortliche Stelle, da z.B. Backupsysteme etc. nicht betroffen sind. Wichtig ist hier, dass die Gründe einer Auskunftsverweigerung dokumentiert werden.

Artikel 30 DSGVO (Verfahrensverzeichnis)

Artikel 30 DSGVO regelt, dass ein Verzeichnis aller Verarbeitungstätigkeiten zu führen ist.

Um alle Verfahren aufzulisten, die aus Office 365 heraus genutzt werden, stellen die Reports in Office 365 (Anmeldung an Office 365 erforderlich) einen guten Ausgangspunkt dar. So erhält man eine Übersicht der genutzten Services in Office 365. Eine ausführliche Auflistung aller genutzten Services kann mittels des Tools Free Office 365 Reporting Tool erzeugt werden. Dieses Tool stellt Microsoft kostenlos zum Download bereit. Eine Übersicht der genutzten Azure Services kann direkt im Azure Portal unter dem Punkt *„Dashboard -> All Resources“* eingesehen werden. Die Reports bieten eine gute Ausgangsposition um Verfahren zu dokumentieren, müssen aber i.d.R. weiter präzisiert werden.

Artikel 32, 33, 34 DSGVO (Sicherheit)

- Artikel 32 - Sicherheit der Verarbeitung
- Artikel 33 - Meldung eines Datenschutzvorfalls an die Aufsichtsbehörde
- Artikel 34 - Benachrichtigung der betroffenen Person(en) eines Datenschutzvorfalls

Diese Artikel verpflichten Unternehmen dazu, eigenverantwortlich zusätzliche / angemessene technische und organisatorische Maßnahmen zu implementieren, welche die Datensicherheit gewährleisten, bzw. verlangen sie Maßnahmen, Regelungen und Prozesse, die im Falle eines Datenschutzvorfalls Anwendung finden. Die Szenarien um die es hier geht sind typischerweise Fragestellungen wie:

- Laptop / Handy mit Firmendaten geht verloren
- Passwörter gehen verloren
- Wie werden Angriffsversuche auf die IT der Unternehmen erkannt
- Nicht autorisierte Zugriffsversuche auf personenbezogene Daten

Technische und organisatorische Maßnahmen in diesem Kontext sind z.B. Multifaktor Authentifizierung, Verschlüsselung, Mobile Devise Management, Right Management Services, Früherkennungssysteme etc.
Microsoft bietet hier, als Teil unterschiedlicher Lizenzmodelle, viele Optionen an.

- **Lizenzmodelle - Multifaktor Authentifizierung, Verschlüsselung, Mobile Devise Management, Rights Management Services, etc.:**
  - → **Enterprise Mobility & Security**
  - → **Microsoft 365 Business & Microsoft 365 Enterprise**
- **Service - Früherkennung:**
  - → **Advanced Threat Analytics**
- **Bezüglich Artikel 32 DSGVO (Sicherheit der Verarbeitung) ist zusätzlich die Funktion Customer Lockbox zu erwähnen. Diese regelt wie ein Supporttechniker von Microsoft auf Daten zugreifen darf.**

Datenschutzfolgenabschätzung

Eine Datenschutzfolgenabschätzung ist immer dann erforderlich, wenn durch die Verarbeitung personenbezogener Daten voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zu erwarten ist. Geregelt wird diese im Artikel 35 DSGVO. Der Artikel beschreibt allerdings nicht, ab wann ein hohes Risiko gegeben ist. Die Artikel-29-Datenschutzgruppe hat dazu eine Leitlinie herausgegeben. Demnach ist im Konzernumfeld eigentlich immer eine Datenschutzfolgenabschätzung notwendig, da zumindest Kriterien wie „Datenverarbeitung in großem Umfang“ oder „Datentransfer außerhalb der EU“ immer erfüllt sind. Ob im konkreten Einzelfall eine Datenschutzfolgeabschätzung notwendig ist, muss juristisch belastbar geprüft werden. Eine Nichtdurchführung muss ausführlich begründet werden.

Praktische Ausführung: Explizite Anleitungen zur technischen Ausführung wurden bisher nicht veröffentlicht. Eine Liste mit Maßnahmen befindet sich in der Erstellungsphase. Die Gewährleistungsziele, die in der ISO/IEC 29100:2011 beschrieben werden, sind u.a. aber auch dazu geeignet, Anforderungen aus dem Artikel 35 DSGVO zu bedienen. Ähnlich verhält es sich mit der internationalen Version, der ISO/IEC 29134:2017. Das nach Artikel 30 DSGVO ohnehin geforderte Verfahrensverzeichnis stellt eine gute Grundlage für eine Datenschutzfolgenabschätzung dar.

Nachfolgend ein paar Beispiele, wo Datenschutzfolgenabschätzungsziele und Gewährleistungsziele aus der ISO korrelieren:

- Gewährleistungsziel „Integrität“:
  - Richtigkeit und Qualität
  - Unversehrtheit und Aktualität der Daten
- Gewährleistungsziel „Vertraulichkeit“:
  - Kein Dritter darf unbefugt Kenntnis oder Zugriff auf personenbezogene Daten erhalten
  - Informationssicherheit
  - Aufbewahrungs- und Weitergabebeschränkungen
- Gewährleistungsziel „Transparenz“:
  - Welche Daten wurden wofür erhoben und verarbeitet?
  - Welche Techniken und Prozesse werden hierfür genutzt?
  - Wer ist jeweils verantwortlich?

Eine Datenschutzfolgenabschätzung kann zur Erfüllung dieser Ziele beitragen, da sie die Risiken für die Integrität, die Vertraulichkeit und die Transparenz der Daten aufzeigen kann und basierend darauf Gegenmaßnahmen definiert werden können.

Microsoft trägt seinen Teil zu den hier aufgeführten Gewährleistungen durch die ISO 27001 / 27018 Zertifizierungen sowie durch weitere Zertifizierungen und regelmäßige Audits bei. Details dazu siehe: Trust Center, Compliance Berichte (Anmeldung an Office 365 erforderlich) und Trust Center - Microsoft Azure.

Zusätzlich ist die Funktion Customer Lockbox zu erwähnen, die regelt, wie ein Supporttechniker von Microsoft auf Daten zugreifen darf.

Auf Seiten des Kunden kann den Pflichten, die sich hier ergeben, durch bereits oben beschriebene Maßnahmen zur Datensicherheit nachgekommen werden. Details siehe Artikel 32, 33, 34 DSGVO (Sicherheit)

Weiterhin können die hier beschriebenen Services dazu genutzt werden, ein stetig laufendes Verfahren zur Überwachung datenschutzrechtlicher Risiken zu implementieren.

Tools, Roadmap und weitere Links

- Compliance Manager in Office 365 – PREVIEW
- GDPR Assessment Tools
- Microsoft GDPR Assessment (Online Version)
- Microsoft GDPR Detailed Assessment
- Office 365 Secure Score (Office 365 Login erforderlich)
- Übersicht Microsoft Partner Ressourcen zum Thema DSGVO
- Das Bundesland Bayern hat einen (fiktiven) Fragebogen zum Thema DSGVO veröffentlicht: https://www.lda.bayern.de/media/dsgvo_fragebogen.pdf

Betroffene Artikel der DSGVO (Liste)

- Artikel 4 Absatz 1, 8
- Artikel 5 Absatz 2
- Artikel 13 Absatz 3
- Artikel 15
- Artikel 17 Absatz 1, 2
- Artikel 18
- Artikel 28 Absatz 1, 2, 3, 4, 5, 29
- Artikel 30 Absatz 2
- Artikel 32
- Artikel 33
- Artikel 34
- Artikel 35
- Artikel 40
- Artikel 42

Schlussbemerkung

Dieses Dokument wurde nach bestem Wissen und nach sorgfältiger Recherche erstellt. Es kann und will jedoch keine fundierte rechtliche, prozessuale und technische Bewertung ersetzen.

Vielen Dank an Herrn Dr. Michael Rath und das Team von Luther Rechtsanwälte für die Zuarbeit und Unterstützung.

Über den Autor

Nicki Borell ist Microsoft MVP, Mitgründer von Experts Inside, Gründer des Labels *„Xperts at Work“* und Partner der atwork GmbH Österreich. Als Team setzen wir erfolgreich IT- und Strategieprojekte im gehobenen Mittelstand und Großkundensegment um. Profitieren Sie von unserer Expertise, unserer Kompetenz und unserem Fachwissen, das wir zusammen mit starken Partnern in jedes unserer Projekte mit einbringen. Kontakt: nb@atwork-it.com | nb@expertsinside.com