SCHINDHELM

NEUES EU-DATENSCHUTZRECHT: COMPLIANCE CHECK

Am 25. Mai 2018 wird die Datenschutzgrundverordnung (DSGVO) der EU wirksam werden, die erhöhte Nachweis- und Kontrollpflichten beinhaltet. Um die Einhaltung des neuen Rechts sicher zu stellen, müssen die Organisationen umfangreiche Kontrollmechanismen etablieren. Das Prinzip der Nachweisbarkeit verlangt von den Organisationen, die Compliance belegen zu können. Ein Verstoß kann zu erheblichen Bußgeldern von bis zu EUR 20 Millionen oder 4 % des jährlichen Umsatzes führen. Wir empfehlen, sich frühzeitig vorzubereiten, um eine Compliance bis Mai 2018 sicher zu stellen.

1. Information

Zunächst sollten Sie sich umfassend über die neuen Regelungen informieren und Ihre Datenverarbeitung prüfen lassen.

2. Eruierung der Datenprozesse

Danach sind die Bereiche ausfindig zu machen, in denen Datenprozesse stattfinden: Typischerweise sind dies vor allem HR und CRM (inkl Marketing).

3. Analyse der Prozesse

Jeder Prozess muss im Einzelnen dahingehend analysiert werden, ob die Datenschutz-prinzipien eingehalten werden. Zusätzlich müssen die Unternehmen die Rechtsgrundlage jedes Datenprozesses bestimmen. Soweit der Prozess auf einer Einwilligung beruht, ist zu prüfen, ob den Betroffenen nachweislich die erforderlichen Informationen gegeben wurden.

4. Analyse der internen Prozesse

Ferner müssen die internen Prozesse sowie die IT-Systeme überprüft werden. Es sind die organisatorischen und technischen Maßnahmen zur Datenschutzsicherung zu definieren und Verantwortlichkeiten zu bestimmen. Die Aufsichtsbehörden erwarten, dass Datenschutzberichte bis in die obersten Managementebenen eskaliert werden. Hinsichtlich der erforderlichen technischen Maßnahmen ist ein IT-Experte zu Rate zu ziehen.

5. Richtlinien und Erklärungen

Sobald die internen Prozesse geprüft wurden, müssen die entsprechenden organisatorischen und technischen Maßnahmen in internen Richtlinien umgesetzt werden. Unternehmen sollten insbesondere über eine Datenschutzrichtlinie zur Verarbeitung von Arbeitnehmerdaten sowie zu Kundendaten verfügen. Ebenfalls sollten Handlungsanweisungen zum Vorgehen bei Datenschutzverstößen und Datenübertragungen existieren. Ferner ist auch Ihre Datenschutzerklärung zu aktualisieren bzw zu erstellen, in denen Sie Personen, die mit Ihnen in Kontakt treten, über die Nutzung Ihrer personenbezogenen Daten informieren.

6. Dokumentation

Für bestimmte Datenverarbeitungsprozesse bestehen Dokumentationspflichten. Wir empfehlen Ihnen generell, jegliche Datenprozesse zu dokumentieren, um Ihrer Nachweisbarkeitspflicht zu genügen.

7. Datenschutzbeauftragter

Bestimmte Arten von Unternehmen sind verpflichtet, einen Datenschutzbeauftragten zu bestellen. Sie müssen prüfen, ob dies auch für Ihr Unternehmen zutrifft.

8. Sensibilisierung und Schulung

Mitarbeiter mit Zugang zu personenbezogenen Daten müssen über die neuen Anforderungen informiert werden.

Überwachung und Sicherheit sind kontinuierliche Prozesse, die Sie fortlaufend während des gesamten Datenverarbeitungs-prozesses zu beachten haben.

Die vorliegende Zusammenfassung gibt einen generellen Überblick über ein Datenschutz-audit. Ob diese für Ihr Unternehmen unter Ihrer Rechtsprechung zutrifft, bedarf der konkreten Analyse.

Für die Unterstützung bei der Durchführung eines solchen Verfahrens, stehen die KollegInnen der jeweiligen Standorte jederzeit gerne zur Verfügung.

SCHINDHELM

NEW EU DATA PROTECTION LAW: COMPLIANCE CHECK

The General Data Protection Regulation (GDPR) of the EU will come into force on 25 May 2018 and it will affect organisations worldwide working with or within the EU. The GDPR promotes accountability and governance. Organisations are required to put into place comprehensive governance measures to ensure compliance. The accountability principle expressly requires the organisations to be able to demonstrate that they comply. Non-compliance can lead to heavy fines up to EUR 20 million or 4 % of the global annual turnover, whichever is higher. You must prepare in advance to assess and ensure compliance by May 2018 by going through the following steps.

1. Getting informed

You have to gather information on the new requirements and set up internal assessment.

2. Identify the data processing activities

You need to identify the areas where data processing activities take place: typically HR (incl. job applications), CRM and marketing (newsletters, fidelity cards, CCTV etc).

3. Evaluate the lawfulness of processing

Each processing activity needs to be evaluated separately, as to whether it is in line with the data protection principles (purpose limitation, data limitation, ensuring confidentiality etc). In addition, organisations need to identify the legal basis for each processing activity (consent or statutory grounds). Where the processing is based on consent, organizations need to review how consent is obtained, whether mandatory information was provided to the data subject and how this is evidenced.

4. Evaluate the internal processes

Both the internal human intervention processes and the IT systems must be reviewed. Organisational and technical measures to ensure data protection shall be defined and responsibilities allocated. Data protection authorities expect data protection reporting lines to run to the top management level. It is also required to consult with an IT expert how data protection and security requirements can be achieved from a technical point of view.

5. Review of policies and statements

Once the internal processes are reviewed, the necessary organisational and technical measures should be incorporated in internal policies. Organisations shall have an HR policy for employee data, another for customer data and further policies for specific processings, such as CCTV, lotteries etc Such policies shall also cover the process around data breaches and data transfers. Also a privacy statement shall be drafted or updated informing the persons interacting with your organisation how you use their personal data.

6. Documentation

Certain activities fall under mandatory documentation obligation. However, we recommend maintaining similar documentation of any processing activities to comply with the general principle of accountability.

7. Evaluate the necessity of a DPO

Certain category of organisations is obliged to appoint a data protection officer. You must consider whether your organisation is affected.

8. Raise awareness, educate your colleagues

Staff which has access to personal data must be educated on the new requirements and a senior member of the management shall monitor the implementation.

Please note, that monitoring and security are ongoing processes that you need to focus on continuously during the whole data processing cycle.
The present summary intends to offer a general guidance on data protection audit which on the basis of the particularities of your organisation and your jurisdiction may well require further analysis.

Should you need a customized assessment, 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.

SCHINDHELM.COM