DER „DIENSTLEISTER“ IM DATENSCHUTZRECHT – RECHTE UND PFLICHTEN

Das Datenschutzgesetz 2000 (DSG) verteilt die Kompetenzen zwischen Auftraggeber (= AG) und Dienstleister (= DL) konsequent und mit weitreichenden Folgen:

Auftraggeber ist im Sinne des Datenschutzgesetzes jede natürliche oder juristische Person Person bzw. Personengemeinschaft, die personenbezogene Daten, die ihr zur Herstellung eines Werkes vertraglich überlassen worden sind, verwendet.

Welche Daten dürfen einem Dienstleister überlassen werden?

Nur **rechtmäßig** vom AG ermittelte Daten, die er also im Rahmen seiner gesetzlichen Zuständigkeit/rechtlichen Befugnis (zB Gewerbeberechtigung) gesammelt hat und die keine berechtigten Geheimhaltungsinteressen der Betroffen verletzen, dürfen einem DL überlassen werden! Diese Datenüberlassung setzt eine (idR) schriftliche Vereinbarung zwischen AG und DL voraus, die die Verpflichtung zur rechtmäßigen und sicheren **Datenverwendung** durch den DL zu enthalten hat. Von deren Einhaltung hat sich der AG durch Einholung der erforderlichen Informationen über die vom DL tatsächlich getroffenen Maßnahmen zu überzeugen.

Welche Pflichten treffen den Dienstleister?

Er darf die ihm überlassenen Daten jedenfalls nur im Rahmen des ihm erteilten Auftrages verwenden (zB als EDV-Dienstleister), dh vor allem diese Datenbestände nicht weiter übermitteln. Er muss alle erforderlichen **Datensicherheitsmaßnahmen** treffen, dh insbesondere nur auf das **Datengeheimnis** verpflichtete Dienstnehmer einsetzen und kann nur dann weitere Dienstleister heranziehen, wenn der Auftraggeber es billigt und davon rechtzeitig verständigt worden ist. Weiters hat er die notwendigen organisatorischen Voraussetzungen dafür zu treffen, dass der AG (dessen Aufgabe es bleibt) seiner Pflicht zur Auskunft, Richtigstellung und Löschung gegenüber dem **Betroffenen** nachkommen kann! Nach **Beendigung** des Auftragsverhältnisses hat der DL alle Unterlagen, Datenverarbeitungsergebnisse, die erhaltenen Datenbestände etc. wieder dem AG rückzuerstatten (oder sie auftragsgemäß aufzubewahren bzw. zu vernichten).

Welche Datensicherheitsmaßnahmen hat der Dienstleister zu treffen?

Die Datensicherheit hat in Abhängigkeit von der **Art** der Daten und dem **Verwendungszweck** nach dem **technischen** Stand der Möglichkeiten und der **wirtschaftlichen** Vertretbarkeit vom DL sichergestellt und das Datenmaterial vor **Datenverlust** geschützt zu werden. Diese Maßnahmen müssen in einer

- **Aufgabenverteilung** zwischen den Organisationseinheiten und Mitarbeitern des DL,
- in der Bindung der Datenverwendung an entsprechende **Aufträge** anordnungsbefugter Organisationseinheiten und Mitarbeiter,
- in der **Belehrung** der Mitarbeiter über Datenschutzpflichten,
- in der Beschränkung der **Zutrittsberechtigung** zu Datenverarbeitungsräumen,
- in der Regelung der **Zugriffsrechte** auf Daten/Programme,
- in der **Maschinen-** und **Programmsicherung** gegen **unbefugte** Inbetriebnahme,
- in **Protokollführungen** über Verwendungsvorgänge und
- in einer **Dokumentation** über all diese getroffenen Maßnahmen bestehen.

Die Datensicherheitsvorschriften müssen für den Mitarbeiter jederzeit verfügbar sein. Der DL (und seine Mitarbeiter) haben das **Datengeheimnis** über die ihnen aus berufsmäßiger Beschäftigung bekannt gewordenen Daten zu wahren. Das **Datengeheimnis** bleibt auch **nach** Beendigung des Dienstverhältnisses weiter bestehen!

Wer ist Ansprechpartner für die Betroffenenrechte?

Ansprechpartner ist der AG, da diesen auch bei Inanspruchnahme eines DL die Verpflichtung zur Auskunftserteilung, Richtigstellung und Löschung trifft und gegen ihn das Widerspruchsrecht geltend zu machen ist! Wenn daher der AG die Datenanwendung einem DL übertragen hat, muss der AG sicher stellen, dass ihm die Erfüllung seiner Pflichten gegenüber dem Betroffenen durch rechtliche, technische und organisatorische Vorsorgemaßnahmen des DL ermöglicht wird.

Kann der Dienstleister auch im Ausland die Datenverarbeitung durchführen?

Geschieht die Datenanwendung im Inland **rechtmäßig**, dann können die Daten auch an einen DL im **Ausland überlassen** werden. Sofern es sich nicht um genehmigungsfreie Fälle handelt (zB zulässigerweise veröffentlichte Daten, Zustimmung des Betroffenen, Datentransfers in anderen EU-Mitgliedstaat, in die Schweiz, Ungarn, Kanada) hat der AG eine Genehmigung der **Datenschutzkommission** einzuholen. Der ausländische DL muss sich weiters schriftlich verpflichten, die oben genannten DL-Pflichten zu übernehmen.

Welche Haftung und Strafen treffen den Dienstleister gemäß DSG?

a) Für **Schadenersatzansprüche** eines Betroffenen haftet der DL bei **schuldhafter** und **gesetzwidriger** Datenverwendung;

b) Ein DL ist **strafrechtlich** verantwortlich, wenn er in der Absicht, sich einen Vermögensvorteil zu verschaffen oder einem anderen einen Nachteil zuzufügen, ihm berufsmäßig zugängliche oder anvertraute schutzwürdige Daten oder schutzwürdige Daten, die er sich widerrechtlich verschafft hat, selbst benützt, veröffentlicht oder anderen zugänglich macht (Freiheitsstrafe bis zu einem Jahr).

   Für vorsätzliche Verletzungen des Datengeheimnisses droht eine Verwaltungsstrafe bis zu € 18.890,--, für gröbliche Missachtung von Datenschutzmaßnahmen bis zu € 9.445,--. (Auch der Versuch ist schon strafbar!)

Stand: Oktober 2003