Danish Crown

Datenschutz grundsätse der Danish Crown Group

September 2024 – Version 2.0

Dokumentenlenkung

Governance	
Version	2.0
Emittent	Lise Lotte Langston (LILOL)
Genehmiger	Thomas Ahle (TAH)
Ausgabedatum	26-09-2024
Datum der Antragstellung	26-09-2024
Umfang	Der Danish Crown Group
Häufigkeit der Überprüfung	Alle 2 Jahre

Versionsgeschichte			
Vs.	Datum	Geändert von	Zusammenfassung der Änderungen und Aktualisierungen
1.0	01.01.2018	Rasmus Schjoldager	Umsetzung der Politik
1.1	01-01-2021	Jesper Green Schou (JEGSC)	Update für verbesserte Kommunikation.
1.2	01-02-2022	Jonas Hvid (JONHV)	Aktualisiert Im Zusammenhang mit der Implementierung von Standards und anderen Richtlinien / SOPs
1.3	02-05-2023	Jonas Hvid (JONHV)	Aktualisierung von Aussteller und Genehmiger
2.0	26-09-2024	Jonas Hvid (JONHV)	Allgemeine Aktualisierung der Richtlinie

Link zu verwandten Gruppendokumenten	
Name der Dokumentdatei	Inhalt des Dokuments
DSGVO-Leitfaden	DSGVO-Leitfaden für alle Mitarbeiter
DSGVO-Leitfaden HR	DSGVO-Leitfaden für HR-Mitarbeiter
DSGVO-Leitfaden Manager	DSGVO-Leitfaden für Führungskräfte
SOP Schlussfolgerung der DPA	Verfahren für den Abschluss von Verträgen mit Datenverarbeitern.
DSGVO-Leitfaden zur Verwendung von Fotos und Erklärungen	Leitfaden für Marketing- und HR-Mitarbeiter, die Bilder intern und online verwenden
SOP Wie man die Rechte der betroffenen Person ausübt	Verfahren zur Ausübung von Betroffenenrechten
SOP Audit Datenverarbeiter	Verfahren zur Sicherstellung der Prüfung von Datenverarbeitern
SOP Übermittlung personenbezogener Daten in Länder außerhalb der EU/des EWR	Verfahren für den Abschluss von Verträgen mit Datenverarbeitern außerhalb der EU/des EWR
SOP Jährliche Überprüfung der DSGVO-Dokumentation	Verfahren zur Sicherstellung einer jährlichen Aktualisierung der DSGVO-Dokumentation
Richtlinie zur Informationssicherheit	Richtlinie für alle Mitarbeiter, die die Anforderungen an den Schutz von Informationen umreißt
IT-Sicherheitsrichtlinie	Leitfaden für alle Mitarbeiter, der die Anforderungen an den Umgang mit IT-Geräten umreißt

Inhalt

Dokumentenlenkung **2**

1. Unsere Grundsätze **4**

1.1 Unser Engagement 4

1.2 Unsere Kultur 4

1.3 Unsere Pflichten zur Förderung der Compliance 4

1.4 Weltweit gleichbleibend hohe Standards 4

2. Schutz personenbezogener Dataen **5**

2.1 Was sind personenbezogene Daten? 5

2.2 Verarbeitung personenbezogener Daten 5

2.2.1 Grundsätze des Datenschutzes 5

2.2.2 Rechtsgrundlage für die Verarbeitung gewöhnlicher und vertraulicher personenbezogener Daten 5

2.2.3 Rechtsgrundlage für die Verarbeitung sensibler personenbezogener Daten 6

2.3 DSGVO-Richtlinien 6

2.4 Lieferanten, die personenbezogene Daten in unserem Auftrag verarbeiten 6

1. Unsere Grundsätze

1.1 Unser Engagement

Das Management von Danish Crown setzt sich nachdrücklich dafür ein, dass die Gruppe die geltenden Datenschutzgesetze einhält. Diese Verpflichtung ist Teil unserer allgemeinen Verpflichtung als verantwortungsbewusster Konzern, integer zu handeln und die Anforderungen der in den Ländern, in denen wir tätig sind, geltenden Gesetze zu erfüllen.

Unsere Verpflichtung zum Schutz personenbezogener Daten ist eine gemeinsame Verantwortung, und jeder von uns ist verpflichtet, unsere gemeinsame Verantwortung zu verstehen, unser Geschäft in einer Weise zu führen, die mit unseren Werten und in Übereinstimmung mit dieser Richtlinie übereinstimmt.

1.2 Unsere Kultur

Bei Danish Crown unterstützen wir eine Compliance-Kultur und bieten allen relevanten Mitarbeitern die notwendige Anleitung und obligatorische Schulung. Auf diese Weise stellen wir sicher, dass alle relevanten Mitarbeiter ein ausgeprägtes Bewusstsein für die Regeln haben und in der Lage sind, die bereitgestellten Richtlinien einzuhalten.

Wir fördern aktiv eine Kultur, in der "das Einhalten der Regeln Business as usual" ist, und fordern unsere Mitarbeiter auf, potenzielle Compliance-Probleme offen anzusprechen.

1.3 Unsere Pflichten zur Förderung der Compliance

Ein Verstoß gegen die nationale und/oder EU-Datenschutz-Grundverordnung kann schwerwiegende Folgen für Danish Crown und die Person haben, die von einer Datenschutzverletzung oder einer unrechtmäßigen Verarbeitung ihrer personenbezogenen Daten betroffen ist. Demnach muss sich jeder Mitarbeiter der folgenden Pflichten bewusst sein:

A) Von allen Mitarbeitern wird erwartet, dass sie aktiv zur Einhaltung der geltenden datenschutzrechtlichen Vorschriften beitragen;

B) Kein Mitarbeiter sollte davon ausgehen, dass die Interessen der dänischen Krone jemals etwas anderes als die Einhaltung der Regeln erfordern;

C) Niemand hat die Befugnis, Befehle oder Anweisungen zu erteilen, die zu einem Verstoß gegen die Regeln führen würden;

D) Jeder Mitarbeiter ist verpflichtet, im Zweifelsfall den Rat und die Anleitung seines unmittelbaren Vorgesetzten und/oder des Group General Counsel einzuholen; und.

E) Jeder Verstoß oder vermutete Verstoß muss dem Group General Counsel gemeldet werden. Es ist auch möglich, ein Anliegen im Rahmen des dänischen Whistleblower-Programms zu melden.

1.4 Weltweit gleichbleibend hohe Standards

Diese Richtlinie gilt in allen Rechtsordnungen, in denen wir tätig sind. Unsere Politik spiegelt die Notwendigkeit weltweit einheitlicher und hoher Standards wider, um unser Engagement zu demonstrieren, unser Geschäft in einer Weise zu führen, die mit unseren Werten vereinbar ist, unabhängig von der Gerichtsbarkeit. Wir sind uns bewusst, dass es mögliche Unterschiede in der lokalen Gesetzgebung geben kann, die sich auf unsere lokalen Aktivitäten auswirken, und der Group General Counsel wird bei Bedarf weitere Ratschläge und Anweisungen geben.

2. Schutz personenbezogener Daten

2.1 Was sind personenbezogene Daten?

Personenbezogene Daten sind alle Informationen, die mit einer identifizierten oder identifizierbaren natürlichen Person ("betroffene Person") in Verbindung gebracht werden können.

Personenbezogene Daten müssen in Übereinstimmung mit der Datenschutz-Grundverordnung ("DSGVO") verarbeitet werden.

Personenbezogene Daten werden in drei Kategorien unterteilt: gewöhnliche personenbezogene Daten, sensible personenbezogene Daten und vertrauliche personenbezogene Daten:

Gewöhnliche personenbezogene Daten umfassen alle personenbezogenen Daten, die nicht als sensible personenbezogene Daten oder vertrauliche personenbezogene Daten eingestuft sind.

Sensible personenbezogene Daten sind Informationen, die gesetzlich als sensibel eingestuft sind, wie z. B. personenbezogene Daten über Gesundheit, Gewerkschaftszugehörigkeit, rassische und ethnische Herkunft, sexuelle und politische Überzeugungen und biometrische Daten.

Vertrauliche personenbezogene Daten sind Informationen, die als gewöhnlich eingestuft werden, aber die allgemeine Meinung der Gesellschaft würde sie als unangemessen erachten, wenn die Daten nicht angemessen gesichert sind. Vertrauliche personenbezogene Daten können Sozialversicherungsnummer, Reisepass, Finanzeinkommen, Strafregister usw. sein.

2.2 Verarbeitung personenbezogener Daten

Die Verarbeitung personenbezogener Daten ist im Grunde alles, was Sie mit personenbezogenen Daten tun können, sowohl die automatisierte Verarbeitung als auch die manuelle Verarbeitung, wie z. B. das Erheben, Strukturieren, Speichern, Offenlegen, Bereitstellen, Löschen und Vernichten.

Die Verarbeitung aller personenbezogenen Daten muss:

- in Übereinstimmung mit den Datenschutzgrundsätzen stehen, die unten in Abschnitt 2.2.1 beschrieben sind;
- über eine Rechtsgrundlage im Sinne der Datenschutzgesetzgebung verfügen, die in den Abschnitten 2.2.2 und 2.2.3 beschrieben ist; und
- in Übereinstimmung mit der DSGVO-Richtlinie für alle Mitarbeiter zu sein.

2.2.1 Grundsätze des Datenschutzes

Die nach den Datenschutzgesetzen geltenden Datenschutzgrundsätze schreiben vor, dass personenbezogene Daten:

- **Grundsatz 1:** Personenbezogene Daten müssen rechtmäßig, fair und transparent verarbeitet werden, indem sichergestellt wird, dass die betroffene Person über den Datenschutz informiert wird.
- **Grundsatz 2:** Personenbezogene Daten dürfen nur für einen bestimmten, ausdrücklichen und legitimen Zweck verarbeitet werden;
- **Grundsatz 3:** Personenbezogene Daten, die für einen bestimmten Zweck verarbeitet werden, müssen für den Zweck, für den sie verarbeitet werden, angemessen und relevant sein. Übermäßige Daten sollten nicht verarbeitet werden;
- **Grundsatz 4:** Die verarbeiteten personenbezogenen Daten müssen korrekt und aktuell gehalten werden;
- **Grundsatz 5:** Personenbezogene Daten, die verarbeitet werden, müssen gelöscht werden, wenn die Daten nicht mehr benötigt werden; und
- **Grundsatz 6:** Personenbezogene Daten, die gespeichert oder übermittelt werden, müssen durch geeignete technische und organisatorische Maßnahmen sicher aufbewahrt werden.

2.2.2 Rechtsgrundlage für die Verarbeitung gewöhnlicher und vertraulicher personenbezogener Daten

Neben der Erfüllung der Grundsätze der Datenverarbeitung (Ziffer 2.2.1) muss jede Verarbeitung auf einer Rechtsgrundlage ("Rechtsgrundlage") beruhen. Die erforderliche Rechtsgrundlage kann erlangt werden, wenn die Verarbeitung personenbezogener Daten ist:

- auf der Grundlage der Einwilligung der betroffenen Person;
- die für die Erfüllung eines Vertrags erforderlich sind;

- notwendig für die Erfüllung einer gesetzlichen Verpflichtung; oder
- zur Wahrung eines berechtigten Interesses erforderlich, sofern eine solche Verarbeitung nicht als schädlich für die betroffene Person angesehen wird.

2.2.3 Rechtsgrundlage für die Verarbeitung sensibler personenbezogener Daten

Es ist generell verboten, sensible personenbezogene Daten in Danish Crown zu verarbeiten, es gibt jedoch einige Fälle, in denen es notwendig ist, sensible personenbezogene Daten zu verarbeiten

z.B. in Bezug auf Gesundheit und Sicherheit sowie HR. In diesen Fällen muss geprüft werden, ob die Verarbeitung sensibler personenbezogener Daten:

- auf der Grundlage der Einwilligung der betroffenen Person; oder
- die für die Einhaltung der Vorschriften und Vorschriften über Beschäftigung, soziale Sicherheit oder Sozialschutz erforderlich sind.

2.3 DSGVO-Richtlinien

Um die Datenschutzgesetzgebung einzuhalten, wurde eine Reihe praktischer Leitlinien entwickelt.

Die Richtlinien sind integraler Bestandteil dieser Konzernrichtlinie zur Einhaltung des Datenschutzes und werden allen relevanten Mitarbeitern im Rahmen der verpflichtenden Schulungen im Rahmen unseres Datenschutz-Compliance-Programms zur Verfügung gestellt.

Weitere Informationen und die Leitlinien zur DSGVO finden Sie auf der Datenschutz-Intranetseite der dänischen Krone, die hier zu finden ist: *Link*

2.4 Lieferanten, die personenbezogene Daten in unserem Auftrag verarbeiten

Um die Datenschutzgesetzgebung einzuhalten, wurde eine Reihe praktischer Leitlinien entwickelt.

Danish Crown ist für den Schutz der personenbezogenen Daten seiner betroffenen Personen verantwortlich. Dies gilt auch, wenn ein Lieferant unsere Daten verarbeitet.

Um die DSGVO einzuhalten, ist es zwingend erforderlich, sicherzustellen, dass ein Datenverarbeitungsvertrag mit einem Lieferanten besteht, dessen Hauptleistung darin besteht, personenbezogene Daten im Auftrag von Danish Crown zu verarbeiten.

Danish Crown kann mit hohen Geldstrafen und Sanktionen belegt werden, wenn Danish Crown keine angemessenen Sicherheitsmaßnahmen für den Datenschutz, einschließlich Datenverarbeitungsvereinbarungen, ergreift. Weitere Anleitungen finden Sie in der DSGVO-Richtlinie, die Sie hier finden: *Link*

2.5 IT-Sicherheit

Die Mitarbeiter von Danish Crown sind verpflichtet, sich an die IT-Sicherheitsrichtlinie von Danish Crown zu halten, die die technischen und organisatorischen Sicherheitsmaßnahmen beschreibt, die jeder Mitarbeiter kennen und einhalten muss. Die IT-Sicherheitsrichtlinie finden Sie auf der Datenschutz-Intranet-Seite der dänischen Krone, die hier zu finden ist: *Link*

2.6 Verletzung der Datensicherheit

Danish Crown hat ein Verfahren eingeführt, das von allen Mitarbeitern im Falle einer Sicherheitsverletzung zu befolgen ist. Ein

Eine Verletzung der Datensicherheit kann als ein Vorfall definiert werden, der die Vertraulichkeit, Integrität oder Verfügbarkeit der personenbezogenen Daten einer betroffenen Person oder die IT-Infrastruktur der dänischen Krone, in der personenbezogene Daten verarbeitet werden, beeinträchtigen kann.

Beispiele für Sicherheitsverletzungen:

- Eine E-Mail mit vertraulichen oder sensiblen personenbezogenen Daten wird an einen oder mehrere falsche Empfänger (sowohl intern als auch extern) gesendet.
- Eine E-Mail mit vertraulichen oder sensiblen persönlichen Daten wird bei der Bildschirmfreigabe während Online-Meetings angezeigt.
- Ein Laptop wird gestohlen oder vergessen / unbeaufsichtigt gelassen.
- Physische Dokumente, die vertrauliche oder sensible personenbezogene Daten enthalten, gehen verloren oder werden verlegt.
- Cyber-Sicherheitsangriffe, bei denen es um personenbezogene Daten geht.
- Ein Dokument, das vertrauliche oder sensible personenbezogene Daten enthält, wurde unzureichend maskiert/verschleiert.

Im Falle einer Sicherheitsverletzung muss diese so schnell wie möglich über den IT Service Desk gemeldet werden. Die IT-Abteilung der dänischen Krone wird anschließend dazu beitragen, den Schaden einzudämmen und zu prüfen, ob der Verstoß den Behörden gemeldet werden muss.

Klicken Sie hier, um eine Sicherheitsverletzung zu melden: *Link*

Danish Crown ist verpflichtet, spätestens 72 Stunden, nachdem Danish Crown von dem Verstoß Kenntnis erlangt hat, zu prüfen, ob ein Verstoß der zuständigen Behörde gemeldet werden muss.

2.7 Wie kann man weitere Beratung einholen?

Bei Danish Crown erkennen wir an, dass ein offener und ehrlicher Dialog eine Voraussetzung ist, um unsere Integrität zu wahren und kontinuierlich zu stärken.

Als Mitarbeiter bei Danish Crown ist es Ihr Recht und Ihre Verantwortung, sich bei jeder Geschäftsentscheidung, bei der Sie sich unsicher sind, beraten zu lassen. Die erste Anlaufstelle in Bezug auf die DSGVO sollte darin bestehen, sich an GDPR@danishcrown.com