Beschreibung des Datenschutzkonzeptes

ThinkSimple | Stefan-George-Ring 29 | D-81929 München
Info@ThinkSimple.de | 089/930 86 – 280

1. März 2016

GLIEDERUNG

ThinkSimple®
Entwickle neue Kompetenzen!

- Tätigkeitsbereich der ThinkSimple
- Umsetzung von Datenschutzanforderungen
- Datenschutzkonzept
  - Aufbau
  - Verfahren
  - Technische und organisatorische Sicherheit
  - Kommunikation mit Kunden

ThinkSimple - Vision & Mission

Vision

Jeder Mensch kennt die eigenen Stärken und setzt diese konsequent ein. Dadurch werden die Leistungsfähigkeit und die Motivation gesteigert, und der Stress reduziert.

Geschäftsidee

Online und mobile Personalentwicklung für Fach- und Führungskräfte im Bereich der Arbeitskompetenzen mit einem ausgezeichneten Preisleistungsverhältnis

Mitarbeiteridee

Wir bieten offenen und aufrichtigen Menschen die Möglichkeit, sich persönlich und beruflich weiter zu entwickeln.

Werte

- Ehrlichkeit
- Vertrauen
- Respekt
- Verantwortung
- Freiheit

Tätigkeitsbereich ThinkSimple

ThinkSimple bietet für den Mittelstand die Online Software für die Personalentwicklung Profile+ an. Damit entstehen positive Effekte:

- Erhöhung der Zufriedenheit und Motivation
- Selbsttest über Stärken und Schwächen
- Selbstorganisiertes und flexibles Lernen
- Stressfreies Arbeiten

Mit Hilfe von Profile+ können Unternehmen, Fach- und Führungskräfte, Personalentwickler sowie Trainer und Coaches mit Hilfe Ihrer Mitarbeiter innen und Mitarbeiter die Arbeitskompetenzen online ermitteln, interaktiv auswerten und selbstständig weiterentwickeln.

Dabei sind wir uns im Rahmen unserer Tätigkeiten ständig bewusst, dass wir mit hoch sensiblen personenbezogen Daten unserer Kundenumgehen. Die Einhaltung aller datenschutzrechtlichen Anforderungen hat daher für uns höchste Priorität, reicht uns aber nicht aus. Datenschutz wird und muss in unserem Hause von allen Mitarbeitern, im täglichen Arbeitsprozess gelebt werden. Daher werden alle Mitarbeiter in das Datenschutzkonzept aktiv eingebunden. Um die von uns geforderten hohen Qualitätsstandards einzuhalten werden alle Mitarbeiter regelmäßig geschult. Zur Prüfung und Einhaltung des Datenschutzes arbeiten wir mit einem TÜV zertifizierten externen Datenschutzbeauftragten zusammen, der das Datenschutzkonzept mit uns entwickelt hat und die Einhaltung aller Vorschriften regelmäßig prüft.

Unser Datenschutzkonzept ist im Schwerpunkt ausgerichtet an den rechtlichen Anforderungen des BDSG*, im Umfeld der Personalauswahl und Personalentwicklung. Es wird ständig darauf geachtet, dass immer der aktuelle Stand der Gesetze und der Rechtsprechung Anwendung finden.

*BDSG: Bundesdatenschutzgesetz

Umsetzung von Datenschutzanforderungen

ThinkSimple®
Entwickle neue Kompetenzen!

Alle Ihre Daten, auch die datenschutzrechtlich schützenswerten personenbezogenen Daten, liegen in einem Rechenzentrum eines mittelständisches Unternehmens, der Mittwald CM Service GmbH & Co KG. Darüber hinaus wird die Sicherheit Ihrer Daten von uns durch einen Vertrag über Auftragsdatenverarbeitung (ADV) gem. § 11 BGSG streng überwacht. Die Anforderungen der technischen und organisatorischen Maßnahmen gem. Der Anlage zu § 9 BDSG werden eingehalten und von uns kontrolliert. Das Rechenzentrum verfügt über einen bestellten Datenschutzbeauftragten mit Qualifizierungsnachweis.

Alle gespeicherten personenbezogenen Daten sind streng mandantengetrennt, so das NUR der Betroffene seine eigenen Daten sehen kann. Auch intern haben unser Mitarbeiter nur bei Störungen oder Servicefällen Zugriff auf personenbezogene Daten.

Alle unser Mitarbeiter sind nach § 5 BDSG auf das Datengeheimnis verpflichtet.

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten erfolgt auf Basis des mit Ihnen geschlossenen Dienstleistungsvertrags.

Für unser Personalentwicklung Software, in die Sie Ihre Daten eingeben, gibt es eine datenschutzrechtliche Verfahrensanweisung, in der konkret geregelt ist, welche Zweckbestimmung die Erhebung hat, wie mit den Daten umzugehen ist und wann sie gelöscht werden müssen.

Auf mobilen Datenträgen dürfen personenbezogene Daten nur nach Stand der Technik verschlüsselt abgelegt werden. Dasselbe gilt für jegliche Datenübertragung mit anderen Institutionen oder Unternehmen. Die Löschung von Daten erfolgt nach den Richtlinien des BSI* und auf Basis der ISO 66399.

Regelmäßig erfolgt eine Aktualisierung und Sensibilisierung unserer Mitarbeiter durch Schulungen zum Datenschutz und der Informationssicherheit.

Es ist sichergestellt, dass alle personenbezogenen Daten die Bundesrepublik Deutschland nicht verlassen.

*BSI=Bundesamt für die Sicherheit in der Informationstechnik

Datenschutzkonzept

Das Datenschutzkonzept basiert auf dem aktuellen Stand des Bundesdatenschutzgesetzes (BDSG).

Daneben kommen je nach Fall und Anforderung weitere gesetzliche Anforderungen hinzu (z.B. aus dem Medienrechts-rahmengesetz (MRRG), Telekommunikationsgesetz (TKG), Telemediengesetz (TMD) sowie Rechtsverordnungen aus dem Bundes-, Landesrecht) und ab 01.01.2018 der EU-Datenschutzverordnung, deren Anforderungen wir derzeit schon in unserem Datenschutzkonzept integrieren.

Unser Datenschutzkonzept gliedert sich in drei Bereiche*:*

1. **Recht*:*** Kontrolle, dass alle rechtlichen Anforderungen im Rahmen des Datenschutzes eingehalten werden.
2. **Organisation*:*** Verwaltung und Organisation aller personenbezogener Daten nach festgelegten Schutzklassen. Einhaltung rechtlicher Vorschriften durch klare Verfahrensanweisungen und klare Regelungen zum Löschen der Daten (Verfahrensverzeichnisse, Verfahrensanweisungen, Anwenderverzeichnisse, Verträge zur Auftragsdatenverarbeitung).
3. **Technische Sicherheit:** Bei der automatisierten Verarbeitung von personenbezogenen Daten nach den Anforderungen des § 9 BDSG und der dazugehörigen Anlage.

Regelmäßig wird ein Datenschutzbericht erstellt. Zudem gibt es ein Meldeprozess zur Abstellung von Mängeln für die Geschäftsleitung. Die Kontrolle der Mängelbeseitigung erfolgt im Auftrag der Geschäftsleitung durch den Datenschutzbeauftragten. In regelmäßigen Abständen werden von Sachverständigen Audits durchgeführt , damit die Einhaltung des Datenschutzkonzeptes gewährleistet wird.

Überblick rechtlicher Anforderungen

ThinkSimple®
Entwickle neue Kompetenzen!

Datensicherheitskonzept für Betroffene. In jedem Projekt wird sichergestellt, dass personenbezogene Daten nur erhoben werden, wenn es rechtlich erlaubt ist (§ 4 BDSG, § 28 BDSG).

Datenschutzverpflichtung unserer Mitarbeiter. Alle unser Mitarbeiter sind gem. § 5 BDSG auf das Datengeheimnis verpflichtet. Auch externe und freie Mitarbeiter werden von uns auf das Datengeheimnis verpflichtet.

Öffentliches Verfahrensverzeichnis gem. § 4e BDSG. In unserem immer aktuell gehaltenen öffentlichen Verfahrensverzeichnis können Betroffene nachlesen, wie wir mit ihren Daten umgehen und welche Verfahren wir einsetzen.

Auskunft an den Betroffenen gem. § 34 BDSG. Jederzeit können wir jeder Person von der wir personenbezogene Daten haben, darüber Auskunft geben, welche Daten vom ihr gespeichert wurden, bzw. wann ihre Daten gelöscht wurden. Hierfür haben wir eigene Formulare entwickelt, um schnellstmöglich Auskunft zu erteilen.

Datenverarbeitung im Auftrag gem. § 11 BDSG. Wenn wir im Auftrag von Kunden personenbezogene Daten erheben, verarbeiten oder nutzen, bzw. wir Dritte mit der Erhebung, Verarbeitung oder Nutzung personenbezogener Daten beauftragen, wird zwingend ein Vertrag geschlossen, in dem nach den Anforderungen des § 11 BDSG konkret und weisungsgebunden geregelt ist, wie der Dritte mit den Daten umgehen muss.

Sonstige rechtliche Anforderungen. Je nach Projektinhalt und spezifischen Anforderungen werden auch andere speziell geregelte datenschutzrechtliche Anforderungen erfüllt, z.B. TMG, TKG, SGB, AO etc.

Überblick organisatorische Anforderungen

ThinkSimple®
Entwickle neue Kompetenzen!

Klare organisatorische Verfahren. Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, wird dies über ein organisatorisches Verfahren geregelt. So werden alle Applikationen mit denen personenbezogene Daten verarbeitet werden in einem Applikationsverzeichnis erfasst und bewertet. Für den fachgerechten Umgang werden Verfahrensanweisungen und Verfahrensverzeichnisse erstellt. An ihnen können Mitarbeiter sich orientieren, wie sie im konkreten Fall mit personenbezogenen Daten umgehen müssen. Letztlich wird über ein aktiv Directory festgehalten, welcher Mitarbeiter, in welchem Verfahren mit personenbezogenen Daten wie umgehen darf (Erheben, Speichern, Verändern, Löschen etc.).

Vierstufiges Datensicherheitskonzept. Für alle Daten gilt ein vierstufiges Sicherheitskonzept wonach alle Daten zu kategorisieren sind. Sicherheitsstufe 1 – streng vertrauliche Daten; Sicherheitsstufe 2 – vertrauliche Daten; Sicherheitsstufe 3 – interne Daten; Sicherheitsstufe 4 – öffentliche Daten. Die Inhalte der Sicherheitsstufen entsprechen der ISO/IEC 27001. Die Einstufung erfolgt durch eine Risikoanalyse.

Datensicherheitskonzept für Ihre Personalentwicklungsdaten. (organisatorische Verfahrensanweisungen, Erfassung der Applikationen und der Berechtigungen der Mitarbeiter, die mit personenbezogenen Daten arbeiten).
Sensibilisierung der Mitarbeiter, das Personalentwicklungsdaten der Sicherheitsstufe Stufe 1 unterliegen und als streng vertraulich eingestuft sind.

Internet- und E-Mailnutzung. Die private Internet- und E-Mailnutzung ist bei uns verboten. Dies wird auch sporadisch kontrolliert und ggf. sanktioniert. (Regelungen und Vorgehensweise bei Verstößen durch Mitarbeiter. Regelungen zur sporadischen Kontrolle (TrafficLog)). Kontrolle der Einhaltung der Löschungspflicht von Log-Daten.

Telefonanlage. Datenschutzkonzept und Regelungen zum Umgang mit Verbindungsdaten sowie deren fristgerechte Löschung.

Überblick technische Anforderungen

ThinkSimple®
Entwickle neue Kompetenzen!

Datensicherheitskonzept Rechenzentrum

Personenbezogen Daten auf einer eigenen Infrastruktur zu Verarbeiten, birgt heutzutage große Sicherheitsrisiken. Vor allem mittelständische Unternehmen können sich neben dem Kerngeschäft einen hoch professionelle IT-Sicherheitsumgebung nicht leisten. Um die IT-Sicherheit und den Schutz Ihrer persönlichen Daten professionell sicherzustellen haben wir uns für die Auslagerung der Daten in ein Rechenzentrum entschieden, welches sich auf IT-Sicherheit und Datenschutz spezialisiert hat. Nach sorgfältiger Prüfung und Auswahl haben wir uns für die Mittwald CM Service GmbH & Co KG entschieden. Darüber hinaus wird die Sicherheit Ihrer Daten von uns durch einen Vertrag über Auftragsdatenverarbeitung (ADV) gem. § 11 BGSG streng überwacht. Die Anforderungen der technischen und organisatorischen Maßnahmen gem. Der Anlage zu § 9 BDSG werden eingehalten und von uns kontrolliert. Das Rechenzentrum verfügt über einen bestellten Datenschutzbeauftragten mit fachlicher Qualifikation.

Der Zugriff auf personenbezogene Daten durch uns oder Mitarbeiter des Rechenzentrums ist nur in Ausnahmefällen möglich und notwendig, z. B. bei Support von Datenbanksystemen, Störungsfälle. Daher sind die Mitarbeiter des externen IT Unternehmens alle auf das Datengeheimnis gem. § 5 BDSG verpflichtet worden.

Die technischen und organisatorischen Maßnahmen zum Schutz personenbezogener Daten im Rechenzentrum entsprechen den Anforderungen des § 9 BDSG (inkl. Anlage zu § 9 BDSG).

Für alle eingesetzten Applikationen, die mit personenbezogenen Daten in Berührung kommen, wurden Verfahrensanweisungen erarbeitet, die dem BDSG entsprechen.

Die Verschlüsselung bei der Datenübertragung entspricht dem Stand der Technik. Die Anweisungen für die Löschung/Sperrung von Daten sowie die Datenträgervernichtung wird in den einzelnen Verfahrensanweisungen detailliert beschrieben.

Die Einhaltung des Datenschutzes an den Arbeitsplätzen und den PCs der Mitarbeiter wird durch regelmäßige Sichtung des Arbeitsplatzes und des Clients kontrolliert (Schreibtisch, Papierkorb, Bildschirmschoner mit PW, PW-Länge und Art).

Datenverarbeitung im Auftrag

Datensicherheitskonzept für Datenverarbeitung im Auftrag gem. § 11 BDSG.

Da die uns von Ihnen anvertrauten personenbezogenen Daten in einem Rechenzentrum eines Partnerunternehmens liegen, und wir über den ADV-Vertrag mit Ihnen für die Sicherheit der Daten verantwortlich sind, haben wir Ihre Anforderungen über einen ADV-Vertrag mit der Mittwald CM Service GmbH & Co KG sichergestellt.

Die Hoheit über diese personenbezogenen Daten liegt ausschließlich der ThinkSimple. Hier wird über den ADV-Vertrag genau festgelegt, wie das Partnerunternehmen mit diesen erhobenen und gespeicherten Daten nach Anweisung umzugehen hat. Es werden grundsätzlich nur die Daten erhoben, verarbeitet, gespeichert oder weitergegeben, die zur Erfüllung des Auftrages zwingend erforderlich sind. Die Daten dürfen nur innerhalb der Bundesrepublik Deutschland verarbeitet und gespeichert werden. Die Weitergabe an Dritte ist ausgeschlossen.

Die Inhalte des Auftragsdatenverarbeitungsvertrags (ADV) richten sich nach § 11 BDSG und werden von uns regelmäßig durch Kontrollen überwacht.

Datenschutzkonzept - Verfahren

Auftragsdatenverarbeitung (zwingende Vertragsinhalte)

Jeder Vertrag zur Auftragsdatenverarbeitung muss folgende Inhalte konkret regeln:

1. Der Gegenstand und die Dauer des Auftrags,
2. der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
3. die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
4. die Berichtigung, Löschung und Sperrung von Daten,
5. die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
6. die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
7. die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
8. mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,
9. der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
10. die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Datenschutzkonzept - Verfahren

Vorabkontrolle; § 4d Abs. 5 BDSG

Bei jeder Einführung einer neuen Applikation (automatisierte Verfahren) wird eine Vorabkontrolle mit Risikoanalyse durchgeführt.

Es wird immer geprüft, ob personenbezogene Daten verarbeitet werden. Ist dies der Fall wird für die Applikation eine Verfahrensbeschreibung erstellt und diese in das öffentliche Verfahrensverzeichnis aufgenommen. Zugleich wird sie in das Applikations-und Anwenderverzeichnis integriert.

Werden personenbezogene Daten besonderer Art verarbeitet, erfolgt IMMER eine tiefgehende Bewertung im Rahmen einer Vorabkontrolle. Dies ist gegeben, wenn Risiken für die Rechte und Freiheiten der Betroffenen vorhanden sind (Persönlichkeitsbewertungen).

Die Vorabkontrolle erfolgt mit den am Prozess beteiligten Organisationseinheiten.

In der Vorabkontrolle wird festgelegt, ob die vorhandenen personenbezogenen Daten überhaupt - und wenn - wie verarbeitet werden dürfen.

Ist der Rahmen der Verarbeitung festgelegt und eine Verarbeitung rechtlich möglich, wird auch hier eine Verfahrensbeschreibung erstellt und diese in das öffentliche Verfahrensverzeichnis aufgenommen. Zugleich wird sie in das Applikations-und Anwenderverzeichnis integriert.

Datenschutzkonzept - Verfahren

Verfahrensbeschreibung

Bei jeder Einführung einer neuen Applikation (automatisierte Verfahren) wird eine Verfahrensbeschreibung erstellt.
Diese muss die Anforderungen des BDSG erfüllen.

Inhalte der Verfahrensbeschreibung:

Das Verfahren ist nur teilweise zur Einsichtnahme bestimmt.

1. Name der verantwortlichen Stelle
2. Bezeichnung und Art des Datenverarbeitungsprogramms
3 Zweckbestimmung
4. Kreis der betroffenen Personen und Art der gespeicherten Daten
5. Art regelmäßig übermittelter Daten und deren Empfänger
6. Regelfristen für die Löschung der Daten
7. Zugriffsberechtigte Personen oder Personengruppen
8. Rechtsgrundlage der Datenverarbeitung
9 Technische und organisatorische Maßnahmen (§ 9 DSG-EKD; § 9 BDSG)
10. Technik des Verfahrens

Anlage zur Spezifizierung der Datenfelder zu Punkt 5

Jeder der aufgeführten Punkte wird genau beschrieben, das Verfahren wird vom DSB geprüft und unterzeichnet.

Jede Veränderung wird dokumentiert.

Datenschutzkonzept - Verfahren

Öffentliches Verfahrensverzeichnis

Alle Verfahren mit personenbezogenen Daten werden in das öffentliche Verfahrensverzeichnis eingetragen.

Dieses Steht auf Anfrage jedem Betroffenen zur Einsicht zur Verfügung.

Das öffentliche Verfahrensverzeichnis hat folgende Inhalte:

1. Name oder Firma der verantwortlichen Stelle
2. Geschäftsführer
    - 2.1 Leitung der Datenverarbeitung
    - 2.2 Datenschutzverantwortlicher
3. Anschrift der verantwortlichen Stelle
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder –nutzung
5. Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können
7. Regelfristen für die Löschung der Daten
8. Geplante Datenübermittlung in Drittstaaten (ist ausgeschlossen)

Datenschutzkonzept - Verfahren

Auskunft an den Betroffenen gem. § 34 BDSG

Sobald ein Betroffener Auskunft über die von ihm gespeicherten Daten verlangt wird der Vorgang durch ein vom Datenschutzbeauftragten festgelegten Prozess und dafür entwickelte Formulare prozessual behandelt.

Die Auskunft hat zeitnah (innerhalb von 7 Tagen) zu erfolgen.

Im Auskunftsprozess muss die Identität des Auskunft beantragenden überprüft werden:

- Persönlich bekannt
- Kopie des Personalausweises
- In Onlineverfahren: über Dateninhaltsprüfung

Der Betroffene erhält:

1. Die zu seiner Person gespeicherten Datenfelder, auch soweit sie sich auf die Herkunft dieser Daten beziehen,
2. den Empfänger oder die Kategorien von Empfängern, an die Daten weitergegeben werden, und
3. den Zweck der Speicherung.

Auf Wunsch erhält er Einblick in das öffentliche Verfahrensverzeichnis.

Personenentwicklungsdaten werden „NICHT“ an den Betroffenen versendet. Der Betroffene hat aber das Recht zur Einsichtnahme vor Ort. Bei Auftragsdatenverarbeitung gibt der Auftraggeber das Verfahren über den Vertrag vor.

Datenschutzkonzept - Verfahren

Benachrichtigung des Betroffenen, § 33 BDSG

Werden erstmals personenbezogene Daten für eigene Zwecke ohne Kenntnis des Betroffenen gespeichert, wird der Betroffene von der Speicherung, der Art der Daten, der Zweckbestimmung der Erhebung, der Verarbeitung oder Nutzung und der Identität der Daten informiert.

Werden personenbezogene Daten geschäftsmäßig zum Zweck der Übermittlung ohne Kenntnis des Betroffenen gespeichert, wird der Betroffene von der erstmaligen Übermittlung und der Art der übermittelten Daten benachrichtigt.

Der Betroffene wird in diesen Fällen auch über die Empfänger unterrichtet, an die seine Daten weitergeleitet wurden, soweit er nach den Umständen des Einzelfalles er nicht mit der Übermittlung an diese rechnen muss.

Eine Benachrichtigung erfolgt NICHT, wenn einer der Ausnahmegründe des § 33 Abs.2 vorliegt; siehe nächste Seite.

Datenschutzkonzept - Verfahren

Benachrichtigung des Betroffenen, § 33 BDSG

Eine Benachrichtigung erfolgt NICHT, wenn einer der Ausnahmegründe des § 33 Abs.2 vorliegt:

1. der Betroffene auf andere Weise Kenntnis von der Speicherung oder der Übermittlung erlangt hat,
2. die Daten nur deshalb gespeichert sind, weil sie auf Grund gesetzlicher, satzungsmäßiger oder vertraglicher Aufbewahrungsvorschriften nicht gelöscht werden dürfen oder ausschließlich der Datensicherung oder der Datenschutzkontrolle dienen und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
3. die Daten nach einer Rechtsvorschrift oder ihrem Wesen nach, namentlich wegen des überwiegenden rechtlichen Interesses eines Dritten, geheim gehalten werden müssen,
4. die Speicherung oder Übermittlung durch Gesetz ausdrücklich vorgesehen ist,
5. die Speicherung oder Übermittlung für Zwecke der wissenschaftlichen Forschung erforderlich ist und eine Benachrichtigung einen unverhältnismäßigen Aufwand erfordern würde,
6. die zuständige öffentliche Stelle gegenüber der verantwortlichen Stelle festgestellt hat, dass das Bekanntwerden der Daten die öffentliche Sicherheit oder Ordnung gefährden oder sonst dem Wohle des Bundes oder eines Landes Nachteile bereiten würde,
7. die Daten für eigene Zwecke gespeichert sind und

a) aus allgemein zugänglichen Quellen entnommen sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist, oder

b) die Benachrichtigung die Geschäftszwecke der verantwortlichen Stelle erheblich gefährden würde, es sei denn, dass das Interesse an der Benachrichtigung die Gefährdung überwiegt,

die Daten geschäftsmäßig zum Zwecke der Übermittlung gespeichert sind und

8. aus allgemein zugänglichen Quellen entnommen sind, soweit sie sich auf diejenigen Personen beziehen, die diese Daten veröffentlicht haben, oder

   es sich um listenmäßig oder sonst zusammengefasste Daten handelt (§ 29 Absatz 2 Satz 2) und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.
9. aus allgemein zugänglichen Quellen entnommene Daten geschäftsmäßig für Zwecke der Markt- oder Meinungsforschung gespeichert sind und eine Benachrichtigung wegen der Vielzahl der betroffenen Fälle unverhältnismäßig ist.

Datenschutzkonzept - Datenschutzklassen

Einteilung personenbezogener Daten in verschiedene Schutzklassen

Personenbezogen Daten haben unterschiedliche Schutzklassen. Sie reichen von öffentlichen Daten bis hin zu streng vertraulichen Daten. In einem festgelegten Prozess werden alle personenbezogenen Daten Schutzklassen zugeordnet.

Schutzklasse 1 – streng vertraulich:

z. B. alle personenbezogenen Daten besonderer Art (Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben)

Schutzklasse 2 – vertraulich

z.B. Bewertungsergebnisse, Bewerbungen, Zeugnisse, Sozialdaten, Bankdaten etc.

Schutzklasse 3 – Intern

z.B. Adress- und Kommunikationsdaten sowie alle internen Daten unseres Unternehmens.

Schutzklasse 4 – öffentlich

z.B. frei im Internet verfügbare Daten, Daten aus Adress- und Telefonbüchern

Eine genaue und abschließende Beschreibung der Zuordnung einzelner Datenkategorien ist in einem Schutzklassenverzeichnis enthalten, welches allen Mitarbeitern zur Einsichtnahme und als Arbeitshilfe zur Verfügung steht.

Datenschutzkonzept - Verfahren

Applikations- und Anwenderverzeichnis

Zur Übersicht und Kontrolle wird ein **Applikationsverzeichnis** und eine **Anwenderverzeichnis** geführt.

Applikationsverzeichnis:

Es enthält alle Informationen über eingesetzte Applikationen die datenschutzrechtlich relevant sein können.

Es ist in 4 Abschnitte eingeteilt:

a. Applikationsbeschreibung (laufende Nummer, Applikationsname, Applikationsbeschreibung)

b. Betriebsdaten und Ansprechpartner

c. Spezifische datenschutzrelevante Informationen:
(Anwendergruppe, Welche Daten werden verarbeitet, Datenklassifikation, Schutzbedarf, Zugangsschutz, Verschlüsselung, Einverständniserklärung des Betroffenen, Vorabkontrolle-Verfahrensbeschreibung).

d. Zusätzliche Informationen zur Hardware und zu den Applikationen:
(Einsatz der Software auf: RZ-Server, Server und Client, Kunden-Server, Kunden-Server und Client, Lizenznummer, Anzahl der Lizenzen).

Das **Anwenderverzeichnis** enthält alle datenschutzrelevanten Informationen von den Personen, die Zugriff auf personenbezogene Daten haben sowie deren Zugriffsberechtigungen. Sie werden über ein active Directory erfasst.

Datenschutzkonzept - Verfahren

Datenschutzverpflichtung und Sensibilisierung der Mitarbeiter

Alle Mitarbeiter der ThinkSimple sind auf das Datengeheimnis verpflichtet.

Diese Verpflichtung erfolgt nach § 5 BDG.

Um Akzeptanz und Umsetzung zu gewährleisten werden alle Mitarbeiter regelmäßig in einer Schulung auf den Umgang mit personenbezogenen Daten im Sinne des BDSG sensibilisiert.

In die Schulungen werden sowohl neue gesetzliche Anforderungen, als auch der spezifische Umgang mit ihnen im Projektumfeld integriert.

In Bezug auf Gefahren durch das Internet und die IT werden Sensibilisierungsschulungen zur Informationssicherheit durchgeführt.

Alle Schulungen sind für die Mitarbeiter verpflichtend.

Datenschutzkonzept - Verfahren

Kontrolle und Audits

Die Geschäftsleitung kontrolliert regelmäßig alle Einrichtungen der ThinkSimple, in denen personenbezogene Daten verarbeitet werden und überprüft die Einhaltung der Datenschutzrichtlinien.

Dazu gehört die Prüfung der Arbeitsplätze, die Einhaltung der Verfahrensbeschreibungen als auch die Einhaltung der technischen und organisatorischen Maßnahmen im Rechenzentrum.

Mängel werden direkt vor Ort den Mitarbeitern mitgeteilt und es werden Wege aufgezeigt, wie datenschutzkonform gearbeitet werden kann.

Ziel ist, die Mitarbeiter nicht zu sanktionieren, sondern sie für ein datenschutzkonformes Arbeiten zu motivieren.

Werden Schwachstellen oder Verletzungen des Datenschutzes gemeldet, geht die Geschäftsleitung diesen unverzüglich nach und prüft, ob Mängel vorliegen.

Alle erkannten Mängel werden der Geschäftsleitung unverzüglich gemeldet und es werden Maßnahmen getroffen, um die Mängel unverzüglich zu beseitigen.

In einem **Datenschutzbericht** wird der Status der Datenschutzumsetzung dokumentiert und es werden weitere notwendige Maßnahmen aufgezeigt.

Verfahren (DSGVO-Teil 1)

Ausrichtung des Datenschutzes nach Risikoklassen der EU-Datenschutzgrundverordnung vom 15.12.2015 (DSGVO)

Ab 01.01.2018 wird das deutsche Datenschutzrecht ersatzlos von der neuen EU-Datenschutzgrundverordnung (EU-DSGVO) ersetzt. Danach unterliegen alle personenbezogenen Daten einer Risikobewertung in Bezug auf den Einsatz in der jeweiligen Institution (Art. 32a ff. EU-DSGVO).

Für das neue europäische Datenschutzrecht sprechen zudem viele weitere gute Argumente (Beispiele).

- **Adäquanzentscheidungen** werden den Datentransfer in Drittstaaten und zu internationalen Organisationen sicherstellen. Die EU-Kommission hat die Kompetenz, zu entscheiden, ob ein bestimmter Drittstaat bzw. eine internationale Organisation wie Facebook oder Google einen ausreichendenden Grad an Datenschutz bietet. Wo es an einer solchen Entscheidung fehlt, darf der Datentransfer nur stattfinden, sofern angemessene Schutzmechanismen die der EU-DSGVO entsprechen greifen.
- **Personenbezug von IP-Adressen.** Nach Rechtsprechung des EuGH sind IP-Adressen personenbezogen Daten. Nach BGH müssen IP-Adressen spätestens nach sieben Tagen anonymisiert werden.
- **Schutz von Kindern.** Der datenschutzrechtliche Schutz von Kindern ist ausgeweitet worden. Die Daten von Kindern unter 13 Jahren dürfen nur noch aufgrund einer Einwilligung der Erziehungsberechtigten verarbeitet werden.
- **Erweiterte Transparenzpflichten.** Die Art. 11 ff. der EU-DSGVO weiten die Transparenzanforderungen aus. Die für die Datenverarbeitung verantwortlichen Stellen müssen danach Datenschutzerklärungen über die von ihnen vorgenommene Datenverarbeitung erstellen und darin auch angeben, wie die betroffenen Personen ihre Rechte, z. B. auf Auskunft oder Löschung, ausüben können (siehe Folie 14).

*Art. 140, Art. GG; 137 Abs. 3 WRV

Verfahren (DSGVO-Teil 2)

Ausrichtung des Datenschutzes nach Risikoklassen der EU-Datenschutzgrundverordnung vom 15.12.2015 (DSGVO)

- **Haftung des Auftragsdatenverarbeiters gegenüber den Betroffenen.** Nach § 7 BDSG ist es den Betroffenen derzeit nur möglich, gegen die datenverantwortliche Stelle einen Ersatzanspruch für den Schaden geltend zu machen, der ihnen durch die unrechtmäßige Verarbeitung ihrer Daten entstanden ist. Diese Haftung wird durch Art. 77 EU-DSGVO auf Auftragsdatenverarbeiter ausgeweitet werden.
- **Compliance-Nachweise.** Datenverantwortliche Stellen müssen dann nach Art. 22 Nr. 1 der EU-DSGVO Datenschutz-Policies und geeignete technische und organisatorische Maßnahmen vorhalten müssen, um die Einhaltung der EU-DSGVO nachzuweisen. Zudem ist nach Art. 23 darauf zu achten, dass sowohl die Systeme, mit denen personenbezogene Daten verarbeitet werden, als auch die entsprechenden Arbeitsabläufe datenschutzfreundlich gestaltet sind. Diese Verpflichtung gilt auch für die verantwortlichen Ersteller von Auftragsdatenverarbeitungsverträgen.
- **Sog. Recht auf Vergessen.** Internetnutzer können danach von Suchmaschinen Betreibern verlangen nicht mehr auf bestimme Inhalte zu verweisen, die das Recht auf ihre Privatsphäre und den EU-Datenschutz verletzen.
- **Deutlich höhere Strafen:**

  Nach dem BDSG sind Bußgelder auf maximal 300.000 € begrenzt.

  Nach der EU-DSGVO können Bußgelder bis zu 1 Million Euro oder 2% ihres weltweiten Jahresumsatzes betragen.

Impressum

ThinkSimple®
Entwickle neue Kompetenzen!

ThinkSimple
Stefan-George-Ring 29
81929 München

Tel.: 089 / 930 86 - 280
E-Mail: Info@ThinkSimple.de
URL: www.ThinkSimple.de