DIGITAL HUB CYBERSECURITY

The Cyberstartup Know & Do

DSGVO
für Cyber Startups

Die Umsetzung der Datenschutz-Grundverordnung in Startups

Anforderungen an den Umgang mit Kundendaten und an die Entwicklung von Softwarelösungen

Autorin: Annika Selzer

Vielen Dank

Der Digital Hub Cybersecurity bedankt sich bei Annika Selzer und unserem Träger Fraunhofer SIT für die Unterstützung bei der Entwicklung dieser Publikation.

Annika Selzer hat Informationsrecht an der Hochschule Darmstadt studiert. Sie ist zertifizierter Datenschutzbeauftragter und Datenschutzauditor (TÜV, Deutschland) sowie zertifizierter GDPR Practitioner (APMG International, United Kingdom). Seit 2011 ist sie Wissenschaftlerin am Fraunhofer-Institut für Sichere Informationstechnologie. Ihr Forschungsschwerpunkt ist die interdisziplinäre Recht-Technik-Forschung, insbesondere im Bereich des Datenschutzrechts.

Inhalt

Vorwort

2018 war das Jahr der Deutschen Datenschutzgrundverordnung (DSGVO), der deutschen Umsetzung der europäischen General Data Protection Regulation (GDPR): Kein Unternehmen konnte es sich leisten, sich nicht damit zu befassen, auch nicht ein Startup. Knapp ein Jahr nach der Einführung beginnt die Politik auszuwerten, was funktioniert, was nicht: wo muss gegebenenfalls nachgesteuert werden?

Das Grundgerüst jedoch hat sich bewährt. Heute gilt die DSGVO als Blaupause für ähnliche Initiativen, zum Beispiel in Kalifornien (USA) oder in China.

Es lohnt sich also, sich mit der DSGVO zu beschäftigen: nicht nur, weil ein Verstoß teuer werden kann, sondern auch weil es Anforderungen bei der internationalen Expansion vereinfachen kann. Startups, die die DSGVO sowohl in ihren Unternehmensprozessen als auch in ihren Lösungen umsetzen, sichern sich so perspektivisch Wettbewerbsvorteile.

Mit diesem „The Cybersecurity Startup Know & Do“ geben wir den Startups das dafür nötige Know-how an die Hand.

Viele Spaß beim Lesen!

Das Team des Digital Hub Cybersecurity

DSGVO und Startups

Spätestens seit Mai 2018 ist die Datenschutz-Grundverordnung – nicht zuletzt wegen ihres hohen Bußgeldrahmens in Millionenhöhe – in aller Munde. Die strengen Regelungen der Verordnung sind bei der Verarbeitung personenbezogener Daten zu beachten,[1] also bei der Verarbeitung von Daten, die sich eindeutig einer bestimmten oder bestimmbaren natürlichen Person zuordnen lassen, wie z. B. der Name, die Anschrift, die Telefon- oder Kreditkartennummer einer lebenden Person.

Startups stehen daher vor dem Problem, in ihrer täglichen Arbeit die Anforderungen der Datenschutz-Grundverordnung auch dann beachten zu müssen, wenn sie über wenige Ressourcen zur Umsetzung verfügen. Für Startups im Bereich der Cybersecurity ergeben sich wichtige Anforderungen insbesondere im Bereich der Kundendatenverarbeitung sowie im Bereich der Softwareentwicklung. Der Beitrag stellt für diese zwei Bereiche wichtige Anforderungen der DSGVO vor.

I. Anforderungen an den Umgang mit personenbezogenen (Kunden-)daten

Für die Verarbeitung personenbezogener Daten seiner Kunden ist ein Startup der sogenannte „(datenschutzrechtlich) Verantwortliche“. Die natürlichen Personen, die Kunde des Startups sind, nennt die Datenschutz-Grundverordnung (DSGVO) „betroffene Personen“. Im Folgenden werden wichtige Anforderungen an die Verarbeitung personenbezogener (Kunden-)daten erklärt.

a. Bestellung eines Datenschutzbeauftragten

Ein Startup muss dann einen Datenschutzbeauftragten benennen, der im Startup zur Umsetzung der rechtlichen Datenschutzvorgaben berät und diese kontrolliert, wenn die Kerntätigkeit des Startups in der Durchführung von Verarbeitungsvorgängen besteht, welche eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erforderlich machen, oder die Kerntätigkeit des Startups in der umfangreichen Verarbeitung besonderer Kategorien personenbezogener Daten liegt.

1 Hinweis: Je nach Verarbeitungskontext und je nachdem wer in dem Verarbeitungskontext personenbezogene Daten verarbeitet, können neben der Datenschutz-Grundverordnung weitere/andere rechtliche Regelungen wie z. B. das Bundesdatenschutzgesetz, das Telemediengesetz usw. einschlägig sein. Welche Regelungen des Datenschutzrechts es konkret zu beachten gilt, sollte somit die grundlegende Prüfung eines jeden Verantwortlichen sein.

Die nationale Gesetzgebung ergänzt diesbezüglich u. a., dass auch diejenigen Startups einen Datenschutzbeauftragten bestellen müssen, die der Pflicht zur Durchführung einer Datenschutz-Folgenabschätzung (s. Abschnitt h) unterliegen und die geschäftsmäßig zum Zwecke der Übermittlung oder zur Markt- und Meinungsforschung personenbezogene Daten verarbeiten. Auch wenn in einem Startup eine bestimmte Mindestanzahl an Personen ständig mit der automatisierten Verarbeitung personenbezogener Daten beschäftigt ist, ist ein Datenschutzbeauftragter zu benennen. Ein Datenschutzbeauftragter kann innerbetrieblich benannt werden oder als externe Dienstleistung eingekauft werden. Innerbetrieblich besteht für den Geschäftsführer selbst jedoch ein Interessenskonflikt, so dass er das Amt des betrieblichen Datenschutzbeauftragten regelmäßig nicht besetzen kann.

b. Rechtmäßigkeit der Verarbeitung

Personenbezogene Daten dürfen nur dann verarbeitet werden, wenn ein Gesetz – oder eine andere rechtsverbindliche Regel wie z. B. eine Betriebsvereinbarung – dies erlaubt oder die betroffene Person eingewilligt hat. Im Rahmen der Datenverarbeitung von Kunden oder Interessenten besteht z. B. eine gesetzliche Erlaubnis für die Verarbeitung personenbezogener Daten, wenn diese für die Erfüllung eines Vertrags, dessen Vertragspartei die betroffene Person ist, oder zur Durchführung vorvertraglicher Maßnahmen erforderlich ist, die auf Anfrage der betroffenen Person erfolgen.

In der Praxis das wohl meistgenutzte Mittel, eine Datenverarbeitung zu legitimieren, stellt die Einwilligung dar. Eine datenschutzkonforme Einwilligung muss von der betroffenen Person freiwillig und für einen bestimmten Fall abgegeben worden sein. Die betroffene Person muss zudem vor der Erteilung der Einwilligung über die geplante Datenverarbeitung informiert worden sein und muss die Einwilligung in einer unmissverständlichen Weise – z. B. durch Unterzeichnung eines Papierausdrucks oder durch aktives Ankreuzen eines Webformulars – abgegeben haben. Da der Verantwortliche – also das Startup, das die Daten verarbeiten möchte – die Einwilligung nachweisen können muss, sind die unterzeichneten Papierausdrucke aufzubewahren bzw. das Ankreuzen der Einwilligungserklärung im Webformular zu protokollieren und das Protokoll aufzubewahren. Die betroffene Person hat das Recht, ihre Einwilligung jederzeit zu widerrufen. Sofern eine Datenverarbeitung durch eine Einwilligung legitimiert werden soll, ist es empfehlenswert, den Einwilligungstext in Kooperation mit dem betrieblichen Datenschutzbeauftragten und/oder einem Rechtsanwalt zu erstellen.

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf

Die Verarbeitung besondere Kategorien personenbezogener Daten – z. B. Daten über die rassische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen sowie Gesundheitsdaten – unterliegt besonders hohen Anforderungen.

Sonderfall:
Rechtmäßigkeit der Verarbeitung für Werbung
An die Verarbeitung personenbezogener Daten zum Hinweis auf Werbung oder werbeähnlichen Inhalten per Fax, Telefon oder E-Mail sind besonders hohe datenschutz- und wettbewerbsrechtliche Anforderungen zu stellen.

Für Startups besonders relevant dürfte der Wunsch nach Zusenden von Newsletter sein. Dies ist i. d. R. nur nach vorheriger Einwilligung möglich. Sofern die Einwilligung elektronisch erfolgen soll, sollte das sogenannte „Double-Opt-In-Verfahren" eingesetzt werden. Nach Eingabe der eigenen E-Mail-Adresse und nach Anklicken des Einwilligungshäkchens für den Newsletterversand erhält die betroffene Person beim Double-Opt-In-Verfahren eine E-Mail, im Rahmen derer sie zur erneuten Bestätigung der Einwilligung aufgefordert wird. Auf diese Weise soll sichergestellt werden, dass die sich zu einem Newsletter anmeldende Person tatsächlich Zugriff auf das der E-Mail-Adresse zugeordnetem Postfach hat.

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf

und

https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf

In jedem Versand eines Newsletters sollte sodann die Möglichkeit zur Abmeldung vom Newsletter bestehen. Über eine Blacklist ist sicherzustellen, dass Personen, die sich von dem Newsletter des Startups abgemeldet haben, nicht erneut in den Newsletterversand einbezogen werden.

c. Zweckbindung und Datenminimierung

Es dürfen nur diejenigen personenbezogenen Daten verarbeitet werden, die für den Zweck der Datenverarbeitung unbedingt notwendig sind. Der rechtmäßige Zweck ist vor der Datenerhebung festzulegen und darf i. d. R. danach nicht mehr geändert werden.

Kann man sich auf der Webseite des Startups beispielsweise eine kostenpflichtige Software herunterladen, so darf das Startup in diesem Zusammenhang die Bankverbindung der betroffenen Person erheben. Dies darf jedoch i. d. R. nicht als Pflichtangabe erhoben werden, wenn die Nutzung der Software nicht mit Kosten verbunden ist.

d. Informationspflichten

Vor der Erhebung personenbezogener Daten müssen umfangreiche Informationspflichten gegenüber den betroffenen Personen erfüllt werden. Welche Informationen als Pflichtangaben zu benennen sind, regelt Art. 13 DSGVO.

Beispielsweise muss ein Startup Bewerber im Rahmen von Stellenausschreibungen über die Datenverarbeitung beim Bewerbungsverfahren sowie seine Mitarbeiter über die Datenverarbeitung im Rahmen der Mitarbeiterverwaltung informieren. Auch die Kunden eines Startups sind über die Datenverarbeitung im Rahmen des Kundendatenmanagements zu informieren. Eine weitere Informationspflicht besteht auch für Webseiten von Startups. In der sogenannten „Datenschutzerklärung" hat das Startup über

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf

Speziell zur Informationspflicht bei Videoüberwachung:

https://www.lda.bayern.de/de/videoueberwachung.html

die Datenverarbeitung, die im Rahmen der Webseitennutzung stattfindet, zu informieren.

e. Dokumentationspflichten

Die Umsetzung der Anforderungen der Datenschutz-Grundverordnung muss ein jeder Verantwortliche nachweisen können. Der Nachweis erfolgt insbesondere auch durch die Dokumentation von Verarbeitungstätigkeiten im sogenannten Verzeichnis von Verarbeitungstätigkeiten. Das Verzeichnis der Verarbeitungstätigkeiten ist zu führen, wenn ein Unternehmen oder eine Einrichtung 250 oder mehr Mitarbeiter beschäftigt. Somit würden Startups grundsätzlich nicht unter die Pflicht zum Führen eines Verfahrensverzeichnisses fallen. Jedoch fallen Verantwortliche grundsätzlich auch mit einer geringeren Anzahl an Beschäftigten unter die Pflicht des Führens eines Verzeichnisses der Verarbeitungstätigkeiten, wenn die Verarbeitung personenbezogener Daten nicht nur gelegentlich erfolgt. Auch wenn eine Entlastung der Pflichten von Startups und Kleinstunternehmen durch die DSGVO – vor allem dann, wenn sie keine besonderen Kategorien personenbezogener Daten verarbeiten – wünschenswert gewesen wäre, fallen Startups daher alleine schon wegen der regelmäßigen Verarbeitung ihrer Kunden- und Mitarbeiterdaten unter die Pflicht zum Führen eines Verfahrensverzeichnisses.

Das Verzeichnis der Verarbeitungstätigkeiten setzt sich aus der Dokumentation einzelner Verarbeitungstätigkeitsbeschreibungen zusammen. Je Verarbeitungstätigkeitsbeschreibung sind u. a. die Zwecke der Verarbeitung, die Beschreibung der Kategorien betroffener Personen (z. B. Mitarbeiter und Kunden) und der Kategorien personenbezogener Daten (z. B. allgemeine Kontaktdaten, Gesundheitsdaten) sowie – wenn möglich – die vorgesehenen Löschfristen der verschiedenen Datenkategorien zu erfassen (eine vollständige Auflistung der Pflichtangaben enthält Art. 30 DSGVO).

Darüber hinaus ist in der Regel die konkrete Umsetzung/Ausführung datenschutzrelevanter Vorgaben zu protokollieren. So ist etwa über ein Löschprotokoll nachvollziehbar zu halten, an welchem Tag in welchem System wie viele Datensätze gelöscht wurden oder etwa das Einholen von datenschutzkonformen Einwilligungen zu protokollieren.

Muster Verfahrensmeldung für Verantwortliche:

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Verantwortlicher.docx

Achtung: Auch wenn man selbst als Auftragsverarbeiter arbeitet, fällt man unter die Pflicht zur Dokumentation. In diesem Fall sind jedoch andere Pflichtangaben je Verfahren erforderlich. Ein Muster für Auftragsverarbeiter findet sich hier:

https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Auftragsverarbeiter.docx

f. Übermittlung an externe Stellen

Eine Übermittlung personenbezogener Daten an externe Stellen unterliegt den gleichen Anforderungen, wie in dem Abschnitt „Rechtmäßigkeit der Verarbeitung“ genannt. Eine Übermittlung an externe Stellen in Drittstaaten, also Staaten außerhalb des Europäischen Wirtschaftsraumes, ist nur erlaubt, wenn in dem Drittstaat/der externen Stelle in einem Drittstaat zusätzlich ein mir dem Datenschutzniveau des

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf

Europäischen Wirtschaftsraumes vergleichbares Datenschutzniveau sichergestellt werden kann.

Die Europäische Kommission kann für Drittstaaten feststellen, dass diese über ein angemessenes Datenschutzniveau verfügen. Eine Datenübermittlung an Empfänger in diesen Drittstaaten bedarf keiner besonderen Genehmigung. Dies gilt aktuell für folgende Länder: Schweiz, Kanada, Israel, Japan, Jersey, Isle of Man, Guernsey, Uruguay, Andorra, Neuseeland, die Färöer-Inseln und Argentinien. Auch Datenübermittlungen an Empfänger in den USA sind zulässig, jedoch beschränkt sich die Zulässigkeit auf diejenigen Empfänger, die dem EU-US-Privacy-Shield beigetreten sind. Der EU-US-Privacy-Shield ist jedoch nicht unumstritten und steht unter „Beobachtung".

Sofern keine Angemessenheitsentscheidung der Europäischen Kommission vorliegt, können zwischen dem europäischen Unternehmen und dem Empfänger im Drittstaat z. B. die sogenannten „EU-Standard-Datenschutzklauseln" vereinbart werden. Die EU-Standard-Datenschutzklauseln sind ein von der Europäischen Kommission entwickeltes Vertragswerk, dass „künstlich" ein angemessenes Datenschutzniveau sicherstellt. Das Vertragswerk ist über die Webseite der Europäischen Kommission erhältlich und ist ohne Änderungen zu übernehmen. Zu unterscheiden sind Standard-Datenschutzklauseln für die Übermittlung an Auftragsverarbeiter und Standard-Datenschutzklauseln für die Übermittlung an Verantwortliche.

Sonderfall:
Übermittlung an externe Stellen als Auftragsverarbeitung

Eine Weitergabe personenbezogener Daten an externe Dienstleister kann auch auf Basis einer sogenannten Auftragsverarbeitung (AV) erfolgen. Gibt ein Startup personenbezogene Daten auf Grundlage einer Auftragsverarbeitung an einen externen Dienstleister – den Auftragsverarbeiter – weiter, so darf der Auftragsverarbeiter die Daten nur nach Weisung des Startup verarbeiten und erhält keine eigenen Rechte an den Daten. Das Startup bleibt für die Datenverarbeitung verantwortlich. Häufig sind auch Cloud-Anbieter, Wartungsdienstleister und Softwarehersteller Auftragsverarbeiter.

Mehr zum Thema:
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Eine Auftragsverarbeitung setzt voraus, dass vor Beginn der Datenverarbeitung durch den Auftragsverarbeiter dieser sorgfältig vom Verantwortlichen, also dem Startup, ausgewählt wird. Im Fokus stehen hierbei die vom Auftragsverarbeiter getroffenen technischen und organisatorischen Maßnahmen, die auf Vollständigkeit und Angemessenheit zu überprüfen sind. Insbesondere können Datenschutz- und Datensicherheitszertifizierungen wichtige Anhaltspunkte für die Auswahl liefern. Die sorgfältige Auswahl ist zu dokumentieren.

Eine Auftragsverarbeitung erfordert zudem verpflichtend den Abschluss eines AV-Vertrages vor Beginn der Datenverarbeitung durch den Auftragsverarbeiter. Die Pflichtinhalte eines solchen Vertrags sind in Art. 28 DSGVO geregelt.

Hilfe für AV-Vertrag:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf

Sofern ein Auftragsverarbeiter aus einem Drittstaat eingesetzt wird, ist zusätzlich ein mit dem Europäischen Wirtschaftsraum vergleichbares Datenschutzniveau herzustellen.

g. Technische und organisatorische Maßnahmen

Die Datenschutz-Grundverordnung verlangt – unter Berücksichtigung des Stands der Technik und der Risiken einer geplanten Datenverarbeitung – das Treffen geeigneter technischer und organisatorischer Schutzmaßnahmen. Die Maßnahmen sollen die Ziele Vertraulichkeit, Verfügbarkeit, Integrität, Belastbarkeit der Systeme und rasche Widerherstellbarkeit nach physischen oder technischen Zwischenfällen sicherstellen. Beispiele für technische und organisatorische Maßnahmen sind etwa Verschlüsselungs- und Pseudonymisierungsverfahren, aber auch die Zutrittskontrolle zu Räumen, in denen personenbezogene Daten verarbeitet werden sowie der Zugriffsschutz auf personenbezogene Daten – etwa durch die Nutzerkennung mit Namen und Passwort – gehören zu den technischen und organisatorischen Maßnahmen. Die Verarbeitung besonderer Kategorien personenbezogener Daten erfordert besonders hohe technische und organisatorische Schutzmaßnahmen. Die Wirksamkeit der getroffenen Maßnahmen ist regelmäßig zu evaluieren.

h. Datenschutz-Folgenabschätzung

Eine Datenschutz-Folgenabschätzung ist ein spezielles Datenschutzinstrument, mit dem die Folgen einer personenbezogenen Datenverarbeitung abgeschätzt werden müssen, sofern diese voraussichtlich ein hohes Risiko für die Rechte und Freiheiten der betroffenen Person hat. Dabei soll sich die Datenschutz-Folgenabschätzung insbesondere mit den Maßnahmen befassen, durch die dieses Risiko eingedämmt werden soll. Eine Datenschutz-Folgenabschätzung hat verpflichtend zu erfolgen, wenn systematische und umfassende Bewertung persönlicher Aspekte natürlicher Personen erfolgen sollen, wenn eine umfangreiche Verarbeitung besonderer Kategorien von personenbezogenen Daten stattfinden soll oder wenn eine systematische umfangreiche Überwachung öffentlich zugänglicher Bereiche stattfinden soll. Die Datenschutz-Aufsichtsbehörden legen weitere Pflichtbereiche fest.

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

Die Datenschutz-Folgenabschätzung hat vor Beginn der Aufnahme der Verarbeitungstätigkeit zu erfolgen. Die inhaltlichen Mindestanforderungen stellen die Beschreibung der geplanten Verarbeitungsvorgänge, die Bewertung der Notwendigkeit der Verarbeitungsvorgänge, die Bewertung der Risiken für die Rechte und Freiheiten der betroffenen Personen sowie die Beschreibung der Abhilfemaßnahmen zur Bewältigung der Risiken dar. Die Datenschutz-Aufsichtsbehörde ist zu konsultieren, sofern die Datenschutz-Folgenabschätzung ergab, dass die geplante Verarbeitung ein hohes Risiko zur Folge hätte und der Verantwortliche dieses Risiko nicht eindämmen kann. Die Durchführung der Datenschutz-Folgenabschätzung ist zu dokumentieren.

i. Datenpannen

Datenpannen – also Vorfälle, bei denen personenbezogene Daten externen, unberechtigten Stellen bekannt werden oder bekannt geworden sein können – sind unverzüglich binnen 72 Stunden, nachdem dem Verantwortlichen die Verletzung bekannt wurde, der zuständigen Datenschutz-Aufsichtsbehörde und ggf. sogar zusätzlich den betroffenen Personen zu melden. Eine Meldung muss nicht erfolgen, wenn die Verletzung des Schutzes personenbezogener Daten voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt.

Sichert ein Startup beispielsweise den Zugriff auf seine Kundendatenbank nicht ausreichend ab, so dass Unberechtigte von außen auf die Kundendatenbank zugreifen konnten und können daher Namen, Geburtsdaten, Adressen und Bankverbindungen eingesehen werden, liegt i. d. R. eine meldepflichtige Datenpanne vor. Häufig erfolgt die Meldung einer Datenpanne bei der zuständigen Aufsichtsbehörde über ein Onlineformular auf der Webseite der Aufsichtsbehörde.

j. Beantworten von Anträgen zu Betroffenenrechten

Das Datenschutzrecht sieht umfangreiche Rechte für die betroffenen Personen vor. Diese sogenannten „Betroffenenrechte" sollen die Datenverarbeitungen, die bei dem Verantwortlichen vorgenommen werden, gegenüber der betroffenen Person transparent machen und sie u. a. in die Lage versetzen, Auskunft über die zu ihrer Person verarbeiteten Daten zu erhalten, unrichtige Daten korrigieren und unrechtmäßig verarbeitete Daten löschen zu lassen bzw. deren Verarbeitung einschränken zu lassen. Möchte eine betroffene Person von ihren Rechten Gebrauch machen, so hat sie einen Antrag bei dem datenschutzrechtlich Verantwortlichen zu stellen. Grundsätzlich hat der Verantwortliche die betroffene Person innerhalb eines Monats nach Eingang des Antrags über die von ihm auf Basis des Antrags der betroffenen Person ergriffenen Maßnahmen zu unterrichten. I. d. R. ist den Betroffenenrechten unentgeltlich nachzukommen. Die Betroffenenrechte stehen den betroffenen Personen nicht schrankenlos zu, bspw. muss der Verantwortliche einem Antrag auf Löschung personenbezogener Daten nicht nachkommen, wenn er einer gesetzlichen Aufbewahrungsfrist für eben diese Daten unterliegt. Insofern haben Startups Prozesse zu etablieren, mit deren Hilfe die Anträge der betroffenen Person in der vorgegebenen Zeit geprüft, ggf. umgesetzt und beantwortet werden können. Eine wichtige Hilfe zur Umsetzung von Betroffenenrechten bietet ein sauber ausgefülltes Verzeichnis der Verarbeitungstätigkeiten (-> Abschnitt e), aus dem hervorgeht, welche Daten welcher betroffenen Personen in welchen Verfahren verarbeitet werden. Ein besonderer Fokus in der Prozessbeschreibung sollte auch auf der Identifizierung bzw. Identitätsprüfung der betroffenen Person liegen, um zu verhindern, dass personenbezogene Daten der Person X einer antragstellenden Person Y beauskunftet werden.

Mehr zum Thema:

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf

und

https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf

Auch das Recht auf Datenübertragbarkeit kann für Startups eine Rolle spielen. So genießt die betroffene Person das Recht auf Datenübertragbarkeit, wenn die Verarbeitung auf Basis einer Einwilligung oder eines Vertrages mit der verantwortlichen Person legitimiert wurde und die Verarbeitung durch Computersysteme – insbesondere in Online-Plattformen – erfolgt. In diesen Fällen steht der betroffenen

Person das Recht eines „Umzugs“ ihrer Daten von einem zum anderen Anbieter zu, was den Anbieterwechsel vereinfachen soll. Dementsprechend sollten Startups zunächst bewerten (lassen), ob sie dem Recht auf Datenübertragbarkeit für ihren konkreten Verarbeitungskontext nachkommen müssen und dann ggf. Prozesse etablieren, um eine „Herausgabe“ bzw. einen „Umzug“ von Daten zu ermöglichen. Das oben gesagte zur Identifizierung gilt entsprechend.

Auch bei den bereits vorgestellten Informationspflichten handelt es sich – formal gesehen – um ein Recht der Betroffenen. Im Gegensatz zu anderen Betroffenenrechten stellen die Informationspflichten jedoch eine „Bringschuld“ des Verantwortlichen dar, d.h. es bedarf keinen Antrag der betroffenen Person.

k. Löschen

Personenbezogene Daten sind zu löschen, sobald sie für den rechtmäßigen Zweck, für den sie ursprünglich erhoben wurden, nicht mehr erforderlich sind. Eine Löschpflicht kann sich auch auf einen entsprechenden Antrag des Betroffenen im Rahmen seiner Betroffenenrechte ergeben. „Löschen“ meint das Behandeln von Daten derart, dass sie nach dem Löschvorgang nicht mehr vorhanden oder unkenntlich sind und nicht mehr verwendet oder rekonstruiert werden können. Das datenschutzkonforme Anonymisieren personenbezogener Daten stellt eine Alternative zum Löschen der personenbezogenen Daten dar.

Entgegen der vorgestellten grundsätzlichen Pflichten zur Löschung personenbezogener Daten, können Gesetze oder andere Rechtsvorschriften (z. B. Betriebsvereinbarungen) eine Löschung für einen bestimmten Zeitraum verbieten. Vor einer Löschung ist daher zu prüfen, ob einer Löschung gesetzliche Vorschriften oder sonstige rechtswirksame Vereinbarungen zu Aufbewahrungspflichten entgegenstehen. Sollten für ein personenbezogenes Datum mehrere gesetzliche Aufbewahrungsfristen bestehen, so ist das Datum solange aufzubewahren, bis die längste gesetzliche Aufbewahrungsfrist verstrichen ist.

Greift ein Startup auf Auftragsverarbeiter zurück, so hat es insbesondere zu beachten, den Auftragnehmer vertraglich zu verpflichten, nach Abschluss der Erbringung der Verarbeitungsleistungen alle personenbezogenen Daten zu löschen oder zurückzugeben und die vorhandenen Kopien zu löschen. Nach Beendigung des Vertragsverhältnisses sollte sich das Startup zudem vom Auftragsverarbeiter schriftlich bestätigen lassen, dass dieser der vertraglich vereinbarten Regelungen zur Löschung nachgekommen ist.

II. Anforderungen an die Entwicklung von Softwarelösungen

Im Zusammenhang mit der Entwicklung von Softwarelösungen sollten Startups auch die Vorschriften zum Datenschutz durch Technikgestaltung und zu datenschutzrechtlichen Voreinstellungen beachten.

„Datenschutz durch Technikgestaltung“ meint, dass der Verantwortliche nicht erst zum Zeitpunkt der Verarbeitung angemessene technisch-organisatorische Maßnahmen zu treffen hat, sondern bereits zum Zeitpunkt der Festlegung der Mittel für die Verarbeitung die Pflicht zum Treffen geeigneter technisch-organisatorischer

Maßnahmen berücksichtigen muss. Insbesondere hat der Verantwortliche sicherzustellen, dass das Einhalten der Datenschutzgrundsätze wie der Zweckbindung und Datenminimierung (-> Abschnitt II.c) durch technisch-organisatorische Maßnahmen sichergestellt wird. Dementsprechend sind bereits während der Konzeptionsphase neuer Softwarelösungen durch Startups die Anforderungen des technische-organisatorischen Datenschutzes zur Umsetzung der Datenschutzgrundsätze zu berücksichtigen.

„Datenschutzfreundliche Voreinstellungen" meint, dass der Verantwortliche technisch-organisatorische Maßnahmen zu treffen hat, die sicherstellen, dass durch Voreinstellung nur personenbezogene Daten, deren Verarbeitung für den jeweiligen bestimmten Verarbeitungszweck erforderlich ist, verarbeitet werden. Insbesondere müssen solche Maßnahmen umgesetzt werden, damit personenbezogene Daten durch Voreinstellungen nicht ohne Eingreifen des jeweiligen Nutzers der Software einer unbestimmten Zahl anderer Personen zugänglich gemacht werden, wie es häufig bei Social-Media-Angeboten aber auch Apps, im Rahmen derer man z. B. sein Fitnesslevel mit seinen Freunden vergleichen kann, der Fall ist.

Zusätzlich zu den Anforderungen zur Technikgestaltung und datenschutzfreundlichen Voreinstellung sind auch die anderen vorgenannten Anforderungen der DSGVO für die Entwicklung von Softwarelösungen relevant. U. a. ist sicherzustellen, dass nur diejenigen personenbezogenen Daten verarbeitet werden, die für den Verarbeitungszweck unbedingt erforderlich sind und das Beauskunften an betroffene Personen sowie ggf. das Berichtigen von Daten muss möglich sein. Ebenso ist die Software so zu gestalten, dass eine fristabhängige Löschung einzelner Daten umgesetzt werden kann. Je nach Verarbeitungskontext kann vor dem Anbieten einer Software an Kunden das Durchführen einer Datenschutz-Folgenabschätzung notwendig werden. Auch ist vor dem Anbieten der Software den Informationspflichten nachzukommen usw.

Zwar trifft die Pflicht des Datenschutzes durch Technikgestaltung und der datenschutzfreundlichen Voreinstellungen primär die Verantwortlichen, die die personenbezogenen Daten ihrer Kunden und Mitarbeiter verarbeiten. Jedoch enthält ein Erwägungsgrund der Datenschutz-Grundverordnung eine Art „Aufforderung" an Produktentwickler, dafür Sorge zu tragen, dass die Anforderungen der Datenschutz-Grundverordnung – und insbesondere die Anforderungen an den Datenschutz durch Technikgestaltung und datenschutzfreundliche Voreinstellungen – bereits in der Produktplanung berücksichtigt werden sollten. Das stärkere Argument zur Umsetzung wird vermutlich jedoch der Umstand sein, dass Verantwortliche regelmäßig nur solche Produkte neu beschaffen können, die die Anforderungen der Datenschutz-Grundverordnung umsetzen.

Zusammenfassende Checklisten

Anforderungen an den Umgang mit personenbezogenen (Kunden-)daten

☐ Wurde abgeklärt, ob ein betrieblicher Datenschutzbeauftragte zu bestellen ist und wurde er ggf. bestellt?

☐ Wurde sichergestellt, dass die Datenverarbeitung auf einer gesetzlichen Grundlage oder einer Einwilligung der betroffenen Personen beruht? Werden die Einwilligungen protokolliert und wird die Möglichkeit des Widerrufs der Einwilligung sichergestellt?

☐ Bei Newsletterversand: Basiert die elektronische Einwilligung auf dem Double-Opt-In-Verfahren? Wird die Einwilligung protokolliert und wird in jedem Newsletter die Möglichkeit der Abmeldung vom Newsletter gewährt? Wird eine entsprechende Blacklist geführt?

☐ Wurde vor Verarbeitungsbeginn der rechtmäßige Zweck der Datenverarbeitung festgelegt?

☐ Wurden Maßnahmen ergriffen, die die betroffenen Personen über die Datenverarbeitung vor der Erhebung personenbezogener Daten informieren (u. a. Datenschutzerklärungen auf der Webseite)?

☐ Wurde ein Verzeichnis der Verarbeitungstätigkeiten erstellt (sofern notwendig)?

☐ Wurde die Entscheidung über die Notwendigkeit einer Datenschutz-Folgenabschätzung getroffen, dokumentiert und die Datenschutz-Folgenabschätzung ggf. durchgeführt?

☐ Bei Datenübermittlungen an externe Stellen: Wurde sichergestellt, dass die Übermittlung auf einer gesetzlichen Grundlage oder einer Einwilligung der betroffenen Personen beruht?

☐ Bei Datenübermittlungen an externe Stellen in Drittstaaten: Liegen zusätzlich Garantien für ein angemessenes Datenschutzniveau vor?

- ☐ Bei Auftragsverarbeitung: Wurde der Auftragsverarbeiter sorgfältig ausgewählt und die Auswahl dokumentiert? Wurde mit dem Auftragsverarbeiter ein AV-Vertrag geschlossen?
- ☐ Bei Datenübermittlungen an Auftragsverarbeiter in Drittstaaten: Liegen zusätzlich Garantien für ein angemessenes Datenschutzniveau vor?
- ☐ Wurde die Datenverarbeitung durch angemessene technische und organisatorische Maßnahmen abgesichert?
- ☐ Wurde sichergestellt, dass den Gesuchen betroffener Personen auf u. a. Auskunft, Datenkorrektur und Löschung nachgekommen werden kann?
- ☐ Wurde das Vorgehen bei Datenpannen festgelegt (insb. in Bezug auf die interne Zuständigkeit)?
- ☐ Wurden Lösch- und Aufbewahrungsfristen festgelegt? Wurde sichergestellt, dass sie in technischen Systemen umsetzbar sind?

(Zusätzliche) Anforderungen an die Entwicklung von Softwarelösungen

- ☐ Wurden (zusätzlich zu den o.g. Anforderungen) bei Neuentwicklungen technische und organisatorische Maßnahmen bereits in der Entwicklungsphase berücksichtigt?
- ☐ Wurden datenschutzfreundliche Voreinstellungen getroffen?

Nützliche Links

Rechtmäßigkeit der Verarbeitung
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf

Sonderfall: Rechtmäßigkeit der Verarbeitung für Werbung
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_3.pdf
und
https://www.datenschutzkonferenz-online.de/media/oh/20181107_oh_werbung.pdf

Informationspflichten
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_10.pdf

Speziell zur Informationspflicht bei Videoüberwachung:
https://www.lda.bayern.de/de/videoueberwachung.html

Muster Verfahrensmeldung für Verantwortliche:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Verantwortlicher.docx

Achtung: Auch wenn man selbst als Auftragsverarbeiter arbeitet, fällt man unter die Pflicht zur Dokumentation. In diesem Fall sind jedoch andere Pflichtangaben je Verfahren erforderlich. Ein Muster für Auftragsverarbeiter findet sich hier:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/content-downloads/Muster%20Verarbeitungsverzeichnis%20Auftragsverarbeiter.docx

Übermittlung an externe Stellen
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_4.pdf
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_13.pdf

Hilfe für AV-Vertrag:
https://datenschutz.hessen.de/sites/datenschutz.hessen.de/files/Formulierungshilfe-Auftragsverarbeitungsvertrag%20nach%20DSGVO_0.pdf

Datenschutz-Folgenabschätzung
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_5.pdf

Beantworten von Anträgen zu Betroffenenrechten
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_6.pdf
und
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_11.pdf

Maßnahmenplan „DSGVO“ in Unternehmen:
https://www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_8.pdf

Digital Hub Cybersecurity

Der Digital Hub Cybersecurity ist die führende Innovations-Community für Cybersecurity in Deutschland. Er vernetzt Akteure aus Unternehmen, Forschung und Gründerszene und schafft Aufmerksamkeit bei Influencern, Investoren und Stakeholdern. Der Digital Hub Cybersecurity ist Teil der Digital Hub Initiative des Bundesministeriums für Wirtschaft und Energie und Teil von Athene, dem Nationalen Forschungszentrum für Angewandte Cybersicherheit. Er hat seinen Sitz in Darmstadt und wird vom Fraunhofer SIT, der TU Darmstadt, der IHK Darmstadt sowie der Stadt Darmstadt unterstützt. **www.digitalhub-cybersecurity.com**

Unser Netzwerk

Das Nationale Forschungszentrum für angewandte Cybersicherheit ATHENE ist ein Forschungszentrum der Fraunhofer-Gesellschaft für ihre beiden Darmstädter Institute SIT und IGD unter Beteiligung der Technischen Universität Darmstadt und der Hochschule Darmstadt. Dieses einzigartige und innovative Kooperationsmodell der universitären und außeruniversitären Forschung kombiniert die Kompetenzen und Stärken der Fraunhofer-Institute mit den Kompetenzen und Stärken der Universitäten und ermöglicht Spitzenforschung zum Wohle von Gesellschaft, Wirtschaft und Staat. ATHENE ist das größte Forschungszentrum für angewandte Cybersicherheit und Privatsphärenschutz in Europa. **www.athene-center.de**

Die Digital Hub Initiative trägt zur Transformation Deutschlands als weltweit führenden Digitalstandort bei. Hierfür fördert die Initiative den Aufbau und die Vernetzung zwölf Digitaler Hubs mit spezifischen Themenschwerpunkten. Unter der gemeinsamen Dachmarke de:hub entsteht durch die enge Kooperation zwischen Startups, etablierter Wirtschaft, Forschungseinrichtungen und Experten ein einzigartiges, innovatives Netzwerk. Um Gründer und Investoren aus dem Ausland für den Digitalstandort Deutschland zu gewinnen, werden in den zwölf Hubs konkrete Programme für die Herausforderungen der Digitalisierung entwickelt.

Zu den Digital Hubs zählen Berlin (IoT & FinTech), Dortmund (Logistics), Dresden/Leipzig (Smart Systems & Smart Infrastructure), Frankfurt/Darmstadt (FinTech & Cybersecurity), Hamburg (Logistics), Karlsruhe (Artificial Intelligence), Köln (InsurTech), Mannheim/Ludwigshafen (Digital Chemistry & Digital Health), München (Mobility & InsurTech), Nürnberg/Erlangen (Digital Health), Potsdam (MediaTech) und Stuttgart (Future Industries). Träger der Digital Hub Initiative ist das Bundesministerium für Wirtschaft und Energie. Teil der Digital Hub Initiative sind die Digital Hubs Berlin, Dortmund, Frankfurt a. M. und Darmstadt, Hamburg, Karlsruhe, Köln, Leipzig und Dresden, Ludwigshafen und Mannheim, München, Nürnberg und Erlangen, Potsdam sowie Stuttgart. **www.de-hub.de**

Kontakt

Digital Hub Cybersecurity

Rheinstr. 75 |64295 Darmstadt

Tel. 06151-869-521

Mail: info[at]digitalhub-cybersecurity.com

https://www.digitalhub-cybersecurity.com

Verantwortlich: Ute Richter

Zuletzt aktualisiert November 2019

Grafikdesign: enver@simsek.design

Bildrechte: Umschlag, istock/ A-Basler

Der Digital Hub Cybersecurity wird gefördert aus Mitteln des Landes Hessen.