iStock, Lackner

Nach mehrjähriger Diskussion tritt die EU-Datenschutz-Grundverordnung (EU) 2016/679 mit 25. Mai 2018 in Kraft. Die bisherige Datenschutzrichtlinie gilt dann als aufgehoben. Letztere stammt aus der „Steinzeit" des Datenschutzes, nämlich aus einer Zeit, in der es Unternehmen wie Facebook, Google, WhatsApp, Instagram und auch das Cloud-Computing noch nicht gab. Es galt also, das Datenschutzrecht diesen Entwicklungen anzupassen und zu modernisieren. Ziel der Datenschutz-Grundverordnung ist einerseits die Stärkung der Grundrechte natürlicher Personen, insbesondere des Schutzes von personenbezogenen Daten innerhalb der EU, und andererseits die Gewährleistung des freien Datenverkehrs innerhalb des Binnenmarktes.

Neue Bürgerrechte. Die neue Verordnung soll Bürgern mehr Rechte und die Kontrolle über ihre personenbezogenen Daten einräumen. Dazu zählen etwa folgende Regelungen: Es bedarf einer klaren Einwilligung der betroffenen Person zur Verarbeitung personenbezogener Daten. Nutzer haben ein Widerspruchsrecht, auch wenn personenbezogene Daten für die Profilerstellung verwendet werden.

Weiters haben Nutzer ein Recht auf Berichtigung und Löschung persönlicher Daten (in Fortsetzung des „Rechtes auf Vergessenwerden" wie der EuGH im Google-Suchmaschinenfall judizierte). Wer Onlinedienste verwendet, muss besser über die Verarbeitung seiner Daten informiert werden. Darüber hinaus ist in der Verordnung auch ein Recht auf Übertragbarkeit von Daten von einem Dienstleister an einen anderen festgeschrieben („Datenportabilität").

Risikoabschätzung durch Betriebe. Für Unternehmen, und zwar auch für KMU, ergeben sich dadurch neue Verpflichtungen. Die Daten-Compliance innerhalb des Unternehmens wird umfassender, zumal das System auf einer Selbstregulierung basiert. Unternehmen müssen nach der Datenschutz-Grundverordnung selbst eine Risikoabschätzung vornehmen und bei heiklen Datenanwendungen entsprechende Maßnahmen setzen. Besteht ein hohes Risiko, ist die Datenschutzbehörde beizuziehen. Dafür entfällt die grundsätzliche Meldepflicht, also die bisher vorgesehene Meldung an das Datenschutzregister.

Dieser risikobasierte Ansatz der Verordnung fordert einiges von den Betrieben, da sie mehr Eigenverantwortung tragen. Insbesondere können detaillierte Analysen ihrer Datenanwendungen und die Ausarbeitung und Umsetzung von Sicherheitsmaßnahmen erforderlich sein. Das kann bis zur Führung eigener Datenregister in den Unternehmen gehen, in denen die Datenanwendungen sowie wesentliche Angaben dazu festgehalten werden.

Datenanwendungen sind vom technischen Standpunkt her datenschutzfreundlich zu konzipieren, also Voreinstellungen müssen datennutzerfreundlich sein (z. B. Voreinstellungen