Ausgabe 02/2018

ISSN: 2194-1025

BvD-NEWS

Das Fachmagazin für den Datenschutz

Berufsverband der
Datenschutzbeauftragten
Deutschlands (BvD) e.V.

DS-GVO: 2018 – ein heißes Jahr in Sachen Datenschutz

DIE UMSETZUNG DER DS-GVO IN DEUTSCHLAND – ab S. 9

DIE ISO 27018 IM LICHTE DER DS-GVO – ab S. 32

DER SPUR DER DATEN FOLGEN – ab S. 64

DATENSCHUTZSCHULUNG – AUF DIE INNOVATIVE ART – ab S. 72

BvD e.V.
DATENSCHUTZ GESTALTEN

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

START-UPS UND DS-GVO – RECHTLICHE HERAUSFORDERUNGEN UND BESONDERHEITEN

Kevin Marschall, LL.M. und Stephan Blazy, LL.M.

Die Datenschutz-Grundverordnung (DS-GVO) ist heiß diskutiert, auch bei Start-Ups. Für sie stellt sich die Frage nach dem Umgang mit der Verordnung. Dass Start-Ups generell unter die Verordnung fallen ist unkritisch. Besonders Dokumentations- und Rechenschaftspflichten, Datensicherheit, Datenschutz-Folgenabschätzung und die Bestellung eines betrieblichen Datenschutzbeauftragten (bDSB) sind von Brisanz.

Bürokratie als Erleichterung – Notwendigkeit für Start-Ups?

Das Ziel von Dokumentationspflichten ist die Herstellung von Transparenz bei der Datenverarbeitung. Hierdurch kann die Einhaltung der Vorgaben unterstützt und diese auch gegenüber der Aufsichtsbehörde demonstriert werden. Die zentrale Vorschrift ist Art. 30 DS-GVO, wonach grundsätzlich jeder Verantwortliche ein Verzeichnis über alle Verarbeitungstätigkeiten zu führen hat, die seiner Zuständigkeit unterliegen.

Müssen Start-Ups überhaupt dokumentieren?

Von Bedeutung ist, ob Start-Ups überhaupt dokumentieren müssen, da Art. 30 Abs. 5 DS-GVO Ausnahmen vorsieht. Diese waren ausweislich des Wortlauts ursprünglich zur Entlastung von KMU gedacht. Diese müssen nicht dokumentieren, wenn sie weniger als 250 Mitarbeiter beschäftigen. Dies dürfte auf nahezu alle Start-Ups zutreffen. Hiervon gibt es jedoch gravierende Rückausnahmen, wenn die Datenverarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen birgt, wenn sie nicht nur gelegentlich erfolgt oder die Datenverarbeitung sich auf besonders schützenswerte Daten wie Gesundheitsdaten oder auf strafrechtliche Verurteilungen und Straftaten bezieht. Entscheidend ist das Geschäftsmodell und die Datenverarbeitungen sowie deren Art und Umfang. So muss ein Start-Up, das eine App im Bereich der Telemedizin anbietet, besondere Arten von Daten der Patienten verarbeiten und ist dann auch Adressat der Pflicht. Ebenso muss dokumentiert werden, wenn die Datenverarbeitung nicht nur gelegentlich erfolgt. Sofern ein Start-Ups regelmäßig Kunden- oder Mitarbeiterdaten verarbeitet, erfolgt die Verarbeitung schon regelmäßig und nicht nur gelegentlich.

Die Dokumentationspflichten sind von allen Start-Ups zu erfüllen. Diese mögen zwar besonders aus Sicht junger Unternehmen lästig erscheinen. Die Dokumentation interner Prozesse ist aber u.a. als Wettbewerbsvorteil zu begreifen. Auch schon innerhalb eines Investor-Pitchs kann ein solides Datenschutz-Konzept Investoren überzeugen, da jedes Unternehmen mit Einhaltung rechtlicher Vorgaben steht und fällt.

Was ist besonders wichtig bei der Dokumentation?

Die Inhalte der Dokumentationspflicht sind in Art. 30 Abs. 1 lit. a bis g DS-GVO festgelegt.

- Name und Kontaktdaten des Start-Ups sowie ggf. die des Datenschutzbeauftragten
- Zwecke der Verarbeitung

  → Die Zwecke müssen für alle Datenverarbeitungsprozesse gesondert festgelegt und dokumentiert werden; ein One-Size-Fits-All-Konzept („Generalzweck") ist unzureichend. Mögliche Zwecke sind beispielsweise „Vertrieb von Produkten", „Durchführung der Zahlungsverarbeitung" oder „Marketing zur Kundengewinnung"
- Beschreibung der Daten- und Betroffenenkategorien (Kategorisierungserfordernis)

  → Dies schließt Daten von Kunden, Webseitenbesuchern, Dienstleistern und Beschäftigten mit ein. Diese Kategorien sollten mit den betreffenden Datenarten verknüpft werden. Hierdurch wird auch bei Ergänzungen sichtbar, welche Daten für welche Kategorien verarbeitet werden.
- Kategorien von Empfängern der Daten

  → Hier muss gefragt werden, ob und an welche Empfänger (z.B. Dienstleister, Steuerberater etc.) übermittelt werden soll; es reicht aus, wenn diese Übermittlung nur beabsichtigt ist. Zu „Empfängern" zählen nicht die rein internen Empfänger der Daten.
- Übermittlungen der Daten in Drittländer

  → Sofern die Daten in Drittländer (außerhalb der EU) übermittelt werden sollen, was häufig bei der Nutzung von Cloud-Storage-Diensten so ist, sind auch diese und die Rechtsgrundlagen der Übermittlung zu dokumentieren.
- Fristen für die Löschung verschiedener Datenkategorien

  → Diese Angabe ist nur mitaufzunehmen, wenn es dem Start-Up überhaupt möglich ist, eine solche Löschfrist zu bestimmen. So kann schon keine Frist zur Löschung bestimmt werden, wenn der Zeitpunkt der Erreichung des Verarbeitungszwecks, wie etwa bei einem laufenden Vertragsverhältnis, unbestimmt ist.
- Allgemeine Beschreibung der Sicherheitsmaßnahmen zum Schutz der Daten

  → Hier kann im Vorfeld eine Art „Mind-Map" über die jeweiligen Prozesse detailliert ausgearbeitet und mit den betreffenden Maßnahmen versehen werden. Diese Übersicht sollte gepflegt werden und „mitwachsen".

Start-Ups im Auftragsverarbeitungs-Bereich

Auch Auftragsverarbeiter müssen diese Pflichten modifiziert mit Bezug zum Auftragsverhältnis erfüllen. So ist es verbreitet, dass Start-Ups externe Ressourcen, wie Cloud-Computing, nutzen. Andererseits können auch Start-Ups selbst als Auftragsverarbeiter, z.B. im Rahmen eines Instant-Messaging-Service, fungieren. Sie müssen dann den Verantwortlichen auch in zahlreichen Fällen – etwa bei der Evaluation von etwaigen Schutzverletzungen/Datenpannen – ▸

DATENSCHUTZ-GRUNDVERORDNUNG (DS-GVO)

unterstützen. Eine Vermischung beider Rollen ist ebenfalls möglich.

Datensicherheit als Grundgerüst jedes Unternehmens

Plant ein Start-Up personenbezogene Daten zu verarbeiten, muss es die Sicherheit der Daten, Systeme und Prozesse gewährleisten können. Für diesen „Dreiklang" geben Art. 5 und 32 DS-GVO den Rahmen vor. Die hiernach zu ergreifenden technischen und organisatorischen Maßnahmen haben sich an dem jeweiligen Zweck der Verarbeitung, dem Stand der Technik sowie dem Risiko der Datenverarbeitung für die Betroffen zu orientieren. Sie müssen ferner geeignet sein, um einer missbräuchlichen Verarbeitung, dem unbeabsichtigten Verlust, der Schädigung oder Zerstörung personenbezogener Daten vorzubeugen.

Maßnahmen und zu berücksichtigende Aspekte

Wie solche Maßnahmen ausgestaltet sein können, verdeutlicht der Beispielkatalog in Art 32 Abs. 1 DS-GVO. So sind ein effektives Risikomanagement für die Sicherheit der Verarbeitung ebenso entscheidend wie Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit der Systeme und Dienste. Auch die Pseudonymisierung und Verschlüsselung personenbezogener Daten sowie die Fähigkeit der Datenwiederherstellung müssen die ergriffenen Maßnahmen abdecken. Derartige Sicherheitsvorkehrungen sind unabhängig von Betriebsgröße, aber abhängig vom Risiko, zu ergreifen. Für junge, speziell datengetriebene Unternehmen ist allerdings der damit verbundene Kostenfaktor mitunter eine Belastung. Auch wenn gemäß Art. 32 DS-GVO die Implementierungskosten mit in die Waagschale einzubringen sind, darf nicht übersehen werden, dass Folgekosten der Implementierung unberücksichtigt bleiben. Bei der Finanzplanung sollten daher auch die Wartungskosten berücksichtigt werden. Dies kann im Extremfall auch zu einer risikosenkenden Veränderung der Datenverarbeitungsprozesse führen, da die zu implementierenden Maßnahmen mit Absenkung des Risikos abnehmen.

[1] S. auch Marschall, DuD 2015, 183 ff.

Innerbetriebliche Schutzbedarfsfeststellung

Um zu beurteilen welche Schutzmaßnahmen genau zu ergreifen sind, muss das Start-up zunächst den Schutzbedarf der Daten ermitteln. Hierfür sind zwei unterschiedliche Bewertungsfaktoren maßgeblich. Der erste Faktor bemisst sich an der Sensitivität der personenbezogenen Daten. Art. 9 und 10 DS-GVO legen etwa besondere Kategorien von Daten fest. Der zweite Faktor konturiert sich an dem Gefährdungspotenzial, das den Betroffenen aus dem jeweiligen Verarbeitungskontext erwächst. Die Maßnahmen orientieren sich daher maßgeblich an dem Risiko, das durch die Verarbeitung entsteht.

Datenpannen – Was ist zu tun?

Eine weitere Herausforderung für Start-Ups ist die Meldepflicht bei Schutzverletzungen. Schutzverletzungen sind nach Art. 4 Nr. 12 DS-GVO Vernichtung, Verlust, Veränderung, unbefugte Offenlegung und Zugang der personenbezogenen Daten. Eine Verletzung darf nicht bagatellisiert werden, sondern das Start-Up muss grundsätzlich nach Art. 33 und 34 DS-GVO die Aufsichtsbehörde und bei einem hohen Risiko auch die Betroffenen informieren, deren Daten von der Verletzung betroffen sind. Hervorzuheben ist hierbei, dass die Hürde für die Annahme einer Schutzverletzung und die Meldung an die Aufsichtsbehörde niedrig ist. Durch die Schutzverletzung muss „lediglich" ein Risiko (!) für die Rechte und Freiheiten der Betroffenen bestehen; nur bloße Unannehmlichkeiten, wie etwa die erneute Zurverfügungstellung der Adressdaten nach einem Serverabsturz (ohne vorhandenes Back-Up) – ohne Dritteinwirkung – dürfte hiervon ausgenommen sein.[1] Demnach wäre etwa auch ein nicht gesichertes Speichermedium mit personenbezogenen Daten, das unauffindbar bleibt, als meldepflichtige Schutzverletzung zu deklarieren. Gerade auch ein unbefugter Zugang oder die Offenlegung zu bzw. von Daten gegenüber Unberechtigten ist – etwa ohne zureichende Zugriffskonzepte – eine häufige Form der Schutzverletzung. Diese kann durch räumliche Open-Office-Konzepte in sog. Start-Laps/Inkubatoren noch begünstigt werden, da sich hier mehrere Start-Ups dieselben Räumen und Infrastrukturen teilen.

Zeit als wesentlicher Faktor

Da Start-Ups selten eine IT-Abteilung mit einem IT-Sicherheitsbeauftragten haben, ist ein risikoadäquater Schutz der Verarbeitung von Relevanz. Nur durch ein schnelles Handeln nach Feststellung der Schutzverletzung kann die 72h-Grenze, innerhalb derer eine (Erst-)Meldung an die Behörde erfolgen muss, eingehalten werden. Hieran zeigt sich deutlich, wie wichtig ein angemessenes Sicherheitskonzept für Start-Ups ist. Auch schon durch weniger aufwändige Schutzvorkehrungen (z.B. Verschlüsselung von Daten) können sie sich schützen.

Abschätzung der Folgen? Risiken erkennen und handeln!

Liegt in der jeweiligen Verarbeitung – z.B. beim Einsatz von personenzugehörigen Geo-Tracking-Systemen – ein hohes Risiko für die Betroffenen so ist unabhängig von der Unternehmensgröße auch eine Datenschutzfolgenabschätzung durchzuführen.

Besonderes Risiko durch neue Technologien und Geschäftsfelder

Für junge und innovative Unternehmen ist von Relevanz, dass in Art. 35 Abs. 1 DS-GVO explizit Datenverarbeitungsformen durch „neue Technologien" ein hohes Risiko zugemessen wird. Hierbei dürften sich alle Start-Ups auf dem Gebieten der technologischen Vernetzung wie dem IoT-, Autonomik- oder Big-Data-Bereich und Co. angesprochen fühlen. Im Einzelfall ist jedoch immer auf das konkrete Risiko für den Betroffenen abzustellen, welches ihm durch den Einsatz der jeweiligen Technologien widerfährt. Das Risiko konturiert sich nicht ausschließlich an der Menge oder Art der Daten, sondern besonders an dem Informationsgehalt über das Individuum, der sich aus ihrer Verarbeitung und dem Kontext ergibt. Es geht also darum, Risiken für die Betroffenen bereits während der Business- und Technikkonzeption zu erkennen und durch die Erkenntnisse der Folgenabschätzung einzudämmen. Liegt das Betätigungsfeld z.B. im Profiling, Scoring, Tracking, der (großflächigen) Überwachung öffentlicher Plätze oder in der Verarbeitung besonderer Kategorien von Daten so ist stets eine Datenschutz-Folgenabschätzung durchzuführen. Einen Überblick über die Pflicht zur Durchführung einer Folgenabschätzung bieten auch die kürzlich veröffentlichen Blacklists der Aufsichtsbehörden.[2]

Einfluss von Datenschutzgrundsätzen

Besteht eine Pflicht zum Handeln, stellt sich anschließend die Frage wie man genau zu Werke gehen soll. Als junger Unternehmer kann es nicht schaden über die wichtigsten Mindestprüfelemente im Bilde zu sein. Zentral sind hier die Grundsätze der Verarbeitung personenbezogener Daten gem. Art. 5 Abs. 1 DS-GVO wie etwa Rechtmäßigkeit der Verarbeitung oder die Speicherbegrenzung. Möchte das Unternehmen beispielsweise eine App entwickeln, so muss die Datenverarbeitung im Lichte dieser Grundsätze analysiert werden und die Grundsätze bei der Produktgestaltung beachtet werden (Privacy by Design und by Default). Wie das Risiko der Datenverarbeitung für den App-Nutzer erwächst, muss in der Folge bewertet werden können. Dem sind die ergriffenen Sicherheits- und Eindämmungsmaßnahmen gegenüberzustellen. Mit ihnen muss sich das Risiko beherrschen lassen. Allgemeingehaltene Checklisten helfen hierbei kaum, da die Verarbeitungsvorgänge und Risiken je nach internen Prozessen stark variieren.

Kommen die Gründer letztlich zu dem Schluss, dass sie die hohen Risiken nicht eindämmen können ist zudem gemäß Art. 36 DS-GVO die Aufsichtsbehörde zu konsultieren. Diese wird dann Empfehlungen aussprechen. Zur Prüfung, ob eine erneute Folgenabschätzung durchzuführen ist, etwa wenn sich substanzielle Abweichungen im Hinblick auf die Risiken für die Betroffenen ergeben, bietet sich eine synoptische Gegenüberstellung der Schnittmengen und Risiken beider Verfahren an. Haben sich die „Rahmenbedingungen" und das Risiko nicht erhöht, kann eine erneute Abschätzung unterbleiben.

Datenschutzbeauftragter – Pflicht oder Kür?

Nach der Verordnung kommt es bei der Bestellpflicht auf die von den Datenverarbeitungen ausgehenden Risiken für die Betroffenen an.[3] Hierbei muss die Kerntätigkeit der Start-Ups gerade aufgrund ihres Wesens, Umfangs ▸

[2] S. etwa für Hamburg https://datenschutz-hamburg.de/assets/pdf/Liste%20Art%2035-4%20DS-GVO%20Hmb.BfDI-%C3%B6ffentlicher%20Bereich_v1.0.pdf; für Schleswig-Holstein s. https://datenschutzzentrum.de/uploads/datenschutzfolgenabschaetzung/20180525_LfD-SH_DSFA_Muss-Liste_V1.0.pdf; für den Bund s. https://www.bfdi.bund.de/SharedDocs/Downloads/DE/Datenschutz/Liste_Verarbeitungsvorgaenge.pdf?__blob=publicationFile&v=2.

[3] S. Marschall/Müller, ZD 2016, 415 ff.

und ihrer Zwecke auf eine regelmäßige oder systematische Beobachtung von Betroffenen ausgerichtet sein. So wären beispielsweise solche Start-Ups zur Bestellung verpflichtet, die – insbesondere bei neuen Technologien – Profilbildungen, Bewertungen oder Katalogisierungen der Betroffenen vornehmen, wie etwa bei Start-Ups, die das Verhalten von Nutzern elektronischer Dienste, wie Apps, aufzeichnen, auswerten und zu kommerziell nutzbaren Ergebnissen aufbereiten. Dies gilt insbesondere dann, wenn im Rahmen der Kerntätigkeit besondere Datenarten verarbeitet werden, was im Bereich Wearable-Computing-Systems der Fall sein kann. Besteht hiernach keine Bestellpflicht für Start-Ups, so müssen diese aber auch das nationale Recht beachten. Nach § 38 BDSG-neu „gelten" die bisher bestandenen Regelungen weitgehend fort. Hiernach ist auch bei mind. 10 Personen die ständig mit der Datenverarbeitung betraut sind ein bDSB zu bestellen; ebenso, wenn eine Datenschutz-Folgenabschätzung durchzuführen ist. Start-Ups müssen im Falle einer personellen Erweiterung oder einer Ausdehnung bestehender Datenverarbeitungen aufs Neue doppelt prüfen, ob eine Bestellung verpflichtend ist.

Eine „Eigenbestellung" zum bDSB als Geschäftsführer ist aufgrund von Interessenskonflikten nicht möglich. Jedoch kann es eine Alternative sein, sich die Dienstleistung extern einzukaufen.

Checkliste

Bestandsaufnahme und Dokumentation folgender Inhalte:

- ○ Welche Verarbeitungsprozesse werden zu welchen Zwecken vorgenommen?
- ○ Welche Datenarten und welche Kategorien von Betroffenen werden im Rahmen des Geschäftsmodells grundsätzlich und prognostisch verarbeitet?
- ○ Wo liegt die Kerntätigkeit des Start-Ups? Branchenbestimmungen?
- ○ Sind das Geschäftsmodell und die Kerntätigkeit mit einem besonderen Risiko für die Betroffenen verbunden?
- ○ Welche Sicherheitsmaßnahmen müssen mindestens zur Begegnung dieser Risiken implementiert werden?
- Bezugnahme zu Schutzverletzungen als Orientierungspunkt hilfreich
- Wie hoch sind die Implementierungskosten der Maßnahmen?
- Beurteilung des Verhältnisses von Risiko und Maßnahmen – werden diese angemessen abgedeckt oder muss ich notfalls die Art und den Umfang der Datenverarbeitung anpassen/reduzieren?

Wie erhalte ich Kenntnis von Schutzverletzungen?

- ○ Wer wird in die Bewertung des Vorfalls eingebunden?
- ○ Ist Hilfe von Extern, auch von der Aufsichtsbehörde, erforderlich?
- ○ Existiert ein Kommunikations- und Handlungskonzept im Umgang mit Schutzverletzungen?

Fazit: Große Herausforderungen, aber machbar!

Die Verordnung stellt gerade Start-Ups vor große Herausforderungen. Ob sich seitens der Politik – wie derzeit diskutiert[4] – noch Erleichterungen für kleine Unternehmen ergeben, ist fraglich. Ein bDSB hilft nachhaltig, die Vorgaben angemessen umzusetzen. Insbesondere auch eine frühzeitige Zusammenarbeit mit der zuständigen Aufsichtsbehörde kann jungen Unternehmen ebenfalls helfen, sich im Bereich des (neuen) Datenschutzrechts einzufinden.

Über die Autoren

Kevin Marschall, LL.M.

Stephan Blazy, LL.M.

sind Geschäftsführer und Gründer der GDPC GbR einer auf Datenschutz und Informationssicherheit spezialisierten Unternehmensberatung mit Sitz in Kassel. Sie beraten Unternehmen und Behörden insbesondere bei der Umsetzung der DS-GVO und fungieren auch als externe DSB.

▶ www.gdpc.de

GLOBAL DATA PROTECTION CONSULTING

[4] https://www.golem.de/news/DS-GVO-ganz-grosse-koalition-fordert-aenderungen-beim-datenschutz-1806-134941.html.

Anzeige

Seminare und Lehrgänge.

Für eine gesetzeskonforme und professionelle Umsetzung von Datenschutz und Compliance.

Haben Sie auf die neue EU-DSGVO umgestellt?

Sichern Sie sich jetzt umfangreiches und aktuelles Know-how für Ihre persönliche berufliche Entwicklung.

TÜV Rheinland bietet ein breit gefächertes Portfolio an Bildungs- und Beratungsdienstleistungen auf höchstem fachlichen Niveau. Mehr als 7.500 Angebote, über 2.500 Referenten. Deutschlandweit.

Zum Thema Datenschutz bieten wir zahlreiche Seminare und modulare Lehrgänge mit der Möglichkeit, ein Zertifikat unter Einbeziehung der neuen EU-DSGVO der unabhängigen Personenzertifizierungsstelle PersCert von TÜV Rheinland zu erwerben. Auch im Bereich Compliance finden Sie bei uns eine Vielzahl praxisorientierter Qualifizierungsangebote.

Datenschutz

Alle Seminare und Lehrgänge beziehen sich selbstverständlich auf die EU-DSGVO und das neue BDSG.

- Datenschutzfachkraft.
- Datenschutzbeauftragter (TÜV).
- Datenschutzauditor (TÜV).
- Externer Datenschutzbeauftragter (TÜV).
- EU-Datenschutz-Grundverordung.
- Datenschutzbeauftragter. Update auf die EU-DSGVO.
- EU-DSGVO und Informationssicherheit. Vom ISMS zum DSMS.
- Auftragsverarbeitung nach EU-DSGVO und neuem BDSG.
- Datenschutz Update – Fortbildung für Datenschützer.
- Übersicht der Verarbeitungstätigkeiten & Datenschutz-Folgenabschätzung.
- Videoüberwachung nach DSGVO und neuem BDSG.

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/datenschutz

Compliance

- Compliance-Officer (TÜV).
- Compliance-Beauftragter: Anforderungen, Aufgaben, Risiken.
- Compliance-Organisation – erste Schritte beim Aufbau.
- Compliance-Risikoanalyse.
- Interne Untersuchungen bei Compliance-Verstößen.
- Geldwäschebeauftragter (TÜV).

Weitere Details, Seminare und Anmeldung unter:
www.tuv.com/seminare-compliance

Weitere Informationen erhalten Sie auch bei:
TÜV Rheinland Akademie GmbH
Am Grauen Stein · 51105 Köln
Sandra Fahling · Tel. 0221 806-3561
sandra.fahling@de.tuv.com

www.akademie.tuv.com

TÜVRheinland®
Genau. Richtig.