Erfüllung der DSGVO/GDPR Anforderungen in Spider Produkten

Was ist DSGVO/GDPR und wer ist betroffen?

Ab dem 25. Mai 2018 gilt europaweit die neue Datenschutz-Grundverordnung (abgekürzt als DSGVO oder GDPR). Diese neue Verordnung kommt überall zur Anwendung, wo persönliche Daten von Menschen eingegeben, verarbeitet und gespeichert werden.

Die Verordnung muss bis zum 25. Mai 2018 durch die Unternehmen umgesetzt werden. Die DSGVO betrifft nicht nur Unternehmen innerhalb der EU, sondern auch Unternehmen, die Geschäftsbeziehungen zur EU unterhalten oder Daten von EU-Bürgern verarbeiten. Ebenso betroffen sind Softwareprodukte, die personenbezogene Daten verarbeiten.

Zur Sicherstellung der fristgerechten Umsetzung dieser umfangreichen Herausforderungen bereiten wir uns seit vielen Monaten auf die neue Datenschutz-Grundverordnung vor. Besondere Schwerpunkte liegen in der Sicherstellung der Betroffenenrechte, der Auftragsverarbeitung, den technischen und organisatorischen Maßnahmen sowie der Fähigkeit, erforderliche Dokumentations-, Melde- und Rechenschaftspflichten ordnungsgemäß zu erfüllen.

Bis einschließlich 24. Mai 2018 handeln und agieren wir nach dem noch geltenden Bundesdatenschutzgesetz. Damit erfüllen Spider-Produkte bis zu diesem Zeitpunkt die aktuellen gesetzlichen Vorgaben. Mit Wirkung ab dem 25. Mai 2018 werden wir als Unternehmen, wie auch unsere Produkte, nach neuem Recht konform handeln.

Hinweis für den Leser

Die nachstehenden Ausführungen beziehen sich auf verschiedene Rechtsgrundlagen. Artikel und Paragraphen werden zum Zwecke der Bezugnahme bzw. Herleitung von Erfordernissen benannt bzw. zitiert. Eine gewisse Grundkenntnis hinsichtlich der neuen Rechtsgrundlagen wird vorausgesetzt.

Weitere Informationen zum Thema DSGVO/GDPR sind auf der Webseite der Europäischen Kommission zu finden.

Personenbezogene Daten

Wer sich mit der DSGVO beschäftigt, wird sehr frühzeitig mit der Frage konfrontiert „Was sind personenbezogene Daten?“.

Personenbezogene Daten (Artikel 4 Nr. 1 DSGVO)

In der Begriffsbestimmung der Europäischen Datenschutz-Grundverordnung, im Artikel 4, Nr. 1 DSGVO ist folgende Definition zu finden:

*… „**personenbezogene Daten** sind alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden kann.“*

In Bezug auf die Spider-Produkte bedeutet dies, dass eine Vielzahl von Modulen, Prozessen und Berichten von der Schaffung einer DSGVO-Konformität betroffen sind. Daten, die hingegen keiner Anwendung der DSGVO bedürfen oder anderen Rechtsgrundlagen unterliegen, bleiben von den Änderungen unberührt. Hierzu zählen bspw. Daten juristischer Personen.

Welche Datenkategorien werden in Spider-Produkten verarbeitet?

Innerhalb der Spider-Produkte werden im Produktstandard folgende Datenkategorien verarbeitet:

- Personeninformationen (bspw. Name, Vorname),
- Kontaktinformationen (bspw. E-Mail-Adressen, Telefonnummern),
- Domain-Informationen (bspw. Domain-Login, Active Directory-Kennungen, Last-Login-Benutzer, Hauptbenutzer oder IP-Adressen)
- Und teilweise Betriebsangehörigkeitsinformationen (bspw. Unternehmenseintritt, -austritt oder Personalnummern)

Die konkret vorliegenden Datenfelder für personenbezogene Daten sind bei **individuellen Anpassungen kundenseitig** zu prüfen und zu dokumentieren. Dies gilt insbesondere für die Möglichkeit zusätzlicher Datenkategorien.

Besondere Kategorien personenbezogener Daten (Artikel 9 Abs. 1 DSGVO)

Ergänzend zu den oben genannten Daten spezifiziert die DSGVO im Artikel 9 Abs. 1 besondere Kategorien personenbezogener Daten, deren Verarbeitung im Grundsatz untersagt ist.

Im Standard sind in Spider-Produkten diese besonderen Datenkategorien nicht enthalten.

Kundenindividuelle Erweiterungen prüfen!

Es ist möglich, dass im Rahmen von **kundenindividuellen Anpassungen** personenbezogene Daten besonderer Kategorien zum Gegenstand der Spider-Produkte geworden sind. Dies sind bspw. zusätzliche Felder oder die Einbindung von Drittsystemen mit personenbezogenen Daten besonderer Kategorien. Hier bedarf es einer **kundenindividuellen Betrachtung, Dokumentation und Definition erforderlicher Maßnahmen**, bspw. bei der Verarbeitung von personenbezogener Daten Minderjähriger oder das Verarbeiten zusätzlicher Informationen wie Geburtsdatum oder Konfession. Insbesondere Kunden, die spezifische genetische, biometrische oder anderweitige Gesundheitsdaten bzw. -merkmale mit unseren Produkten erheben, speichern oder verarbeiten, sind hiervon betroffen.

Verarbeitung personenbezogener Daten (Artikel 4 Nr. 2 DSGVO)

Im Rahmen von Risiko- und Compliance-Prüfungen ist ggf. Auskunft über die Verarbeitung von personenbezogenen Daten in Spider-Produkten zu erteilen. Eine Frage nach einer entsprechenden Verarbeitung ist zu bejahen. Die Begriffsbestimmung gemäß Artikel 4 Nr. 2 DSGVO besagt eindeutig:

*„**Verarbeitung**“ ist jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführte Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung.*

In Spider-Produkten werden personenbezogene Daten definierter Datenkategorien verarbeitet. Ohne eine Verarbeitung dieser Daten wären Spider-Produkte nicht funktionsfähig oder würden ihren Zweck erheblich einschränken.

Einschränkung der Verarbeitung (Artikel 4 Nr. 3 DSGVO)

Die Einschränkung der Verarbeitung personenbezogener Daten ist ein zu berücksichtigendes Betroffenenrecht. Allerdings beeinflussen verschiedene Faktoren dieses Betroffenenrecht.

Aufgrund der Sicherstellung der technischen Funktionalitäten und nicht vorhandener Kritikalität in der Verarbeitung der personenbezogenen Daten wird eine Verarbeitungseinschränkung in Spider-Produkten nicht realisiert.

Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5 DSGVO)

Die Spider-Produkte werden für unterschiedliche Geschäftsprozesse eingesetzt. Die Erfüllung der Anforderungen der DSGVO ist von mehreren Faktoren abhängig. Folgende häufige Faktoren seien beispielhaft genannt:

- Art und Ausprägung der begleitenden oder zugrundeliegenden Geschäftsprozesse
- Umfang der kundenindividuellen Erweiterungen oder Ausprägungen im Einsatz der Spider-Produkte
- Grad der Einbindung von personenbezogenen Daten aus Fremdsystemen und der Gestaltung der Schnittstellen

Eine Betrachtung, die nur den Produktstandard umfasst, reicht nicht aus. Eine allgemeine Aussage zur Erfüllung der verschiedenen DSGVO-Anforderungen des Spider-Produktes in einer Kundenumgebung ist aufgrund der flexiblen Anpassungsmöglichkeiten **immer kundenindividuell** zu prüfen. Die Einschätzungen in diesem Dokument beziehen sich auf die grundlegenden Standardfunktionen in den Spider-Produkten.

Die Spider-Produkte werden die verschiedenen DSGVO-Anforderungen gemäß Artikel 5 technisch unterstützen. Neben der reinen Erfüllung der Anforderungen geht es

auch um Einfachheit und das Erzielen zusätzlicher Vorteile, die mit der Umsetzung in den Produkten erreicht wird. Aus den Erfahrungen im Einsatz bei unseren Kunden werden identifizierte Anforderungen und Verbesserungen aufgenommen und in zukünftigen Produktversionen realisiert.

Angemessenheit und Erheblichkeit von personenbezogenen Daten, sowie die Beschränkung derer Verarbeitung auf das notwendige Maß (Artikel 5, Nr. 1, lit. c DSGVO)

In den Produkten sollen nur personenbezogene Daten verarbeitet werden, die für die originären Geschäftsprozesse oder Funktionen erforderlich sind.

Bei kundenindividuellen Anpassungen oder Erweiterungen der Spider-Produkte sowie beim Anbinden von Drittsystemen (bspw. Microsoft Active Directory), die personenbezogene Daten liefern, sind diese Grundsätze individuell zu prüfen und sicherzustellen.

Berichtigung und Löschung personenbezogener Daten (Artikel 5, Nr. 1, lit. d DSGVO)

Grundsätzlich können personenbezogene Daten in Spider gepflegt, geändert und auch gelöscht werden.

Bei Daten, die aus zuliefernden Systemen verwendet werden, ist eine Änderung in Spider i.d.R. nicht möglich, da diese Daten regelmäßig überschrieben werden. Eine Änderung dieser Daten muss in den jeweiligen Quellsystemen erfolgen.

Das Löschen von personenbezogenen Daten, die aus Fremdsystemen angeliefert werden, kann in den Spider-Produkten nicht einheitlich gelöst werden. Bspw. können gesetzliche Löschfristen diese überlagern. Eine verbesserte Unterstützung für das Löschen von nicht mehr angelieferten personenbezogenen Daten ist produktseitig vorgesehen.

Angemessene Speicherung personenbezogener Daten, sowie deren mögliche Anonymisierung (Artikel 5, Nr. 1, lit. e DSGVO).

Für verwaltete personenbezogene Daten, die keine Abhängigkeit zu zuliefernden Systemen haben und die für den originären Geschäftsprozess nicht mehr als erforderlich gelten (bspw. Unternehmensaustritt eines Mitarbeiters), stehen Löschfunktionen zur Verfügung. In zukünftigen Versionen werden Funktionen zur Anonymisierung bspw. für statistische Zwecke bereitgestellt, was eine Alternative zum physischen Löschen darstellt.

Schutz und Sicherheit personenbezogener Daten mittels technischer und organisatorischer Maßnahmen zur Wahrung derer Integrität und Vertraulichkeit (Artikel 5, Nr. 1 lit. f DSGVO)

Die Sicherheit von personenbezogenen Daten wird über Berechtigungskonzepte und der Trennung personenbezogener Daten von sonstigen Prozessdaten sichergestellt.

Zusätzliche, geeignete technische und organisatorische Maßnahmen sind kundenseitig zu treffen.

Geeignete Möglichkeiten zum Nachweis der Einhaltung der oben genannten Punkte im Rechenschaftsfall (Artikel 5, Nr. 2 DSGVO)

Änderungen an personenbezogenen Daten können über Änderungsprotokolle eingesehen werden, für die separate Berechtigungen erteilt werden können. In zukünftigen Produktversionen werden Verbesserungen für die Auswertung zum Nachweis vorgesehen.

Rechtmäßigkeit der Verarbeitung (Artikel 6 DSGVO)

Die Rechtmäßigkeit der Verarbeitung personenbezogener Daten in Spider-Produkten bedingt sich durch die Rechtsgrundlagen gemäß folgender Artikel:

Artikel 6, Nr. 1, lit. c DSGVO

"Die Verarbeitung ist zur Erfüllung einer rechtlichen Verpflichtung erforderlich, der der Verantwortliche unterliegt."

Artikel 6, Nr. 1, lit. f DSGVO

„Die Verarbeitung ist zur Wahrung der berechtigten Interessen des Verantwortlichen oder eines Dritten erforderlich, sofern nicht die Interessen oder Grundrechte und Grundfreiheiten der betroffenen Person, die den Schutz personenbezogener Daten erfordern, überwiegen, insbesondere dann, wenn es sich bei der betroffenen Person um ein Kind handelt.“

Beide Passagen beziehen sich im Schwerpunkt hierbei implizit auf Pflichten aus dem BGB, HGB, UWG und UrhG.

Bedingungen für die Einwilligung (Artikel 7 DSGVO)

Erfolgt mittels Software beim Betroffenen direkt eine Erhebung von personenbezogenen Daten, so werden technische Möglichkeiten zur Erteilung von Einwilligungen, deren Protokollierung und deren Erläuterung erforderlich. Auch ein Widerruf der Einwilligung wird unter den genannten Voraussetzungen benötigt.

Self-Service-Funktionen

Self-Service-Funktionen, bei denen ein Benutzer (Betroffener im Sinne der DSGVO) direkt seine personenbezogenen Daten erfasst, müssen die Bedingungen zur Einwilligung berücksichtigen. Im Produktstandard findet in den Spider-Produkten keine direkte Erhebung der Daten durch den Betroffenen selbst statt. Der größte Teil der personenbezogenen Daten wird aus Fremdsystemen beigestellt und in Spider-Produkten verarbeitet. Sollten durch **kundenindividuelle Erweiterungen** Self-Service Funktionen möglich sein, müssen kundenseitig geeignete Maßnahmen zur Erfüllung der Anforderungen getroffen werden. Bei der Verarbeitung von Beschäftigungsdaten (bspw. Microsoft Active Directory) können Einwilligungen über die begleitenden kundenseitigen Verarbeitungsprozesse oder vorgelagerte Informationsprozesse abgebildet werden.

Einwilligung bei personenbezogenen Daten aus Fremdsystemen oder für die Erhebung zusätzlicher Daten

Bei der Zulieferung von personenbezogenen Daten aus Drittsystemen (bspw. Microsoft Active Directory) obliegt die Einholung einer Einwilligung der hierfür verantwortlichen Stelle.

Für zusätzliche personenbezogene Daten, die in Spider eingegeben und verarbeitet werden, ist eine Einwilligung der Betroffenen erforderlich. Dies ist in den begleitenden kundenseitigen Verarbeitungsprozessen sicherzustellen.

Informationspflicht (Artikel 13 und 14 DSGVO)

Bei der direkten und indirekten Erhebung personenbezogener Daten existiert eine Informationspflicht gegenüber dem Betroffenen.

Die Erfüllung einer aktiven Informationspflicht kann mit den aktuellen Produktversionen über kundenindividuelle Einstellungen und Erweiterungen erfolgen. Häufig werden zur Information der Betroffenen E-Mail-basierte Informationsverfahren eingesetzt. Grundsätzlich stellt sich die Frage, ob überhaupt eine aktive Benachrichtigung der Betroffenen aus den Spider-Produkten sinnvoll ist, da die Produkte i.d.R. für dedizierte Teilaufgaben eingesetzt werden und indirekt die prozessrelevanten personenbezogenen Daten aus Fremdsystemen nutzten.

Verarbeitung von Beschäftigungsdaten

Für die häufig anzutreffende Verarbeitung von Beschäftigungsdaten (bspw. aus Microsoft Active Directory) empfehlen wir die Erfüllung der Informationspflicht in den begleitenden kundenseitigen Verarbeitungsprozessen oder vorgelagerten Informationsprozessen sicherzustellen.

Direkte Benachrichtigung der Betroffenen

Sofern eine direkte Benachrichtigung der Betroffenen aus den Spider-Systemen dennoch erforderlich sein sollte, sind die konkreten Informationsprozesse kundenindividuell abzubilden. Zukünftige Produktversionen werden die Möglichkeiten zur Bereitstellung von Erklärungen zur Erfüllung von Informationspflichten weiter verbessern.

Auskunftsrecht (Artikel 15 DSGVO)

Betroffene Personen haben ein generelles Auskunftsrecht, wenn ihre personenbezogenen Daten verarbeitet werden.

Das Auskunftsrecht kann mit den heutigen Produktversionen grundsätzlich erfüllt werden. Unterstützend werden wir Dokumentationen und Berichte zur Erfüllung der Auskunftspflicht bereitstellen.

In zukünftigen Produktversionen werden Funktionen erweitert, die eine einfache Möglichkeit zur Bereitstellung von Erklärungen zur Erfüllung von Informationspflichten bereitstellen.

Recht auf Berichtigung (Artikel 16 DSGVO)

In Spider-Produkten bestehen grundsätzlich Berichtigungsmöglichkeiten für personenbezogene Daten. Diese können über das Berechtigungskonzept definierten Berechtigungsgruppen vorbehalten sein.

Bei Zulieferung von personenbezogenen Daten aus Drittsystemen sind die Berichtigungen im Drittsystem durchzuführen. Änderungen an personenbezogenen Daten gelten nur ab dem Zeitpunkt der Eingabe bzw. Übernahme. Änderungshistorien sind demnach ausgenommen.

Recht auf Löschung (Artikel 17 DSGVO)

In Spider-Produkten bestehen grundsätzlich Löschmöglichkeiten für personenbezogene Daten. Diese können über das Berechtigungskonzept definierten Berechtigungsgruppen vorbehalten sein.

Besonderheit bei personenbezogenen Daten aus angebundenen Drittsystemen

Bei Zulieferung von personenbezogenen Daten aus Drittsystemen ist die Löschung im Drittsystem durchzuführen. Das Löschen von personenbezogenen Daten, die aus Fremdsystemen angeliefert werden, kann in den Spider-Produkten nicht einheitlich und damit nicht im Produktstandard gelöst werden. Bei der Löschung von personenbezogenen Daten sind u.a. gesetzliche Aufbewahrungsfristen zu berücksichtigen. Demnach ist abhängig von den eingebundenen Drittsystemen und der Art des Geschäftsprozesses die Umsetzung für das Löschen zu gestalten.

Recht auf Einschränkung der Verarbeitung (Artikel 18 DSGVO)

Da eine Rechtmäßigkeit der Verarbeitung u.a. gemäß Artikel 6, Nr. 1, lit. f DSGVO vorausgesetzt wird und somit berechtigte Gründe das Recht auf Einschränkung überwiegen dürften, werden keine dedizierten technischen Maßnahmen ergriffen.

Mitteilungspflicht (Artikel 19 DSGVO)

Die Mitteilungspflicht bei Veränderung von personenbezogenen Daten sind in den begleitenden kundenseitigen Verarbeitungsprozessen (bspw. Account Management) zu berücksichtigen. Sofern eine automatische Mitteilung aus Spider-Produkten gewünscht wird, kann dies über eine Erweiterung und Einrichtung der Spider-Produkte realisiert werden.

Recht auf Datenübertragbarkeit (Artikel 20 DSGVO)

Eine Datenübertragbarkeit der personenbezogenen Daten ist nicht relevant, da Spider-Produkte ausschließlich für interne Unternehmensprozesse und -systeme eingesetzt werden.

Widerspruchsrecht (Artikel 21 DSGVO)

Da eine Rechtmäßigkeit der Verarbeitung u.a. gemäß Artikel 6, Nr. 1, lit. f DSGVO vorausgesetzt wird und somit berechtigte Gründe das Recht auf Widerspruch überwiegen dürften, werden keine technischen Maßnahmen ergriffen.

Datenschutz durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen (Artikel 25 DSGVO)

Spider-Produkte und eingesetzte Infrastrukturprodukte (bspw. Microsoft SQL Server) beinhalten verschiedene technische Funktionalitäten zur Unterstützung technischer und organisatorischer Maßnahmen.

Die konkreten technischen und organisatorischen Maßnahmen sind kundenindividuell zu treffen. Spider-Produkte werden mit begleiteten Dokumentationen und Empfehlungen unterstützten.

Verzeichnis von Verarbeitungstätigkeiten (Artikel 30 DSGVO)

Zur Erfüllung der Dokumentationspflichten gemäß Artikel 30 DSGVO ist u.a. ein Verzeichnis aller Verarbeitungstätigkeiten mit personenbezogenen Daten zu führen.

Für die Spider-Produkte werden standardisierte und modifikationsfähige Vorlagen für ein Verarbeitungsverzeichnis bereitgestellt. Der kundenseitige Verwendungszweck und Erweiterungen sind zu ergänzen.

Hintergrund

Der Aufsichtsbehörde muss das Verzeichnis der Verarbeitungstätigkeiten auf Anfrage zur Verfügung gestellt werden (Artikel 30 Abs. 4 DSGVO und Erwägungsgrund 82). Unternehmen, die der deutschen behördlichen Aufsicht unterstehen, müssen das Verarbeitungsverzeichnis in deutscher Sprache führen (§23 Abs. 1 und 2 Verwaltungsverfahrensgesetz VwVfG).

Eine Ausnahme gemäß Artikel 30 Abs. 5 DSGVO ist auszuschließen, selbst wenn der quantitative Faktor von weniger als 250 Mitarbeiter gegeben ist. Dieses begründet sich in den erforderlichen IT-Protokollierungen, die wesentlich für die Funktionsweise der Spider-Produkte notwendig sind.

Stand April 2018

brainwaregroup

Spider Lifecycle Managementsysteme GmbH

Paul Dessau Str. 8, 22761 Hamburg