



Leitfaden

Umsetzung der datenschutzrechtlichen Anforderungen bei
der Implementierung einer Customer Data Platform (CDP)



Im Marketing dreht sich seit einigen Jahren alles intensiv um Personalisierung und Customer Experience. Ein wichtiges Instrument, um diese beiden Erfolgsfaktoren zu nutzen, sind Customer Data Platforms (CDP). CDPs ermöglichen es Unternehmen, Kundendaten effektiv, über verschiedene Quellen, Kanäle und Gesellschaften eines Konzerns hinweg, zu sammeln, zu verwalten und zu nutzen. Durch die damit einhergehende 360-Grad-Sicht auf die Kunden kann ein besseres Kundenverständnis aufgebaut und gleichzeitig die Erwartung der Kunden passgenauer erfüllt werden. Die Marketing-Ansprache kann auf den Kunden zugeschnitten und individualisiert erfolgen.

Bei der Implementierung von CDPs sind mehrere Aspekte zu berücksichtigen. Neben der technologischen Ausgestaltung (Auswahl der Technologie und Integration in die bestehende IT-Infrastruktur) und der Entwicklung der Marketingstrategie sowie der Definition von Marketing Use Cases müssen insbesondere die (datenschutz-)rechtlichen Anforderungen beachtet werden.

Verstöße gegen diese Anforderungen können nicht nur zu rechtlichen Konsequenzen führen, sondern auch das Vertrauen der Kunden beeinträchtigen und letztlich durch Abwanderung von Kunden den Umsatz negativ beeinflussen.¹

Mit unserer multidisziplinären Erfahrung in der Implementierung von CDPs unterstützen wir als renommiertes Beratungsunternehmen, wenn es darum geht, die (datenschutz-)rechtlichen Anforderungen bei der CDP-Implementierung zu prüfen.

Um Unternehmen bei dieser Herausforderung zu helfen, stellen wir Ihnen mit diesem Paper eine Checkliste zur Verfügung, die Ihnen sowohl als Fachbereich, aber auch als Rechtsabteilung dabei hilft, die (datenschutz-)rechtlichen Anforderungen im Rahmen der CDP-Implementierung zu prüfen. Unsere Checkliste dient als Leitfaden für zwei Anwendungsfälle:

1. Vor der Implementierung, um sicherzustellen, dass Ihr Unternehmen angemessene Maßnahmen ergreift, um die (datenschutz-)rechtlichen Anforderungen zu erfüllen.
2. Während bzw. nach der Implementierung, um festzustellen, ob Ihr Unternehmen alle angemessenen Maßnahmen ergriffen und rechtskonform umgesetzt hat.

Unser Ziel ist es, Ihnen dabei zu helfen, Ihre CDP-Implementierung auf eine solide rechtliche Grundlage zu stellen und das Vertrauen Ihrer Kunden zu wahren. Nachfolgend finden Sie drei Kategorien mit Prüfungsthemen inklusiv Beispielbeschreibungen.

¹ Insbesondere „Privacy as an Enabler of Customer Trust“, Cisco 2024 Data Privacy Benchmark Study (<https://www.cisco.com/c/en/us/about/trust-center/data-privacy-benchmark-study.html#~key-findings>), „Data Transparency’s Essential Role in Building Customer Trust“ Cisco 2022 CONSUMER PRIVACY SURVEY, (https://www.cisco.com/c/dam/en_us/about/doing_business/trust-center/docs/cisco-consumer-privacy-survey-2022.pdf)



I. Relevante (Datenschutz-)Gesetze, aus denen sich Anforderungen in Bezug auf die Implementierung einer CDP ergeben (z. B. UWG, CCAP)

1. Prüfen Sie, in welchen Ländern Ihr Unternehmen/Ihre Unternehmensgruppe Gesellschaften hat und welche (länderspezifischen) Gesetze bei der Implementierung einer CDP berücksichtigt werden müssen.

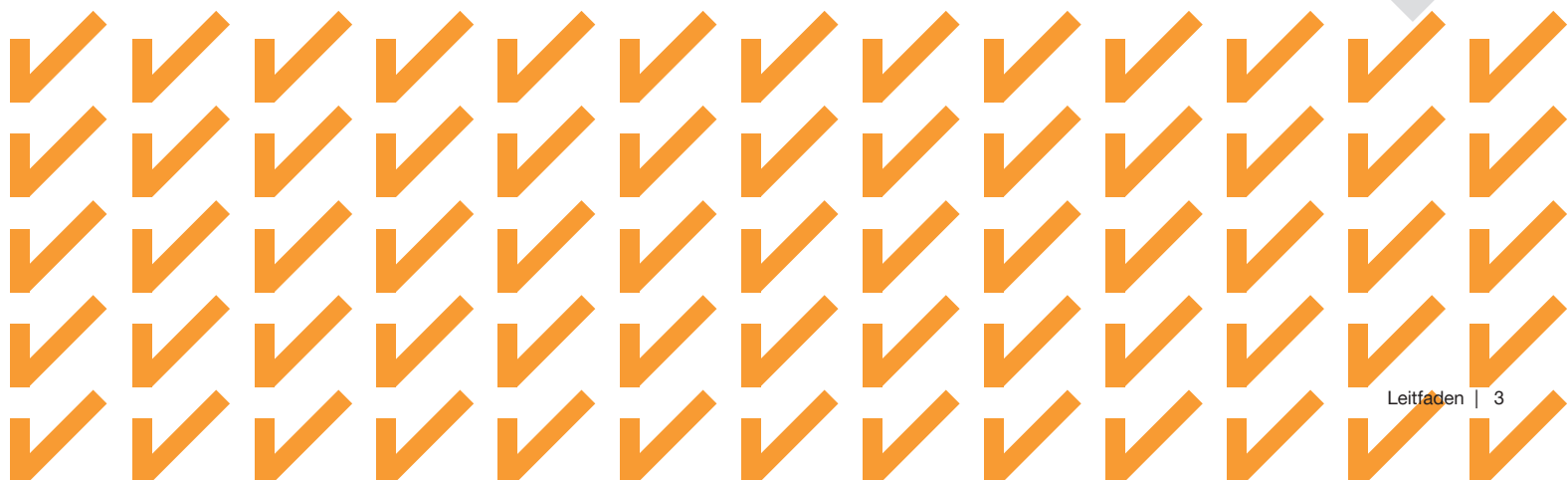
Zum Beispiel:

Bei einer juristischen Person in Deutschland müssen mindestens die Anforderungen aus der DS-GVO, des UWG und des TTDSG sowie – je nach Einzelfall – weitere Gesetze bei der Umsetzung berücksichtigt werden.

-
2. Stellen Sie sicher, dass die branchenspezifischen regulatorischen Anforderungen bei der Implementierung berücksichtigt werden.

Zum Beispiel:

Berücksichtigung der Geheimhaltungspflicht nach §203 StGB in der Versicherungsbranche.



I I. Zweckbindung, Einwilligungserfordernis und Opt-in/Opt-out-Mechanismen

1. Prüfen Sie, zu welchem Zweck Sie die personenbezogenen Daten in der CDP verarbeiten möchten und auf welche Rechtsgrundlagen die jeweilige Datenverarbeitung unter Berücksichtigung des zuvor definierten Zwecks gestützt werden kann.

Zum Beispiel:

Der Zweck des Zusammenfügens der personenbezogenen Daten ist die Erstellung eines 360°-Profils; dies ermöglicht die Ausspielung passgenauer Werbung gegenüber dem Kunden. Als Rechtsgrundlagen können sowohl Art. 6 Abs. 1 lit. f) DS-GVO („berechtigzte Interessen“) sowie Art. 6 Abs. 1 lit. a) DS-GVO („Einwilligung“) in Betracht kommen. Es müsste detailliert geprüft werden, ob die Datenverarbeitung „noch“ auf Art. 6 Abs. 1 lit. f) DS-GVO gestützt werden kann oder eine Einwilligung eingeholt werden muss.

-
2. Der Hauptzweck einer CDP besteht darin, personenbezogene Daten aus verschiedenen Quellen (z. B. Vertragsdatenbank, Website) sowie ggfs. auch aus verschiedenen Gesellschaften eines Konzerns zusammenzufügen und damit ein 360°-Profil des Kunden zu erstellen. Prüfen Sie, ob es sich dabei um ein Profiling im Sinne des Art. 4 Nr. 4 DS-GVO (jede Art der automatisierten Verarbeitung personenbezogener Daten, um auf dessen Grundlage bestimmte persönliche Aspekte zu bewerten) handelt. Falls ja, prüfen Sie weiter, ob es sich dabei um ein Profiling nach Art. 22 DS-GVO handelt und daraus Entscheidungen resultieren, die entweder für den Betroffenen eine rechtliche Wirkung entfalten oder ihn in ähnlicher Weise erheblich beeinträchtigen können. Sollten Sie beides bejahen, kommt als Rechtsgrundlage voraussichtlich die Einwilligung nach Art. 6 Abs. 1 lit. a) DS-GVO in Betracht.

Zum Beispiel:

Ein Profiling im Sinne des Art. 22 DS-GVO wird voraussichtlich vorliegen, wenn sich dieses auf die finanzielle Lage einer Person, ihren Zugang zu Gesundheitsdienstleistungen, einem Arbeitsplatz oder Bildung auswirkt.

Achtung: Diese beispielhafte Einschätzung ersetzt keine Bewertung des konkreten Einzelfalles.

-
3. Sofern Sie feststellen, dass die erforderliche(n) Einwilligung(en) derzeit (noch) nicht eingeholt werden, stellen Sie sicher, dass die entsprechenden Einwilligungen der Kunden eingeholt werden, bevor die personenbezogenen Daten in die CDP übertragen und mit weiteren Daten zusammengeführt werden.

Zum Beispiel:

Entwerfen Sie eine datenschutzkonforme Einwilligung, die die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Gesellschaften in einer CDP zum Gegenstand hat und implementieren Sie diese an den relevanten Kunden-Touchpoints. Stellen Sie ggfs. sicher, dass diese Einwilligung in das vorhandene Consent-Management-System überführt wird, so dass sich das ggfs. mit dem Consent-Management-System verbundene CDP an der jeweils erforderlichen Einwilligung bedienen kann.

4. Stellen Sie sicher, dass die Einwilligungen datenschutzrechtskonform ausgestaltet sind/ werden und die für eine CDP relevanten Verarbeitungsvorgänge, wie die Zusammenführung von personenbezogenen Daten aus verschiedenen Quellen und Konzerngesellschaften bzw. die Bereitstellung der personenbezogenen Daten gegenüber verschiedenen Konzerngesellschaften, darüber legitimiert werden können. Maßgeblich ist dabei insbesondere der Grundsatz der Transparenz. Nur wenn dieser gewahrt wird, können die Kunden die Einwilligung informiert, in Kenntnis aller Umstände, und damit rechtmäßig erteilen.

Zum Beispiel:

Eine Einwilligung im Kontext einer CDP genügt dann dem Transparenzgrundsatz und kann informiert erteilt werden, wenn der Kunde alle Umstände im Kontext der Einwilligung zur Zusammenführung der personenbezogenen Daten/ Profiling erhält, um überhaupt in der Lage zu sein, einen freien Willen zu bilden und in der Folge die Entscheidung über die Einwilligung zu treffen; insbesondere Umfang und Tragweite der Einwilligung müssen dem Einwilligenden bewusst sein. Es muss ihm erläutert werden, wofür seine Daten im Rahmen des Profilings genau verwendet werden.



5. Überprüfen Sie, ob die CDP-Optionen für die Verwaltung von Einwilligungen und Widerruf der Kunden sowie Aktualisierung von Einwilligungen bietet.

Zum Beispiel:

In welcher Regelmäßigkeit werden die Einwilligungen aktualisiert? Gibt es Schnittstellen zu einem Consent-Management-System?

6. Stellen Sie sicher, dass nur die personenbezogenen Daten zusammengefügt werden, für die unter Berücksichtigung der zuvor definierten Zwecke eine datenschutzrechtliche Rechtsgrundlage besteht und diese daher zusammengefügt werden dürfen.

Zum Beispiel:

Stellen Sie sicher, dass die ausgewählte CDP die technische Möglichkeit besitzt, die Daten unterschiedlicher juristischen Personen zu trennen (Mandantentrennung). Mögliche technische Maßnahmen dahingehend, können eine applikationsseitige Trennung, Trennung der Datenhaltung und mandantenspezifische Accounts für den jeweiligen Datenzugriff, physische oder virtuelle Trennung der Umgebung sowie Authentifizierungsverfahren oder eine mandantenspezifische Verschlüsselung sein. Maßgeblich sind jedoch der Einzelfall und der individuelle Schutzbedarf der personenbezogenen Daten.



III. Weitergehende Anforderungen aus der DS-GVO 1/4

1. Datenminimierung und Rollen-/Berechtigungskonzept:
 - a) Stellen Sie organisatorisch sicher, dass die Daten nur für die zuvor definierten Zwecke von den dafür berechtigten Mitarbeitern und Gesellschaften genutzt werden und nicht „unbefugt“ weiterverarbeitet werden.

Zum Beispiel:

Stellen Sie Data Governance Rules bereit, die darstellen, unter welchen Bedingungen die verfügbaren Daten in Ihrer CDP verwendet werden dürfen. Unter Data Governance Rules sind interne Standards bzw. Datenrichtlinien für die Erfassung, Speicherung, Verarbeitung und Löschung von (personenbezogenen) Daten zu verstehen. Data Governance umfasst die Prozesse und Verantwortlichkeiten, die für die Qualität und Sicherheit der in einem Unternehmen genutzten (personenbezogenen) Daten relevant sind. Unternehmen können damit festlegen, wer welche (personenbezogene) Daten in welchen Situationen und mit welchen Methoden nutzen kann.

- b) Stellen Sie technisch sicher, dass auf die personenbezogenen Daten in der CDP nur Mitarbeitende Zugriff nehmen können, die dazu entsprechend berechtigt sind und ergänzen Sie Mechanismen, die eine Verwendung der Daten zu anderen Zwecken unterbindet. Schützen Sie die personenbezogenen Daten ausreichend vor unbefugtem Zugriff.

Zum Beispiel:

Implementieren Sie ein Rollen- und Berechtigungskonzept und berücksichtigen dabei die Grundsätze der Zweckbindung und Datenminimierung („Need-to-Know“ Prinzip). Einige Anbieter bieten die Funktion der Kennzeichnung von Daten in der CDP an. Diese Kennzeichnung und Klassifizierung ermöglicht es, Unternehmensrichtlinien, vertragliche Verpflichtungen, Compliance-Anforderungen und regionale Vorschriften in der CDP zu berücksichtigen und die erweiterte Datennutzung unabhängig vom zuvor festgelegten oder erlaubten Zweck automatisch zu unterbinden.

2. Betroffenenrechte:

- a) Prüfen Sie je Gesellschaft und Staat, welche nationalen Besonderheiten in Bezug auf die Betroffenenrechte von Kunden bei der Verarbeitung von personenbezogenen Daten in einer CDP berücksichtigt werden müssen.

Beispiel: In Deutschland ergibt sich beispielsweise das Recht auf Auskunft, Berichtigung, Löschung aus der DS-GVO sowie dem BDSG. Aus dem BDSG ergeben sich Ausnahmetatbestände, die unter Umständen Anwendung finden können. In Kalifornien existiert im CCPA und CPRA ein sehr weitgehendes Recht auf Datenlöschung (auch Dritte müssen über das Löschersuchen informiert werden).

- b) Überprüfen Sie, ob die CDP die Ausführung der relevanten Betroffenenrechte, insbesondere der Widerruf der Einwilligung und das Auskunftersuchen, sicherstellen kann.

Zum Beispiel:

Können die Anfragen der Betroffenen im User Interface der CDP oder zum Beispiel auch mittels API technisch umgesetzt werden? Können Einwilligung auch nur teilweise widerrufen und dies in der CDP entsprechend berücksichtigt werden?

3. (Internationale) Datenübermittlung:

- a) Prüfen Sie, ob die Übermittlung von personenbezogenen Daten innerhalb der CDP an andere Konzernunternehmen oder auch an Dritte (z. B. Service Provider, Cloud-Anbieter) den (datenschutz-)rechtlichen Anforderungen entspricht.

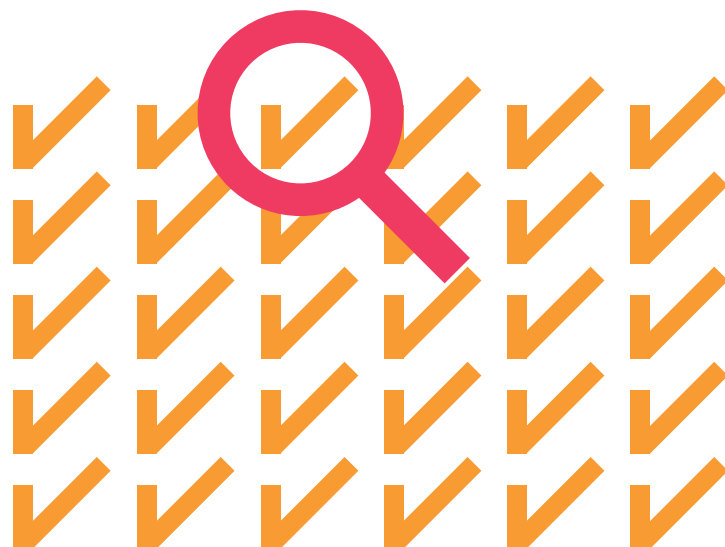
Zum Beispiel:

Prüfen Sie die Lage des Cloud Servers. Prüfen Sie, ob Konzernunternehmen, die Teil der CDP sind, außerhalb der EU ansässig sind.

- b) Stellen Sie sicher, dass bei Datenübermittlungen an Unternehmen außerhalb der EU ein angemessenes Datenschutzniveau besteht bzw. geeignete Garantien zum Einsatz kommen.

Zum Beispiel:

Die Konzernunternehmen, die eine CDP gemeinsam nutzen, müssen untereinander EU-Standardvertragsklauseln (EU SCC) abgeschlossen haben.



III. Weitergehende Anforderungen aus der DS-GVO 2/4

4. Auftragsverarbeitungsvertrag (AVV):

Stellen Sie sicher, dass mit jedem Dienstleister, der Zugriff auf die personenbezogenen Daten auf der CDP hat und dabei die personenbezogenen Daten nur nach Weisung des auftraggebenden Unternehmens verarbeitet, ein schriftlicher Auftragsverarbeitungsvertrag geschlossen wird/ist.

Zum Beispiel:

Die CDP ist eine SaaS-Lösung und der CDP-Anbieter verarbeitet die personenbezogenen Daten nur auf Weisung des auftraggebenden Unternehmens. Mit dem CDP-Anbieter muss entsprechend ein AVV geschlossen werden.

5. Datenretention und Löschkonzepte:

a) Prüfen Sie, welche (gesetzlichen oder betrieblichen) Aufbewahrungsfristen für die jeweils gespeicherten Datenkategorien relevant sind und bewerten Sie, wann die Daten aus der CDP gelöscht oder anonymisiert werden müssen.

Zum Beispiel:

Daten, die auf Basis einer Einwilligung verarbeitet werden, müssen ggfs. unmittelbar nach Widerruf der Einwilligung gelöscht oder anonymisiert werden. Je nach Datenkategorie und Zweck, der mit der weiteren Aufbewahrung verfolgt wird, wäre es denkbar, (Teile der) personenbezogenen Daten für einen konkret definierten Zeitraum, bspw. 180 Tage, aufzubewahren und anschließend automatisiert zu löschen. In jedem Fall ist eine Einzelfallprüfung erforderlich.

b) Stellen Sie (technisch) sicher, dass die personenbezogenen Daten entsprechend der zuvor definierten Aufbewahrungs-/Löschfristen auch tatsächlich aus der CDP gelöscht werden.

Zum Beispiel: Verwendung von APIs die automatisch die Löschung der Daten in der CDP ermöglichen, wenn eine Einwilligung entzogen wird.



III. Weitergehende Anforderungen aus der DS-GVO 3/4

6. Minderjährigenschutz

- a) Prüfen Sie, ob von Ihrem Unternehmen angebotene Dienste als „Dienste der Informationsgesellschaft“ im Sinne von Art. 4 Nr. 25 DS-GVO gewertet werden und zumindest auch von Minderjährigen (unter 16 Jahren) genutzt werden können.

Zum Beispiel:

Solche Dienste können Leistungen wie Online-Informationsangebote oder Werbung, Werkzeuge für die Informationssuche, den Zugang zu Daten und deren Abruf sowie Videoabruf (Video-on-demand) oder das Versenden von Werbung per E-Mail (Newsletter) sein. Diese Leistungen können unter Umständen nach der Zusammenführung von Daten in der CDP bezweckt sein.

- b) Sofern Sie festgestellt haben, dass Ihr Unternehmen „Dienste der Informationsgesellschaft“ anbieten, die von Minderjährigen (unter 16 Jahren) genutzt werden können, stellen Sie sicher, dass Ihr Unternehmen zur Legitimation der Datenverarbeitung im Zusammenhang mit dem jeweiligen Dienst von den Sorgeberechtigten die Einwilligung einholen oder zumindest die Zustimmung erhalten können (Art. 8 DS-GVO). Sehen Sie dafür ein entsprechendes Verfahren vor.

Zum Beispiel:

Fragen Sie auf der Website das Alter des Kunden ab („Sind Sie unter 16 Jahre?“). Sofern der Kunde angibt, dass er „unter 16 Jahren“ ist, könnte als zusätzlicher Schritt im Rahmen eines Bestätigungsprozesses die elterliche E-Mail-Adresse abgefragt werden, ähnlich wie bei einem Double-Opt-In-Verfahren bei der Newsletter-Anmeldung. Anschließend erhält der Sorgeberechtigte eine E-Mail, welche die wesentlichen Informationen zur Datenverarbeitung beinhaltet. Hierzu gehören zwingend die personenbezogenen Daten des Kindes, Kontaktdaten des Verantwortlichen sowie der Umfang der Datenverarbeitung. Aufgrund dessen steht es dem Sorgeberechtigten frei, die E-Mail zu bestätigen und somit seine Einwilligung zur Datenverarbeitung zu erteilen. Das Verfahren sollte von der Sensibilität der zu verarbeitenden Daten und dem jeweiligen Verarbeitungszweck abhängig gemacht werden.

Achtung: Diese beispielhafte Einschätzung ersetzt keine Bewertung des konkreten Einzelfalles.

- c) Art. 8 DS-GVO regelt den o.g. Spezialfall. Sofern keine „Dienste der Informationsgesellschaft“ im Zusammenhang mit der Datenverarbeitung stehen, können die allgemeinen Rechtsgrundlagen aus Art. 6 Abs. 1 DS-GVO für die Verarbeitung von personenbezogenen Daten von Minderjährigen in Betracht kommen. Prüfen Sie daher genau, ob beispielsweise eine Interessenabwägung nach Art. 6 Abs. 1 lit. f DS-GVO unter Beachtung des besonderen Schutzbedürfnisses von Minderjährigen gelingen oder der Minderjährige nach Art. 6 Abs. 1 lit. a) DS-GVO in die Zusammenführung der personenbezogenen Daten unter Berücksichtigung der Einsichtsfähigkeit selbst einwilligen kann.

Zum Beispiel:

Im Zusammenhang mit einer CDP könnte beispielsweise die Weitergabe von Kundendaten – auch von Minderjährigen – an weitere Konzerngesellschaften die Interessenabwägung nach Art. 6 Abs. 1 lit. f) DS-GVO als Rechtsgrundlage in Betracht kommen. Im Rahmen der Interessenabwägung muss dabei dem Minderjährigen ein besonders hohes Schutzinteresse gewährt werden.

Achtung: Diese beispielhafte Einschätzung ersetzt keine Bewertung des konkreten Einzelfalles.

- d) Sofern Sie festgestellt haben, dass personenbezogene Daten auch von Minderjährigen auf der CDP zusammengeführt und zu weiteren Zwecken verarbeitet werden, prüfen Sie die relevanten Datenschutzinformationen nach Art. 13, 14 DS-GVO dahingehend, ob sie für den Minderjährigen einfach und verständlich sind und er insbesondere den Umfang der Datenverarbeitung hinreichend erkennen kann. Passen Sie die Datenschutzinformationen ggfs. an.

Zum Beispiel:

Für Websites, die sich zumindest auch an Minderjährige richten, bedeutet dies, dass die Datenschutzinformationen in einer kindgerechten, einfachen Sprache abgefasst werden müssen.

III. Weitergehende Anforderungen aus der DS-GVO 4/4

7. Auditierbarkeit und Dokumentation:

- a) Stellen Sie sicher, dass die CDP entsprechende Funktionalitäten zur Erstellung von Audit-Trails vorsieht.

Zum Beispiel:
Protokollierung von Datenzugriffen und -änderungen je CDP-User.

- b) Stellen Sie sicher, dass die Verarbeitungstätigkeiten, die im Zusammenhang mit der CDP stehen, in dem Verarbeitungsverzeichnis Ihres Unternehmens entsprechend der Anforderungen aus Art. 30 DS-GVO dokumentiert werden. Prüfen Sie bereits vorhandene Dokumentationen auf Aktualität.

Zum Beispiel:
Das Verarbeitungsverzeichnis enthält Informationen über die Art der verarbeiteten Daten, den Zweck der Verarbeitung, die Kategorien von betroffenen Personen und Empfängern der Daten sowie die geplanten Löschrufen.

8. Datenschutz-Folgenabschätzung:

Prüfen Sie, ob eine Datenschutz-Folgenabschätzung (DSFA) erforderlich ist und führen Sie diese - sofern erforderlich - durch, um potenzielle Risiken für die Rechte und Freiheiten der Betroffenen zu identifizieren und geeignete Maßnahmen zur Risikominimierung zu ergreifen.

Zum Beispiel:
Big-Data-Analyse von Kundendaten, die mit Angaben aus Drittquellen angereichert wurden, erfordern nach Auffassung der DSK (Datenschutzkonferenz - Konferenz der unabhängigen Datenschutzaufsichtsbehörden des Bundes und der Länder) immer die Durchführung einer DSFA.

9. Datensicherheit:

- a) Prüfen Sie die Sicherheitsmaßnahmen, insbesondere die technischen und organisatorischen Maßnahmen, der CDP, um sicherzustellen, dass die Kundendaten angemessen geschützt sind.

Zum Beispiel:
Der CDP-Anbieter ist ISO 27001 zertifiziert.

- b) Stellen Sie sicher, dass die Daten während der Übertragung und Speicherung verschlüsselt sind.

Zum Beispiel:
Datenübertragung basierend auf Verschlüsselungsmechanismen mit Hilfe eines SFTP.

- c) Prüfen Sie, ob je nach Zweck der Datenverarbeitung, bestimmte Datenkategorien pseudonymisiert werden könnten.

Zum Beispiel:
Datensätze werden im Rahmen des Listenverfahrens anhand einer Tabelle bestimmten Pseudonymen zugeordnet. Hierbei ist darauf zu achten, dass kein direkter Bezug zu den Daten hergestellt wird.



Sind Sie bereit für eine erfolgreiche CDP-Implementierung?

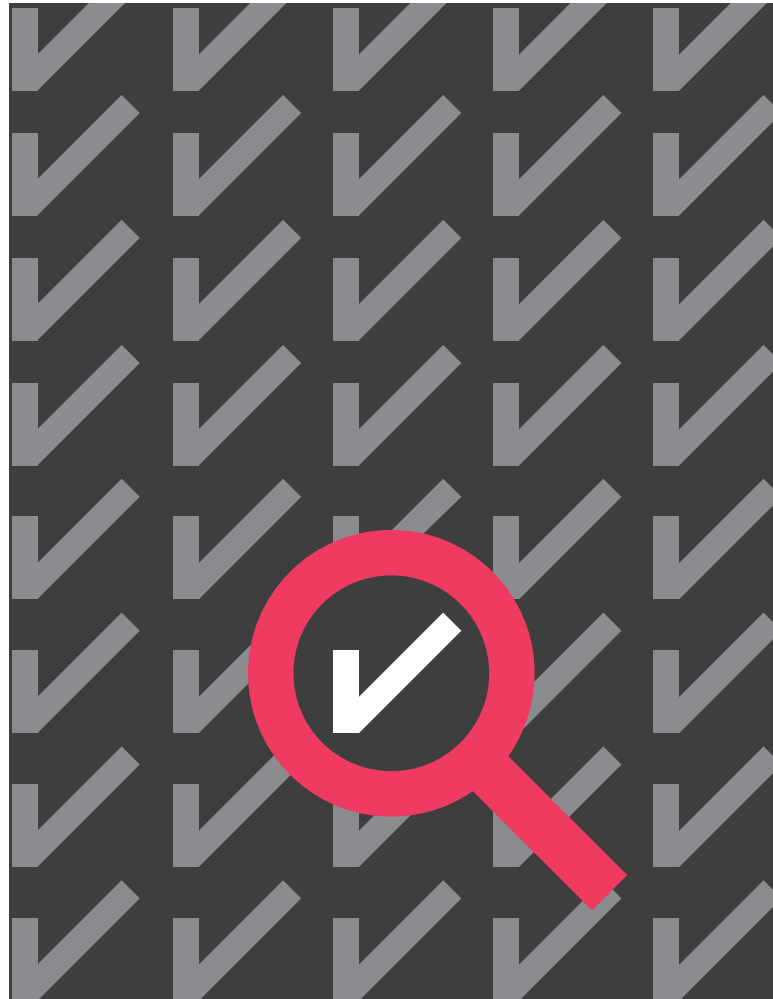
PwC ist der ideale Legal- und Tech-Partner, um Ihre rechtlichen Anforderungen zu prüfen und die daraus resultierenden Anforderungen technisch umzusetzen.

Wie Sie sehen, hat eine erfolgreiche Implementierung zwei Schlüsselbereiche: Neben den technischen Aspekten ist auch die Einhaltung der (datenschutz-)rechtlichen Anforderungen essenziell. Mit unserem Team von Rechtsexpert:innen, die sich mit den neuesten rechtlichen Bestimmungen und Vorschriften im Bereich der CDP-Implementierung auskennen, können wir Ihre Anforderungen gründlich prüfen und sicherstellen, dass Sie alle rechtlichen Anforderungen erfüllen. Dadurch gewährleisten wir die Einhaltung der DS-GVO sowie ggfs. weiterer Gesetze und stärken das Vertrauen Ihrer Kunden.

Unsere technischen Expert:innen sind in der Lage, die von Ihnen definierten Anforderungen nahtlos in Ihre bestehende technische Infrastruktur zu integrieren und eine reibungslose Funktionalität Ihrer CDP-Implementierung sicherzustellen. Kontaktieren Sie uns unter den nachfolgenden Kontaktdaten, um mehr über unsere Dienstleistungen zu erfahren und vereinbaren Sie ein erstes kostenloses Beratungsgespräch mit uns.

Kathrin Averwald, LL.M. (CIPP/E)
Rechtsanwältin für Datenschutz- und IT-Recht
PwC Deutschland
kathrin.averwald@pwc.com

Constantin Hourmouzis
Senior Manager, Technologieberatung
PwC Deutschland
constantin.hourmouzis@pwc.com



Über uns

In unserer globalen, sich rasch verändernden Wirtschaftswelt sind Kooperation, Umstrukturierung, Transaktion, Finanzierung und gesellschaftliche Verantwortung Themen, die unsere Mandanten zunehmend beschäftigen. Für verschiedenste komplexe Aufgabenbereiche benötigen sie rechtliche Handlungssicherheit. Deshalb beraten wir sie ganzheitlich und in enger Zusammenarbeit mit den Steuer-, Human-Resources- und Finanzexpert:innen von PwC und unserem internationalen Legal-Netzwerk in über 100 Ländern. Ob weltweit agierendes Unternehmen, öffentliche Körperschaft oder vermögende Privatperson, jedem Mandanten steht bei uns eine Ansprechperson zur Seite, die ihn in allen wirtschaftsrechtlichen Belangen verantwortungsvoll unterstützt. So helfen wir unseren Mandanten, ihren wirtschaftlichen Erfolg langfristig zu sichern.

PwC Legal. Mehr als 300 Rechtsanwält:innen an 18 Standorten. Integrierte Rechtsberatung für die Praxis.

© August 2024 PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft. Alle Rechte vorbehalten.

„PwC Legal“ bezeichnet in diesem Dokument die PricewaterhouseCoopers Legal Aktiengesellschaft Rechtsanwaltsgesellschaft, die zum Netzwerk der PricewaterhouseCoopers International Limited (PwCIL) gehört. Jede der Mitgliedsgesellschaften der PwCIL ist eine rechtlich selbstständige Gesellschaft.