Gewerbeverein Swisttal
Eine starke Gemeinschaft

SWISTTALER UNTERNEHMERFRÜHSTÜCK
...ZIELBEWUSST GESTALTEN!

DSGVO – ein Kurzüberblick

VON RECHTSANWALT HANS-PETER KRÖGER
HÖHENRING 98
53913 SWISTTAL
TELEFON: 02254-830 100
INFO@RECHTSANWALT-KROEGER.DE

Inhalt:

Einleitung

Die Europäische Union hat die Verarbeitung personenbezogener Daten durch Unternehmen und Behörden neu geregelt: ab dem 25. Mai 2018, 0:00 Uhr, gilt in der EU ein einheitliches Datenschutzrecht: die Datenschutzgrundverordnung (DSGVO).

Worum geht's?

Das zentrale Anliegen der DSGVO ist der besondere, an die Zeitumstände angepasste **Schutz von personenbezogenen Daten**. Hierfür müssen Unternehmen zukünftig aktiv Einwilligungen zur Datenverarbeitung einholen, dabei einen konkreten Verwendungszweck angeben, weitreichende Dokumentationspflichten über die Datenverwendung befolgen und Löschkonzepte entwickeln für den Fall, dass die gemeinschaftliche Geschäftsbeziehung - etwa beim Auslaufen eines Abonnements - beendet wird.

Den politisch Verantwortlichen ist es ernst mit dem neuen, einheitlichen Datenschutz; **Sanktionen** sollen wirksam, verhältnismäßig und abschreckend sein - d.h. Geldbußen von bis zu 20 Mio. € oder bis zu 4 % des globalen Unternehmensumsatzes werden die Regel sein, bislang gab es die Deckelung bei 300.000 EUR. Hinzu kommen noch Schadensersatzansprüche der betroffenen Unternehmen. Weiterhin wird das europaweite Verbandsklagerecht eingeführt. Und last but not least: Verbraucherschutzvereine dürfen – wie bei uns in Deutschland jetzt schon der Fall - gegen Datenschutzverstöße klagen.

Was bedeutet es für Sie?

Im Gegensatz zu global agierenden Konzernen mit entsprechender Erfahrung und Kapazitäten für die Vorbereitung, sieht es bei den kleinen und mittelständischen Unternehmen naturgemäß anders aus. Sie fragen sich, wie sie künftig in ihrem geschäftlichen Alltag mit den Daten - etwa für ihren Kunden-Newsletter - umgehen sollen und empfinden angesichts der drakonischen Strafen und der ablaufenden Frist Panik.

Damit dennoch europaweit ein gleichmäßiges Datenschutzniveau und gleichzeitig der freie, ungehinderte Datenverkehr gewährleistet ist, wird der besonderen Situation und den Bedürfnissen der Kleinstunternehmen sowie der kleinen und mittleren Unternehmen

Rechnung getragen. Im Erwägungsgrund 13 der Verordnung ist eine abweichende Regelung hinsichtlich des Führens eines Verzeichnisses für Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, enthalten. Konkret bedeutet dies, dass Unternehmen **erst ab 10 mit der Datenverarbeitung betrauten Mitarbeitern** überhaupt die normierten Pflichten und Zuständigkeiten für die Verantwortlichen und Auftragsverarbeiter und eine gleichmäßige Kontrolle der Verarbeitung personenbezogener Daten vorsehen müssen.

Bereits jetzt kristallisiert sich jedoch heraus, dass viele Unternehmen – egal ob klein oder groß – angesichts großer Unsicherheiten im Umgang mit Personendaten und drohender Strafen auf Nummer sicher gehen und die neuen Datenschutzregeln ernst nehmen und umsetzen werden.

Artikel 4 DSGVO: Wichtige Begriffe

- **personenbezogene Daten**: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (im Folgenden „betroffene Person“) beziehen; als identifizierbar wird eine natürliche Person angesehen, die direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen identifiziert werden kann, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind (Bsp.: Name, Wohnort, Steuernummer, Religionszugehörigkeit);

- **Verarbeitung**: jeder mit oder ohne Hilfe automatisierter Verfahren ausgeführten Vorgang oder jede solche Vorgangsreihe im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung;

- **Einschränkung der Verarbeitung**: die Markierung gespeicherter personenbezogener Daten mit dem Ziel, ihre künftige Verarbeitung einzuschränken;

- **Profiling**: jede Art der automatisierten Verarbeitung personenbezogener Daten, die darin besteht, dass diese personenbezogenen Daten verwendet werden, um bestimmte persönliche Aspekte, die sich auf eine natürliche Person beziehen, zu bewerten, insbesondere um Aspekte bezüglich Arbeitsleistung, wirtschaftliche Lage, Gesundheit, persönliche Vorlieben, Interessen, Zuverlässigkeit, Verhalten, Aufenthaltsort oder Ortswechsel dieser natürlichen Person zu analysieren oder vorherzusagen;

- **Pseudonymisierung**: die Verarbeitung personenbezogener Daten in einer Weise, dass die personenbezogenen Daten ohne Hinzuziehung zusätzlicher Informationen nicht mehr einer spezifischen betroffenen Person zugeordnet werden können, sofern diese zusätzlichen Informationen gesondert aufbewahrt werden und technischen und organisatorischen Maßnahmen unterliegen, die gewährleisten, dass die personenbezogenen Daten nicht einer identifizierten oder identifizierbaren natürlichen Person zugewiesen werden;

- **Dateisystem**: jede strukturierte Sammlung personenbezogener Daten, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird;

- **Verantwortlicher:** die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheidet; sind die Zwecke und Mittel dieser Verarbeitung durch das Unionsrecht oder das Recht der Mitgliedstaaten vorgegeben, so können der Verantwortliche beziehungsweise die bestimmten Kriterien seiner Benennung nach dem Unionsrecht oder dem Recht der Mitgliedstaaten vorgesehen werden;

- **Auftragsverarbeiter**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verarbeitet;

- **Empfänger:** eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, denen personenbezogene Daten offengelegt werden, unabhängig davon, ob es sich bei ihr um einen Dritten handelt oder nicht. Behörden, die im Rahmen eines bestimmten Untersuchungsauftrags nach dem Unionsrecht oder dem Recht der Mitgliedstaaten möglicherweise personenbezogene Daten erhalten, gelten jedoch nicht als Empfänger; die Verarbeitung dieser Daten durch die genannten Behörden erfolgt im Einklang mit den geltenden Datenschutzvorschriften gemäß den Zwecken der Verarbeitung;

- **Dritter**: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen, dem Auftragsverarbeiter und den Personen, die unter der unmittelbaren Verantwortung des Verantwortlichen oder des Auftragsverarbeiters befugt sind, die personenbezogenen Daten zu verarbeiten;

- **Einwilligung**: jede von der betroffenen Person freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willensbekundung in Form einer Erklärung oder einer sonstigen eindeutigen bestätigenden Handlung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

- **Verletzung des Schutzes personenbezogener Daten**: eine Verletzung der Sicherheit, die zur Vernichtung, zum Verlust oder zur Veränderung, ob unbeabsichtigt oder unrechtmäßig, oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt, die übermittelt, gespeichert oder auf sonstige Weise verarbeitet wurden;

- **genetische Daten**: personenbezogene Daten zu den ererbten oder erworbenen genetischen Eigenschaften einer natürlichen Person, die eindeutige Informationen über die Physiologie oder die Gesundheit dieser natürlichen Person liefern und insbesondere aus der Analyse einer biologischen Probe der betreffenden natürlichen Person gewonnen wurden;

- **biometrische Daten**: mit speziellen technischen Verfahren gewonnene personenbezogene Daten zu den physischen, physiologischen oder verhaltenstypischen Merkmalen einer natürlichen Person, die die eindeutige Identifizierung dieser natürlichen Person ermöglichen oder bestätigen, wie Gesichtsbilder oder daktyloskopische Daten;

- **Gesundheitsdaten**: personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person, einschließlich der Erbringung von Gesundheitsdienstleistungen, beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

- **Hauptniederlassung**:

  1. bedeutet im Falle eines Verantwortlichen mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union, es sei denn, die Entscheidungen hinsichtlich der Zwecke und Mittel der Verarbeitung personenbezogener Daten werden in einer anderen Niederlassung des Verantwortlichen in der Union getroffen und diese Niederlassung ist befugt, diese Entscheidungen umsetzen zu lassen; in diesem Fall gilt die Niederlassung, die derartige Entscheidungen trifft, als Hauptniederlassung;

  2. bedeutet im Falle eines Auftragsverarbeiters mit Niederlassungen in mehr als einem Mitgliedstaat den Ort seiner Hauptverwaltung in der Union oder, sofern der Auftragsverarbeiter keine Hauptverwaltung in der Union hat, die Niederlassung des Auftragsverarbeiters in der Union, in der die Verarbeitungstätigkeiten im Rahmen der Tätigkeiten einer Niederlassung eines Auftragsverarbeiters hauptsächlich stattfinden, soweit der Auftragsverarbeiter spezifischen Pflichten aus dieser Verordnung unterliegt;

- **Vertreter**: eine in der Union niedergelassene natürliche oder juristische Person, die von dem Verantwortlichen oder Auftragsverarbeiter schriftlich gemäß Artikel 27 DSGVO bestellt wurde und den Verantwortlichen oder Auftragsverarbeiter in Bezug auf die ihnen jeweils nach dieser Verordnung obliegenden Pflichten vertritt;

- **Unternehmen**: eine natürliche und juristische Person, die eine wirtschaftliche Tätigkeit ausübt, unabhängig von ihrer Rechtsform, einschließlich Personengesellschaften oder Vereinigungen, die regelmäßig einer wirtschaftlichen Tätigkeit nachgehen;

- **Unternehmensgruppe**: eine Gruppe, die aus einem herrschenden Unternehmen und den von diesem abhängigen Unternehmen besteht;

- **verbindliche interne Datenschutzvorschriften**: Maßnahmen zum Schutz personenbezogener Daten, zu deren Einhaltung sich ein im Hoheitsgebiet eines Mitgliedstaats niedergelassener Verantwortlicher oder Auftragsverarbeiter verpflichtet, im Hinblick auf Datenübermittlungen oder eine Kategorie von Datenübermittlungen personenbezogener Daten an einen Verantwortlichen oder Auftragsverarbeiter derselben Unternehmensgruppe oder derselben Gruppe von Unternehmen, die eine gemeinsame Wirtschaftstätigkeit ausüben, in einem oder mehreren Drittländern ;

- **Aufsichtsbehörde**: eine von einem Mitgliedstaat gemäß Artikel 51 eingerichtete unabhängige staatliche Stelle;

- **betroffene Aufsichtsbehörde**: eine Aufsichtsbehörde, die von der Verarbeitung personenbezogener Daten betroffen ist, weil

  1. der Verantwortliche oder der Auftragsverarbeiter im Hoheitsgebiet des Mitgliedstaats dieser Aufsichtsbehörde niedergelassen ist,

  2. diese Verarbeitung erhebliche Auswirkungen auf betroffene Personen mit Wohnsitz im Mitgliedstaat dieser Aufsichtsbehörde hat oder haben kann oder

  3. eine Beschwerde bei dieser Aufsichtsbehörde eingereicht wurde;

- **grenzüberschreitende Verarbeitung**: entweder

  1. eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten von Niederlassungen eines Verantwortlichen oder eines Auftragsverarbeiters in der

Union in mehr als einem Mitgliedstaat erfolgt, wenn der Verantwortliche oder Auftragsverarbeiter in mehr als einem Mitgliedstaat niedergelassen ist, oder

2. eine Verarbeitung personenbezogener Daten, die im Rahmen der Tätigkeiten einer einzelnen Niederlassung eines Verantwortlichen oder eines Auftragsverarbeiters in der Union erfolgt, die jedoch erhebliche Auswirkungen auf betroffene Personen in mehr als einem Mitgliedstaat hat oder haben kann;

- **maßgeblicher und begründeter Einspruch**: ein Einspruch im Hinblick darauf, ob ein Verstoß gegen diese Verordnung vorliegt oder nicht oder ob die beabsichtigte Maßnahme gegen den Verantwortlichen oder den Auftragsverarbeiter im Einklang mit dieser Verordnung steht, wobei aus diesem Einspruch die Tragweite der Risiken klar hervorgeht, die von dem Beschlussentwurf in Bezug auf die Grundrechte und Grundfreiheiten der betroffenen Personen und gegebenenfalls den freien Verkehr personenbezogener Daten in der Union ausgehen;

- **Dienst der Informationsgesellschaft**: eine Dienstleistung im Sinne des Artikels 1 Nummer 1 Buchstabe b der Richtlinie (EU) 2015/1535 des Europäischen Parlaments und des Rates;

- **internationale Organisation**: eine völkerrechtliche Organisation und ihre nachgeordneten Stellen oder jede sonstige Einrichtung, die durch eine zwischen zwei oder mehr Ländern geschlossene Übereinkunft oder auf der Grundlage einer solchen Übereinkunft geschaffen wurde.

Artikel 30 DSGVO: Verzeichnis der Verarbeitungstätigkeiten

1. **Jeder Verantwortliche und gegebenenfalls sein Vertreter** führen ein Verzeichnis aller Verarbeitungstätigkeiten, die ihrer Zuständigkeit unterliegen. Dieses Verzeichnis enthält abschließend folgenden Angaben:

- ✓ **den Namen und die Kontaktdaten** des Verantwortlichen und gegebenenfalls des gemeinsam mit ihm Verantwortlichen, des Vertreters des Verantwortlichen sowie eines etwaigen Datenschutzbeauftragten;

- ✓ **die Zwecke** der Verarbeitung;
- ✓ **eine Beschreibung** der Kategorien betroffener Personen und der Kategorien personenbezogener Daten;
- ✓ **die Kategorien** von Empfängern, gegenüber denen die personenbezogenen Daten offengelegt worden sind oder noch offengelegt werden, einschließlich Empfänger in Drittländern oder internationalen Organisationen;
- ✓ **gegebenenfalls Übermittlungen** von personenbezogenen Daten an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;
- ✓ wenn möglich, die vorgesehenen **Fristen für die Löschung** der verschiedenen Datenkategorien;
- ✓ wenn möglich, eine allgemeine Beschreibung der **technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1.

2. **Jeder Auftragsverarbeiter und gegebenenfalls sein Vertreter** führen ein Verzeichnis zu allen Kategorien von im Auftrag eines Verantwortlichen durchgeführten Tätigkeiten der Verarbeitung, die Folgendes enthält:

- ✓ den **Namen und die Kontaktdaten** des Auftragsverarbeiters oder der Auftragsverarbeiter und jedes Verantwortlichen, in dessen Auftrag der Auftragsverarbeiter tätig ist, sowie gegebenenfalls des Vertreters des Verantwortlichen oder des Auftragsverarbeiters und eines etwaigen Datenschutzbeauftragten;
- ✓ die **Kategorien von Verarbeitungen**, die im Auftrag jedes Verantwortlichen durchgeführt werden;
- ✓ gegebenenfalls **Übermittlungen von personenbezogenen Daten** an ein Drittland oder an eine internationale Organisation, einschließlich der Angabe des

betreffenden Drittlands oder der betreffenden internationalen Organisation, sowie bei den in Artikel 49 Absatz 1 Unterabsatz 2 genannten Datenübermittlungen die Dokumentierung geeigneter Garantien;

- ✓ wenn möglich, eine allgemeine **Beschreibung der technischen und organisatorischen Maßnahmen** gemäß Artikel 32 Absatz 1.

1. Das in den Absätzen 1 und 2 genannte Verzeichnis ist **schriftlich** zu führen, was auch in einem elektronischen Format erfolgen kann.

2. Der Verantwortliche oder der Auftragsverarbeiter sowie gegebenenfalls der Vertreter des Verantwortlichen oder des Auftragsverarbeiters stellen der Aufsichtsbehörde das Verzeichnis auf Anfrage zur Verfügung.

3. Die in den Absätzen 1 und 2 genannten Pflichten gelten nicht für Unternehmen oder Einrichtungen, die weniger als 250 Mitarbeiter beschäftigen, **es sei denn**, die von ihnen vorgenommene Verarbeitung birgt ein Risiko für die Rechte und Freiheiten der betroffenen Personen, die Verarbeitung erfolgt nicht nur gelegentlich oder es erfolgt eine Verarbeitung besonderer Datenkategorien gemäß Artikel 9 Absatz 1 bzw. die Verarbeitung von personenbezogenen Daten über strafrechtliche Verurteilungen und Straftaten im Sinne des Artikels 10.

Wichtige Links:

- ✓ Weg zur DSGVO – Selbsteinschätzung: https://www.lda.bayern.de/tool/start.html
- ✓ Landesbeauftragte für Datenschutz und Informationsfreiheit Nordrhein-Westfalen: Frau Helga Block: https://www.ldi.nrw.de
- ✓ IT-Sicherheitsirrtümer
  - https://www.bsi-fuer-buerger.de/BSIFB/DE/Risiken/Sicherheitsirrtuemer/sicherheitsirrtuemer_node.html