|  |
| --- |
|  |
|  |
| Handbuch Datenschutz |

Inhalt

[Einleitung 5](#_Toc802538)

[Geltungsbereich 5](#_Toc802539)

[Die Governance-Struktur 5](#_Toc802540)

[**1.** Die Datenschutz-ORGANISATION auf Konzernebene 5](#_Toc802541)

[**1.1. Lokale Datenschutz-Organisation** 6](#_Toc802542)

[1.1.1. Management 6](#_Toc802543)

[1.1.2. Lokale Datenschutz-Organisation innerhalb der EU/EWR-Märkte 6](#_Toc802544)

[1.1.3. Lokale Datenschutz-Organisation außerhalb der EU/EWR-Märkte 6](#_Toc802545)

[Die Verarbeitung personenbezogener Daten 7](#_Toc802546)

[**2.** Was sind personenbezogene Daten? 7](#_Toc802547)

[**3.** Der Begriff „Verarbeitung personenbezogener Daten“ 7](#_Toc802548)

[Grundsätze der Verarbeitung personenbezogener Daten 7](#_Toc802549)

[**4.** Die wichtigsten Grundsätze 7](#_Toc802550)

[**5.** Die Rechte der Datensubjekte 8](#_Toc802551)

[**6.** Datentransfer und die Verwendung von Verarbeitern 8](#_Toc802552)

[**7.** Vorfälle und Verstöße 8](#_Toc802553)

[**8.** Schulungen 9](#_Toc802554)

[**9.** Mehr Informationen 9](#_Toc802555)

[Rollen und Zuständigkeiten 10](#_Toc802556)

[Überwachung und Beaufsichtigung 12](#_Toc802557)

[Glossar 12](#_Toc802558)

[Abweichungen 12](#_Toc802559)

[Zugehörige Richtlinien und Sonstiges 12](#_Toc802560)

[Kontakt 12](#_Toc802561)

[Revisionshistorie des Handbuchs 12](#_Toc802562)

[Anhang 1 13](#_Toc802563)

[GDPR - Zusätzliche Anforderungen in 13](#_Toc802564)

[den EU- und EWR-Märkten 13](#_Toc802565)

[Einleitung 13](#_Toc802566)

[Geltungsbereich und Aufbau 13](#_Toc802567)

[Personenbezogene Daten und ihre Verarbeitung 14](#_Toc802568)

[**1.** Personenbezogene Daten laut DSGVO 14](#_Toc802569)

[**1.1. Was sind personenbezogene Daten?** 14](#_Toc802570)

[**1.2. Was bedeutet „Verarbeitung personenbezogener Daten“?** 14](#_Toc802571)

[Datenschutz-Organisation 16](#_Toc802572)

[Die Carlsberg DSGVO-Compliance-Rahmenbedingungen 16](#_Toc802573)

[Was sind die Carlsberg DSGVO-Compliance-Rahmenbedingungen? 16](#_Toc802574)

[**1.** Das Carlsberg-DSGVO-Haus 17](#_Toc802575)

[**2.** Die wichtigsten Grundsätze der Verarbeitung personenbezogener Daten 17](#_Toc802576)

[**2.1.** **Gesetzeskonformität, Fairness und Transparenz** 18](#_Toc802577)

[**2.2. Zweckbindung** 19](#_Toc802578)

[**2.3. Datenminimierung** 19](#_Toc802579)

[**2.4. Genauigkeit** 20](#_Toc802580)

[**2.5. Begrenzte Aufbewahrung** 20](#_Toc802581)

[**2.6. Vertraulichkeit und Datenschutz** 20](#_Toc802582)

[**2.7. Verantwortung (Accountability)** 21](#_Toc802583)

[**3.** Die Rechte der Datensubjekte 21](#_Toc802584)

[**4.** Zusammenarbeit mit Dritten 22](#_Toc802585)

[**5.** Anforderungen an Datentransfers 22](#_Toc802586)

[**6.** Verstöße gegen den Datenschutz 23](#_Toc802587)

[**7.** Kontakt 23](#_Toc802588)

Einleitung

Die Carlsberg Gruppe („Carlsberg“) verarbeitet im Rahmen ihrer geschäftlichen Tätigkeiten personenbezogene Daten von Menschen. Egal, wie personenbezogene Daten gesammelt oder erhoben werden, wir müssen uns stets vergewissern, dass die geltenden Datenschutzbestimmungen eingehalten werden, um das Vertrauen der Menschen und Geschäftspartner, deren personenbezogene Daten Carlsberg verarbeitet, nicht zu verlieren.

Geltungsbereich

Carlsberg hat eine Richtlinie für Datenaufzeichnung und Datenschutz (im Folgenden kurz „Richtlinie“ genannt) eingeführt, welche alle Teile von Carlsberg dazu verpflichtet, diese Richtlinie, das vorliegende Handbuch Datenschutz (im Folgenden kurz „Handbuch“ genannt) und die geltenden Datenschutzbestimmungen zu jeder Zeit zu beachten.

Für den Schutz personenbezogener Daten ist jeder verantwortlich; Carlsberg verlangt, dass alle Mitarbeiter, Geschäftspartner und sonstigen Beteiligten, mit denen Carlsberg verkehrt, sich zum Schutz personenbezogener Daten laut geltenden Gesetzen und Vereinbarungen verpflichtet fühlen.

Dieses Handbuch behandelt die globalen Carlsberg-Methoden zur Wahrung des Schutzes personenbezogener Daten und in Anhang 1 detaillierter die Einhaltung der Datenschutzbestimmungen der DSGVO innerhalb der Europäischen Union und des Europäischen Wirtschaftsraumes (EWR).

Die hierin enthaltenen Grundsätze, Konzepte und Anforderungen und Ähnliches sind immer im Rahmen der jeweils vor Ort geltenden Rechtsvorschriften zu lesen, zu verstehen und auszulegen, die von Land zu Land variieren können.

Die Governance-Struktur

# Die Datenschutz-ORGANISATION auf Konzernebene

Die Organisation des persönlichen Datenschutzes bei Carlsberg besteht auf Gruppenebene aus dem Leiter Datenschutz (Head of Data Protection, HDP) der Konzern-Rechtsabteilung, der dem General Counsel (Generalsyndikus) untersteht, und dem Datenschutz-Manager (DPM), der dem HDP berichtet.

Jeder Carlsberg-Markt ernennt einen Datenschutzverantwortlichen (Data Protection Responsible, DPR), der dem lokalen Management gegenüber für die Einhaltung der geltenden Datenschutzbestimmungen, der Richtlinie und des Handbuches verantwortlich ist. Da die IT-Systeme ein integraler Bestandteil der Sicherstellung der Einhaltung der Datenschutzbestimmungen sind, haben die Global Business Services (GBS) nicht nur einen speziellen Datenschutzverantwortlichen, sondern auch Vertreter auf Konzernebene. Dies wird in folgender Abbildung ersichtlich:



Übersetzung Abb. 1:

ExCom

Rechtsabteilung, Generalsyndikus GBS

Leiter Datenschutz Leiter Datenschutz-Governance

Datenschutz-Manager Datenschutz-Governance-Spezialist

Markt Markt Markt GBS und ISC Zentrale Funktionen

Datenschutzverantwortlicher (4x) Ansprechpartner Datenschutz

Abbildung : Die Datenschutz-Organisation auf Konzernebene

## **Lokale Datenschutz-Organisation**

### Management

Das Management aller Märkte und globalen Funktionen (ISC und GBS) ist für die lokale Sicherstellung der Einhaltung der Richtlinien, des Handbuchs und der relevanten Datenschutzbestimmungen verantwortlich. Das Management sorgt dafür, dass es eine lokale Datenschutz-Organisation wie unten beschrieben gibt.

### Lokale Datenschutz-Organisation innerhalb der EU/EWR-Märkte

Die lokale Datenschutz-Organisation innerhalb der EU/EWR-Märkte wird üblicherweise in der Abteilung Finanzen verankert (siehe Anhang 1).

Wenn es der Generalsyndikus genehmigt, dürfen die Märkte oder globalen Funktionen von dieser vorgeschlagenen Standardorganisation abweichen, um spezifischen Verhältnissen eines Marktes besser gerecht zu werden (z.B. Cluster von Märkten oder Märkte mit kleiner Vertriebsorganisation).

### Lokale Datenschutz-Organisation außerhalb der EU/EWR-Märkte

Die lokale Datenschutz-Organisation außerhalb der EU/EWR-Märkte braucht einen lokalen Datenschutzverantwortlichen (DPR) und je nach Bedarf ihn unterstützende Vertreter, je nach spezifischem Risikoprofil und geltenden Datenschutzbestimmungen.

Dieser DPR ist üblicherweise in der Rechtsabteilung verankert. Die sonstige Organisationstruktur und die Rollen und Zuständigkeiten werden von Fall zu Fall zwischen dem lokalen Management und dem Generalsyndikus vereinbart.

Die Verarbeitung personenbezogener Daten

# Was sind personenbezogene Daten?

„Personenbezogene Daten“ sind alle Daten, die sich auf eine identifizierte oder identifizierbare Person („Datensubjekt“) beziehen. Dabei kann es sich um Namen, E-Mail-Adressen, Initialen, Lohndaten usw. handeln.

Bestimmte personenbezogene Daten betrachtet man als *sensible personenbezogene Daten*. Die Verarbeitung sensibler Daten verlangt besondere Sorgfalt.

Anonymisierte personenbezogene Daten werden nicht als personenbezogene Daten betrachtet.

# Der Begriff „Verarbeitung personenbezogener Daten“

Der Begriff „Verarbeitung personenbezogener Daten“ kann in einigen Ländern weiter, in anderen enger ausgelegt werden. Jedes Kästchen in untenstehender Abbildung kann als eine Form der „Verarbeitung“ angesehen werden.



Übersetzung Abb. 2:

Verarbeitung personenbezogener Daten:

Besteht aus Erheben, Nutzen, Speichern, Übertragen oder Löschen personenbezogener Daten

Erheben Nutzen Speichern Übertragen Löschen

Sammeln von Daten Verwenden als Teil in Systemen, Übertragen Löschen oder
zu geschäftlichen Zwecken geschäftl. Prozesse Archiven, Clouds oder Teilen Anonymisieren

Abbildung : Diese Abbildung zeigt Beispiele dafür, was der Begriff der „Verarbeitung personenbezogener Daten“ alles umfasst

Grundsätze der Verarbeitung
personenbezogener Daten

# Die wichtigsten Grundsätze

Carlsberg verpflichtet sich zum Schutz aller personenbezogenen Daten, die Carlsberg verarbeitet, zum Beispiel Daten über Mitarbeiter, Geschäftspartner, Kunden und Verbraucher. Carlsberg schützt die personenbezogenen Daten, die Carlsberg im Rahmen seiner geschäftlichen Tätigkeit nutzt, in Übereinstimmung mit relevanten lokalen Gesetzen und den folgenden wichtigsten Grundsätzen[[1]](#footnote-1) für die Verarbeitung personenbezogener Daten bei Carlsberg.

Die Grundsätze werden im Folgenden beschrieben:



Übersetzung von Abb. 3:

|  |  |  |
| --- | --- | --- |
| 1 | Gesetzeskonformität, Fairness und Transparenz | Personenbezogene Daten dürfen nur auf rechtlicher Grundlage, fair und transparent verarbeitet werden |
| 2 | Zweckbindung | Personenbezogene Daten dürfen nur zu bestimmten, ausdrücklich genannten und legitimen Zwecken verarbeitet werden |
| 3 | Datenminimierung | Personenbezogene Daten dürfen nur in angemessenem, relevantem und für den Zweck notwendigem Umfang verarbeitet werden |
| 4 | Genauigkeit | Die verarbeiteten personenbezogenen Daten müssen genau stimmen und bei Bedarf aktualisiert werden. |
| 5 | Begrenzte Aufbewahrung | Die personenbezogenen Daten müssen gelöscht oder anonymisiert werden, wenn sie nicht mehr für die Verarbeitungszwecke benötigt werden |
| 6 | Vertraulichkeit und Sicherheit | Die personenbezogenen Daten müssen unter angemessener Beachtung des Datenschutzes verarbeitet werden. Die Schutzmaßnahmen hängen von den Risiken ab, die wiederum von Zweck(en) und Art der personenbezogenen Daten abhängen. |

Abbildung : Die sechs wichtigsten Grundsätze der Verarbeitung personenbezogener Daten

Diese Grundsätze bilden Carlsbergs allgemeine Datenschutz-Methoden, die nach den jeweils geltenden gesetzlichen Vorschriften des jeweiligen Landes auszulegen sind.

# Die Rechte der Datensubjekte

Carlsberg wird die Rechte der Datensubjekte gemäß den geltenden lokalen Datenschutzbestimmungen erfüllen[[2]](#footnote-2).

# Datentransfer und die Verwendung von DATENVerarbeitern

Jeder Austausch personenbezogener Daten innerhalb von Carlsberg unterliegt der Intra Group Agreement (Vereinbarung zum gruppeninternen Austausch) für Datentransfers und Datenverarbeitung. Carlsberg beantragt, dass die Binding Corporate Rules (Konzernregeln) den Datenübertragungsteil des Intra Group Agreement ersetzen; alle Geschäftseinheiten von Carlsberg werden nach Genehmigung des Antrags (ca. 2020) das Verfahren der Binding Corporate Rules verbindlich einhalten.

Jede Verarbeitung personenbezogener Daten durch eine externe Partei erfordert eine entsprechende Datenverarbeitungsvereinbarung, sofern es sich nicht um geltende internationale und lokale rechtliche Anforderungen außerhalb von EU/EWR handelt.

# Vorfälle und VerstöSSe

Carlsberg verpflichtet sich, sämtliche personenbezogenen Daten so gut wie möglich zu schützen, muss aber gleichzeitig zugeben, dass technische und/oder menschliche Irrtümer, Handlungen oder Unterlassungen oder böswillige oder absichtliche Handlungen zum Beispiel von Mitarbeitern oder Dritten nicht auszuschließen sind. Ein Verstoß gegen geltendes Datenschutzrecht bedeutet, dass die in Carlsbergs Besitz befindlichen personenbezogenen Daten durch unberechtigten Zugriff oder zufälliges Löschen oder Zerstören beeinträchtigt werden. Um wirksam mit einem potentiellen Verstoß gegen den Schutz personenbezogener Daten umgehen zu können, hat Carlsberg entsprechende Verfahren etabliert, die bei einem Verstoß zu befolgen sind.

Wenn Sie den Verdacht haben, dass ein Verstoß gegen die Datenschutzbestimmungen stattgefunden hat oder stattfinden könnte, kontaktieren Sie unverzüglich den lokalen Datenschutzverantwortlichen.

# Schulungen

Alle Mitarbeiter von Carlsberg, die mit personenbezogenen Daten arbeiten, erhalten Schulungen zu den geltenden Datenschutzbestimmungen.

Diese Schulungskurse finden laufend statt und beinhalten die Ausbildung nach dem Handbuch Datenschutz und den jeweiligen lokalen Bestimmungen und Verfahren. Die Schulung sollte möglichst in bereits bestehende Fortbildungskurse eingebettet werden. Unsere neuen Mitarbeiter erhalten spätestens drei Monate nach Beginn ihrer Tätigkeit bei uns angemessene Schulungen, es sei denn, ihre Aufgabe erfordert eine sofortige Unterweisung.

# Mehr Informationen

Näheres erfahren Sie auf der Compass-SharePoint-Website, auf der Sie alle allgemeinen und bereichsspezifischen Richtlinien einschließlich der Richtlinie für Datenaufzeichnung und Datenschutz finden. Oder Sie besuchen die Datenschutz-SharePoint-Website der Konzern-Rechtsabteilung.

Rollen und Zuständigkeiten

|  |  |  |  |
| --- | --- | --- | --- |
| Rollen |  | Rollenbeschreibung | Zuständige Ebene |
| ExCom (Exekutivausschuss) |  | Verantwortlich für die Genehmigung der Richtlinie. | Global |
| Leiter der Rechtsabteilung |  | Urheber dieser Richtlinie mit der Gesamtverantwortung gegenüber ExCom für Datenaufbewahrungs- und Datenschutzfragen in der Carlsberg Gruppe. Sorgt dafür, dass Datenschutzrisiken in der Gruppe angemessen behandelt und bei Bedarf ExCom, dem Rechnungsprüfungsausschuss und dem Aufsichtsrat mitgeteilt werden. | Global |
| Head of Data Protection (Leiter Datenschutz)  |  | Ist verantwortlich für Erstellung und Aktualisierung dieses Handbuchs und für die gesamte praktische Umsetzung des Datenschutzes einschließlich der praktischen Umsetzung der Richtlinie für Datenaufzeichnung und Datenschutz sowie des Handbuchs Datenschutz in der gesamten Gruppe. | Global |
| Lokaler Datenschutzverantwortlicher |  | Ist gegenüber dem lokalen Management verantwortlich für die tägliche Einhaltung der Vorschriften der Richtlinie und des vorliegenden Handbuchs. | Lokal |
| Management der lokalen Firma und der Konzernfunktionen |  | Sorgt dafür, dass vorliegende Richtlinie und dieses Handbuch implementiert und eingehalten wird und dass alle betroffenen Mitarbeiter sie und die darin enthaltenen Anforderungen kennen. | Lokal |
| Leiter der Konzern-IT und der lokalen IT |  | Sind verantwortlich dafür, dass die relevanten IT-Systeme mit der Richtlinie und diesem Handbuch übereinstimmen. | GlobalLokal |
| Lokale Rechtsabteilung |  | Ist verantwortlich für die Unterstützung der lokalen Umsetzung und Operationalisierung der Richtlinie und dieses Handbuchs.  | Lokal |

Überwachung und Beaufsichtigung

Die Wirksamkeit dieses Handbuchs wird von Managern überwacht und beaufsichtigt und als Teil der internen Revision und ihrer Ergebnisse befolgt.

Glossar

HDP: Head of Data Protection (Leiter Datenschutz)

DPM: Datenschutz-Manager

DPR: Datenschutzverantwortlicher

DPC: Ansprechpartner für Datenschutz

Abweichungen

Abweichungen von diesem Handbuch sind vom Urheber des Handbuchs zu genehmigen.

Zugehörige Richtlinien und Sonstiges

* + - * + Richtlinie für Datenaufzeichnung und Datenschutz
				+ Datenschutz und Richtlinie für akzeptablen Gebrauch
				+ Richtlinie für Sicherheit
				+ Verfahren bei Verstößen gegen den Datenschutz
				+ Gruppeninterne Vereinbarung (Intra Group Agreement)

Kontakt

Näheres erfahren Sie bei Ihrem lokalen Datenschutzverantwortlichen (DPR) oder beim Leiter Datenschutz (HDP).

Revisionshistorie des Handbuchs

|  |  |  |
| --- | --- | --- |
| Version | Datum der Veröffentlichung | Genehmigung von Revisionen |
| 0,9 | Dezember 2018 | HDP/General Counsel (Generalsyndikus) |

Anhang 1

DSGVO: Zusätzliche Anforderungen in

den EU- und EWR-Märkten

Einleitung

Dieser Anhang wendet sich **ausschließlich** an die **Carlsberg-Geschäftseinheiten, die in den Ländern der EU/des Europäischen Wirtschaftsraums (EWR) tätig sind**. Dieser Anhang erläutert, ergänzend zum Handbuch, die nach der EU-Datenschutzgrundverordnung (DSGVO) verpflichtenden Anforderungen an den Schutz personenbezogener Daten.

Geltungsbereich und Aufbau

Dieser Anhang ist in drei Hauptbereiche unterteilt:

1. Personenbezogene Daten und ihre Verarbeitung
2. Datenschutz-Organisation
3. Die Carlsberg DSGVO-Compliance-Rahmenbedingungen

Personenbezogene Daten und
ihre Verarbeitung

# Personenbezogene Daten laut DSGVO

## **Was sind personenbezogene Daten?**

Mit Bezug auf die Definition in Abschnitt 2 des Handbuchs gilt die DSGVO für die Nutzung aller elektronisch oder manuell verarbeiteten personenbezogenen Daten.

Es gibt drei Arten personenbezogener Daten: 1. nicht sensible Daten, 2. sensible Daten und 3. Strafregisterdaten. Nach EU-Recht gehören zu den sensiblen Daten solche wie Rassenzugehörigkeit, ethnische Herkunft, politische, religiöse oder philosophische Anschauungen, Mitgliedschaft in einer Gewerkschaft, sowie genetische, biometrische, gesundheitliche Daten und Daten zur sexuellen Orientierung. Carlsberg muss bei jeder Verarbeitung sensibler Daten oder von Strafregisterdaten die Einhaltung der spezifischen Anforderungen der DSGVO sicherstellen, z.B. die der ausdrücklichen Einwilligung und Anforderungen höherer Sicherheitsebenen.

## **Was bedeutet „Verarbeitung personenbezogener Daten“?**

Der Begriff „Verarbeitung personenbezogener Daten“ wird in der DSGVO umfassend verstanden; er beinhaltet alle im Folgenden genannten Arten der Verarbeitung personenbezogener Daten:

* Aufzeichnung
* Organisation
* Strukturierung
* Anpassung oder Änderung
* Wiedergewinnung
* Beratung
* Nutzung
* Offenlegung durch Versenden
* Vertrieb oder anderweitiges Verfügbarmachen
* Ausrichtung oder Kombination
* Einschränkung oder Vernichtung
* Archivierung oder Clouds und
* Löschen von Daten.

Carlsberg muss sich in jedem Stadium des Lebenszyklus‘ personenbezogener Daten an die weiter oben beschriebenen wichtigsten Grundsätze der Datenverarbeitung halten. Im Folgenden sehen Sie Beispiele für die Verarbeitung personenbezogener Daten zu einem bestimmten Zweck als Teil eines oder mehrerer geschäftlicher Vorgänge bei Carlsberg:

* + Carlsberg *darf* personenbezogene Daten erheben, wenn Carlsberg Bewerber für freiwerdende Positionen sucht.
	+ Personenbezogene Daten *dürfen aufgezeichnet werden*, wenn Carlsberg im Rahmen von Beschwerdeverfahren die Tätigkeiten von Mitarbeitern aufzeichnet.
	+ Die personenbezogenen Daten werden von Carlsberg oder von Dienstleistungserbringern in Systemen, Archiven, Clouds usw. gespeichert, um sie für geschäftliche Zwecke zu behalten.
	+ Die Daten dürfen bei Carlsberg *intern geteilt oder transferiert werden* oder extern mit Dritten geteilt oder an sie transferiert werden, wenn es dazu dient, die Zwecke der Datenverarbeitung zu erfüllen.

Es ist wichtig festzuhalten, dass jede Datenverarbeitung, auch die, die an Dienstleistungserbringer outgesourct wird, als eine Datenverarbeitung anzusehen ist, für die Carlsberg verantwortlich ist.

* + Sobald die Daten nicht mehr gebraucht werden, *werden sie von Carlsberg gelöscht oder anonymisiert*, und wenn sie mit Externen geteilt wurden, muss Carlsberg diese bitten, die Daten dementsprechend zu löschen.

Datenschutz-Organisation

Carlsberg-Firmen in Märkten innerhalb von EU/EWR sind dazu verpflichtet, eine eigene lokale Datenschutz-Governance zu etablieren. Die lokale Datenschutz-Organisation innerhalb der EU/EWR-Märkte wird üblicherweise in der Abteilung Finanzen verankert, wie die Abbildung unten zeigt:



Übersetzung von Abb. 4:

 Leiter Datenschutz / Datenschutz-Manager

GBS-Markt Finanzabteilung Rechtsabteilung

Ansprechpartner Datenschutz Datenschutzverantwortlicher Ansprechpartner Datenschutz

Vertrieb Personal Marketing Marktspezifisch

Ansprechpartner Datenschutz Ansprechp. Datenschutz Ansprechp. DS Zu definieren

Abbildung : Die lokale Datenschutz-Organisation innerhalb der EU/EWR-Märkte

Die Carlsberg DSGVO-Compliance-
Rahmenbedingungen

# Was sind die Carlsberg DSGVO-Compliance-Rahmenbedingungen?

Die Carlsberg DSGVO-Compliance-Rahmenbedingungen innerhalb der EU/EWR-Märkte sind in folgende sieben Hauptbereiche unterteilbar:

1. Das Carlsberg-DSGVO-Haus
2. Die wichtigsten Grundsätze der Verarbeitung personenbezogener Daten
3. Anfragen der Datensubjekte
4. Zusammenarbeit mit Dritten
5. Anforderungen an Datentransfers
6. Verstöße gegen den Datenschutz
7. Kontakt

# Das Carlsberg-DSGVO-Haus

Das Carlsberg-DSGVO-Datenschutz-Haus besteht aus diesen drei Elementen:

1. **Dateninventar:** Das Dateninventar sollte für jede Carlsberg-Firma eine Aufzeichnung aller Datenverarbeitungsaktivitäten aller Bereiche umfassen und pflegen. Dieses Verzeichnis ist notwendig, damit Carlsberg einen Überblick darüber behält, welche personenbezogenen Daten in der Carlsberg Gruppe in den unterschiedlichen Ländern der EU/des EWR verarbeitet werden.
2. **Governance:** Die Governance (Unternehmensführung) betrifft die Richtlinien, Handbücher und Verfahren, die für jede einzelne Firma innerhalb der EU/EWR-Märkte gelten. Aufgabe der Governance ist es, dafür zu sorgen, dass die relevanten Richtlinien, Handbücher und Standard-Betriebsverfahren (standard operating procedures, SOP) vorhanden sind und dass Carlsberg jederzeit beweisen kann, dass die Richtlinien, Handbücher, SOPs und Leitfäden im Rahmen des Tagesgeschäfts täglich befolgt werden.
3. **Einbettung**: Zu der sogenannten Einbettung gehören die Carlsberg-Schulungen und das Erzeugen eines allgemeinen Bewusstseins, was die Anwendung und Einhaltung der DSGVO anbelangt.

Das in der nächsten Abbildung gezeigte „DSGVO-Haus“ veranschaulicht die DSGVO bei Carlsberg.



Übersetzung von Abb. 5:

DSGVO bei Carlsberg

Ziel Richtlinie für Datenaufzeichnung und Datenschutz

Treiber Dateninventar Governance Einbettung

Förderer Datenschutz-Folgenbewertung, Anfragen von Datensubjekten, Handbuch

 Drittparteien-Risiko, Leitlinien, Umgang mit Datenschutz-Verstößen

 Schulung, Verfahren, Bewusstseinsbildung

 Tools & Vorlagen, Gruppeninterne Vereinbarungen, Bindende Firmen-Vorschriften

Abbildung : Das Carlsberg-DSGVO-Haus

# Die wichtigsten Grundsätze der Verarbeitung personenbezogener Daten

Die Carlsberg DSGVO-Compliance-Rahmenbedingungen enthalten einen weiteren wichtigen Grundsatz zusätzlich zu den oben im allgemeinen Teil des Handbuchs genannten sechs wichtigsten Grundsätzen. Nachstehend sehen Sie die sieben Grundsätze:



Übersetzung von Abb. 6:

|  |  |  |
| --- | --- | --- |
| 1 | Gesetzeskonformität, Fairness und Transparenz | Personenbezogene Daten dürfen nur auf rechtlicher Grundlage, fair und transparent verarbeitet werden |
| 2 | Zweckbindung | Personenbezogene Daten dürfen nur zu bestimmten, ausdrücklich genannten und legitimen Zwecken verarbeitet werden |
| 3 | Datenminimierung | Personenbezogene Daten dürfen nur in angemessenem, relevantem und für den Zweck notwendigem Umfang verarbeitet werden |
| 4 | Genauigkeit | Die verarbeiteten personenbezogenen Daten müssen genau stimmen und bei Bedarf aktualisiert werden. |
| 5 | Begrenzte Aufbewahrung | Die personenbezogenen Daten müssen gelöscht oder anonymisiert werden, wenn sie nicht mehr für die Verarbeitungszwecke benötigt werden |
| 6 | Vertraulichkeit und Sicherheit | Die personenbezogenen Daten müssen unter angemessener Beachtung des Datenschutzes verarbeitet werden. Die Schutzmaßnahmen hängen von den Risiken ab, die wiederum von Zweck(en) und Art der personenbezogenen Daten abhängen. |
| 7 | Verantwortung (Accountability) | Carlsberg ist verantwortlich für die Einhaltung der DSGVO und muss diese beweisen können, z.B. durch eindeutige Zuständigkeiten und Nachvollziehbarkeit der Speicherung und Nutzung personenbezogener Daten |

Abbildung 6: Die sieben wichtigsten Grundsätze innerhalb der EU/EWS-Märkte

Die den wichtigsten Grundsätzen beigemessene Bedeutung kann jedoch von Land zu Land unterschiedlich sein.

Daher müssen innerhalb der EU/EWR-Märkte die sieben Grundsätze im Einklang mit der DSGVO sowie zusätzlicher lokaler Datenschutzbestimmungen gelesen, verstanden und ausgelegt werden.

Der Extra-Grundsatz gemäß DSGVO ist die Verantwortung (Accountability). Die einzelnen Grundsätze werden unten im Kontext der DSGVO ausführlicher beschrieben:

## **Gesetzeskonformität, Fairness und Transparenz**

**Gesetzeskonformität:** Carlsberg hat eine geeignete gesetzeskonforme Grundlage (oder Grundlagen) für die Verarbeitung personenbezogener Daten gefunden.

**Fairness:** Carlsberg hat sich darüber Gedanken gemacht, wie die Datenverarbeitung die betreffenden Personen beeinträchtigen könnte und kann etwaige ungünstige Auswirkungen rechtfertigen.

**Transparenz:** Carlsberg erfüllt die Verpflichtungen zur Transparenz des Rechts auf Information.

Bevor personenbezogene Daten verarbeitet werden können, muss sichergestellt werden, dass Carlsberg dafür eine gesetzliche und rechtmäßige Grundlage hat. Die relevante lokale DSGVO gibt vor, was in einem bestimmten Markt erforderlich ist.

Das bedeutet: Bevor Carlsberg personenbezogene Daten verarbeitet, ist zu prüfen, ob die Verarbeitung personenbezogener Daten erlaubt ist. Die gesetzliche Grundlage hängt üblicherweise ab von:

* + - * + dem Zweck, zu dem Carlsberg die personenbezogenen Daten sammelt und
				+ der Art der personenbezogenen Daten (ob es sich um sensible oder spezielle Kategorien von Daten handelt).

Die Verarbeitung personenbezogener Daten kann auf einer der folgenden gesetzlichen Grundlagen basieren:



Übersetzung von Abb. 7:

Einverständnis: Ein Datensubjekt muss der Verarbeitung seiner Daten zustimmen

Legitime Interessen: Es gibt ein gewichtetes und ausgeglichenes Interesse an der Verarbeitung, das nicht von anderen Interessen außer Kraft gesetzt wird

Vertragliche Notwendigkeit: Die Datenverarbeitung ist erforderlich, um einen Vertrag abzuschließen oder zu erfüllen

Rechtmäßigkeit der Verarbeitung (in der Mitte, ohne Text)

Gesetzliche Verpflichtungen: Der Datenverantwortliche ist gesetzlich zur Verarbeitung der pers. Daten verpflichtet

Abbildung 7: Gesetzliche Grundlagen für die Verarbeitung personenbezogener Daten

Zusätzlich zu den gesetzlichen Grundlagen muss Carlsberg dafür sorgen, dass die Verarbeitung mit der DSGVO im Ganzen sowie mit zusätzlichen lokalen Datenschutzvorschriften übereinstimmt.

Transparenz bedeutet nach der DSGVO (unter anderem), dass die betreffende Person vor Beginn der Datenverarbeitung darüber informiert sein muss, einschließlich Zweck, Aufbewahrungsfristen etc. Dies gilt, egal ob das Datensubjekt ein Mitarbeiter oder eine externe Person wie ein Verbraucher, ein Lieferant oder ein Besucher der Website ist.

Bevor Sie personenbezogene Daten überarbeiten dürfen, müssen Sie überprüfen, dass die Datensubjekte, deren personenbezogene Daten Carlsberg verarbeitet, die erforderlichen Informationen erhalten haben oder erhalten werden.

## **Zweckbindung**

Carlsberg verarbeitet die personenbezogenen Daten ausschließlich zu den genau anzugebenden, ausdrücklich erwähnten und legitimen Zwecken, zu denen die personenbezogenen Daten ursprünglich erhoben wurden und nicht zu anderen als dem oder den Zwecken.

## **Datenminimierung**

Carlsberg darf personenbezogene Daten nur in angemessenem Umfang verarbeiten, soweit die Daten relevant und im Sinne der Verarbeitungszwecke notwendig sind.

Carlsberg sollte nicht mehr personenbezogene Daten verarbeiten, als es für den Zweck erforderlich ist. Außerdem sollte Carlsberg keine unwichtigen personenbezogenen Daten erheben und verarbeiten.

Wenn Carlsberg Daten verarbeitet, die zum vorgegebenen Zweck nicht erforderlich sind, ist dies wahrscheinlich unrechtmäßig (da gesetzliche Grundlagen meist an die Notwendigkeit gebunden sind) und ein Verstoß gegen das Datenminimierungsprinzip. Einzelpersonen haben auch das Recht, die Löschung ihrer Daten im Hinblick darauf zu verlangen.

## **Genauigkeit**

Carlsberg ergreift alle angemessenen Schritte, um dafür zu sorgen, dass die gespeicherten und verarbeiteten personenbezogenen Daten nicht falsch oder irreführend sind und dass sie, falls notwendig, aktuell gehalten und unter Berücksichtigung des Zweckes verarbeitet, gelöscht oder korrigiert werden. Dies muss unverzüglich geschehen.

Entsprechend diesem Grundsatz kann es sein, dass Carlsberg die personenbezogenen Daten aktuell halten muss – je nachdem, wozu Carlsberg sie verwendet.

## **Begrenzte Aufbewahrung**

Carlsberg bewahrt personenbezogene Daten nicht länger auf, als es zu dem oder den Zwecken, zu denen die Daten verarbeitet werden, erforderlich ist. Wenn Carlsberg keinen rechtmäßigen Zweck mehr für die Speicherung oder Verarbeitung personenbezogener Daten verfolgt, sind die betreffenden Daten zu löschen oder zu anonymisieren.

Carlsberg muss also Aufbewahrungs- und Löschungsfristen für von Carlsberg verarbeitete personenbezogene Daten festlegen und umsetzen.

Allerdings ist der Standard, zu dem personenbezogene Daten als wirklich anonymisiert gelten dürfen, normalerweise sehr streng. In der Praxis bedeutet dies zum Beispiel, dass Carlsberg bei einer Zusammenstellung von Mitarbeitergehältern aufgrund von anonymisierten Daten alle identifizierbaren Daten wie Namen, Initialen usw. aus dem Datensatz löschen muss.

## **Vertraulichkeit und Datenschutz**

Dieser Grundsatz bedeutet, dass Carlsberg geeignete Sicherheitsmaßnahmen ergreifen muss, um zu verhindern, dass die personenbezogenen Daten zufällig oder absichtlich gefährdet werden.

Carlsberg muss dafür Sorge tragen, dass technische, organisatorische und physikalische Sicherheitsmaßnahmen an den für die Speicherung und Verarbeitung personenbezogener Daten relevanten Orten angewandt werden.

Zu derartigen Maßnahmen können das Absperren von Räumen und Gebäuden, Zugangskontrollen, Alarmsysteme und Brandschutz- und Brandverhütungssysteme gehören.

Außerdem muss Carlsberg sicherstellen, dass personenbezogene Daten nicht an Unberechtigte weitergegeben werden, auch nicht an die eigenen Mitarbeiter, sofern diese nicht durch einen bestimmten Zweck zur Verarbeitung dieser personenbezogenen Daten berechtigt sind.

Dies muss bei Carlsberg durch die Anwendung von Verschlüsselungstechniken, durch Lehrgänge, Zugangsbeschränkungen, Vertragsklauseln mit Dritten usw. sichergestellt werden.

## **Verantwortung (Accountability)**

Der Grundsatz der Verantwortung bedeutet hier, dass Carlsberg für die Einhaltung der DSGVO verantwortlich ist und jederzeit in der Lage sein muss, diese Einhaltung auch unter Beweis zu stellen.

Dies bedeutet, dass Carlsberg die verantwortungsbewusste Speicherung und Verarbeitung personenbezogener Daten klar nachvollziehbar nachweisen können muss. Dies lässt sich zum Beispiel erreichen, indem man Rollen und Zuständigkeiten für die Nutzung der fraglichen Daten klar zuweist, oder durch Mechanismen wie System Logging (Protokollierung), Eigenkontrolle oder Überprüfung von Log-Dateien.

# Die Rechte der Datensubjekte

Carlsberg muss die Rechte der Datensubjekte gemäß den geltenden lokalen Datenschutzbestimmungen erleichtern. Es ist wesentlich, dass Carlsberg Datensubjekte bei der Ausübung ihrer Rechte unterstützt. In den EU/EWR-Märkten haben Datensubjekte das Recht, Folgendes zu verlangen:



Übersetzung dieser Abb.:

|  |  |  |
| --- | --- | --- |
| 1 | Informationspflicht | Individuen haben das Recht, sich über Erhebung und Nutzung ihrer pers. Daten zu informieren – gemäß DSGVO ein wichtiges Kriterium für Transparenz |
| 2 | Zugangsrecht | Gibt Personen das Recht auf eine Kopie ihrer pers. Daten sowie andere ergänzende Informationen |
| 3 | Recht auf Berichtigung | Die DSGVO gibt Personen das Recht, falsche Daten über sich berichtigen und unvollständige vervollständigen zu lassen. |
| 4 | Recht auf Löschung | Die DSGVO verleiht Personen das Recht, ihre Daten löschen zu lassen – das sogenannte „Recht auf Vergessenwerden“ |
| 5 | Recht auf Einschränkung der Verarbeitung | Personen dürfen verlangen, dass ihre pers. Daten nur eingeschränkt genutzt werden. Dieses Recht ist nicht absolut und gilt nur unter Umständen. |
| 6 | Recht auf Datenübertragbarkeit | Erlaubt Personen, ihre pers. Daten in allen Stadien zu erhalten und wiederzuverwenden |
| 7 | Widerspruchsrecht | Gibt Personen das Recht, unter bestimmten Umständen gegen die Verarbeitung ihrer pers. Daten Einspruch zu erheben. So haben sie ein absolutes Recht auf Erteilung eines Nutzungsverbots für Direktmarketing. |
| 8 | Rechte in Bezug auf automatisierte Entscheidungen im Einzelfall und Profiling | Wenn Ihre Datenverarbeitung unter Art. 22 fällt, sollten Sie sich vergewissern, dass die Betroffenen informiert werden und regelmäßig prüfen, ob Ihre Systeme wie beabsichtigt funktionieren |
| 9 | Recht auf Beschwerden | Gibt Personen das Recht, sich über die Nutzung ihrer Daten durch Carlsberg zu beschweren |

# Zusammenarbeit mit Dritten

Carlsberg beauftragt eine Anzahl externer Dienstleister, Dienstleistungen für Carlsberg zu erbringen, was mit sich bringt, dass diese Lieferanten personenbezogene Daten im Auftrag von Carlsberg verarbeiten. In diesen Situationen ist Carlsberg als der Datenverantwortliche und der Lieferant als der Datenverarbeiter zu betrachten.

Ein Datenverantwortlicher ist diejenige Person oder Institution, die den Zweck und die Methoden der Datenverarbeitung festlegt. Beispielsweise ist Carlsberg der Datenverantwortliche, wenn es um die Verarbeitung personenbezogener Daten von Mitarbeitern im Rahmen der internen Personalverwaltung geht.

Ein Datenverarbeiter ist jemand, der vom Datenverantwortlichen damit beauftragt wird, im Auftrag und ausschließlich in Übereinstimmung mit dem Datenverantwortlichen personenbezogene Daten zu verarbeiten. Wenn Carlsberg einen Gehaltsdienstleister damit beauftragt, Zahlungen an die Mitarbeiter zu verwalten, fungiert derjenige Dienstleister als Datenverarbeiter.

Bevor Carlsberg einen Datenverarbeiter beauftragt, muss Carlsberg:

* überprüfen, dass der Lieferant die personenbezogenen Daten schützen kann (Due Diligence);

Eine Datenverarbeitungsvereinbarung ist eine Reihe von Vertragsklauseln, die sicherstellen, dass von Carlsberg mit der Verarbeitung personenbezogener Daten beauftragte externe Lieferanten dazu verpflichtet werden, die betreffenden personenbezogenen Daten zu schützen und sie ausschließlich wie von Carlsberg angewiesen zu nutzen.

* dafür sorgen, dass der Lieferant ausreichende Garantien abgibt, die personenbezogenen Daten zu schützen, und
* dass eine Datenverarbeitungsvereinbarung zwischen Carlsberg und dem Lieferanten abgeschlossen wird.

Es wird immer in der Verantwortung von Carlsberg liegen, dass die personenbezogenen Daten von Datenverarbeitern hinreichend geschützt werden; jedes derartige Versäumnis eines Lieferanten kann zu einem bedeutenden Risiko für Carlsberg werden.

In manchen Situationen kann Carlsberg Dritten personenbezogene Daten zur Verfügung stellen, auch verbundenen Unternehmen innerhalb der Carlsberg Gruppe, die nicht von Carlsberg engagiert werden, um im Auftrag von Carlsberg personenbezogene Daten zu verarbeiten. Dies wäre beispielsweise dann der Fall, wenn Carlsberg gesetzlich dazu verpflichtet würde, lokalen Steuerbehörden personenbezogene Daten über seine Mitarbeiter zu geben. In solchen Situationen gilt Carlsberg immer noch als Datenverantwortlicher, aber der Dritte wird dann auch als solcher angesehen, weil der Dritte personenbezogene Daten zu seinen eigenen Zwecken verarbeitet.

# Anforderungen an Datentransfers

Der Transfer – oder das bloße Teilen – personenbezogener Daten mit anderen, sei es intern oder extern, darf nur unter ganz bestimmten Umständen stattfinden, nämlich wenn folgende Anforderungen gelten:

1. Es bedarf einer gesetzlichen Grundlage zum Teilen oder Übertragen personenbezogener Daten an Drittparteien, die dann ebenfalls als Datenverantwortliche fungieren.
2. Personenbezogene Daten dürfen nicht zufällig oder inoffiziell miteinander geteilt werden.
3. Der Zweck des Transfers oder Teilens muss mit dem Zweck übereinstimmen, zu dem die Daten gesammelt wurden.
4. Die übertragenen Daten sind auf das Maß zu beschränken, welches erforderlich ist, um den Zweck zu erreichen.
5. Das Transferieren personenbezogener Daten an Dritte, die auch als Datenverantwortliche fungieren, wie Lieferanten, Tochtergesellschaften innerhalb der Carlsberg Group oder Behörden, bedarf einer gesetzlichen Grundlage. Deswegen ist zu überprüfen, dass eine der oben beschriebenen gesetzlichen Grundlagen für den Transfer personenbezogener Daten vorliegt.

# VerstöSSe gegen den Datenschutz

Um wirksam mit einem potentiellen Verstoß gegen den Schutz personenbezogener Daten umgehen zu können, hat Carlsberg entsprechende Verfahren etabliert, die bei einem Verstoß zu befolgen sind.

Wenn Sie den Verdacht haben, dass ein Verstoß gegen die Datenschutzbestimmungen stattgefunden hat oder stattfinden könnte, kontaktieren Sie unverzüglich den lokalen Datenschutzverantwortlichen.

# Kontakt

Nähere Informationen erhalten Sie bei Ihrem lokalen Datenschutzverantwortlichen. Bitte kontaktieren Sie ihn auch, um zu fragen, wie Sie:

* vorgehen müssen, bevor Sie Daten neu erheben,
* dafür sorgen, dass Carlsbergs Dateninventar richtig aktualisiert wird,
* vorgehen müssen, um Datensubjekte richtig zu informieren,
* vorgehen müssen, wenn Sie eine Anfrage oder Beschwerde von einem Datensubjekt erhalten,
* vorgehen müssen, wenn Sie vorab Fragen zum sicheren Transfer personenbezogener Daten haben, bevor damit begonnen wird, und
* vorgehen müssen, wenn Sie personenbezogene Daten mit Externen teilen oder an Externe transferieren wollen (z.B. einen neuen Datenverarbeiter oder Datenverantwortlichen beauftragen).

|  |  |  |
| --- | --- | --- |
|  |  | November 2018Carlsberg Breweries A/S100 Ny Carlsberg Vej1799 Copenhagen VDenmark |

1. Wenn eine lokale Datenschutzvorschrift einen höheren Standard verlangt, wird dieser Standard befolgt. Ihr lokaler Datenschutzverantwortlicher wird Sie in die für Sie relevanten Grundsätze einweisen. [↑](#footnote-ref-1)
2. Die Rechte von Datensubjekten nach der EU-Datenschutz-Grundverordnung (DSGVO) werden in Anhang 1 näher erläutert. [↑](#footnote-ref-2)