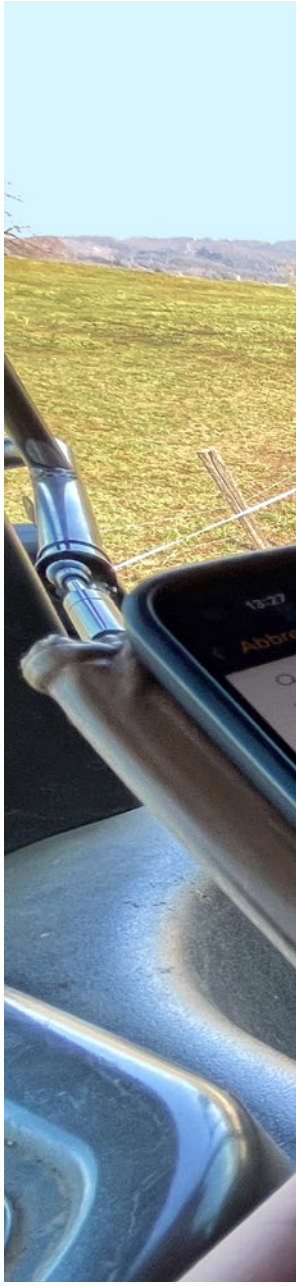
Datenschutz beginnt im Betrieb



Seit 1. September schützt das neue Datenschutzgesetz die Personendaten besser. Davon profitiert auch die Landwirtschaft, bei der grosse Mengen Daten anfallen und mit Dritten geteilt werden. Sicherheit über die eigenen Personen- und Betriebsdaten erlangen Landwirtschaftsbetriebe, indem sie den Überblick über ihren Datenaustausch behalten und Verträge mit Drittanbietern überprüfen.

Text: Dimitri Korostylev

Es ist Praxis in der Landwirtschaft, dass beispielsweise Molkereien, Schlachthöfe und Landtechnikhersteller Daten von Landwirtinnen und Landwirten sammeln und diese teilweise weitergeben. Wenn sich die Landwirtinnen und Landwirte mit ihrem Betrieb auf einer Agrar-Handelsplattform registrieren, eine App für die Einstallung, den Wasser- und Futterverbrauch oder den Tierbestand nutzen, werden ihre Daten abgefragt. Teilweise sind diese Daten personenbezogen, teilweise sind es reine Betriebsdaten.

Dimitri Korostylev
Rechtsanwalt, Senior Consultant,
Swiss Infosec AG

Vor diesem Hintergrund stellt sich für die Landwirtinnen und Landwirte die Frage, wie es um den Schutz ihrer Betriebsdaten steht und wann ihre Betriebsdaten weitergegeben werden dürfen.

Personenbezogenheit der Betriebsdaten

Es ist zu unterscheiden zwischen Personendaten und reinen Betriebsdaten. Es handelt sich bei Personendaten um solche Angaben, die sich auf eine bestimmte oder bestimmbare natürliche Person beziehen. So sind beispielsweise Arbeits-, Fahrt- und Stillstandzeiten von Maschinen der betroffenen Landwirtinnen und Landwirte als Personendaten zu klassifizieren. Dies gilt auch für solche Informationen, die von anderen Landwirtinnen und Landwirten zur Verfügung gestellt werden. So kann es zu einem Befall bei einer Kultur aufgrund eines neuen Schädlings kommen, der für andere auch gefährlich ist. Diese Informationen des betroffenen Landwirts werden verteilt, damit die anderen Landwirtinnen und Landwirte vor Beginn des Pflanzenbefalls reagieren können. Reine Betriebsdaten hingegen sind beispielsweise Informationen des Wasser- und Futterverbrauchs und des Tierbestandes. Diese reinen Sachdaten haben keinen Personenbezug und fallen nicht unter das Schweizer Datenschutzgesetz.

Betriebs- und Geschäftsgeheimnisse

Als Betriebs- und Geschäftsgeheimnisse des Landwirtschaftsbetriebs gelten alle Tatsachen, Umstände und Vorgänge, die sich auf den Landwirtschaftsbetrieb beziehen. Diese Daten sind nicht offen für alle, sondern nur einem begrenzten Personenkreis zugänglich. Die Landwirtinnen und Landwirte haben ein berechtigtes Interesse, dass diese Informationen nicht verbreitet wer-

Wer einen digitalen Feldkalender nutzt, generiert nicht nur jene Daten, die eingegeben werden. Was der Anbieter alles speichertund auswertet, ist in der Datenschutzvereinbarung beschrieben. Bild: Stefan Gantenbein

den. Zudem müssen diese Daten angemessen gesichert werden.

Unternehmen dürfen die Daten von Landwirtinnen und Landwirten beispielsweise nur dann speichern, wenn der Speicherung zugestimmt wurde. Erlaubt ist die Speicherung auch, wenn die Unternehmen die Daten für die Abwicklung eines Auftrags brauchen oder wenn es sich nicht um Personendaten handelt, die darüber hinaus keine Geschäftsgeheimnisse sind. Letzteres dürfte nur selten der Fall sein.

Unter das Betriebs- und Geschäftsgeheimnis fallen beispielsweise Umsätze, Ertragslagen und Geschäftsbücher. Auch Pächter- und Kundenlisten, Bezugsquel-

Unser Tipp

Analysieren und prüfen

Unter dem Strich empfehlen wir den Landwirtinnen und Landwirten insbesondere folgende Massnahmen:

- Analyse, bei welchen Datenbearbeitungen Personendaten bzw. Betriebsdaten vorliegen.
- Prüfung der Verträge mit Drittunternehmen.
- Prüfung der Massnahmen im Bereich der Datensicherheit.

len oder Konditionen wie Pachtpreise sowie Kalkulationsunterlagen gehören dazu. Sogar Wetterdaten können zu einem

Reine Sachdaten fallen nicht unter das Datenschutzgesetz.

Geschäftsgeheimnis werden, wenn sie mit einem bestimmten Grundstück und dessen Bewirtschaftungsdaten verknüpft sind. Eine Schlagkarte ist ein Geschäftsgeheimnis, weil darin unter anderem Dünge- und Pflanzenschutzmassnahmen auf bestimmten Parzellen dokumentiert sind.

Kein Geheimnis ohne Schutz

Voraussetzung für ein Geschäftsgeheimnis ist, dass es geschützt ist. In einem landwirtschaftlichen Betrieb sollte ein passwortgeschützter Zugriff auf die Daten sichergestellt werden. Dasselbe sollte für betriebsspezifische Daten wie Milchleistung, Futterrationen und Hektarerträge gelten. Zum Beispiel lässt sich mit der Parzellennummer über das Grundbuch der Eigentümer ermitteln. Hier haben Landwirtinnen und Landwirte ein Recht darauf, dass ihre Zustimmung eingeholt wird, wenn Abnehmer Daten erheben und weitergeben wollen. Davon dürften die meisten Daten betroffen sein.

Datensicherheit und Haftung

Landwirtinnen und Landwirte sollten die Datensicherheit ihrer Personen- und Betriebsdaten sicherstellen. Wichtig ist zunächst einmal, dass sich die Landwirtinnen und Landwirte die Verträge ansehen, die sie mit ihren Vertragspartnern abschliessen. Leider ist dies in der Praxis eher die Ausnahme als die Regel. Landwirtinnen und Landwirte müssen sich also zunächst einmal fragen, ob ihre Daten genutzt werden dürfen, und wenn ja, wie und in welchem Umfang. Wenn Daten genutzt werden, die für den jeweiligen Auftrag nicht nötig sind, sollten sie der Erhebung und Nutzung widersprechen dürfen.

Bei den Landwirtschaftsbetrieben stellt sich die Frage der Haftung, wenn beispielsweise die Daten gehackt werden und die Landwirtinnen und Landwirte dadurch Nachteile erleiden. In diesem Fall haftet das Unternehmen, welches die Daten von den Landwirtinnen und Landwirten erhalten hat, nur, wenn ihm ein Verschulden vorgeworfen werden kann. Dies ist immer eine Frage des Einzelfalls. ■

Personenbezogene Daten

Informationen, die zur Identifizierung einer Person führen können, existieren seit der Menschheitsgeschichte. Der Begriff der personenbezogenen Daten wurde jedoch erst in den 1970er-Jahren mit dem Aufkommen der ersten digitalen Technologien formal definiert. Unter dem Begriff versteht man heute alle Daten, die sich auf eine identifizierte oder identifizierbare Person beziehen. Unter diese Definition fallen im Wesentlichen vier Kategorien:

Informationen, die eine Person explizit identifizieren. Dies kann beispielsweise ein vollständiger Name, eine E-Mail-Adresse, die den vollständigen Namen des Benutzers enthält, oder Aufzeichnungen des Gesichts einer Person sein.

Informationen, die eine Person nicht explizit selbst identifizieren, sondern eindeutig für eine Person sind und deren Identifizierung ermöglichen, wenn weitere Informationen miteinbezogen werden. Beispiel: Fingerabdrücke.

Informationen, die möglicherweise nicht eindeutig für eine Person sind, sondern nur zu einem kleinen Personenkreis gehören. Beispiel: IP-Adresse.

Informationen, die eine Person nicht als solche identifizieren, sondern Informationen über eine Person oder deren Aktivitäten liefern. Beispiel: Geo-Daten.

Weitere Informationen rund ums Thema Daten und Datenschutz: www.infosec.ch → Blog

Grundsätze des neuen Datenschutzgesetzes

Der Begriff **Privacy by Design** (Datenschutz durch Technikgestaltung) stützt sich auf den Grundsatz, dass das Produkt oder die Dienstleistung so ausgelegt oder programmiert ist, dass der Schutz personenbezogener Daten von Anwenderinnen und Anwendern technisch gegeben ist. So dürfen beispielsweise keine Daten abgefragt werden, die technisch nicht notwendig sind.

Der Grundsatz **Privacy by Default** (Datenschutz durch Voreinstellungen) hat zum Ziel, dass die Voreinstellungen eines Produkts oder einer Dienstleistung bei Inbetriebnahme bereits auf die maximale Sicherheitsstufe eingestellt sind und nur heruntergesetzt werden, wenn Anwenderinnen und Anwender die Einstellungen ändern. **sg**