SCHINDHELM

NEUES EU-DATENSCHUTZRECHT: GRUNDSÄTZE FÜR DIE VERARBEITUNG PERSONENBEZOGENER DATEN

Die neue europäische Datenschutz-Grundverordnung (DSGVO) wird ab dem 25. Mai 2018 in allen EU-Staaten wirksam und betrifft weltweit Unternehmen, welche auf dem europäischen Markt tätig sind. Sie gewährt den EU-Bürgern ein höheres Schutzniveau ihrer personenbezogenen Daten. Die Grundsätze, denen jede Verarbeitung personenbezogener Daten entsprechen muss, finden sich in Art. 5 Abs. 1 und 2 der DSGVO und sind die folgenden.

1. Rechtmäßigkeit, Treu und Glauben, Transparenz

Die Verarbeitung personenbezogener Daten muss auf Basis einer Rechtsgrundlage erfolgen. Die Daten müssen nach Treu und Glauben sowie in einer für die betroffene Person nachvollziehbaren Weise verarbeitet werden. Den Betroffenen sind Informationen zu der Verarbeitung der Daten in präziser, transparenter, verständlicher und leicht zugänglicher Form sowie einfacher und klarer Sprache zur Verfügung zu stellen.

2. Zweckbindung

Die Daten dürfen nur für festgelegte, eindeutige und legitime Zwecke erhoben werden. Eine Weiterverarbeitung von Daten in einer mit diesen Zwecken nicht zu vereinbarenden Weise ist unzulässig. Die Interessenabwägung, die direkt mit der Zweckbindung zusammenhängt, wird als zentraler Erlaubnistatbestand angesehen. Daher muss der konkrete Zweck der Verarbeitung personenbezogener Daten für jeden Einzelfall genau eruiert werden.

3. Datenminimierung

Die Datenerhebung und -verarbeitung ist auf die Daten zu reduzieren, welche für die Erfüllung des erfolgten Zwecks tatsächlich erforderlich sind.

4. Richtigkeit

Unternehmen müssen in Zukunft nachweisen können, dass personenbezogene Daten sachlich richtig und auf dem neuesten Stand sind. Unrichtige Daten sind daher unverzüglich zu löschen oder zu berichtigen. Unternehmen müssen eigenverantwortlich regelmäßige „Aktualisierungsroutinen“ durchführen.

5. Speicherbegrenzung

Zeitlich ist das Speichern in personenbezogener Form grundsätzlich auf die Zweckerreichung begrenzt. Ferner müssen gesetzlich vorgeschriebene Speicherfristen eingehalten werden. Das Unternehmen muss ebenfalls prüfen, ob nicht eine Pseudonymisierung oder Anonymisierung der Daten in Betracht kommt. Bei einer Pseudonymisierung sind die Daten ohne die Verbindung mit weiteren Informationen keiner Person zuordenbar. Hierzu sind technische und organisatorische Maßnahmen zu ergreifen.

6. Integrität, Vertraulichkeit

In Zukunft müssen Maßnahmen etabliert werden, um unbefugter und unrechtmäßiger Verarbeitung sowie unbeabsichtigtem Verlust oder unbeabsichtigter Zerstörung bzw. der Schädigung von Daten vorzubeugen. Die erforderlichen Vorkehrungen sind vor allem in IT-technischer und organisatorischer Hinsicht (z.B. durch Zugriffs- und Berechtigungskonzepte, Verschlüsselung) zu treffen. Diesbezüglich sind insbesondere Art. 32 (Sicherheit der Verarbeitung) sowie Art. 35 (Datenschutz-Folgenabschätzung) zu beachten. Wird der Schutz personenbezogener Daten verletzt und besteht ein Risiko für die Rechte und Freiheiten von natürlichen Personen, ist dies nach Art. 33 der Datenschutzbehörde zu melden. Gegebenenfalls – bei hohem Risiko – ist die betroffene Person selbst zu informieren.

7. Accountability

Gemäß dem Grundsatz der „Accountability“ (Art. 5 Abs. 2) müssen Unternehmen die Einhaltung der vorgenannten Grundsätze dokumentarisch nachweisen können.

Bei weiteren Fragen stehen die Kolleginnen und Kollegen der jeweiligen Standorte jederzeit gerne zur Verfügung.

SCHINDHELM

NEW EU DATA PROTECTION LAW: PRINCIPLES ON THE PROCESSING OF PERSONAL DATA

The new European General Data Protection Regulation (GDPR) will apply directly from 25 May 2018 across all EU member states, and will affect companies worldwide who do business on the European market. It ensures a higher level of protection of the personal data of EU citizens. The principles, which must be complied with whenever personal data is processed, are laid down in Subsections 1 and 2 of Article 5 of the GDPR and are as follows:

1. Lawfulness; fairness; transparency

The processing of personal data must be carried out on a legal basis (consent or other legitimate basis). Data must be processed in a fair and transparent way which is comprehensible for the person involved. Information on the processing shall be provided to the affected person in a clear and plain language and in a precise, transparent, easy to understand and easily accessible format.

2. Purpose limitation

Data may only be collected for determined, explicit and legitimate purposes. Further, processing of such data is allowed only where the processing is compatible with the purpose for which the data were initially collected. In many cases, the balancing of interests between the controller and the affected person, which relates directly to the principle of purpose limitation, may constitute a legal ground for the processing. Therefore, the specific purpose for processing must be precisely determined for each individual case.

3. Data minimisation

The collection and processing of personal data shall be limited to what is indeed necessary for the purposes for which they are processed.

4. Accuracy

In the future, companies must be able to demonstrate that personal data is accurate and kept up-to-date. Consequently, inaccurate data is to be deleted or rectified without delay. Businesses are responsible for maintaining regular 'update routines'.

5. Storage limitation

Personal data may be stored for no longer than is necessary in light of the purposes for which the personal data were processed. In addition, time limits for storage set forth by law shall also be complied with. Businesses shall consider whether pseudonymisation or anonymisation may be applied. Personal data which have undergone pseudonymisation cannot be attributed to a natural person without the use of additional information. For this purpose, technical and organisational measures shall be implemented.

6. Integrity, confidentiality

In order to prevent unauthorised or unlawful processing and accidental loss, destruction or damage of personal data appropriate measures shall be introduced. Such measures are to be taken especially in the fields of IT and organisation (e.g. access and authorisation concepts, encryption). In this respect, especially Article 32 (Security of processing) and Article 35 (data protection impact assessment) need to be observed. In the case of a personal data breach which is likely to result in a risk to the rights and freedom of natural persons, the controller shall notify the competent data protection authority. Where necessary – where the risk is high – the affected persons themselves must also be notified.

7. Accountability

In accordance with the principle of accountability (Art. 5 Abs. 2) the companies shall be responsible for and be able to demonstrate compliance with the above mentioned principles by means of documentary evidence.

Should you have any queries, please do not hesitate to contact one of our offices.

AUSTRIA

GRAZ
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner
Rechtsanwälte GmbH
graz@scwp.com

LINZ
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner
Rechtsanwälte GmbH
linz@scwp.com

WELS
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner
Rechtsanwälte GmbH
wels@scwp.com

WIEN
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner
Rechtsanwälte GmbH
wien@scwp.com

BELGIUM

BRÜSSEL
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner
Rechtsanwälte GmbH
brussels@scwp.com

BULGARIA

SOFIA
SCHINDHELM
Dr. Cornelia Draganova & Colleagues
sofia@schindhelm.com

VARNA
SCHINDHELM
Dr. Cornelia Draganova & Colleagues
varna@schindhelm.com

CHINA

SHANGHAI
SCHINDHELM
Schindhelm Rechtsanwaltsgesellschaft mbH
shanghai@schindhelm.com

TAICANG
SCHINDHELM
Schindhelm Rechtsanwaltsgesellschaft mbH
taicang@schindhelm.com

CZECH REPUBLIC

PILSEN
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner v.o.s
Advokátní kancelář
plzen@scwp.com

PRAG
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner v.o.s
Advokátní kancelář
praha@scwp.com

GERMANY

DÜSSELDORF
SCHINDHELM
Schmidt Rogge Thoma Rechtsanwälte
Partnergesellschaft mbB
duesseldorf@schindhelm.com

HANNOVER
SCHINDHELM
Schindhelm Rechtsanwaltsgesellschaft mbH
hannover@schindhelm.com

OSNABRÜCK
SCHINDHELM
Schindhelm Rechtsanwaltsgesellschaft mbH
osnabrueck@schindhelm.com

HUNGARY

BUDAPEST
SCWP SCHINDHELM
Zimányi & Fakó Rechtsanwälte
budapest@scwp.hu

ITALY

BOLOGNA
DIKE SCHINDHELM
DIKE Associazione Professionale
bologna@schindhelm.com

ROMANIA

BUKAREST
SCHINDHELM
Schindhelm & Asociatii S.C.A.
bukarest@schindhelm.com

POLAND

BRESLAU
SDZLEGAL SCHINDHELM
Kancelaria Prawna
Schampera, Dubis, Zając i Wspólnicy sp.k.
wroclaw@sdzlegal.pl

WARSCHAU
SDZLEGAL SCHINDHELM
Kancelaria Prawna
Schampera, Dubis, Zając i Wspólnicy sp.k.
warszawa@sdzlegal.pl

SLOVAKIA

BRATISLAVA
SCWP SCHINDHELM
Saxinger, Chalupsky & Partner s.r.o.
bratislava@scwp.com

SPAIN

BILBAO
LOZANO SCHINDHELM
Lozano, Hilgers & Partner SLP
bilbao@schindhelm.com

DENIA
LOZANO SCHINDHELM
Lozano, Hilgers & Partner SLP
denia@schindhelm.com

MADRID
LOZANO SCHINDHELM
Lozano, Hilgers & Partner SLP
madrid@schindhelm.com

PALMA DE MALLORCA
LOZANO SCHINDHELM
Lozano, Hilgers & Partner SLP
palma@schindhelm.com

VALENCIA
LOZANO SCHINDHELM
Lozano, Hilgers & Partner SLP
valencia@schindhelm.com

Herausgeber, Medieninhaber, Redaktion: Schindhelm Rechtsanwaltsgesellschaft mbH | German Centre for Industry and Trade, Shanghai Tower 1, Atrium 3. Floor, Unit 321 88, Keyuan Road, Zhangjiang Hi-Tech Park, Pudong, Shanghai 201203 | Tel: +86 21 289866-60 | shanghai@schindhelm.com | Handelsregister: Amtsgericht Osnabrück HRB 18976. Schindhelm Rechtsanwaltsgesellschaft mbH ist Mitglied der SCWP Schindhelm Services SE, Allianz europäischer Wirtschaftskanzleien | Alle Angaben erfolgen trotz sorgfältiger Bearbeitung ohne Gewähr und können im Einzelfall die individuelle Beratung nicht ersetzen. Die Haftung der Autoren oder der Herausgeberin ist ausgeschlossen.