Doing Business in the Netherlands! –

Ein rechtlicher Leitfaden für Unternehmen

2024

Your goal.Our drive.

BUREN

LEGAL | TAX | NOTARY

7 Datenschutz

7.1 Anwendbare Vorschriften

Die wichtigsten Vorschriften für den Schutz personenbezogener Daten in den Niederlanden sind:

- Verordnung (EU) 2016/679 vom 27.April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (DSGVO); und
- Das niederländische Gesetz zur Umsetzung der DSGVO (*Uitvoeringswet Algemene verordening gegevensbescherming* - UAVG) vom 16.Mai 2018.

Die Datenschutz-Grundverordnung

Die DSGVO ist ein einheitliches Datenschutzgesetz, das in der gesamten EU, im EWR gilt und in den Niederlanden unmittelbar Anwendung findet. Sie erlaubt es den EU-Mitgliedstaaten, zusätzliche Durchführungsbestimmungen zu erlassen - z.B. in Bezug auf besondere Kategorien personenbezogener Daten im Sinne von Artikel 9 Absatz 1 der DSGVO, und bestimmte Ausnahmen für wissenschaftliche oder historische Forschung oder statistische Zwecke, für Authentifizierungs- und Sicherheitszwecke usw. vorzusehen. Die Niederlande hat von diesem Recht durch die Einführung des UAVG Gebrauch gemacht.

Die DSGVO definiert “personenbezogene Daten” als alle Daten, die entweder direkt oder indirekt zu bestimmten Personen (den betroffenen Personen) zurückverfolgt werden können. Gesundheitsdaten, genetische Daten, Daten über Rasse oder ethnische Zugehörigkeit und andere besondere Kategorien personenbezogener Daten sowie personenbezogene Daten im Zusammenhang mit strafrechtlichen Verurteilungen und Straftaten genießen zusätzlichen Schutz.

Die DSGVO definiert einen “Verantwortlichen” als die Partei, die den Zweck und die Mittel der Verarbeitung festlegt, und einen “Auftragsverarbeiter” als die Partei, die personenbezogene Daten im Auftrag eines Verantwortlichen verarbeitet. Sowohl die Verantwortlichen als auch die Auftragsverarbeiter unterliegen den Vorschriften der DSGVO.

Die DSGVO sieht vor, dass die Verantwortlichen, zum Nachweis der Einhaltung der Vorschriften, interne Richtlinien entwickeln und Maßnahmen umsetzen, die den Grundsätzen des Datenschutzes durch Technikgestaltung und durch datenschutzfreundliche Voreinstellungen entsprechen.

Die Verarbeitung personenbezogener Daten (einschließlich der Weitergabe an Dritte) muss rechtmäßig, transparent und fair sein. Sie muss auf bestimmte Zwecke und auf die für diese Zwecke erforderlichen Daten beschränkt sein (Datenminimierung).

Weitere Grundsätze sind, dass die Daten:

- richtig sind;
- sicher aufbewahrt werden; sowie
- nicht länger als nötig aufbewahrt werden (Speicherbegrenzung).

Die DSGVO verpflichtet die Unternehmen außerdem, die betroffenen Personen darüber zu informieren, wie ihre Daten verwendet werden, und die Einhaltung der DSGVO zu dokumentieren. Betroffene Personen haben das Recht, auf ihre personenbezogenen Daten zuzugreifen, Berichtigungen zu verlangen und ihre Daten unter bestimmten Bedingungen löschen (oder einschränken) zu lassen.

Die Verantwortlichen und die Auftragsverarbeiter müssen in den folgenden Fällen einen Datenschutzbeauftragten (DSB) benennen:

- wenn es sich um öffentliche Behörden handelt;
- wenn ihre Haupttätigkeit in der regelmäßigen und systematischen Überwachung von betroffenen Personen in großem Umfang besteht; oder
- wenn ihre Haupttätigkeit in der Verarbeitung sensibler personenbezogener Daten in großem Umfang besteht (einschließlich der Verarbeitung von Informationen über strafbare Handlungen).

Die Datenschutzrichtlinie für elektronische Kommunikation und das niederländische Cookie-Gesetz

Zusätzliche Bestimmungen zum Datenschutz und zum Schutz der Privatsphäre im Zusammenhang mit der Telekommunikation sind in der Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12.Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (ePrivacy-Richtlinie) sowie im niederländischen Cookie-Gesetz (*Cookiewet*) enthalten.

Die Datenschutzrichtlinie 2002/58/EG für elektronische Kommunikation wurde durch das niederländische Telekommunikationsgesetz (*Telecomunicatiewet*) umgesetzt, das unerbetene Kommunikation per E-Mail (sowie Faxe und automatische Kommunikationssysteme) für kommerzielle, nichtkommerzielle oder wohltätige Zwecke verbietet, es sei denn, der Absender kann die vorherige Zustimmung des Empfängers nachweisen.

Nach dem Cookie-Gesetz ist für die Verwendung von Cookies eine informierte Zustimmung erforderlich, es sei denn, es handelt sich um Cookies, die:

- erforderlich sind, um die Kommunikation zu erleichtern; oder
- für den von den Nutzern angeforderten Dienst unbedingt erforderlich sind; oder
- darauf abzielen, Informationen über die Qualität und/oder Wirksamkeit der erbrachten Dienstleistungen zu erhalten, und dies keine oder nur geringe Auswirkungen auf das persönliche Leben der Nutzer haben.

Diese Regeln gelten sowohl für First Party- Cookies- als auch für Tracking-Cookies.

7.2 Geografischer Geltungsbereich

Die DSGVO findet gemäß Artikel 3 Absatz 1 DSGVO Anwendung für die Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters im Europäischen Wirtschaftsraum (EWR) erfolgt, unabhängig davon, ob die Verarbeitung im EWR stattfindet. Der Begriff “Niederlassung” erstreckt sich auf jede tatsächliche und effektive Tätigkeit - selbst eine minimale -, die durch eine feste Einrichtung im EWR ausgeübt wird.

Unternehmen, die nicht im EWR ansässig sind, unterliegen ebenfalls der DSGVO, wenn sie Waren und Dienstleistungen für Personen im EWR anbieten oder das Verhalten von betroffenen Personen im EWR überwachen. Nicht-EWR-Unternehmen, die dies regelmäßig oder in Kombination mit bestimmten risikoreichen Tätigkeiten tun, müssen einen im EWR niedergelassenen Vertreter benennen. Nach den Vorschriften müssen Websites, die sich an ein EWR-Publikum richten oder Besucher aus dem EWR verfolgen, die DSGVO einhalten.

Für Datenübermittlungen aus den Niederlanden in andere EWR-Länder gelten keine besonderen Anforderungen. Für die Übermittlung personenbezogener Daten in Länder außerhalb des EWR ist jedoch - von wenigen Ausnahmen abgesehen - entweder eine Entscheidung der Europäischen Kommission erforderlich, dass das Zielland ein angemessenes Schutzniveau (Safe Harbour) gewährleistet (dies gilt beispielsweise für das Vereinigte Königreich, die Schweiz, Kanada, Israel und Japan), oder es müssen angemessene Garantien zum Schutz der Rechte der betroffenen Personen vorgesehen werden (z. B. die Standardvertragsklauseln der Kommission oder verbindliche unternehmensinterne Vorschriften).

Am 16.Juli 2020 veröffentlichte der EuGH seine Entscheidung in der Sache “Datenschutzbeauftragter geg. Facebook Irland, Maximillian Schrems”, gemeinhin als “Schrems II” bezeichnet. Darin wurde der EU-US-Datenschutzschild für ungültig erklärt. Dieser sollte Unternehmen auf beiden Seiten des Atlantiks einen DSGVO-konformen Mechanismus zur Übermittlung personenbezogener Daten aus der EU in die USA bieten und dadurch den transatlantischen Handel fördern.

Am 10.Juli 2023 hat die Europäische Kommission ihren Angemessenheitsbeschluss für den “Datenschutzrahmen EU-US” angenommen. In dem Beschluss wird festgestellt, dass die Vereinigten Staaten ein angemessenes Schutzniveau - vergleichbar mit dem der EU - für personenbezogene Daten gewährleisten, welche gemäß dem neuen Rahmenwerk von der EU an US-Unternehmen übermittelt werden. Auf der Grundlage des neuen Angemessenheitsbeschlusses können personenbezogene Daten gefahrlos aus der EU an US-Unternehmen, die an dem Rahmenwerk

teilnehmen, übermittelt werden, ohne dass zusätzliche Datenschutzgarantien eingeführt werden müssen.

Der Angemessenheitsbeschluss folgte auf die Verabschiedung der Durchführungsverordnung “Enhancing Safeguards for United States Signals Intelligence Activities” durch US-Präsident Biden am 7.Oktober 2022 und auf eine Verordnung des US-Justizministers. Der Datenschutzrahmen EU - US führt neue verbindliche Garantien ein, um alle vom Europäischen Gerichtshof geäußerten Bedenken auszuräumen, einschließlich der Beschränkung des Zugriffs auf EU-Daten durch US-Nachrichtendienste auf das notwendige und verhältnismäßige Maß und der Einrichtung eines Gerichts zur Datenschutzüberprüfung (DPRC), zu dem EU-Bürger Zugang haben. Der neue Rahmen bringt erhebliche Verbesserungen im Vergleich zu dem Mechanismus, der unter dem EU-US-Datenschutzschild bestand. Stellt das DPRC beispielsweise fest, dass Daten unter Verstoß gegen die neuen Garantien erhoben wurden, kann es die Löschung der Daten anordnen. Die neuen Garantien im Bereich des staatlichen Zugriffs auf Daten werden die Verpflichtungen ergänzen, die US-Unternehmen, die Daten aus der EU importieren, eingehen müssen.

US-Unternehmen können dem Datenschutzrahmen EU-US beitreten, indem sie sich verpflichten, eine Reihe detaillierter Datenschutzverpflichtungen einzuhalten, z. B. die Verpflichtung, personenbezogene Daten zu löschen, wenn sie für den Zweck, für den sie erhoben wurden, nicht mehr erforderlich sind, und die Kontinuität des Schutzes zu gewährleisten, wenn personenbezogene Daten an Dritte weitergegeben werden. Das Funktionieren des Datenschutzrahmen EU-US wird in regelmäßigen Abständen von der Europäischen Kommission zusammen mit Vertretern der europäischen Datenschutzbehörden und der zuständigen US-Behörden überprüft. Die erste Überprüfung wird innerhalb eines Jahres nach Inkrafttreten des Angemessenheitsbeschlusses stattfinden, um zu überprüfen, ob alle relevanten Elemente vollständig in den US-Rechtsrahmen umgesetzt wurden und in der Praxis wirksam funktionieren - Grundsätze des Datenschutzes durch Technikgestaltung und des Datenschutzes durch datenschutzfreundliche Voreinstellungen. Am 4.Juni 2021 veröffentlichte die Europäische Kommission modernisierte SCCs (Standardvertragsklauseln) für Datenübermittlungen von Verantwortlichen oder Auftragsverarbeitern in der EU/im EWR (oder sonstige der DSGVO unterliegende) an Verantwortliche oder Auftragsverarbeiter mit Sitz außerhalb der EU/des EWR (die nicht der DSGVO unterliegen). Diese modernisierten SCCs ersetzen die drei SCC-Sätze, die unter der vorherigen Datenschutzrichtlinie 95/46/EG angenommen wurden. Seit dem 27.September 2021 ist es nicht mehr möglich, Verträge zu schließen, die diese früheren SCCs enthalten. Am 27.Dezember 2022 lief die Schonfrist für die Verwendung von Verträgen, die diese früheren SCC enthalten, ab.

7.3 Rolle und Befugnisse der Datenschutzbehörde

Die niederländische Datenschutzbehörde (Autoriteit Persoonsgegevens) wurde durch das UAVG als unabhängige Aufsichtsbehörde im Sinne der DSGVO eingerichtet. Die Datenschutzbehörde hat die Aufgabe, die Verarbeitung personenbezogener Daten im Einklang mit den Bestimmungen der DSGVO und dem Gesetz zu überwachen.

Zu den Aufgaben der niederländischen Datenschutzbehörde gehören:

- Beratung von Einzelpersonen und Organisationen in Form von Informationen und Ratschlägen;
- Unterstützung von Organisationen durch Bereitstellung praktischer Instrumente;
- Überprüfung von Anträgen auf vorherige Konsultation und von Genehmigungsanträgen für die Verarbeitung von Daten über strafrechtliche Verurteilungen und Straftaten; und
- Förderung der Erstellung von Verhaltenskodizes.

Sie ist befugt, Verstöße zu untersuchen, Anordnungen zur Unterbindung von Verstößen zu erlassen und Geldbußen von bis zu 20 Mio. EUR oder 4 % des weltweiten Jahresumsatzes zu verhängen, je nachdem, welcher Betrag höher ist.

Amsterdam

WTC - Turm Seven
level 14
Strawinskylaan 1441
NL-1077 XX Amsterdam
Niederlande

Postfach 78058
NL-1070 LP Amsterdam
Niederlande

T +31 (0)20 333 8390

Beijing

ZhongYu Plaza, Room
1602
North Gongti Road 6
100027 Beijing
China

T +86 (10)8 5235 780

Den Haag

Schenkkade 50
NL-2595 AR Den Haag
Niederlande

Postfach 18511
NL-2502 EM Den Haag
Niederlande

T +31 (0)70 318 4200

Luxemburg

5, rue Goethe
L-1637 Luxemburg
Luxemburg

T +352 (0)2644 0919

Shanghai

Room 1661, Building B
North KaiXuan Road 1188
200063 Shanghai
China

T +86 (21)6 1730 388

burenlegal.com

BUREN
LEGAL | TAX | NOTARY