Revidiertes Datenschutzgesetz – Handlungsbedarf für KMU

Das revidierte Datenschutzgesetz tritt am 1. September 2023 in Kraft. Dabei werden Pflichten für Unternehmer ausgebaut und Sanktionen bei Verletzungen datenschutzrechtlicher Vorschriften verstärkt. Jedes Unternehmen ist von der Revision betroffen. Der Zeitpunkt ist daher ideal, um den Handlungsbedarf im Unternehmen zu überprüfen.

Überblick

Sarah Dietschweiler
Master of Law
Rechtsanwältin und Notarin
sd@hueberli.com

Hueberli—Lawyers

Das revidierte Datenschutzgesetz (rDSG) legt einen Fokus auf eine verstärkte Governance. Während die Grundsätze der Datenbearbeitung weitestgehend unverändert bleiben, wird die Transparenz der Datenbearbeitungen verbessert und die Rechte der betroffenen Personen werden gestärkt. Unternehmen, welche die Datenschutz-Grundverordnung der EU (DSGVO) bereits umsetzen, haben dabei einen Vorsprung bei der Implementierung der Neuregelungen. Dennoch gibt es im rDSG teilweise abweichende oder weitergehende Regelungen, als die DSGVO sie vorsieht. Im Rahmen der Überprüfung der Datenschutzkonformität sowie der Einführung der Neuregelungen des rDSG gibt es diverse Aspekte zu berücksichtigen. In der nachfolgenden Übersicht werden die wichtigsten Handlungsfelder aufgeführt.

Handlungsbedarf für KMU

Bestandesaufnahme: In einem ersten Schritt erfolgt eine Analyse der Datenbearbeitungen. Dabei werden diverse Leitfragen beantwortet: Welche Personendaten bearbeiten wir zu welchen Zwecken? Von wem erhalten wir Daten? An wen geben wir Daten weiter? Etc.

Die Identifizierung der Datenbearbeitungen im Unternehmen ist unabdingbar, um weitere datenschutzrechtliche Pflichten einzuhalten sowie um ein gewisses Verständnis über den Umgang mit den bearbeiteten Personendaten zu schaffen. Das Ergebnis der Bestandesaufnahme kann sodann in einem Bearbeitungsverzeichnis dokumentiert werden. Obwohl für die meisten Unternehmen aufgrund der KMU-Ausnahmeregelung gemäss rDSG keine Pflicht zur Führung eines Verzeichnisses besteht, ist diese Vorgehensweise empfehlenswert. Insbesondere dient ein Bearbeitungsverzeichnis als Grundlage zur Erstellung einer konformen Datenschutzerklärung.

Datenschutzerklärung: Unternehmen müssen betroffene Personen über die Bearbeitung von Personendaten informieren. Die meisten Unternehmen werden bereits eine Datenschutzerklärung auf ihrer Website veröffentlicht haben. Mit dem rDSG wird jedoch die Informationspflicht verstärkt. Aus diesem Grund ist es empfehlenswert, bestehende Datenschutzerklärungen auf ihre Vollständigkeit und Rechtsmässigkeit zu überprüfen.

Auftragsbearbeitungsverträge: Unternehmen trifft die Pflicht, für den rechtmässigen Umgang mit Personendaten zu sorgen. Wenn die Bearbeitung einem Auftragsbearbeiter (z.B. IT-Provider) anvertraut wird, bleibt das Unternehmen grundsätzlich für die rechtmässige Datenbearbeitung verantwortlich. Daher ist das Unternehmen verpflichtet, sämtliche Auftragsbearbeiter zu identifizieren und sogenannte Auftragsbearbeitungsverträge abzuschliessen. Wurden bereits Standard-Auftragsbearbeitungsverträge abgeschlossen, ist eine Überprüfung auf deren Konformität empfehlenswert.

Daten-Export: Sämtlicher Auslandtransfer von personenbezogenen Daten muss einer Identifikation und Überprüfung zugrunde gelegt werden. Wenn im Empfängerstaat kein angemessenes Datenschutzniveau herrscht, wie z.B. in den USA, muss der Daten-Export besonders abgesichert werden. Insbesondere ist die Verwendung der EU-Standardvertragsklauseln («SCC») angezeigt, wobei diese punktuell an schweizerisches Recht angepasst werden müssen.

Technische und organisatorische Massnahmen (TOMs): Personendaten müssen angemessen gegen unrechtmässige Bearbeitungen geschützt werden. Unternehmen sind daher verpflichtet, angemessene Massnahmen (z.B. betreffend Schutz der IT-Systeme sowie Zutritts-, Zugangs- und Zugriffskontrollen) zu treffen und entsprechend zu dokumentieren.

Betroffenenrechte: Betroffenen Personen stehen diverse Rechte im Zusammenhang mit der Bearbeitung von Personendaten zu. Mit dem rDSG wurden diese teilweise an die DSGVO angeglichen; einige Abweichungen bleiben jedoch bestehen. Im Zusammenhang mit den Betroffenenrechten sollten Unternehmen entsprechende Prozesse zur Umsetzung einführen. Beispielsweise hat jede betroffene Person das Recht, Auskunft über ihre eigenen Pesonendaten zu erhalten. Auf Auskunftsgesuche muss ein Unternehmen innerhalb von 30 Tagen reagieren können. Des Weiteren können Betroffene eine Datenkorrektur oder die Herausgabe ihrer Daten verlangen. Um Betroffenenrechte zu gewähren, sollten Unternehmen eine zuständige Stelle bestimmen.

«Privacy by Design» / «Privacy by Default»: Privacy by Design verlangt die Berücksichtigung der datenschutzrechtlichen Bestimmungen bereits bei der Planung der Datenbearbeitungen. Dies umfasst beispielsweise die Pflicht von Verantwortlichen über ein System zu verfügen, welches einen Zugang zu den bearbeiteten Daten, das Löschen derselben sowie das Vergeben von individuellen Zugriffsrechten

ermöglicht. Privacy by Default verlangt die Einführung von datenschutzfreundlichen Voreinstellungen, insbesondere bei Online-Diensten.

Interne Prozesse: Eine Überprüfung oder Einführung diverser interner Prozesse ist angezeigt. Hierzu gehört insbesondere ein Prozess zur Datenschutz-Folgenabschätzung (DSFA). Die DSFA soll der Selbstbeurteilung eines datenschutzrechtliche relevanten Vorhabens dienen. Auch in Bezug auf die Meldung und die Bearbeitung von Verletzungen betreffend die Datensicherheit haben Unternehmen Prozesse einzuführen, respektive bestehende an die neuen Vorschriften anzupassen. Nicht zuletzt sollten Unternehmen ihre Mitarbeiter im Kontext des Datenschutzes und allfälliger drohender Sanktionen schulen und periodisch weiterbilden.

Sanktionen

Um den Neuregelungen Nachdruck zu verleihen, führt das revidierte Datenschutzgesetz eine persönliche Strafbarkeit ein. Während die DSGVO Bussen gegen die Unternehmen vorsieht, kann nach rDSG der verantwortliche Mitarbeiter strafrechtlich zur Verantwortung gezogen werden. Die Verletzung von datenschutzrechtlichen Informations-, Auskunfts- und Mitwirkungspflichten kann dabei mit Bussen von bis zu CHF 250’000.– bestraft werden. Nicht zu vernachlässigen ist überdies das drohende Reputationsrisiko im Falle einer Verletzung von datenschutzrechtlichen Vorschriften. Kunden erwarten einen verantwortungsbewussten Umgang mit ihren Personendaten.

Fazit

Ein sensibler und bewusster Umgang mit Personendaten ist für jedes Unternehmen unerlässlich. Um für das Inkrafttreten des revidierten Datenschutzgesetzes vorbereitet zu sein, lohnt sich eine frühzeitige Überprüfung der Datenschutzkonformität sowie Einführung der Neuregelungen. Hueberli Lawyers AG berät Sie gerne in datenschutzrechtlichen Fragestellungen. Wir freuen uns über Ihre Kontaktaufnahme.[1]

Hueberli—Lawyers

Sarah Dietschweiler, MLaw
Rechtsanwältin und Notarin
sd@hueberli.com

Hueberli Lawyers AG
Wattwil – Rapperswil – Zürich
+41 71 988 30 00 – www.hueberli.com

[1] Stand Mai 2023.