SCHINDHELM

NEUES EU-DATENSCHUTZRECHT: DATENSCHUTZVERSTÖSSE

Datenschutzverstöße können ab dem 25. Mai 2018 nach der DSGVO schärfer und erleichtert sanktioniert werden. Unternehmen und anderen datenverarbeitenden Stellen drohen nicht nur erleichtert durchsetzbare Schadensersatzansprüche Betroffener, sondern darüber hinaus die Verhängung höherer Bußgelder der Aufsichtsbehörden.
Hinzu tritt das gestiegene Risiko von Reputationsschäden, die aus meldepflichtigen Datenschutzverstößen resultieren können.
Unternehmen und sonstige datenverarbeitende Stellen sollten ihre Organisation daher so gestalten, dass sie nicht nur fähig sind, auf Datenschutzverstöße schnell und effektiv zu reagieren, sondern alles Notwendige unternehmen, um sie im Vorfeld zu vermeiden.

ERKENNEN

Das Wichtigste ist, Datenschutzverstöße überhaupt erkennen zu können. Nur wer weiß, dass etwas nicht in Ordnung ist, kann es in Ordnung bringen. Um diese Erkenntnisfähigkeit sicherzustellen, sind regelmäßige Schulungen der Mitarbeiter und die Einbeziehung des Datenschutzbeauftragten unumgänglich.

DOKUMENTIEREN

Nach der DSGVO sind alle Datenschutzverstöße samt dessen Ursachen und Auswirkungen zu dokumentieren. Anhand dieser Dokumentation kann insbesondere auch abgeleitet werden, ob und welche vorhandenen Schnittstellen, Prozesse und Maßnahmen effektiv sind oder optimiert werden müssen.

MASSNAHMEN ERGREIFEN

Natürlich sind Erkennen und Dokumentieren allein nicht ausreichend. Gemeinsam mit der zuständigen Fachabteilung, des IT-Administrators und dem Datenschutzbeauftragten sollten vielmehr zudem die zu ergreifenden Maßnahmen abgesprochen werden. Unabhängig vom Vorliegen eines Datenschutzverstoßes ist anzuraten, die Datensicherheitsmaßnahmen regelmäßig auf Effektivität und Effizienz zu prüfen und das jeweilige Prüfungsergebnis zu dokumentieren.

RISIKO PRÜFEN

Unmittelbar im Anschluss an die Entscheidung über die zu ergreifenden Maßnahmen sollte das bereits entstandene Risiko für die Rechte und Interessen derjenigen, deren Daten betroffen sind, und das Maß der Risikoreduzierung, das infolge der zu treffenden Maßnahmen eintritt, betrachtet und auf das verbleibende Restrisiko durch den Datenschutzbeauftragten überprüft werden. Im Rahmen der Risikobetrachtung ist zu analysieren, ob und inwiefern infolge der offengelegten Daten Aussagen insbesondere über die wirtschaftliche Lage, Gesundheit, Zuverlässigkeit oder Arbeitsleistung der Betroffenen möglich sind und wie viele Personen dies betrifft.

VERSTÖSSE MELDEN

Abhängig von dem Ergebnis der Risikoprüfung ist zu entscheiden, ob es sich um ein geringfügiges, normales oder hohes Restrisiko handelt. Die getroffene Entscheidung und die dieser zugrundeliegenden Erwägungen sind zu dokumentieren. Bei geringfügigen Restrisiken kann auf eine Meldung verzichtet werden. Bei als normal eingeschätzten Restrisiken ist die jeweils zuständige Aufsichtsbehörde über die Art des Datenschutzverstoßes, die Art und Anzahl der betroffenen Datensätze und Betroffenen sowie die festgestellten Restrisiken und geplanten bzw. bereits ergriffenen Maßnahmen zu informieren. Im Anschluss werden das OB und WIE von weiteren Maßnahmen mit der Aufsichtsbehörde abgesprochen. Bei als hoch eingestuften Restrisiken sind sowohl die Aufsichtsbehörde als auch die Betroffenen selbst zu informieren. Sprachlich ist gegenüber den Betroffenen besonderes Augenmerk auf Verständlichkeit und Transparenz der übermittelten Informationen zu legen.

Es empfiehlt sich, den Prozess zum Vorgehen bei Datenschutzverstößen in einem sog. Krisenplan festzuhalten.

Bei weiteren Fragen stehen die KollegInnen der jeweiligen Standorte jederzeit gerne zur Verfügung.

SCHINDHELM

NEW EU DATA PROTECTION LAW: DATA BREACHES

As of 25 May 2018, the General Data Protection Regulation (GDPR) introduces harsh sanctions for data breaches with extended scope of applicability. Companies and other data processing entities become potential subjects not only to the data subjects' claims for damages, the enforceability of which has been enhanced, but also to increased administrative fines to be imposed by supervisory authorities.

In addition to the above sanctions the entities may also suffer reputational damages resulting from data breaches which will be now subject to mandatory notification. Companies and other data processing entities shall set up an organisation enabling them, where possible, to prevent data breaches and, where it nevertheless occurs, to react to it in an effective and timely manner.

DETECTING BREACHES

At first, entities must be able to detect data breaches. Only who knows that something went wrong, can fix it. For identifying data breaches the training of the staff on a regular basis and the involvement of the Data Protection Officer is inevitable.

RECORD KEEPING

The documentation of all data breaches is a legal obligation set forth in the GDPR. The data breaches, its causes and its effects shall be carefully recorded. Such records then makes also transparent which interfaces, processes and measures are effective and which ones must be optimised.

TAKING MEASURES

Obviously, detecting and recording alone would not suffice. The competent department, the IT consultant and the Data Protection Officer - if any - must also jointly define the necessary measures. Furthermore, irrespective of a data breach it is advisable to regularly test the security measures for effectiveness and efficiency and to record each testing result.

ASSESSING THE RISKS

Once the necessary measures have been determined, the risks already occurred to the rights and interests of the affected persons, the extent of risk reduction achievable by the intended measures and the residual risk that remains after the intended measures are adopted, shall be analysed. The risk assessment shall give considerations as to whether the affected personal data allow conclusions on the economic situation, the health, the reliability or the job performance of the affected persons and how many persons are affected.

NOTIFYING THE BREACH

In light of the outcome of the risk assessment, the company decides whether there is a slight, a normal or a high residual risk. The evaluation and the reasoning for the classification of the risks shall be documented. In case of slight residual risks, there is no notification obligation. In the event of normal risks the issue must be escalated to the competent supervisory authority, including information on the nature of the data breach, nature and scope of data and data subjects as well as the identified remaining risks and the measures intended and taken. Then the company must determine the further measures together with the supervisory authority. High risks incidents must be notified both to the supervisory authority and the data subjects. In terms of language, the company needs to ensure that the information provided is transparent and comprehensible.

Entities are encouraged to set up a contingency plan describing the processes and the exact to-dos for the event that a data incident occurs.

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

MÜNCHEN
SCHINDHELM
Schindhelm Rechtsanwaltsgesellschaft mbH
muenchen@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 / WROCLAW
SDZLEGAL SCHINDHELM
Kancelaria Prawna
Schampera, Dubis, Zając i Wspólnicy sp.k.
wroclaw@sdzlegal.pl

WARSCHAU / WARSZAWA
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.