Datenschutzaspekte bei Dienstleistungen im Pflanzenbau

http://www.igreen-projekt.de/

VORVERSION

22. April 2013

Vorwort

Dieses Dokument wurde im Rahmen des Projekts iGreen (http://www.igreen-projekt.de/) erstellt. Bei dieser Version handelt es sich um eine Vorversion; die aktuelle Version findet sich jeweils auf der iGreen-Website.

Beteiligte

DFKI, ULD, DLR-RNH, BLU, IIS/FH BINGEN, CCI, CLAAS, AMAZONE, JOHN DEERE

Hinweis: Das Unabhängige Landeszentrum für Datenschutz Schleswig-Holstein (ULD) hat im Auftrag des Deutschen Forschungszentrums für Künstliche Intelligenz GmbH (DFKI) an diesem Report mitgewirkt. Die Einbindung der durch das ULD durchgeführten Arbeiten oblag dem Auftraggeber.

Struktur dieses Dokuments

Dieses Dokument besteht aus fünf Kapiteln.

Kapitel 1 gibt einen Grobüberblick über die Datenschutz- und Datenhoheits-Problematik im Agrarbereich.

Kapitel 2 listet die Akteure und Datentypen, die im Zusammenhang relevant sind.

Kapitel 3 gibt eine Einführung in den Datenschutz und das Bundesdatenschutzgesetz mit besonderem Fokus auf den Agrarbereich.

Kapitel 4 erläutert spezielle Datenschutzaspekte anhand von drei konkreten Szenarien.

Kapitel 5 gibt ein Fazit zu den besprochenen Themen aus Sicht unterschiedlicher Akteure.

1 Einleitung

Mitarbeiter der an dem iGreen-Projekt beteiligten Lohnunternehmer bearbeiten im Rahmen von Tests und Versuchen der Anwendungsszenarien Aufträge ihrer Kunden (Landwirte) und erlangen hierbei verschiedene Daten. Dies sind zum Beispiel standort- und flächenbezogene Aufzeichnungen ausgebrachter Mittel oder registrierter Ernteerträge, die jeweiligen Einsatzzeiten, Wegeaufzeichnungen sowie aufgezeichnete Betriebsdaten. Daneben werden zwangsläufig aber auch personenbezogene Daten erhoben. Fraglich ist, ob bzw. inwieweit diese personen- und/ oder flächenbezogenen Daten erhoben, verwendet und gespeichert werden dürfen. Problematisch ist der Umgang mit den personenbezogenen Daten, da diese rechtlich besonders geschützt sind.

Die zunehmende Technisierung unseres Alltags dürfte mittlerweile in allen Branchen angekommen sein. Sobald Maschinen ein Produktionsfaktor sind bieten sie Potential durch zusätzliche Technik bzw. Verbesserung der technischen Komponenten die Produktivität zu erhöhen. Diese Entwicklung hat natürlich auch im Agrarbereich Einzug gehalten. Die modernen Erntemaschinen und Traktoren sind nicht mehr mit den Modellen aus den früheren Jahrzehnten vergleichbar. Nicht nur, dass sie Größer und Leistungsstärker geworden sind, auch die technischen Helfer in den Maschinen haben zugenommen. Ein Trend, der auch auf dem PKW-Markt beobachtet werden kann. Im Maschinenpark eines Agrarbetriebs geht es dabei aber nicht um Einparkhilfen oder Bremsassistenzsysteme. Die modernen Maschinen sind ausgestattet mit einer Vielzahl von Sensoren, ggf. auch der Möglichkeit einer Georeferenzierung und mobilen Datenspeichern, um diese Daten zu speichern. Diese Technik soll die Effizienz bei dem Einsatz der Maschinen erhöhen, die Beteiligten entlasten und Daten für die Betriebsführung der Flächen liefern.

Die Maschinen bieten somit die Möglichkeit in einem sehr umfangreichen Maße Daten zu speichern und für eine spätere Bearbeitung bereitzustellen. Da es im Agrarbereich viele Interessengruppen (Landwirt, Lohnunternehmer, Landmaschinenhersteller etc.) an solchen Daten gibt und unter den verschiedenen Gruppen die verschiedensten vertraglichen Verbindungen bestehen, nimmt die Komplexität in Bezug auf die datenschutzrechtliche Betrachtung zu. Im Rahmen dieser Arbeit sollen die datenschutzrechtlichen Aspekte bei der Datenverarbeitung bzw. Datenweitergabe im Agrarbereich im Allgemeinen und anhand von verschieden Szenarien behandelt werden. Bevor sich diesen themenspezifischen Problembereichen gewidmet wird, erfolgt eine Skizzierung der Datenflüsse im Agrarbereich und eine Einführung in die datenschutzrechtlichen Regelungen.

Dabei liegt der Schwerpunkt auf der datenschutzrechtlichen Betrachtung und dem Schutz von personenbezogenen Daten. Regelungen etwa zum allgemeinen Vertragsrecht, das Recht am eingerichteten und ausgeübten Gewerbebetrieb, Wettbewerbsrecht oder auch Fragen zu Betriebs- und Geschäftsgeheimnissen waren nicht Teil der Betrachtung.

Zunehmende Datenerhebung und Vernetzung

Die Ergebnisse des iGreen-Projektes können die Innovations- und Wettbewerbsfähigkeit der deutschen Landwirtschaft sicherlich deutlich befördern. Viele Landwirte nutzen bereits Navigationssysteme, GPS-Empfänger und mobiles Internet, um ihre Feldbewirtschaftung vor Ort zu optimieren. Das Internet auf den Acker zu bringen, hat viele Vorteile. Eine Vernetzung von Bordrechner, Handys und Hof-PC

ermöglicht einen jederzeitigen Datenzugriff von jedem Ort aus. Vermehrt nutzen Landwirte auch amtliche Geodaten und von Maschinenherstellern bereitgestellte Informationen sowie mobile Entscheidungshilfen der Beratungsdienste. Arbeitet der Landwirt mit Lohnunternehmern oder Maschinenringen zusammen, bieten diese häufig Dienstleistungen an, die die Nutzung der neuen Technologien einschließen.

Im Rahmen des iGreen-Projektes werden diese technischen Möglichkeiten in besonderem Maße genutzt und weiterentwickelt. Die Nutzung der neuen technischen Möglichkeiten bringt jedoch auch mit sich, dass Daten der Landwirte erhoben, aufgezeichnet, gespeichert und weitergegeben werden. Maschinenhersteller, Lohnunternehmer und Maschinenringe erhalten ggf. Zugriff auf diese Daten, insbesondere wenn der Lohnunternehmer diese bei seiner Arbeit auf dem Feld des Landwirtes erhebt und an den Maschinenhersteller dadurch weitergibt, dass dieser auf dem Traktor installierte Software zur Verfügung stellt und betreut oder eine sog. „Cloud“ bereitstellt. Mit „Cloud“ sind in diesem Zusammenhang ein oder mehrere Server gemeint, die vom Maschinenhersteller oder einem weiteren externen privatwirtschaftlichen Anbieter bereitgestellt und betreut werden und Datenspeicherungs- und -verarbeitungsdienste anbieten. Betroffen sind u.a. standort- und flächenbezogene Aufzeichnungen ausgebrachter Mittel oder registrierter Ernteerträge, Einsatzzeiten und Wegeaufzeichnungen sowie aufgezeichnete Betriebs- und Flächendaten. Aus Sicht der Landwirte sollte mit diesen Daten grundsätzlich sensibel umgegangen werden. Das Selbstbestimmungsrecht in Bezug auf die Datenverwendung sollte gewahrt bleiben. Wichtig ist, dass bei allen rechtlichen Möglichkeiten ein von der Praxis akzeptiertes Datenschutzkonzept geschaffen wird.

Erwartungen der Landwirte

Es sollten insbesondere folgende 6 grundsätzliche Erwartungen der Landwirte an den Schutz ihrer Daten bedacht werden:

1. Die technischen und organisatorischen Maßnahmen und die Regeln zum Datenschutz in der arbeitsteiligen Agrarbranche sollten das Schutzniveau des Bundesdatenschutzgesetzes erreichen. Dazu gehört insbesondere das Einwilligungserfordernis. Der Schutz sollte allerdings darüber hinausgehen, denn das Bundesdatenschutzgesetz schützt nur „personenbezogene Daten“. Die beteiligten Personen erhalten mitunter auch Zugriff auf Betriebs- und Geschäftsdaten, die nicht immer auch einen Personenbezug aufweisen. Diese Daten sind jedoch mindestens genauso sensibel für die Betroffenen. Deshalb ist davon auszugehen, dass das Interesse der Landwirte daran, dass Betriebs- und Geschäftsgeheimnisse den gleichen Schutz genießen wie personenbezogene Daten, groß ist. Ein gleicher Schutz scheint insbesondere auch deshalb geboten, weil für die Beteiligten im konkreten Einzelfall nicht immer eindeutig erkennbar ist, ob die in Rede stehenden Daten Personenbezug aufweisen oder nicht.

Bei einem Landwirt, der als Einzelunternehmer tätig ist, können Informationen über die Lage einer Fläche dieser Person zugeordnet werden. Ist das landwirtschaftliche Unternehmen jedoch eine Personen- oder Kapitalgesellschaft, ist der Bezug ggf. nicht mehr herzustellen. Bei den betroffenen Landwirten könnte dies zu Unsicherheiten darüber führen, ob ein konkretes Datum, das der Lohnunternehmer, der Maschinenring und der Maschinenhersteller oder der Anwendungsbereitsteller erhält, geschützt ist oder aus dem Schutz „herausfällt“. Daher sollte die Erhebung, Verarbeitung oder Nutzung von „Informationen“ des Landwirts durch Dritte grundsätzlich unter dem Einwilligungsvorbehalt stehen.

2. Die im Bundesdatenschutzgesetz verankerten Rechte der Betroffenen sollten gewahrt bleiben. Diese sind die Ansprüche auf Auskunft, Berichtigung, Löschung und Sperrung. Es stellt sich die Frage, ob nicht grundsätzlich jede Handlung der Datenverwendung durch Dritte dem Landwirt vorab mitgeteilt werden sollte. Das Vertrauen der Landwirte in einen sensiblen Umgang mit ihren Daten, die sie aus der Hand geben, könnte dadurch gewahrt bleiben.

3. Der Landwirt kann verschiedene Rollen einnehmen: Die des Maschinenbedieners, des Maschineneigentümers, die des Flächeneigentümers, des Landbewirtschafters (insbesondere des Pächters) und des Instandhalters etc. Gewährleistet sein sollte daher, dass die Daten der Landwirte geschützt sind, wenn mindestens eine dieser Rollen nicht von dem betreffenden Landwirt selbst ausgeübt wird.

4. Die Einhaltung der 7 goldenen Regeln (Rechtmäßigkeit, Einwilligung, Zweckbindung, Erforderlichkeit und Datensparsamkeit, Transparenz und Betroffenenrechte, Datensicherheit und Kontrolle) sollte auch unabhängig von der konkret eingesetzten Technologie gelten. Jede verwendete Anwendung sollte einen umfassenden Schutz der Daten gewährleisten. Die Zustimmung zum Einsatz von Cloud-Technologien heißt nicht, dass seitens des Landwirts ein geringeres Schutzniveau akzeptiert wird.

5. Bereits bei der Anbahnung von Verträgen, an denen Landwirte beteiligt sind, sollten die Landwirte darauf hingewiesen werden, inwiefern sie bewusst oder durch den Einsatz bestimmter (z.B. GPS-gestützter) Technologien unbewusst Daten preisgeben. Die Einholung einer Einwilligungserklärung auch für betriebliche Daten (s.o.) sollte dabei selbstverständlich sein.

6. Des Weiteren stellt sich die Frage, ob nicht grundsätzlich Vorsorge auch für den Missbrauch von Daten getroffen werden sollte. Hier gilt es, die technischen Voraussetzungen zu schaffen, um den Schutz vor unbefugtem Datenzugriff möglichst ganz auszuschließen.

Daten in der „Cloud“

Wer steckt dahinter?

In der Agrarbranche wird zunehmend das Thema kooperatives Wirtschaften in der „Cloud“, also auf privatwirtschaftlich betriebenen Internet-Servern, beworben. Die Argumente, mit denen solche Portale begründet werden sollen, stoßen vor allem in drei Richtungen:

- Es würden verbesserte Voraussetzungen zur Rückverfolgbarkeit von Agrarprodukten geschaffen.
- Service-Plattformen im Internet bieten Landwirten, Lohnunternehmen und Maschinenringen die technische Voraussetzung, überbetriebliche Maschineneinsätze, z.B. Ernteketten, zentral zu steuern und alle eingehenden Daten zentral zu überwachen.
- Auf zentralen Servern hinterlegte Daten gingen nicht verloren, der Dienstleister übernimmt entsprechend die Haftung (Sicherung der erfassten Daten).

Bereits jetzt ist zu beobachten, dass große und international aufgestellte Unternehmen aus den Bereichen Lebensmitteleinzelhandel oder Landtechnik ihre Lieferanten und Käufer dazu bewegen wollen, sich zur Teilnahme an solchen „Cloud-Netzwerken“ bereit zu erklären. Inzwischen zeigen auch große Unternehmen aus dem Bereich der IT-Dienstleistungen ein gesteigertes Interesse an Agrardaten. Die Vorratsdatenspeicherung von Agrardaten mit Blick auf den zunehmend knapperen

Produktionsfaktor Boden verspricht offensichtlich neuartige Pfründe in der von vielen Branchen umkämpften Wertschöpfungskette zwischen Landwirten und Nahrungsmittelverarbeitern. Landwirte und Lohnunternehmer, die auf diese Wertschöpfung in der Primärproduktion angewiesen sind, konkurrieren zukünftig mit Akteuren in der „Cloud“. Wettbewerb kann nie schaden. Allerdings dürfen entsprechende Aktivitäten in der „Wolke“ nicht verschleiert, sondern müssen transparent veröffentlicht werden.

Was wird versprochen?

Der offensichtliche Vorteil für die Maschinendienstleister besteht darin, dass sie von einem zentralen Arbeitsplatz mit Logistikprogrammen auf den zentralen Server zugreifen und mit wenig Aufwand ihre Maschinenflotten steuern können. Als Beiprodukt fällt quasi noch die pflanzenbauliche Dokumentation an, die dem Landwirt zurückgespielt werden kann und ihm das Nachkommen seiner Dokumentationspflichten erleichtert.

Was ist daran problematisch?

Den meisten Landwirten ist nicht klar, welche Daten an verschiedenen Stellen erhoben und in die „Cloud“ gesendet werden. Wenn, zum Beispiel von Erntemaschinen diverse Erntedaten in Echtzeit erfasst und an die „Cloud“ geschickt werden, können sie dort ggf. personenbezogen mit dem Bewirtschafter der Fläche verknüpft werden. Dabei ist es unerheblich, welcher Dienstleister welche Daten liefert – so lange verschiedene Dienstleister ihre Daten über dasselbe Portal verarbeiten, lassen sich die Maßnahmen georeferenziert über das GPS-Protokoll eindeutig einer Fläche und damit auch einem Bewirtschafter zuordnen (Abb.). Technisch wäre es dann z.B. möglich, dass man zentral für jeden einzelnen Landwirt verfolgen kann, auf welchen seiner Flächen gerade welche Qualitäten geerntet werden. Derjenige, der auf diese Daten Zugriff hat, kann sich einen erheblichen Wissens- und Wettbewerbsvorsprung verschaffen, indem er verfolgt, wo zu welchen Zeitpunkten welche Erntemengen und Qualitäten eingeholt werden. Da sich dieses „Insiderwissen“ beispielsweise bei der Spekulation und Preisfindung auf Nahrungsmittelmärkten auch gegen die Interessen der Landwirte richten kann, ist deren Misstrauen gegenüber der Cloud vergleichsweise hoch. Maschinendienstleister sind noch wesentlich stärker betroffen, da in der Cloud aus den GPS-gestützten Bewegungsprofilen der zentral gesammelten Maschinendaten das Know-how eines Lohnunternehmers bezüglich Kundenkontakten und Wirtschaftlichkeit des Maschineneinsatzes ausgelesen werden kann.

Wo kann das hinführen?

Das Wissen über die regionale Produktivität und Produktion ist für die Steuerung von Agrarmärkten unerlässlich. Deshalb soll es im Rahmen der privatwirtschaftlichen Vorratsdatenspeicherung auf zentralen Servern gesammelt werden. Den höchsten Gewinn verspricht dieses Wissen natürlich dem, der es exklusiv für sich nutzen kann. Selbst wenn sich einzelne Landwirte gegen diese Form der Datenerfassung entscheiden, reicht es aus, in einer Region die Daten von einer repräsentativen Auswahl an Flächen zu erfassen, um z.B. gesicherte Prognosen über Ernteverläufe zu erstellen. Dieses Wissen ist auch für Investoren interessant, die in die großflächige Landwirtschaft einsteigen wollen. Durch Analyse von Daten, die sie von den Betreibern „Cloud“-gestützter Internetportale einkaufen, können sie ihre Investitionen gezielt steuern. Im Extremfall könnte es dazu führen, dass immer mehr landwirtschaftliche Flächen von wenigen Betrieben bewirtschaftet werden, die weniger eine nachhaltige Landbewirtschaftung denn eine hohe Rendite anstreben. Sollte sich eine Investition nicht mehr lohnen und die Investoren aus der Landwirtschaft aussteigen, so würden in der Zwischenzeit doch Fakten geschaffen:

- Kleine, eingesessene landwirtschaftliche Betriebe müssen vor der Finanzkraft der Investoren in Verbindung mit dem eingekauften „Insiderwissen“ aus der „Cloud“ noch stärker weichen als dass es durch den Strukturwandel ohnehin der Fall ist.
- Institutionen, die durch den Zusammenschluss mehrerer landwirtschaftlicher Betriebe getragen werden, verlieren an Bedeutung, da die sie stützenden Betriebe sich nicht halten, bzw. immer größere Betriebe sich zunehmend selbst organisieren können.
- Wenn sich gleich mehrere Investoren aufgrund mangelnder Rendite aus einzelnen Regionen wieder zurückziehen, ist fraglich, wer vor Ort die Mittel investieren kann, um die hinterlassene Lücke zu schließen.

Kann man sich verweigern?

Ob Landwirte und Dienstleister den Nutzen von Datendiensten in der „Cloud“ höher beurteilen als ihre Bedenken, bleibt abzusehen. Kritisch wird es, wenn Landtechnikhersteller ihre Maschinen so einrichten, dass Maschinenaufträge nur noch über solche Datendienste angelegt werden können, oder wenn marktrelevante Ketten des Lebensmitteleinzelhandels ihre Lieferanten direkt oder indirekt dazu zwingen, „qualitätsbestimmende Maßnahmen“ in Echtzeit auf von ihnen vorgegebenen Systemen zu dokumentieren. Die Teilnahme an solchen Infrastrukturen wäre dann quasi alternativlos und weder Landwirte noch deren Dienstleister könnten sich gegen die zentrale Vorratsdatenspeicherung auf betriebsfremden Servern wehren.

Was können Landwirte tun?

Da es bislang kaum ernstzunehmende technische Alternativen zu insbesondere „Cloud“-gestützten Programmen zur Steuerung von Maschinenflotten gibt, bleiben Landwirten nur folgende Möglichkeiten:

1. Keine Landtechnik kaufen, die direkt oder indirekt Daten an zentrale Server schickt.
2. Keinen Maschinendienstleister beauftragen, der solche Landtechnik einsetzt.
3. Sicherstellen, dass bei überbetrieblicher Planung und Organisation von Arbeitseinsätzen keine Daten auf zentralen Servern erfasst werden, insbesondere nicht durch den beauftragten Dienstleister.

Während Landwirte sich bei den ersten beiden Punkten schnell am Markt orientieren und entsprechend handeln können, ist es beim dritten Punkt schwierig. Das Vertrauen der Landwirte zu Dienstleistern wird belastet, wenn sich diese als Datensammler und –bündler für die Vorratsdatenspeicherung bei privatwirtschaftlichen „Cloud“-Diensten einspannen lassen.

Gibt es Alternativen?

Das eigentliche Problem, das Landwirte und Maschinendienstleister mit „Cloud“-gestützten Programmen lösen wollen, ist, verschiedene Computersysteme in ihrem Betrieb miteinander zu vernetzen, um verschiedene Prozesse, wie z.B. die Maschinenlogistik oder die Arbeitsdokumentation zentral zu steuern. Statt aber über eine „Cloud“ zu gehen, hieße die Alternative, sich selbst die passenden Programme auf eigene Server zu installieren – und selbst zu verantworten. Um im Internet permanent von außen erreichbar zu sein, benötigen auch Landwirte und Lohnunternehmer eine fixe IP-Internetadresse und einen kostengünstigen 24/7-erreichbaren Server. Diese Funktionen bieten zunehmend die in den Betrieben verfügbaren DSL-Router bzw. Telefonanlagen, so dass sich mit der Datenübertragung von der Maschine des Lohnunternehmers in das Büro des Landwirts zukünftig keine zwischengeschaltete „Cloud“-Datendrehscheibe rechtfertigen lässt. Bisher ist jedoch für die meisten,

insbesondere kleineren landwirtschaftlichen Betriebe die Hemmschwelle zu hoch, sich einen eigenen Server anzuschaffen. Dies liegt weniger an den Kosten – Mini-Server sind teils schon unter 100,-€ zu haben – als am Aufwand, die Server einzurichten und zu warten. Hilfreich wären entsprechend vorkonfigurierte Server, die dem Landwirt das Einrichten seiner eigenen Dateninfrastruktur erleichtern. Die andere Möglichkeit wäre, auf technische Lösungen zu warten, welche dafür Sorge tragen, dass nur derjenige die erfassten Daten zu sehen bekommt, der zur Einsicht jeweils berechtigt ist. Auftragsinformationen, die ein Landwirt einem Dienstleister zur Verfügung stellt, müssten entsprechend verschlüsselt werden, dass sie der Dienstleister erst offline auf seinem Computer mit dem Gegenschlüssel wieder öffnen kann. Entsprechend müssten Landmaschinen die über ihre Sensoren erfassten Daten verschlüsseln, so dass entweder erst der Dienstleister, oder bei sensiblen Daten wie z.B. zur Ertragsdatenerfassung, erst der Landwirt diese Daten entschlüsseln und auswerten kann. Für Landwirte wird die Entwicklung eines koordinatenbasierten Verschlüsselungssystems vorgeschlagen, bei dem die verschlüsselten Rohdaten der Maschinen weiterhin unbürokratisch vorgehalten und verteilt werden könnten. Die erforderlichen Gegenschlüssel für georeferenziert verschlüsselte Daten könnte der berechtigte Landwirt personalisiert von einem amtlichen InVeKoS-Flächeninformationssystem beziehen, in dem er als aktueller Bewirtschafter einer Fläche registriert ist.

Ein Zwischenfazit

Eine gut gesteuerte Kommunikation von Daten zwischen den verschiedenen Akteuren in der Landwirtschaft, insbesondere Landwirten und ihren Dienstleistern, verspricht, diverse Arbeitsprozesse in der Landwirtschaft zu erleichtern. Am Internet als Medium der Datenkommunikation führt derzeit kaum ein Weg vorbei. Als technische Lösungen werden derzeit vielerlei Dienste auf den Markt gebracht, bei denen Daten über zentrale Server (die „Cloud“) kommuniziert, bzw. auf diesen zwischengespeichert werden.

Bedenklich dabei ist, dass auf diesen zentralen Servern viele Informationen zusammentreffen, aus denen sich nicht nur ausführliche Bewirtschaftungsprofile für konkrete Flächen erstellen lassen, sondern auch personenbezogene Profile der Bewirtschafter. Insbesondere Dienstleister, wie Maschinenringe und Lohnunternehmen sollten die Bedenken ihrer Kunden sehr ernst nehmen, was den vertraulichen Umgang mit Daten angeht, die über solche zentrale Serverstrukturen laufen.

Die Datenkommunikation über sog. „Clouds“ selbst ist weniger problematisch, wenn sichergestellt wird, dass sich aus den kommunizierten Daten eben keine ausführlichen Nutzerprofile erstellen lassen. Dies kann z.B. dadurch geschehen, dass die über die „Cloud“ kommunizierten Daten für Dritte nur verschlüsselt sichtbar sind und die Datenverarbeitung selbst, insbesondere Erfassung und Auswertung, getrennt von den zentralen Servern offline erfolgt.

Alternativ sollten Landwirte und ihre Dienstleister auf Lösungen setzen, bei denen ihre eigenen Daten in einem geschlossenen Datenraum verbleiben. Insbesondere die in der „Kritischen Infrastruktur Landwirtschaft“ von der Gesellschaft geforderte Ausfallsicherheit spricht für den Aufbau einer entsprechend abgesicherten regionalen Vernetzung. „Cloud“-Strukturen erhöhen das Ausfallrisiko bei Blackout-Szenarien erheblich. Landmaschinen mit werkseitig integrierter Mobilfunkkommunikation und Anbindung an eine zentrale „Cloud“ könnten Opfer von „Cyber-Attacken“ werden. Die Auswirkungen der „Monokultur Internet“ auf die „Kritische Infrastruktur Landwirtschaft“ und insbesondere auf die arbeitsteilige Primärproduktion im vertrauensvollen Zusammenspiel zwischen Landwirten und Lohnunternehmern sollten vorrangig im Rahmen einer Technikfolgenabschätzung untersucht und bewertet werden.

2 Datenverarbeitung im Agrarbereich

Beschreibung

In diesem Kapitel wird ein abstrakter Überblick über Datenverarbeitung im Agrarbereich gegeben. Dabei werden insbesondere Beteiligte (Parteien), anfallende Datenarten, die Orte der Datenhaltung und -verarbeitung sowie Datenströme zwischen den Beteiligten aufgelistet.

Konkrete Szenarien werden in Kapitel 4 erläutert.

Beteiligte

Rollen und mit der Ausübung verbundene informationstechnische Prozesse

- **Maschinenbediener**
    - Der Maschinenbediener führt Aufträge aus und ist verantwortlich für die sachgerechte Bedienung der Maschine.
        - Erheben von positionsbezogenen Daten auf der bearbeiteten Fläche
        - Starten, stoppen, einfügen, löschen, verändern und versenden von Auftragsdaten
        - Während der Arbeit entstehen Prozessdaten (Zeit, Position, Attribut), Fehler- und Alarmmeldungen der Maschine, die in Speichern der Maschine protokolliert werden
        - Positionsbezogene Aufbringung und Entfernung von Stoffen in das/aus dem Feld
- **Prozessverantwortlicher**
    - Der Prozessverantwortliche trägt das organisatorische und wirtschaftliche Risiko eines ausgeführten Prozesses.
        - Nutzen von Daten für die Planung, Steuerung und Auswertung von Prozessen
- **Maschinenbetreiber**
    - Der Maschinenbetreiber trägt das wirtschaftliche Risiko für die Nutzung der Maschine.
        - Erfassen, verarbeiten und nutzen von Maschinen-, Geo-, Wetter- und Personendaten
- **Flächeneigentumer**
    - Der Flächeneigentümer / Pächter stellt landwirtschaftliche Nutzflächen zur Verfügung und hat eine Interesse an einer nachhaltigen Nutzung
        - Nutzen von Informationen, die für die Bereitstellung der Fläche erforderlich sind (z.B. Pachtvertrag, evtl. Grundbuchinformationen, Nutzungseinschränkungen z.B. WSG)
        - Nutzen von Informationen, die bzgl. der Fläche wertbestimmend sind oder sein könnten
- **Flächenbewirtschafter**
    - Der Flächenbewirtschafter trägt das wirtschaftliche Risiko für die auf der Fläche durchgeführten pflanzenbaulichen Prozesse.
        - Er erfasst verarbeitet und nutzt vorrangig flächenbezogene Informationen, die Personenbezug haben können. Dieser kann im Rahmen der

Komplettbewirtschaftung auch ein Lohnunternehmer sein.

- **Maschinenhersteller**
    - Vereinzelt statten Hersteller von selbstfahrenden Großmaschinen ihre Maschinen mit versteckten SIM-Karten aus, die dann alle erfassten Daten direkt zum Hersteller schicken. Diese Art der Datenerfassung ist rechtswidrig. Forderung: Die SIM-karten dürfen nicht werksseitig eingebaut werden. Ausnahme: Der Lohnunternehmer wünscht den Einbau der SIM-Karten ausdrücklich.
- **Instandhalter**
    - Der Instandhalter ist für die sachgerechte Ausführung von Sicherstellung und Wiederherstellung bestimmungsgemäßer Maschineneigenschaften verantwortlich.
        - Verarbeiten und nutzen von in der Maschine abgelegten Prozessdaten, Alarmmeldungen und Fehlerinformationen. Diese Informationen sind bislang ohne Personenbezug gespeichert, lassen sich aber mit Hilfe anderer Informationsquellen rekonstruieren.
        - Er kann Fehler- und Alarmspeicher zurück setzen
        - Er kann unsachgemäße Nutzung der Maschine feststellen. Diese Informationen können bei gemieteten oder geleasten Maschinen relevant werden. Im allgemeinen gehören entsprechende Daten dem Eigentümer; Weiterleitungen dieser Informationen müssen vertraglich geregelt werden und müssen transparent sein.
        - Er kann auf evtl. in der Maschine verbliebene Auftragsdaten (Chipkarte) zugreifen.
        - Durch die Kombination von Telematikdiensten mit Diagnosewerkzeugen lässt sich ein Raumbezug herstellen.
- **Prozessplaner**
    - Der Prozessplaner nimmt Aufträge interner oder externer Kunden entgegen, sezt sie in eine zeitliche Beziehung und weist Ressourcen aus "seinem" Unternehmen oder auch anderen Unternehmen zu.
        - Er erfasst, verarbeitet und nutzt Kundendaten
        - Er erfasst, verarbeitet und nutzt Flächeninformationen
        - Er erfasst, verarbeitet und nutzt Wetterdaten und ggf. auch Proben des Erntegutes (z.B. Feuchtigkeit, kann gedroschen werden)
- **Netzbetreiber**
    - Der Netzbetreiber transportiert Daten zwischen den beteiligten Akteuren. Dazu nutzen die Akteure fahrzeug- oder personengebunden Endgeräte. Bei einem Netz känn es sich um einen kommerziellen Carrier handeln. Das Netz kann aber auch "selbst" aufgebaut und betrieben werden.
        - Die transportierten Daten können Positions- und Zeitinformationen, Maschinen- und Personendaten enthalten
    - Die Daten werden mit Transportinformationen angereichert (Absender, Empfänger, Zeitpunkt der Übertragung, Erfolg der Übertragung)
- **Maschineneigentümer**
    - Der Maschineneigentümer trägt das wirtschaftliche Risiko für die dazu getätigte Investition.

        - Er nutzt Daten zu Art und Umfang der Nutzung
- **Prozessdatenverarbeiter**
    - Der Prozessdatenverarbeiter ist für die bestimmungsgemäße Weiterverarbeitung erfasster Informationen z.B. für Zwecke der Auswertung verantwortlich.
        - Er verarbeitet und speichert Daten für Abrechnungszwecke (Fakturierung)
        - Er verarbeitet speichert Daten für Bewertungszwecke (Schlagkartei)
        - Die Daten haben in den meisten Fällen Personenbezug zu den direkt oder indirekt am Prozess beteiligten Akteuren
- **Weitere potenzielle Teilnehmer/Rollen**
    - Behörde
    - Bewirtschafter
    - Landwirt
    - Lohnunternehmer
    - Labor
    - Eigentümer der Fläche
    - Flächennachbar
    - Fahrer
    - Bediener
    - Betreiber der Maschine
    - Betriebsleiter
    - Ausführende Organe
    - Gesetzgeber
    - Arbeitgeber
    - Arbeitnehmer
    - Sozialversicherungsträger
    - Auftraggeber
    - Auftragnehmer
    - Berufsgenossenschaft
    - Tarifpartner
    - Datendienstleister

Datenarten

- Personenbezogen
    - Arbeitszeiten Bediener
    - Aufenthaltsorte Arbeitskräfte
    - Berechtigungen, Befähigungen (Sachkundenachweis PS, Führerschein)
    - Arbeitsvertragliche Beziehung
    - Tätigkeit
    - Arbeitsschutz
    - Fehlzeiten
    - Prozesswissen, Betriebsgeheimnisse
    - Arbeitsentgeld

- Maschinen-/systembezogen
    - Tätigkeit
    - GPS-Positionsdaten Maschine
    - Ertragsdaten
    - Qualitätsmerkmale Erntegüter
    - Qualitätsmerkmale der durchgeführten Arbeit
    - Betriebsmittel Art/Menge
    - Eigentumsgrenzen
    - Bewirtschaftungsgrenzen
    - Räumliche Bewirtschaftungsauflagen
    - Zeitliche Bewirtschaftungsauflagen
    - Bodeneigenschaften aus Bodenproben
    - Nutzungsauflagen (z.B. Grünland, Bio)
    - Geschäftsbeziehung, Aufträge
    - Prozesswissen, Betriebsgeheimnisse
- Wetterdaten
- Daten zum Bodenzustand
- Stammdaten in Farm-Managementsystemen
- Verfahrensbezogene Daten in Farm-Managementsystemen
- Auftragsbezogene Daten auf Chipkarten
- Maschinenbezogene Daten in Jobrechnern und Terminals
- Protokollinformationen in Kommunikationsknoten
- Diverse Daten in
    - mobilen Applikationen
    - Webservern
    - Diagnosesystemen
    - USB-Sticks

Datenhaltung/-speicherung

- Technik
    - Maschine des Betreibers
    - Personengebundenes Erfassungsgerät
    - Zeiterfassung
    - Managementsysteme
    - Chipkarte
    - Telemetrie
    - Luftbilder
    - Schlagkartei
    - Flottenmanagement-Anwendung
    - Server
        - bei LU

        - bei LW
        - bei Maschinenhersteller
        - bei Beratung
- Sensoren
    - GPS-Empfänger
    - Bodenproben
    - Vermessung
    - Ertragssensor
    - Qualitätssensor

3 Datenschutzrechtliche Aspekte

Allgemeines

Datenschutzrechtliche Grundlagen

Die folgenden Ausführungen beziehen sich auf die aktuelle Rechtslage in Deutschland. Hierbei liegt der Schwerpunkt der Betrachtung auf deutschem Datenschutzrecht. Europäische Regelungen (insbesondere die Datenschutz-Richtlinien) werden ggf. als Auslegungsgrundlage hinzugezogen. Es ist jedoch damit zu rechnen, dass in den nächsten Jahren die Europäische Datenschutz-Grundverordnung [Entwurf, EU 25.01.2012] beschlossen wird. Diese würde mit Inkrafttreten zu geltendem Recht auch in Deutschland werden und u. a. weite Teile des Bundesdatenschutzgesetzes (BDSG) ersetzen.

Anwendbares Datenschutzrecht

Beim Datenschutz geht es um den Schutz personenbezogener Daten, d. h. Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren Person (§ 3 Abs. 1 BDSG). Wann immer personenbezogene Daten verarbeitet (Exkurs s. u.) werden, sind in der Regel Datenschutzvorgaben zu beachten. Welche rechtlichen Bestimmungen bei der Verarbeitung personenbezogener Daten zur Anwendung kommen, hängt nicht nur von der Art der Daten und den näheren Umständen der Datenverarbeitung ab, sondern auch davon, in welchen Ländern die Daten verarbeitet werden. Zu untersuchen ist somit zunächst allgemein die zur Anwendung kommende Rechtsordnung (also: internationale Regelungen, das Recht der Europäischen Union oder nationale Rechtsordnungen); anschließend muss festgestellt werden, welche Datenschutzbestimmungen jeweils inhaltlich anwendbar sind. So bestehen u. a. datenschutzrechtlich relevante Normen allgemein für personenbezogene Daten, für personenbezogene Daten im Zusammenhang mit der Bereitstellung von Telemedien und für personenbezogene Daten im Zusammenhang mit der Übermittlung im Rahmen von Telekommunikationsdiensten.

Im **Agrarbereich** mit seinen vielfältigen Formen der Datenverarbeitung dürften vor allem die

allgemeinen Datenschutzregelungen anwendbar sein. Soweit jedoch Webdienste etwa zur Auftragserteilung und Verwaltung oder auch Telekommunikationsdienste zur Übermittlung von (Telemetrie-) Daten von Landmaschinen eingebunden werden, können auch Sonderregelungen in Betracht kommen.

Insoweit sind in einer ersten Prüfung die anwendbaren Rechtsordnungen und deren Datenschutzbestimmungen aufzuführen, sodann ist zu erörtern, in welchen Fällen welche Rechtsordnung maßgeblich ist, und in einem dritten Schritt sind die konkret inhaltlich anwendbaren Datenschutzregelungen innerhalb der jeweils anwendbaren Rechtsordnung zu identifizieren.

Die unterschiedlichen Rechtsordnungen führen dazu, dass sie auf einen konkreten Sachverhalt Anwendung finden könnten, zum Beispiel in Abhängigkeit vom Wohnort des Adressaten oder vom Sitz des Anbieters als der für die Datenverarbeitung verantwortlichen Stelle (Exkurs s. u.).

Exkurs „Verarbeitung von personenbezogenen Daten“:

Der Begriff „Verarbeiten von Daten“ wird umgangssprachlich für alle Arten der Datenverarbeitung verwendet, während im Bundesdatenschutzgesetz unterschieden wird zwischen Erheben (Beschaffen von Daten über den Betroffenen - § 3 Abs. 3 BDSG), Verarbeiten (Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten - § 3 Abs. 4 BDSG) und Nutzen (jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt - § 3 Abs. 5 BDSG) von Daten. Dieser Text verwendet im Interesse einer besseren Lesbarkeit auch für nicht-juristische Leser und Leserinnen die Begriffe „Verarbeiten von Daten“ und „Verwenden von Daten“ in ihren umfassenden Bedeutungen, es sei denn, dass auf die spezielleren Begriffe eingegangen wird. Was jeweils gemeint ist, ergibt sich aus dem Kontext.

Exkurs „verantwortliche Stelle“:

Verantwortliche Stelle gemäß § 3 Abs. 7 BDSG ist jede Person oder Stelle, die personenbezogene Daten für sich selbst erhebt, verarbeitet oder nutzt oder dies durch andere im Auftrag vornehmen lässt. Da das nationale Recht richtlinienkonform auszulegen ist, ist für eine weitere Präzisierung Art. 2 Abs. 1 lit. d) der EG-Datenschutzrichtlinie heranzuziehen; danach ist nur verantwortlich, wer Entscheidungsgewalt über den Zweck und die Mittel der Datenverarbeitung hat.

Liegt eine Auftragsdatenverarbeitung vor, so ist (nur) der Auftraggeber verantwortliche Stelle.

Deutsches Datenschutzrecht

Grundlage des deutschen Datenschutzrechts ist das Verfassungsrecht. Dem deutschen Gesetzgeber ist durch das Grundgesetz ein Schutzauftrag für die informationelle Selbstbestimmung der in Deutschland ansässigen Personen aufgegeben worden [BVerfGE 65, 1 (42)]. Dieser Auftrag ist durch die Rechtsprechung des Bundesverfassungsgerichts in den letzten Jahren bestätigt worden [BVerfG NJW 2008, 822]. Teilweise wird sogar ein „Kommunikationsgrundrecht“ der Bürger angenommen [Leisner 2008, 2902 ff]. Die personenbezogenen Daten der Bürger werden als besonders schützenswert angesehen. In seiner inhaltlichen Ausprägung gibt dieses Recht dem Grundrechtsträger die Möglichkeit, grundsätzlich selbst über die Erhebung und Verwendung seiner personenbeziehbaren Daten zu entscheiden. Dabei handelt es sich um einen Schutz, der auch in den Fällen angestrebt wird, in denen eine Verarbeitung von Daten gar nicht oder nicht hauptsächlich in Deutschland stattfindet. Die Grundrechte können aber jeweils durch ausdrückliche oder verfassungsimmanente Schranken beschränkt werden. Zu berücksichtigen sind dabei in erster Linie Grundrechte Dritter.

Ebenso werden durch das Grundgesetz das Briefgeheimnis sowie das Post- und Fernmeldegeheimnis geschützt (Art. 10 Abs. 1 Grundgesetz). Entsprechende spezialgesetzliche Regelungen einschließlich Ausnahmen enthalten das Telekommunikationsgesetz (TKG) (siehe hier §§ 88, 89) und das Postgesetz (§§ 39 ff. Postgesetz); weitere Ausnahmen des Schutzes dieser Geheimnisse sind in der Strafprozessordnung (§§ 99 ff. StPO) genannt. Das Strafgesetzbuch (StGB) enthält Strafvorschriften für den Fall der Verletzung dieser Geheimnisse (§§ 202, 206 StGB).

Spezialgesetzliche Regelungen zum Datenschutz

Spezialgesetzliche Regelungen zum Datenschutz finden sich unter anderem in dem Bundesdatenschutzgesetz (BDSG) und den Landesdatenschutzgesetzen (LDSGe), dem Telemediengesetz (TMG) sowie dem Telekommunikationsgesetz (TKG). Das BDSG, die LDSGe sowie die datenschutzrechtlichen Bestimmungen im TMG sind Folgen der Umsetzung der aufgeführten europäischen Datenschutzrichtlinien.

Aufgrund der föderalen Struktur der Bundesrepublik sind die Kompetenzen zwischen Bund und Ländern aufgeteilt: Fragen, die die Verwaltung der Länder betreffen, werden überwiegend durch Landesgesetz geregelt, so auch die Umsetzung der EG-Datenschutzrichtlinie in der Landes- und Kommunalverwaltung. Daher gibt es Landesdatenschutzgesetze, die sich an die öffentlichen Stellen der Länder richtet (Beispielsweise Landesverwaltung, Kommunalverwaltung, Polizei, (Hoch-) Schulen, städtische Krankenhäuser, Körperschaften und Anstalten des öffentlichen Rechts, die von Ländern oder Kommunen getragen werden.). Die Umsetzung der EG-Datenschutzrichtlinie in der Bundesverwaltung sowie in der Privatwirtschaft (sogenannten „nicht-öffentliche Stellen“) erfolgt hingegen durch Bundesgesetz, vorrangig durch das BDSG. Für datenschutzrechtliche Belange in Angeboten privatwirtschaftlicher Unternehmen ist unabhängig von der Form des Angebotes neben den allgemeinen Regelungen insbesondere der dritte Abschnitt des BDSG (§§ 27 ff. BDSG) einschlägig. Da die Mehrheit der entwickelten Dienste im **Agrarbereich** dem Bereich Privatwirtschaft zuzuordnen ist, liegt ein Fokus der folgenden Darstellungen auf den Regelungen des BDSG.

Im **Agrarbereich** dürfte in der Regel die Bundesgesetzgebung zu beachten sein. Nur in Ausnahmefällen dürften öffentliche Stellen des Landes als landwirtschaftlicher Betrieb auftreten. Denkbar wäre dieses bei Versuchsanlagen etwa von Hochschulen oder anderen öffentlich-rechtlich organisierten Forschungseinrichtungen sowie einige Landwirtschaftskammern, die als Körperschaften öffentlichen Rechts organisiert sind.

Soweit jedoch Dienste im **Agrarbereich** Beziehungen zum Internet bzw. zur Telekommunikation aufweisen und eine Kommunikation und Übermittlung von Inhalten etwa über ein Webinterface oder Mobilfunk erfolgt, so sind die Regelungen für Telemedien- und Telekommunikationsdienste zu beachten. Diese sind im TMG und TKG bundeseinheitlich geregelt.

Relevant sind weiterhin einige Normen des Strafgesetzbuches, insbesondere § 203 StGB, der die Verletzung von Privatgeheimnissen unter Strafe stellt. Das Strafgesetzbuch enthält Regelungen für den Bruch von Schweigepflichten durch Ärzte, Rechtsanwälte, Mitarbeiter privater Versicherungen und weiterer Personengruppen. Wer von diesen verpflichteten Personen unbefugt ein anvertrautes Geheimnis offenbart, bricht die Schweigepflicht. Bedeutend ist hier, dass eine unbefugte Datenübertragung an Dritte und auch ein bloßes Zugänglichmachen solcher Daten an Dritte strafbewehrt ist. Dies hat beispielsweise Folgen für die Verarbeitung medizinischer Daten durch Dritte (Beispielsweise die Archivierung von radiologischen Aufnahmen durch Dienstleister oder die Niederschrift ärztlicher Befunde durch externe Schreibdienste.), die daher in vielen Fällen gar nicht

durch Dritte erbracht werden darf oder spezieller gesetzlicher Rechtfertigungen bzw. Einwilligungen (z. B. in Form einer Schweigepflicht¬entbindungs¬erklärung) bedarf.

Im Rahmen dieser Ausarbeitung werden die Berufsgeheimnisträger nicht weiter betrachtet. Denkbar wären Berührungspunkte allenfalls zu Wirtschaftsprüfern oder Amtsträgern, die den o. g. besonderen Verpflichtungen unterliegen.

Zusammenfassend gilt: Für privatwirtschaftlich organisierte Datenverarbeitung in Deutschland sind vor allem die Regelungen des BDSG zu beachten. Bei der Datenverarbeitung durch eine Landesverwaltung (etwa Hochschulen) sind die jeweiligen Landesdatenschutzgesetze heranzuziehen. Für den Bereich der Internetdienste wie Webseiten als Telemedien oder sonstige Dienste sind vorrangig die Bestimmungen des TMG sowie ergänzend des BDSG bzw. der Landesdatenschutzgesetze einschlägig. Soweit Telekommunikationsdienste wie die Übertragung von Standortdaten mittels Mobilfunk angeboten werden, kommt das TKG zur Anwendung.

Der Anwendungsbereich der Datenschutzbestimmungen ist eröffnet, wenn personenbezogene Daten durch öffentliche oder nicht-öffentliche Stellen erhoben, verarbeitet oder genutzt werden (§ 1 BDSG und § 1 TMG). Ausgeschlossen sind Datenerhebungen, -verarbeitungen und -nutzungen, die ausschließlich für persönliche und familiäre Tätigkeiten erfolgen (§ 1 Abs. 2 Nr. 3 BDSG). Der Gesetzgeber will damit in Umsetzung des Art. 3 Abs. 2 Spiegelstr. 3 EG-Datenschutzrichtlinie klarstellen, dass lediglich solche Erhebungen, Verarbeitungen oder Nutzungen der personenbezogenen Daten in den Anwendungsbereich der Datenschutzbestimmungen fallen, die kommerzielle Verarbeitungen, mithin geschäftsmäßig für berufliche oder gewerbliche Zwecke erfolgende Verarbeitungen, zum Gegenstand haben. Im Fall einer rein privaten Verarbeitung ist das BDSG daher nicht anwendbar [Dammann, in: Simitis 2006, § 1 Rn. 116]. Etwas anderes gilt, wenn die Tätigkeit aus dem persönlich-familiären Bereich herausragt, so z. B. bei Webangeboten, auch wenn diese an und für sich privater Natur sind [EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971, Tz. 46 f.; Weichert, in: Däubler et al. 2010, § 1 Rn. 9].

Mag im **Agrarbereich** ein Teil der Datenverarbeitung im Rahmen von Familienbetrieben erfolgen, so handelt es sich hierbei in der Regel gerade nicht um eine persönliche und familiäre Tätigkeit, sondern um Datenverarbeitung im Rahmen der Betriebsführung. Das Datenschutzrecht ist somit auch hierauf anwendbar.

Voraussetzung für die Anwendung der Datenschutzbestimmungen ist demnach das Vorliegen eines personenbezogenen Datums. Personenbezogene Daten sind gemäß § 3 Abs. 1 BDSG alle Informationen über eine bestimmte oder bestimmbare natürliche Person.

Generelle Regelungen

Grundsätzlich ist die Erhebung, Verarbeitung und Nutzung von personenbezogenen Daten nach den Datenschutzgesetzen verboten, es sei denn, dass eine Rechtsvorschrift dieses erlaubt oder eine Einwilligung des Betroffenen vorliegt (vgl. § 4 Abs. 1 BDSG). Dabei gilt die Zweckbindung. Das bedeutet, dass sich die verantwortliche Stelle vor der Erhebung, Verarbeitung und Nutzung der Daten Gedanken darüber machen muss, für welchen Zweck sie die Daten benötigt, und dass sie diesen Zweck eindeutig festlegt. Die Daten dürfen nur für diesen Zweck verwendet werden (vgl. u. a. § 28 Abs. 1 Satz 2 BDSG). Möchte die verantwortliche Stelle später die Daten auch für andere Zwecke verarbeiten bzw. den Zweckbereich erweitern, so ist auch hierfür eine Rechtsgrundlage oder die Einwilligung des Betroffenen notwendig (vgl. u. a. § 28 Abs. 5 BDSG). Einher geht damit, dass möglichst nur Daten

verarbeitet werden, die für die Erreichung des Zwecks auch erforderlich sind, wie das Erforderlichkeitsprinzip besagt. Eine Verarbeitung von Daten auf Vorrat ist dem deutschen Recht bisher fremd. Bei der Gestaltung von Datenverarbeitungssystemen muss man sich an den Grundsätzen der Datenvermeidung und Datensparsamkeit orientieren (vgl. § 3a BDSG). Außerdem muss für den Betroffenen die Verarbeitung seiner personenbezogenen Daten so transparent wie möglich erfolgen.

Wird im **Agrarbereich** etwa ein Lohnunternehmer beauftragt, so dürfen die hierbei anfallenden Daten nur im Rahmen der Zwecke verwendet werden, wofür sie erhoben wurden. Diese Zwecke sollten im (schriftlichen) Auftrag benannt werden, sofern sie sich nicht aus dem Vertragszweck selber ergeben. Besondere Vereinbarungen über den Zweck müssen z. B. getroffen werden, wenn Daten über die Vertragserfüllung hinaus aufbewahrt werden sollen (etwa zur Vereinfachung erneuter Auftragserteilungen).

Verantwortliche Stellen müssen prüfen, ob sie einen Datenschutzbeauftragten benötigen (vgl. §§ 4f ff. BDSG). Auch müssen sie gewährleisten, dass die Rechte des Betroffenen auf Auskunft, Berichtigung, Löschung und Sperrung seiner personenbezogenen Daten umgesetzt werden können (vgl. § 6 BDSG).

Im **Agrarbereich** dürfte in vielen Fällen insbesondere § 28 BDSG als Rechtsgrundlage für die Datenverarbeitung herangezogen werden. Diese Norm stellt für die Erhebung, Speicherung, Veränderung und Übermittlung von personenbezogenen Daten zu eigenen Geschäftszwecken eine Art Generalnorm dar. Besondere Einschränken gibt es dabei vor allem für sensible Daten wie Gesundheitsdaten oder auch Daten zum Sexualleben und zur religiösen oder politischen Einstellung (vgl. § 28 Abs. 7 i. V. m. § 3 Abs. 9 BDSG). Sollen Daten zum Zwecke der Übermittlung erhoben und verarbeitet werden, so sind insbesondere die §§ 29 ff. BDSG zu beachten.

Telemedien

Neben den allgemeinen datenschutzrechtlichen Bestimmungen des BDSG gelten für die Anbieter von Telemedien die speziellen datenschutzrechtlichen Vorgaben der §§ 11-15 TMG. Telemedien sind gemäß § 1 Abs. 1 TMG alle elektronischen Informations- und Kommunikationsdienste, soweit sie nicht die Tatbestandsmerkmale eines Telekommunikationsdienstes nach § 3 Nr. 24 TKG oder des Rundfunks nach § 2 Rundfunkstaatsvertrag erfüllen. Der Begriff der Telemedien ist zwar im TMG nicht legaldefiniert. Aus § 1 Abs. 1 TMG ergibt sich jedoch, dass Telemedien alle elektronischen Informations- und Kommunikationsdienste erfassen sollen, „soweit sie nicht Telekommunikationsdienste nach § 3 Nr. 24 Telekommunikationsgesetz, die ganz in der Übertragung von Signalen über Telekommunikationsnetze bestehen, telekommunikationsgestützte Dienste nach § 3 Nr. 25 des Telekommunikationsgesetzes oder Rundfunk sind“. Im **Agrarbereich** kann insbesondere die Datenerfassung, Datenverwaltung und Datenanzeige über Webzugänge durch Telemedien erfolgen.

Datenschutzrechtlich relevant sind für Telemedien die Regelungen des vierten Abschnitts des TMG. § 11 TMG legt den Anwendungsbereich der datenschutzrechtlichen Bestimmungen des TMG fest, § 12 TMG enthält die allgemeinen Grundsätze, die Anbieter von Telemedien bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten berücksichtigen müssen. § 13 TMG bestimmt die wesentlichen Informationsverpflichtungen eines Diensteanbieters, und §§ 14 und 15 TMG enthalten die Voraussetzungen für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ohne die Einwilligung des Betroffenen.

Gemäß § 11 TMG finden die Datenschutzbestimmungen des TMG auf Dienst- und Arbeitsverhältnisse und die Steuerung von Arbeits- und Geschäftsprozessen keine Anwendung. Demnach gilt im

Umkehrschluss aber auch, dass die §§ 11 ff. TMG für sämtliche sonstige Datenerhebungen, -verarbeitungen und -nutzungen von Telemedien zu beachten sind.

Grundsätzlich schützen die datenschutzrechtlichen Regelungen des TMG demnach den Nutzer von Telemedien. Nutzer im Sinne des TMG ist gemäß § 11 Abs. 2 TMG jede natürliche Person, die Telemedien nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen. Bei letzterer Auflistung handelt es sich nicht um eine abschließende Regelung, sondern nur um eine exemplarische Darstellung der wohl häufigsten Nutzungsarten von Telemedien.

§ 11 Abs. 3 TMG schließt die Anwendung der §§ 11-15 TMG für Telemedien, die überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, aus, mit Ausnahme des § 15 Abs. 8 TMG (Speicherung von Nutzungsdaten zum Zwecke der Rechtsverfolgung) und § 16 Abs. 4 Nr. 3 TMG (Bußgeld bei Verstoß gegen § 15 Abs. 8 TMG). Hiervon betroffen sind in erster Linie Access- und E-Mail-Provider [BT-Drs. 16/3078, S. 15 Gesetzesbegründung zum TMG].

Der positiven Formulierung des § 12 Abs. 1 TMG lässt sich entnehmen, dass die Datenschutzbestimmungen des TMG ausschließlich für diejenigen personenbezogenen Daten Anwendung finden, die bei der Bereitstellung der Telemedien anfallen.

Telekommunikationsdienste

Die Übertragungen von personenbezogenen Daten durch Diensteanbieter im Bereich Telekommunikation (Nachrichten / E-Mail / Mobilfunk etc.) unterfallen in Deutschland den Regelungen des TKG. Telekommunikationsdienste sind hierbei nach § 3 Nr. 24 TKG in der Regel gegen Entgelt erbrachte Dienste, die ganz oder überwiegend in der Übertragung von Signalen über Telekommunikationsnetze bestehen, einschließlich Übertragungsdiensten in Rundfunknetzen. In Abgrenzung zu Telemedien betreffen die Regelungen des TKG vor allem die technische Abwicklung von Kommunikation. Die Datenschutzregelungen finden sich in den §§ 88 ff. TKG. Zentraler Bestandteil hiervon ist vor allem das Fernmeldegeheimnis (§ 88 TKG), das auf Art. 10 Abs. 1 des Grundgesetzes zurückgeht. Dem Fernmeldegeheimnis unterliegen der Inhalt der Telekommunikation und ihre näheren Umstände, insbesondere die Tatsache, ob jemand an einem Telekommunikationsvorgang beteiligt ist oder war. Das Fernmeldegeheimnis erstreckt sich auch auf die näheren Umstände erfolgloser Verbindungsversuche (§ 88 Abs. 1 TKG). Diensteanbietern ist es nach § 88 Abs. 3 TKG untersagt, sich oder anderen über das für die geschäftsmäßige Erbringung der Telekommunikationsdienste einschließlich des Schutzes ihrer technischen Systeme erforderliche Maß hinaus Kenntnis vom Inhalt oder den näheren Umständen der Telekommunikation zu verschaffen. Es gilt eine strenge Zweckbindung. Eine Verwendung dieser Kenntnisse für andere Zwecke, insbesondere die Weitergabe an andere, ist nur zulässig, soweit das TKG oder eine andere gesetzliche Vorschrift dies vorsieht und sich dabei ausdrücklich auf Telekommunikationsvorgänge bezieht.

Weitere Datenschutzregelungen finden sich in den §§ 91 ff. TKG. Die Besonderheit ist dabei, dass diese weitgehend auch für Daten von juristischen Personen gelten und somit nicht nur personenbezogene Daten natürlicher Personen umfassen (§ 91 Abs. 1 Satz 2 TKG). Im **Agrarbereich** können sich somit auch landwirtschaftliche Unternehmen oder Lohnunternehmerfirmen auf die Regelungen des TKG berufen. Zu unterscheiden ist zwischen Bestandsdaten (§ 95 TKG – Daten, die für den Vertrag wesentlich sind und in der Regel bei Vertragsschluss angegeben werden) und Verbindungsdaten (§ 96 TKG – Daten, die bei der Nutzung des Dienstes anfallen). Beide Datenarten genießen einen rechtlichen Schutz, wobei der Schutz der Verbindungsdaten weitergehend ist. Insbesondere dürfen Verbindungsdaten in der Regel nur zur Erbringung des Dienstes, zu

Abrechnungszwecken und aus Sicherheitsgründen (z. B. Verhinderung von Missbrauch) verwendet werden (vgl. § 96 Abs. 1 TKG). Es gibt besonders enge Vorschriften für den Zugriff auf diese Daten durch Strafverfolgungsbehörden.

Sollen Standortdaten verwendet werden (z. B. bei der Erfassung von Geodaten durch die landwirtschaftlichen Maschinen), so sind die Vorgaben des § 98 TKG einzuhalten: Standortdaten […] dürfen nur im zur Bereitstellung von Diensten mit Zusatznutzen erforderlichen Umfang und innerhalb des dafür erforderlichen Zeitraums verarbeitet werden, wenn sie anonymisiert wurden oder wenn der Teilnehmer dem Anbieter des Dienstes mit Zusatznutzen seine Einwilligung erteilt hat. In diesen Fällen hat der Anbieter des Dienstes mit Zusatznutzen bei jeder Feststellung des Standortes des Mobilfunkendgerätes den Nutzer durch eine Textmitteilung an das Endgerät, dessen Standortdaten ermittelt wurden, zu informieren. Dies gilt nicht, wenn der Standort nur auf dem Endgerät angezeigt wird, dessen Standortdaten ermittelt wurden. Haben die Teilnehmer ihre Einwilligung zur Verarbeitung von Standortdaten gegeben, müssen sie auch weiterhin die Möglichkeit haben, die Verarbeitung solcher Daten für jede Verbindung zum Netz oder für jede Übertragung einer Nachricht auf einfache Weise und unentgeltlich zeitweise zu untersagen.

Soweit somit Standortdaten durch landwirtschaftliche Maschinen erhoben werden, muss dieses transparent für den Nutzer sein. Insbesondere muss auch die Möglichkeit haben, die Standortdatenerfassung zu unterbinden. Eine heimliche Übermittlung von Standortdaten etwa an den Hersteller der Maschinen ist nicht zulässig.

Europäische Datenschutzbestimmungen

Verantwortliche Stellen müssen, soweit sie ihren Hauptsitz in der Europäischen Union haben, das Recht der Europäischen Union beachten. Im Gegensatz zu den bereits aufgeführten Rechtsinstrumenten sind die Datenschutzbestimmungen der Europäischen Union für die Mitgliedstaaten der Europäischen Union bindend. Im Bereich des Datenschutzes sind seit dem 01.12.2009 in Art. 16 des Vertrags über die Arbeitsweise der Europäischen Union (AEUV) und Art. 8 EU-Grundrechtecharta jeweils Grundrechte zum Schutz personenbezogener Daten verankert. Dabei handelt es sich bei Art. 16 AEUV in erster Linie um eine Kompetenzregelung zugunsten der Europäischen Union, während Art. 8 EU-Grundrechtecharta das eigentliche Grundrecht auf Datenschutz mit entsprechenden Schrankenregelungen in Art. 52 Abs. 1 EU-Grundrechtecharta darstellt.

Beide Regelungen sind vom Wortlaut her identisch. Die Rechtsprechung des Europäischen Gerichtshofes hat bereits ohne die Verbindlichkeit des Art. 8 EU-Grundrechtecharta ein europäisches Grundrecht auf Datenschutz anerkannt. Danach werden privatrechtliche Sachverhalte von dem europäischen Grundrecht auf Datenschutz erfasst [EuGH, Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971, Tz. 24; EuGH, Rs. C-275/06 (Promusicae), Slg. 2008, S. I-271, Tz. 57]. Zusätzlich ist über Art. 6 Abs. 3 des Vertrags der Europäischen Union (EUV) auch Art. 8 der Europäischen Menschenrechtskonvention (EMRK) zu berücksichtigen, da die Europäische Union die Grundrechte, wie sie in der EMRK festgelegt werden, achtet.

Die EG-Datenschutzrichtlinie 95/46/EG schafft einen allgemeinen Rechtsrahmen zum Schutz der Privatsphäre natürlicher Personen bei der Verarbeitung personenbezogener Daten. Die Datenschutzrichtlinie für elektronische Kommunikation 2002/58/EG hingegen strebt ein harmonisiertes Rechtsregime für alle Formen elektronischer Kommunikation an. Sie erfasst sowohl Telemedien- als auch Telekommunikationsdienste. Für Internetdienste zusätzlich von Bedeutung sind die Richtlinie

2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten [Richtlinie 2006/24/EG, S. 54-63] und die Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation [Richtlinie 97/66/EG, S. 1-8.]. Beide Richtlinien befassen sich zwar nicht vordergründig mit Datenschutz, haben aber durchaus Datenschutzrelevanz. Sie beinhalten Regelungen zur Kommunikation im Internet.

Richtlinien selbst erzeugen keine direkte innerstaatliche Wirkung in den Mitgliedstaaten der Europäischen Union. Richtlinien sind gemäß Art. 288 Abs. 3 AEUV (Art. 249 Abs. 3 EGV) an die Mitgliedstaaten der Europäischen Union gerichtet und nur hinsichtlich des zu erreichenden Ziels verbindlich. Sie sind von den einzelnen Mitgliedstaaten in nationales Recht umzusetzen. Die Mittel und die Form der Umsetzung können die Mitgliedstaaten frei wählen. Insoweit ist zurzeit nur das umgesetzte nationale Recht verbindlich für die Betreiber von Internetdiensten.

Die EU-Richtlinien sind insoweit von Bedeutung, als sie in allen Mitgliedstaaten der Europäischen Union in nationales Recht umgesetzt werden müssen und damit das gesamte mitgliedstaatliche Recht im Bereich des Datenschutzes und der Telekommunikation im Wesentlichen harmonisiert ist. Hierdurch wurde ein europaweit einheitliches Datenschutzniveau geschaffen, wodurch primär der grenzübergreifende Datenverkehr im Binnenmarkt gefördert werden soll. Insoweit können die EU-Richtlinien, trotz der fehlenden unmittelbaren Wirkung, zur Begründung eines Mindeststandards und zur Überprüfung der datenschutzrechtlichen Vorgaben für Internetdienste herangezogen werden. Insbesondere können die EU-Richtlinien als Auslegungsregeln für das nationale Recht genutzt werden.

Anfang 2012 hat die Europäische Kommission einen ersten Entwurf für eine EU-Verordnung („Regulation“) vorgelegt, die in der folgenden Zeit diskutiert werden und dann – möglicherweise geändert und angepasst – die EG-Datenschutzrichtlinie 95/46/EC in den nächsten Jahren ersetzen soll. Eine EU-Verordnung ist anders als eine EU-Richtlinie unmittelbar anwendbar, ohne dass es einer nationalgesetzlichen Umsetzung der einzelnen Mitgliedstaaten bedarf. Für künftige rechtliche Analysen noch vor dem Inkrafttreten der EU-Verordnung wird neben den geltenden EU-Richtlinien auch der Diskussionsstand zur EU-Verordnung zu betrachten sein.

Internationale Datenschutzbestimmungen

Auf internationaler weltweiter Ebene gibt es keine verbindlichen einheitlichen Regelungen zum Datenschutz. Die OECD hat 1980 die „Leitlinien für den Schutz des Persönlichkeitsbereichs und den grenzüberschreitenden Verkehr personenbezogener Daten“ entwickelt [OECD Declaration on Transborder Data Flows, Nr. 135]. Diese Leitlinien stellen jedoch kein verbindliches Völkerrecht dar, sondern sind dazu gedacht, einen Hinweis für die Entwicklung nationaler Datenschutzgesetze zu geben.

Ebenfalls lediglich empfehlenden Charakter haben die „Richtlinien zur Verarbeitung personenbezogener Daten in automatisierten Dateien“ der Generalversammlung der Vereinten Nationen (UN) vom Dezember 1990 [UN Resolution 45/95]. Es handelt sich auch hier nicht um bindendes Völkerrecht.

Weiterhin ist international Art. 8 der Europäischen Menschenrechtskonvention (EMRK) zu berücksichtigen. Diese Regelung ist regional begrenzt auf die Mitgliedstaaten des Europarates. Sie enthält keine speziellen Regelungen zum Datenschutz und hat im Ergebnis einen reinen Schutzcharakter, da es sich um ein Grundrecht handelt.

Neben diesen internationalen Regelungen zum Datenschutz ist das sogenannte „Safe-Harbor-Abkommen“ zu berücksichtigen. Dieses Abkommen wurde zwischen den USA und der Europäischen Union abgeschlossen. Inhaltlich stellt es einzelne Datenschutzprinzipien auf, die teilweise ein ähnlich hohes Schutzniveau wie die EG-Datenschutzrichtlinie aufweisen. US-Unternehmen, die sich den Prinzipien des Abkommens unterworfen haben und von der Europäischen Kommission anerkannt wurden, sollen ein den EU-Bestimmungen entsprechendes Datenschutzniveau gewährleisten. Diese US-Unternehmen sind in einer weltweit öffentlich einsehbaren Liste des US-Handelsministeriums im Internet aufgeführt.

Im deutschen **Agrarbereich** dürfte der überwiegende Teil der Datenverarbeitung in Deutschland bzw. der EU stattfinden. Allerdings kann es internationale Bezüge geben, wenn etwa außereuropäische Dienstleister (etwa für Serverdienstleistungen oder Cloud-Speicher) eingebunden werden. Auch kann dieses relevant sein, wenn Telemetriedaten bzw. Standortdaten über landwirtschaftliche Fahrzeuge an außereuropäische Hersteller übermittelt werden. Hierbei reicht es aus, dass Administratoren auch Nicht-EU-Ländern Zugriff auf (ggf. in der EU beheimate) Server haben. Schon dann müssen hierfür ggf. besondere vertragliche Regelungen mit dem Betroffenen vereinbart bzw. dessen Einwilligung hierfür eingeholt werden.

Zuständigkeiten und Aufsichtsbehörden

In Deutschland haben alle Bundesländer eigene Landesdatenschutzbeauftragte. Hinzu kommt auf Bundesebene der Bundesbeauftrage für Datenschutz und die Informationsfreiheit (BfDI) als weitere Aufsichtbehörde. Dabei ist zu beachten, dass zwischen Bund und Ländern keine Über- / Unterordnungsverhältnisse bestehen. Vielmehr gelten klar umgrenzte Zuständigkeiten.

Die Landesdatenschutzbeauftragten sind für die Datenverarbeitung durch die Landesbehörden zuständig. Im **Agrarbereich** relevant ist jedoch vor allem, dass die Landesdatenschutzbeauftragten auch für die privaten Stellen im eigenen Bundesland zuständig sind. Hierbei ist beachten, dass einige Bundesländer unterschiedliche Stellen für den öffentlich-rechtlichen und den privaten Bereich eingerichtet haben.

Der BfDI ist hingegen zuständig für öffentliche Stellen des Bundes. Hinzu kommen einige wenige Sonderzuweisungen, insbesondere für die Bereiche Postwesen und Telekommunikation.

Örtlich ist der Landesdatenschutzbeauftragte zuständig, wo die für die Datenverarbeitung verantwortliche Stelle ihren Sitz hat.

Begriffsbestimmung

Personenbezogene Daten

Ausschlaggebend für die erforderliche Berücksichtigung der Datenschutzgrundsätze ist ein Personenbezug der infrage stehenden Daten. Ein Personenbezug von Daten ist regelmäßig dann anzunehmen, wenn es sich um Informationen über eine bestimmte oder bestimmbare natürliche Person (Betroffener) handelt (Art. 2 lit. a) EG-Datenschutzrichtlinie, § 3 Abs. 1 BDSG). Insoweit werden alle Angaben erfasst, die einer Person zugeordnet werden können. Dazu gehören neben dem Namen und dem Geburtsdatum auch Angaben zur Anschrift, zum Beruf und zu privaten Aktivitäten [Tinnefeld et al. 2005, S. 279]. Ob ein Datum personenbezogen ist oder nicht, hängt in erster Linie davon ab, ob

dieses Datum Aussagen zu bestimmten oder bestimmbaren Personen zulässt. Insoweit können auch Bild- und Tonaufnahmen personenbezogene Daten darstellen. Insbesondere auch Verhaltensweisen haben in der Regel einen Personenbezug. Dies betrifft auch z. B. die Art, in der ein Lohnunternehmer seine Tätigkeit ausübt oder auch ggf. Rückschlüsse von Bodenbeschaffenheit auf die Fähigkeiten eines Landwirts.

Für die Anwendbarkeit der datenschutzrechtlichen Bestimmungen des TMG ist grundsätzlich von einem weiten Begriff des personenbezogenen Datums auszugehen [Heckmann 2007, Kapitel 1.12, Rn. 10.]. Für Internetdienste bedeutet dies, dass alle Daten, die einen Rückschluss auf einen bestimmten Nutzer zulassen, unter den Begriff des personenbezogenen Datums fallen. Dies bedeutet auch, dass die meisten Daten, die in den einzelnen Prozessphasen im **Agrarbereich** – die Beauftragung, die Auftragsdurchführung, die Bezahlung und die Abwicklung – anfallen, einen Personenbezug aufweisen können.

Nicht erfasst vom Datenschutzrecht werden unternehmensbezogene Daten. Hierzu gehören in der Regel die Firmen- bzw. Betriebsgeheimnisse, soweit sie nicht den Kundestamm oder die Mitarbeiter des Unternehmens betreffen. Im **Agrarbereich** sind etwa Informationen über Grundstücke und deren Beschaffenheit in der Regel unternehmensbezogen. Allerdings kann sich ein Personenbezug ergeben, wenn sich hieraus Rückschlüsse auf etwa Einzellandwirte und deren Art, Landwirtschaft zu betreiben, ziehen lassen.

Automatisierte Verarbeitung

Gemäß § 1 Abs. 2 Nr. 3 BDSG findet das BDSG Anwendung, wenn die personenbezogenen Daten durch nicht-öffentliche Stellen unter Einsatz von Datenverarbeitungsanlagen erhoben, verarbeitet oder genutzt werden.

Erheben ist das Beschaffen von Daten über den Betroffenen (§ 3 Abs. 3 BDSG).

Verarbeiten ist nach § 3 Abs. 4 BDSG das Speichern, Verändern, Übermitteln, Sperren und Löschen personenbezogener Daten. Dabei ist Speichern das Erfassen, Aufnehmen oder Aufbewahren personenbezogener Daten auf einem Datenträger zum Zwecke ihrer weiteren Verarbeitung oder Nutzung. Verändern ist das inhaltliche Umgestalten gespeicherter personenbezogener Daten. Übermitteln ist das Bekanntgeben gespeicherter oder durch Datenverarbeitung gewonnener personenbezogener Daten an einen Dritten in der Weise, dass die Daten an den Dritten weitergegeben werden oder der Dritte zur Einsicht oder zum Abruf bereitgehaltene Daten einsieht oder abruft. Sperren ist das Kennzeichnen gespeicherter personenbezogener Daten, um ihre weitere Verarbeitung oder Nutzung auszuschließen. Löschen ist das Unkenntlichmachen gespeicherter personenbezogener Daten.

Nutzen ist jede Verwendung personenbezogener Daten, soweit es sich nicht um Verarbeitung handelt (§ 3 Abs. 5 BDSG).

Durch das Anmelden bzw. Einloggen, das Speichern der (Nutzungs-)Daten und das gegebenenfalls erforderliche Abrechnen der Nutzung von Telemedien erfolgt eine entsprechende Datenerhebung, -verarbeitung und -nutzung.

Verantwortliche Stelle

Die Einhaltung der Datenschutzgrundsätze müssen die für die Datenverarbeitung Verantwortlichen gewährleisten. Verantwortlich in diesem Sinne sind nach § 3 Abs. 7 BDSG die natürlichen oder

juristischen Personen, Behörden, Einrichtungen oder andere Stellen, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheiden. Im Gegensatz dazu ist ein Auftragsdatenverarbeiter – eine Person oder Stelle, die personenbezogene Daten im Auftrag des Verantwortlichen verwendet – nicht selbst gegenüber dem Nutzer verantwortlich für die Einhaltung der Datenschutzgrundsätze in Bezug auf die entsprechenden Daten, siehe § 3 Abs. 7 und § 11 Abs. 1 Satz 1 BDSG.

Bei Telekommunikationsdiensten sind die Diensteanbieter generell als verantwortliche Stellen zur Einhaltung der Datenschutzvorschriften nach §§ 91 ff. TKG anzusehen. Insbesondere sind sie zur Wahrung des Fernmeldegeheimnisses verpflichtet (§ 88 Abs. 2 TKG).

Betroffener

Betroffener im Sinne des § 3 Abs. 1 BDSG ist diejenige Person, deren Daten erhoben, verarbeitet und genutzt werden.

Teilnehmer/Nutzer

Im Bereich der Telekommunikation und der Telemedien werden die Begriffe „Teilnehmer“ und „Nutzer“ verwendet:

Ein **Teilnehmer** im Bereich der Telekommunikation ist der Vertragspartner (Natürliche oder juristische Person) von Anbietern von Telekommunikationsdiensten (§ 3 Nr. 20 TKG), ein Nutzer eine natürliche Person, die Telekommunikationsdienste nutzt (§ 3 Nr. 14 TKG). Dieser muss nicht notwendigerweise Teilnehmer sein.

Im Bereich der Telemedien ist ein **Nutzer** „jede natürliche oder juristische Person, die Telemedien und die technischen Voraussetzungen nutzt, insbesondere um Informationen zu erlangen oder zugänglich zu machen“ (vgl. § 2 Nr. 3 Telemediengesetz (TMG)). Soweit weitere personenbezogenen Daten des Nutzers erhoben, verarbeitet und genutzt werden, ist der Nutzer auch Betroffener im Sinne des § 3 Abs. 1 BDSG (Beispielsweise bei der Nutzung einer Online-Banking-Funktionalität (den Telemedien zuzurechnen) im Rahmen eines banküblichen Vertragsverhältnisses.).

Diensteanbieter

Im Rahmen von Telemedien ist der Diensteanbieter jede natürliche oder juristische Person, die eigene oder fremde Telemedien zur Nutzung bereithält oder den Zugang zur Nutzung vermittelt; bei audiovisuellen Mediendiensten auf Abruf ist Diensteanbieter jede natürliche oder juristische Person, die die Auswahl und Gestaltung der angebotenen Inhalte wirksam kontrolliert (§ 2 Nr. 1 TMG).

Im Rahmen von Telekommunikationsdiensten ist Diensteanbieter jeder, der ganz oder teilweise geschäftsmäßig Telekommunikationsdienste erbringt oder an der Erbringung solcher Dienste mitwirkt (§ 3 Nr. 6 TKG).

Datenschutzrechtliche Grundlagen

Werden personenbezogene Daten erhoben, verarbeitet oder genutzt, so sind die Verantwortlichen verpflichtet, die sich für natürliche Personen aus den Datenschutzbestimmungen ergebenden Rechte zu gewährleisten. Aus den Bestimmungen der EG-Datenschutzrichtlinie lassen sich verschiedene

Grundsätze für die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ableiten. Diese Grundsätze erfahren durch die weiteren Bestimmungen noch darzustellende Einschränkungen.

Verbot mit Erlaubnisvorbehalt

Im Grundsatz dürfen personenbezogene Daten unabhängig von dem Medium erhoben, verarbeitet und genutzt werden, wenn eine Einwilligung des Betroffenen vorliegt oder eine Rechtsvorschrift dies erlaubt (Art. 7 EG-Datenschutzrichtlinie, § 4 Abs. 1 BDSG, § 12 Abs. 1 letzte Alternative TMG). Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten steht damit unter einem Gesetzesvorbehalt. Juristisch wird von einem Verbot mit Erlaubnisvorbehalt gesprochen [Tinnefeld et al. 2005, S. 316]. Diese Regelung schützt das Grundrecht auf informationelle Selbstbestimmung [BVerfGE 65, S. 1 (46)]: Jede natürliche Person soll in die Lage versetzt werden, selbst darüber zu bestimmen, welche personenbezogenen Daten erhoben, verarbeitet oder genutzt werden dürfen und wo und von wem diese Daten verwendet werden. Im Ergebnis ist demnach eine Verwendung personenbezogener Daten ohne Einwilligung des Betroffenen oder Rechtsgrundlage unzulässig.

Rechtsgrundlage

Rechtsgrundlagen im **Agrarbereich** können sich insbesondere aus dem BDSG ergeben. Zentrale Norm ist § 28 Abs. 1 BDSG. Hiernach gilt: „Das Erheben, Speichern, Verändern oder Übermitteln personenbezogener Daten oder ihre Nutzung als Mittel für die Erfüllung eigener Geschäftszwecke ist zulässig

1. wenn es für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich ist,
2. soweit es zur Wahrung berechtigter Interessen der verantwortlichen Stelle erforderlich ist und kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung überwiegt, oder
3. wenn die Daten allgemein zugänglich sind oder die verantwortliche Stelle sie veröffentlichen dürfte, es sei denn, dass das schutzwürdige Interesse des Betroffenen an dem Ausschluss der Verarbeitung oder Nutzung gegenüber dem berechtigten Interesse der verantwortlichen Stelle offensichtlich überwiegt.“

Kurz gesagt, die Verarbeitung von personenbezogenen Daten ist zulässig, wenn sie zur Vertragserfüllung erforderlich ist (z. B. wenn der Lohnunternehmer im Rahmen des Auftrags Daten erfassen muss), ein berechtigtes Interesse hieran besteht oder die Daten aus allgemein zugänglichen Quellen stammen (z. B. kann dieses für einige Geodaten der Fall sein). In den letzten beiden Fällen ist zusätzlich das Interesse des Betroffenen dagegen abzuwägen.

Eine weitere wichtige Rechtsgrundlage ist § 32 BDSG, das die Datenverarbeitung zum Zwecke eines Beschäftigungsverhältnisses (also im Rahmen eines Arbeitsvertrags bzw. Anstellungsvertrags) regelt. Dies ist im **Agrarbereich** insbesondere im Verhältnis selbständiger Lohnunternehmer-Auftraggeber wichtig, kann aber auch bei unselbständigen Lohnunternehmern gegenüber ihrem Chef relevant sein.

Soweit Telekommunikationsdienste betroffen sind, ergeben sich weitere Rechtsgrundlagen für die Verarbeitung von Bestandsdaten und Verbindungsdaten aus dem Telekommunikationsgesetz. Für Telemedien (wie etwa Webseiten) und die Verarbeitung von Bestandsdaten und Nutzungsdaten in diesem Bereich ist das Telemediengesetz heranzuziehen.

Einwilligung

Grundsätzlich wird im europäischen Datenschutzrecht von einem Einwilligungserfordernis ausgegangen, Art. 2 lit. h) EG-Datenschutzrichtlinie. Dieses ist in das deutsche Recht u. a. mit § 4a BDSG, § 12 TMG und § 94 TKG umgesetzt worden. Jeder Anbieter von Internetdiensten ist entsprechend diesen Vorschriften verpflichtet zu prüfen, ob die Nutzer eine wirksame Einwilligung für die Erhebung, Verarbeitung und Nutzung ihrer personenbezogenen Daten erteilt haben. Eine Einwilligung ist eine Willenserklärung des Betroffenen dahingehend, dass seine personenbezogenen Daten erhoben, verarbeitet und genutzt werden dürfen. Diese muss freiwillig für den konkreten, ihm bekannten Sachverhalt erteilt worden sein.

Eine Einwilligung soll in der Regel schriftlich erteilt werden, soweit nicht wegen besonderer Umstände eine andere Form angemessen ist. Soweit Daten im Rahmen einer elektronischen Kommunikation erhoben, verarbeitet oder genutzt werden, ist eine Einwilligung auch in elektronischer Form möglich. § 13 Abs. 2 TMG und § 94 TKG setzen insoweit Erwägungsgrund 17 der EG-Datenschutzrichtlinie um und bestätigen, dass auch Diensteanbieter in den Bereichen Telemedien und Telekommunikationsdienste eine elektronische Einwilligung zur Erhebung, Verarbeitung und Nutzung der personenbezogenen Daten erhalten können [Heckmann 2007, Kapitel 1.12, Rn. 53]. Die Form der Einwilligung muss allerdings sicherstellen, dass der Nutzer seine Einwilligung bewusst und eindeutig erteilt, die Einwilligung protokolliert wird, der Nutzer den Inhalt der Einwilligung jederzeit abrufen und mit Wirkung für die Zukunft widerrufen kann.

Zweckbindung

Weiterhin dürfen personenbezogene Daten nur für den Zweck verwendet werden, für den sie erhoben wurden (Art. 6 Abs. 1 lit. c) EG-Datenschutzrichtlinie, § 28 ff. BDSG, § 12 Abs. 2 TMG). Dieser Grundsatz sichert für den Betroffenen die Transparenz über die Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten. Eine über den Erhebungszweck hinausgehende Verarbeitung oder Nutzung der personenbezogenen Daten des Betroffenen ist ohne seine Einwilligung oder eine weitere Erlaubnisnorm nicht zulässig.

Viele „Hauptzwecke“, zu denen personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind in den §§ 28 ff. BDSG aufgeführt. Dabei handelt es sich zwar lediglich um Beispiele, die nicht abschließend aufgezählt werden; es hat sich aber gezeigt, dass sie einen Großteil der typischen Datenerhebungen abdecken. So können personenbezogene Daten von Unternehmen für eigene (§ 28 f. BDSG) oder für fremde (§ 29 BDSG) Geschäftszwecke erhoben werden. Anerkannte Zwecke, für die eine Erhebung, Verarbeitung oder Nutzung personenbezogener Daten erforderlich sein kann, sind unter anderem Vertragserfüllung, Gefahrenabwehr, Werbung, Markt- und Meinungsforschung und auf anderen berechtigten Interessen beruhende Zwecke, die jedoch ausreichend spezifiziert sein müssen.

Eine Zweckänderung ist grundsätzlich möglich. Für diese bedarf es allerdings einer weiteren Erlaubnisnorm. Der Grundsatz der Rechtmäßigkeit muss insoweit erfüllt werden; für die Zweckänderung ist daher erneut eine Einwilligung des Betroffenen oder eine Rechtsgrundlage erforderlich. Rechtsnormen, die eine Zweckänderung für die personenbezogenen Daten rechtfertigen, lassen sich ebenfalls u. a. im BDSG (§ 28 Abs. 2 BDSG) und im TMG (§ 14 Abs. 2, § 15 Abs. 3, 4, 8 TMG) finden.

Erforderlichkeit und Datensparsamkeit

Im Zusammenhang mit der Zweckbindung der Datenverarbeitung steht der Grundsatz der Erforderlichkeit. Der Grundsatz der Erforderlichkeit findet seinen Niederschlag in Art. 6 und 7 der EG-Datenschutzrichtlinie. Dies bedeutet, dass nur diejenigen Daten erhoben, verarbeitet und genutzt werden dürfen, die für den jeweiligen Zweck erforderlich sind. Eine über den Zweck hinausgehende Erhebung personenbezogener Daten ist in der Regel nicht zulässig. Im Ergebnis bedeutet dies, dass für jeden Vorgang erneut überprüft werden muss, welche Daten für diesen Vorgang überhaupt notwendig sind und ob eventuell der Personenbezug nicht erforderlich ist und dementsprechend die Daten gar nicht erst erhoben oder möglichst bald anonymisiert, pseudonymisiert oder gelöscht werden können.

Im Rahmen von Telemedien bedeutet dies für den Diensteanbieter, in jeder Phase die Erforderlichkeit der Daten und deren etwaigen Personenbezugs zu prüfen und die technischen Vorkehrungen zu schaffen, dass personenbezogene Daten nur in dem erforderlichen Umfang erhoben, verarbeitet und genutzt werden. Dies erstreckt sich auch auf technisch bedingt anfallende Daten, z. B. durch Internetübertragungsprotokolle, sowie auf (temporäre) Zwischenspeicherungen bestimmter Daten. Hier haben sich Auswahl und Gestaltung von Datenverarbeitungssystemen an dem Ziel auszurichten, so wenig personenbezogene Daten wie möglich zu erheben, zu verarbeiten oder zu nutzen (Grundsatz der Datenvermeidung und Datensparsamkeit, § 3a BDSG).

Eine immer mögliche Verfügbarkeit aller erhobenen Daten ist in den seltensten Fällen erforderlich. Daraus folgt insbesondere, dass personenbezogene Daten, die für Vorgänge nicht (mehr) erforderlich sind und für die auch keine sonstigen Aufbewahrungspflichten etwa nach der Abgabenordnung bestehen, zu löschen sind und nicht auf Vorrat gehalten werden dürfen.

Sollte es im **Agrarbereich** die Bestrebung geben, dass datenverarbeitende Stellen, Daten möglichst lange aufbewahren, so widerspricht dies dem Grundsatz der Erforderlichkeit. Personenbezogene Daten dürfen nicht über die Erfüllung des Zwecks hinaus gespeichert werden, sofern es hierfür nicht eine besondere Rechtsgrundlage gibt (z. B. in der Abgabenordnung) oder die Einwilligung des Betroffenen vorliegt. Weder die „Kundenpflege“ noch andere Interessen an den Daten erlauben eine längere Aufbewahrung der Daten ohne Einwilligung des Betroffenen. In der Praxis sollte daher entweder rechtzeitig (ggf. schon bei Beauftragung) die Einwilligung der Betroffenen eingeholt werden, dass Daten noch für einen anderen (konkret beschriebenen) Zweck gespeichert werden.

Alternativ können Daten ohne Personenbezug gespeichert werden, in dem sie vollständig anonymisiert werden (etwa in Form einer Statistik). Hierbei muss jedoch sichergestellt sein, dass die anonymisierten Daten keinen Rückschluss auf die Betroffen, deren Daten etwa die Grundlage der Statistik darstellen, erlauben. Hierfür ist es in der Regel notwendig, eine genügend große Anonymitätsgruppe zu bilden.

Pseudonymisierung

Bei einer Pseudonymisierung von Daten werden identifizierende Merkmale von Personen durch andere Kennzeichen oder Identifikatoren so ersetzt, dass für Dritte die Identifikation unmöglich oder sehr erschwert ist: „Pseudonymisieren ist das Ersetzen des Namens und anderer Identifikationsmerkmale durch ein Kennzeichen zu dem Zweck, die Bestimmung des Betroffenen auszuschließen oder wesentlich zu erschweren“ (§ 3 Abs. 6a BDSG).

Anwendungsbereiche liegen vor allem im Bereich der medizinischen Diagnose und Forschung, bei der beispielsweise in einem Datensatz Patientennamen durch Patientennummern ersetzt werden. Auf diese

Weise kann ein Empfänger dieser Datensätze Patienten noch individuell unterscheiden, aber Patienten nicht mehr identifizieren.

Im Rahmen eines ISOXML-Datensatzes wäre in Bezug auf Mitarbeiter/Maschinenbediener die Verwendung des Feldes „WorkerID“ und die Löschung der Daten unter „WorkerDesignator“ eine Pseudonymisierung, da dann nur derjenige anhand der WorkerID die Maschinenbediener namentlich bestimmen kann, der über die Zuordnung „WorkerID – WorkerDesignator“ verfügt. Wenn über diese Zuordnung lediglich der Organisator der Maschineneinsätze (Lohnunternehmer) verfügt, wäre diese Pseudonymisierung wirkungsvoll. Wählt man hingegen (ungeschickterweise) als WorkerID einen allgemein bekannten Identifier (etwa die Mobilfunknummer des Maschinenbedieners) oder einen Identifier, der für Dritte auflösbar ist (etwa die Seriennummer des Führerschein, die Rentenversicherungsnummer o.ä.), so ist die Pseudonymisierung wenig wirkungsvoll und daher ungeeignet.

Ein weiteres Beispiel wäre die Kennzeichnung von Boden- oder Futtermittelproben für eine Laborauswertung mit Hilfe einer Kennummer, die einen landwirtschaftlichen Betrieb bezeichnet. Während die Zuordnung von einer Kennnummer zum Betrieb (oder zum Namen des Inhabers) bei der Proben nehmenden Stelle verbleibt, könne die Proben samt Kennummern an ein externes Labor gegeben werden. Dieses liefert die Ergebnisse samt Kennummer an die Proben nehmende Stelle zurück, die dann die Laborergebnisse dem Betrieb zuordnen kann.

Relevant ist, dass Dritte keine Kenntnis der Zuordnung zwischen Kennnummer und identifizierenden Daten haben und aus der Kennummer keine Schlüssel ziehen können. Würde man beispielsweise als Kennnummer eine Betriebsnummer des ZID nehmen, so wäre die Zuordnung zwischen Kennnummer und Betrieb auch Dritten zugänglich (etwa der ZID, antragsbearbeitenden Stellen aus dem Bereich der Agrarförderung, ggf. Beratern etc.). Ebenso lassen sich für ein beauftragtes Labor aus der der Betriebsnummer des ZID Schlüsse über Bundesland und Gemeinde ziehen und den Kreis infrage kommender Betriebe deutlich einschränken.

In Abschnitt „Schutz von personenbezogenen Daten und von Betriebs- und Geschäftsgeheimnisse durch Anonymisierung, Pseudonymisierung und Aggregation“ wird dies an einem Beispiel für einen Maschinendatensatz erläutert.

Anonymisierung

Das Bundesdatenschutzgesetz definiert Anonymisieren als „das Verändern personenbezogener Daten derart, dass die Einzelangaben über persönliche oder sachliche Verhältnisse nicht mehr oder nur mit einem unverhältnismäßig großen Aufwand an Zeit, Kosten und Arbeitskraft einer bestimmten oder bestimmbaren natürlichen Person zugeordnet werden können.“ (§ 3 Abs. 6 BDSG).

Personenbezogene Daten sind zunächst so zu verändert, dass die identifizierenden Informationen wegfallen, beispielsweise Namen oder eindeutige Identifikatoren wie Kfz-Kennzeichen, Personalnummern etc. Dennoch können die verbleibenden Daten so geartet sein, dass selbst ohne Kenntnis identifizierender Daten eine Wiedererkennung mit Zusatzwissen möglich ist.

Beispiel: Enthält eine Sammlung von Datensätzen über Personen die Datenfelder, „Name“, „Landkreis“, „Größe der bewirtschafteten Fläche“, „Durchschnittshektarertrag Weizen“, „Beruf, falls Nebenerwerb“, so ist der naheliegende Ansatz einer Anonymisierung, zunächst das Feld „Name“ zu löschen. In vielen Fällen sind die resultierenden Daten hinreichend anonym – nicht allerdings nicht in Bezug auf einen Nebenerwerbslandwirt mit dem Beruf „Landrat“.

Einen guten Anhaltspunkt für die Qualität einer Anonymisierung bietet die Frage, wie groß die Gruppe derjenigen Personen ist , auf die die Merkmale eines Datensatzes zutreffen („Wie viele Personen werden durch diesen Datensatz beschrieben?“), die Größe der sogenannten Anonymititätsgruppe.

Im oben genannten Beispieldatensatz umfasst die Gruppe mit dem Berufsfeld „Landrat“ genau eine Person, die zudem öffentlich bekannt ist. Hätte man hingegen das zusätzlich das Feld „Beruf“ gelöscht, so wären mehrere Personen infrage gekommen, die der reduzierte Datensatz beschreibt. Eine andere Möglichkeit wäre gewesen, das Feld „Beruf“ zu löschen oder die Beschreibung des Berufes durch Zusammenfassung und Ersetzung auf Oberkategorien zu ändern (etwa: „Beamter“, „ Öffentlicher Dienst“, „Verwaltung“ o. ä.). Auch hier hätte sich die Anonymitäts-gruppe merklich vergrößert.

Unterschieden wird weiterhin zwischen einer „absoluten Anonymisierung“ und einer „faktischen Anonymisierung“. Bei der absoluten Anonymisierung werden die personenbezogenen Daten so verändert, dass die betroffenen Personen wieder direkt noch indirekt identifiziert werden können. Dies hat zur Folge, dass die Daten nach der Anonymisierung nicht mehr personenbezogen sind und unter den Geltungsbereich der Datenschutzgesetze fallen.

Bei einer faktischen Anonymisierung werden die Daten so verändert, dass eine Identifizierung zwar prinzipiell noch möglich erscheint, der dazu erforderliche Aufwand an Kosten, Zeit, Arbeitskraft oder Zusatzwissen jedoch unverhältnismäßig ist. Dies ist ein risikobasierter Absatz; ein „Restrisiko der Anonymisierung“ verbleibt [Metschke/Wellbrock 2002, S. 21]. Das Restrisiko kann sich auch im Laufe der Zeit ändern, etwa weil Zusatzinformationen leichter verfügbar werden oder sich Arbeitsabläufe automatisieren lassen.

Daher ist es sinnvoll, strengere Maßstäbe als bei „öffentlichen Daten“ an die Verarbeitung dieser Date anzulegen und sie zumindest in praktischer Hinsicht weiterhin wie personenbezogene Daten zu behandeln (z.B. keine Veröffentlichung, Zugriffschutz, vertragliche Regelungen für die Weiterverwendung, etc.).

In Abschnitt „Schutz von personenbezogenen Daten und von Betriebs- und Geschäftsgeheimnisse durch Anonymisierung, Pseudonymisierung und Aggregation“ wird dies an einem Beispiel für einen Maschinendatensatz erläutert.

Aggregieren

Aggregieren ist kein gesetzlich definierter Begriff des Datenschutzrechts. Als Aggregation kann eine Zusammenfassung von Einzelgrößen zu einer Gesamtgröße bezeichnet werden, sofern die Einzelgrößen hinreichend homogen sind. Dies führt in der Regel zu einem gewollten Verlust von Detailinformationen, etwa um Datenmengen zu reduzieren, Wesentliches von Unwesentlichem unterscheiden zu können oder um unwesentliche Schwankungen von Detailwerten ausgleichen zu können. Beispiele sind Durchschnittsbildungen (etwa Gesamtertrag pro Hektar) oder Summenbildung (Jahresniederschlagssumme).

Den Verlust von Detailinformationen kann man dazu ausnutzen, einen Personenbezug zu entfernen oder die Identifizierbarkeit von Personen zu erschweren oder unmöglich zu machen. Dazu muss man Daten so aggregieren, dass die Anonymitätsgruppe wächst.

Bezogen auf das oben genannte Beispiel wurden Berufsfelder aggregiert, so das ein Landrat oder eine Landrätin der Gruppe „Beamter/öffentlicher Dienst/Verwaltung“ zugeordnet und innerhalb dieser Gruppe nicht das einzige Mitglied ist.

Betrachtet man in dem oben genannten Beispiel den Maximalwert der bewirtschafteten Fläche innerhalb eines Landkreises, so dürfte dessen Eigentümer bzw. Bewirtschafter zumindest örtlich bekannt sein. In diesem Fall wäre eine Aggregationsstrategie, Flächengrößen zu gruppieren (etwa „< 10 h, 10-50 ha, 50-150 ha, > 150 ha“) und anstelle der Fläche die Flächengruppe weiter zu verarbeiten. Die Gruppen sind dabei so zu wählen, dass einerseits eine Analyse noch statistisch sinnvoll ist, andererseits die Gruppen so gewählt werde, dass der Eigentümer bzw. Bewirtschafter der größten Fläche nicht mehr das einzige Mitglied seiner Gruppe ist.

Datensicherheit

Neben diesen materiellen Grundsätzen sind technisch-organisatorische Anforderungen (§ 9 BDSG i. V. m. der Anlage zu § 9 BDSG, § 13 Abs. 4 TMG, § 109 TKG) bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten zu beachten. Dazu gehört das Gewährleisten von Datensicherheit: Bei der Erhebung, Verarbeitung und Nutzung personenbezogener Daten müssen diejenigen technischen und organisatorischen Maßnahmen getroffen werden, die erforderlich und angemessen sind, um den angestrebten Schutzzweck zu erfüllen. Beispiele für organisatorische Maßnahmen sind Geschäftsordnungen, Zuständigkeitszuweisungen oder Dienstanweisungen; Beispiele für technische Maßnahmen sind Schließsysteme an Türen, Verschlüsselung von Datenübertragungen und –speichern, Backupverfahren und die Durchsetzung von Lese- oder Schreibrechten auf Datenbestände.

Technisch-organisatorische Maßnahmen der Anlage zu §9 BDSG

In § 9 des BDSG und der Anlage zu § 9 sind technisch-organisatorische Anforderungen in Form sogenannter „Kontrollen“ festgelegt, um (rechtliche) Datenschutzanforderungen in der Praxis durch technische und/oder organisatorische Maßnahmen umzusetzen. Diese Kontrollen bezeichnen zunächst in Form eines Kontrollziels, was kontrolliert werden soll, machen aber keine konkreten Vorgaben für das „Wie“. Die in der Anlage zu § 9 festgelegten Kontrollen umfassen die Begriffe

- Zutrittskontrolle (Kontrolle des physikalischen Zutritts zu Datenverarbeitungsanlagen)
- Zugangskontrolle (Kontrolle der Benutzung von Datenverarbeitungsanlagen)
- Zugriffskontrolle (Kontrolle des logischen Zugriffs auf Daten, d. h lesen, kopieren, verändern, entfernen, auf Daten),
- Weitergabekontrolle (Kontrolle der Zugriffs während einer Datenübertragung und der Übertragungswege),
- Eingabekontrolle (Feststellbarkeit von Datenbestandsänderungen, d.h. Eingaben, Veränderungen oder Löschungen von Daten, und ihres Urhebers),
- Auftragskontrolle (Umsetzung von Weisungen des Auftragebers und Verhinderung nichtweisungskonformen Verhaltens),
- Verfügbarkeitskontrolle (Schutz gegen zufällige Zerstörung oder Verlust),
- Trennungsgebot (Schutz gegen ungewollte zweckübergreifende Verarbeitung).

(Trennungsgebot: Der Gesetzestext enthält für diese Maßnahme keine Kurzbezeichnung in Form einer „-kontrolle“. Gefordert wird, dass die Einhaltung von Zweckbindung und Zwecktrennung auch durch technisch-organisatorische Maßnahmen gewährleistet wird.)

Für die Kontrollen Zugangs-, Zugriffs- und Weitergabekontrolle nennt der Gesetzestext explizit Verschlüsselungsverfahren als geeignete Maßnahmen (Anlage zu § 9 Satz 1 BDSG, dort Satz 2). Andere konkrete Maßnahmen nennt der Gesetzgeber nicht. Die nachfolgende Aufzählung enthält zum leichteren Verständnis einige Beispiele für Maßnahmen, um die Kontrollziele zu erreichen.

Beispielhafte Zuordnung von Kontrollzielen und Datensicherheitsmaßnahmen:

- Zutrittskontrolle: verschlossene Server- und Technikräume bzw. -Schränke, abgeschlossene Büros, Datenträger unter Verschluss.
- Zugangskontrolle: Authentifizierung von Benutzern (z. B. Passwortschutz von Betriebssystemen, Geräten und Anwendungen), automatische Bildschirmsperren
- Zugriffskontrolle: Autorisierung von Nutzeraktionen, Ausgestaltung eines Berechtigungskonzepts (Nutzerrechte, Gruppenrechte) für einzelne Aktivitäten (Schreiben, Lesen, Löschen, Kopieren, Übermitteln etc.)
- Weitergabekontrolle: Verschlüsselung von Daten bei Übertragung (z. B. SSL, VPN), Authentisierung der Kommunikationspartner, gesicherte Transportbehälter
- Eingabekontrolle: Protokollierung der Dateneingabe und -veränderungen
- Auftragskontrolle: Abgrenzung der Kompetenzen zwischen Auftraggeber und Auftragnehmer, Vertraglichere Regelungen gemäß § 11 BDSG, Vorgaben des Auftraggebers für die Verarbeitung, Prüfung der Zuverlässigkeit
- Verfügbarkeitskontrolle: Sicherung der Daten (Backup, Recovery) und ggf. der Datenverarbeitungssysteme (USV, zweite Netzanbindung, Ersatzgeräte)
- Trennungskontrolle: getrennte Verarbeitung von Daten mit unterschiedlichen Zwecken, unterschiedliche Bildschirmanzeigen/Datenpräsentation je nach Verarbeitungszweck, Einschränkung von Leserechten

Es bleibt den datenverarbeitenden Stellen überlassen, geeignete (Sicherheits-) Maßnahmen auszuwählen, um die Kontrollziele erreichen. Ein Verfahren zur systematischen Auswahl der Maßnahmen ist in Abschnitt „Maßnahmenauswahl“ enthalten.

Dabei haben sie einen Spielraum bezüglich der Stärke (und damit indirekt der Aufwände und Kosten) der Sicherheitsmaßnahmen, denn „erforderlich sind Maßnahmen nur, wenn ihr Aufwand in einem angemessenen Verhältnis zu dem angestrebten Schutzzweck steht.“ (§ 9 Satz 2 BDSG).

Der Gesetzgeber macht keine direkten Vorgaben, welche Stärke die Sicherheitsmaßnahmen haben müssen oder wie ein „angemessenes Verhältnis“ aussehen kann. Daher gibt es zu diesem Punkt zahlreiche Kommentarliteratur und Hinweise der Datenschutzbeauftragten, etwa in Form von Handreichungen und Orientierungshilfen, die sich aber meist auf konkrete Fragestellungen beziehen (etwa „Datenschutz im Krankenhaus“, „Datenschutzgerechte Vernichtung und Löschung von Daten“).

Eine ähnliche Situation ergibt sich, wenn anstelle des Bundesdatenschutzgesetztes (für privatrechtlich organisierte Datenverarbeiter wie Firmen und Vereine sowie für Bundesbehörden) die Landesdatenschutzgesetze anzuwenden sind, etwa bei der Datenverarbeitung durch öffentlich-rechtliche Institutionen wie Universitäten und einige Landwirtschaftskammern als Körperschaften öffentlichen Rechts. Einige Landesdatenschutzgesetze enthalten nahezu textgleiche Formulierungen zur Datensicherheit wie das BDSG, andere setzten auf einer abstrakteren Ebene an und normieren

Schutzziele (siehe unten) für die Datenverarbeitung, die durch technisch-organisatorische Maßnahmen erreicht werden soll. Auch hier macht der Gesetzgeber (bis auf Spezialfälle) keine konkreten Vorgaben für Sicherheitsmaßnahmen, sondern überlässt die Wahl dem Datenverarbeiter.

In allen Fällen stellt sich daher die Frage, wie aus den Vorgaben der Kontrollen (BDSG) und der Schutzziele (einige LDSGe) angemessene Sicherheitsmaßnahmen abzuleiten sind. In der Praxis bedient man sich häufig Methoden aus dem Bereich der IT-Sicherheit bzw. der Informationssicherheit und wählt Sicherheitsmaßnahmen auf der Basis einer Risikoanalyse aus.

Schutzziele

Die Formulierung von Schutzzielen soll das Problem lösen, dass konkrete Sicherheitsmaßnahmen zweckmäßigerweise im Einzelfall risikobasiert festzulegen sind („angemessenes Verhältnis“) und sich ihre konkrete Ausprägungen nach dem Stand der Technik vergleichsweise schnell ändern (z. B. Absicherungen von Webanwendungen durch Firewalls, Web-Application-Firewalls, Penetrationstests, Verwendung von Frameworks satt Eigenentwicklungen etc.). Beides sind schlechte Voraussetzungen für detaillierte gesetzliche Festlegungen in Form von Maßnahmekatalogen, die universell für personenbezogene Datenverarbeitungen gelten sollen. Für konkrete Datenverarbeitungen kann es hingegen konkrete (unter-)gesetzliche Vorgaben geben (z. B. Technische Richtlinien).

Als modernes Instrument des Datenschutzes etabliert sich inzwischen in vielen Gesetzen das Modell der Schutzziele. Sechs Schutzziele sind z. B. im Landesdatenschutzgesetz Schleswig-Holstein (§ 5) aufgeführt. Hierbei sind nicht alle Schutzziele für alle Anwendungen gleich stark relevant. Je nach Einsatzszenario kann z. B. die Integrität anders zu gewichten sein als die Nicht-Verkettbarkeit. Die Schutzziele und ihre Relevanz für den Prototyp werden im Folgenden erläutert.

a. Verfügbarkeit

Verfahren und Daten müssen zeitgerecht zur Verfügung stehen und ordnungsgemäß angewendet werden können.

Dieses Schutzziel betrifft z. B. die Frage, ob die eingesetzten IT-Systeme stets zeitnah zur Verfügung stehen. Ist etwa der Einsatz einer Landmaschine von der Verfügbarkeit eines IT-Systems abhängig, dann muss dieses auch einsatzbereit sein bzw. Alternativmöglichkeiten bestehen, um die Auftragserfüllung selbst bei Ausfall einzelner Systeme zu gewährleisten.

b. Integrität

Daten müssen unversehrt, vollständig, zurechenbar und aktuell bleiben.

Dies betrifft u. a. auch Protokolle über den Einsatz von Landmaschinen. Wie oben dargestellt kann es jedoch aus Gründen des Datenschutzes erforderlich sein, dass Unschärfen eingebunden werden und eine Zurechenbarkeit gerade durch Anonymisierung oder Pseudonymisierung erschwert wird. Allerdings muss dieses erkennbar sein und darf nicht zu Missverständnissen bzw. Missinterpretationen führen.

c. Vertraulichkeit

Es kann nur befugt auf Verfahren und Daten zugegriffen werden.

Es muss z. B. ein Rechtesystem bestehen, das den Zugriff auf die gespeicherten Daten auf die hierfür im Rahmen ihres Aufgabenbereichs befugten Personen einschränkt. Die Hersteller der Landmaschinen

dürfen auf die Daten nur zugreifen, wenn hierfür eine Rechtsgrundlage besteht bzw. im Rahmen eines Auftragsdatenverarbeitungsverhältnisses. Durch Verschlüsselung können Daten ebenfalls vor den Zugriff durch Unbefugte geschützt werden, insbesondere bei Datenübertragungen.

d. Transparenz

Die Verarbeitung von personenbezogenen Daten kann mit zumutbarem Aufwand nachvollzogen, überprüft und bewertet werden. Dies bezieht sich sowohl darauf, dass entsprechende Dokumente bzw. Verfahrensbeschreibungen existieren, an denen die verwendeten Verfahren nachvollzogen werden können. Auch für Betroffene muss Transparenz etwa im Rahmen der Formulierung der Einwilligungserklärung oder von Datenschutzerklärungen hergestellt werden.

e. Intervenierbarkeit

Verfahren müssen so gestaltet werden, dass sie den Betroffenen die Ausübung der ihnen zustehenden Betroffenenrechte wirksam ermöglichen.

Insbesondere muss der Betroffene seine Rechte auf Auskunft, Löschung und Berichtigung umsetzen können. Entsprechende Verfahren müssen vorhanden sein, so dass die Auskunft vollständig ist und eine echte physikalische Löschung erfolgen kann. Betroffene sollten nachfragen und sich ggf. beschweren können, ohne dass dafür besondere Hürden zu überwinden sind, und sie sollten mit ihrem Anliegen ernst genommen werden.

f. Nicht-Verkettbarkeit

Personenbezogene Daten können nicht oder nur mit unverhältnismäßig hohem Aufwand für einen anderen als den ausgewiesenen Zweck erhoben, verarbeitet und genutzt werden.

Es muss verhindert werden, dass personenbezogene Daten aus unterschiedlichen Quellen so zusammengeführt werden und sich hieraus neue Erkenntnisse über den Betroffenen ergeben, ohne dass er dieses will. In diesen Fällen sind verschiedene Verarbeitungsprozesse und Datenquellen strikt voneinander getrennt zu halten.

Für die Ausgestaltung von IT-Systemen im Agrarbereich und deren Betrieb sollten sich Entwickler und Betreiber an diesen Grundsätzen orientieren.

Maßnahmen

Wie oben dargestellt gibt es im Bereich der Datenschutzgesetze des Bundes und der Länder nur sehr wenige konkrete Maßnahmenfestlegungen; vielmehr können und müssen die Maßnahmen in Abhängigkeit des Einzelfalls und des potentiellen Risikos ausgesucht und implementiert werden.

Da viele Anwender gleichgelagerte Risiken haben, gibt es Sammlungen und Kataloge mit Standardmaßnahmen, oft sogar priorisiert im Hinblick auf Risiken. Diese haben meist bestimmte technische Systeme im Fokus (z. B. „Sicherheitsmaßnahmen bei Windows-Betriebssystemen“, „Sicherheitsmaßnahmen für Webanwendungen“, „Sicherheitsmaßnahmen bei WLAN“). Daneben gibt es Vorgehensbeschreibungen, wie man systematisch aus einer Darstellung der Verfahren und den eingesetzten technischen Systemen Risiken abschätzt und adäquate Sicherheitsmaßnahmen wählt. Beispiele hierfür sind die internationalen Normen ISO 27001/27002 sowie IT-Grundschutz (Standard BSI 100-2).

Ziel ist es, das Risiko **für die Betroffen** im Hinblick auf die Verletzung der Schutzziele (siehe

Abschnitt „Schutzziele“) durch Auswahl geeigneter Sicherheitsmaßnahmen auf ein akzeptables Maß zu senken. Wenn durch die gleichen Maßnahmen (etwa: Zutrittskontrolle zu Servern, Verschlüsselung) auch Risiken der Datenverarbeiter gesenkt werden (z. B. Verlust von Verfügbarkeit, Schutz von Betriebs- und Geschäftsgeheimnissen), ist dies umso besser.

In vielen Fällen gehen die Interessen der Betroffenen und der Organisation konform (z.B. Verfügbarkeit eines Services oder einer Anwendung). In anderen Fällen mag dies nicht der Fall sein (etwa wenn ein Arbeitgeber ein Interesse an einer vollumfänglichen Protokollierung hat, Arbeitnehmer als Betroffene hingegen eine unzulässige Leistungs- und Verhaltenskontrolle befürchten). Zwar gibt es dann im Rahmen der datenschutzrechtlichen Regelungen Festlegungen, wie solche Zielkonflikte zu lösen sind, doch müssen diese Lösungen sich dann in den Festlegungen konkreter technischer und organisatorischer Maßnahmen wiederfinden. Bei der Nutzung der oben genannten Normen ist daher zu beachten, dass auch das Risiko für die Betroffen, und nicht nur das Risiko für die Organisationen, auf ein akzeptables Maß gesenkt wird. Daher ist bei der Risikoanalyse auch die Sicht der Betroffenen einzunehmen.

Transparenz

Für den Betroffenen müssen Erhebung, Verarbeitung und Nutzung seiner personenbezogenen Daten transparent sein. Dies bedeutet, dass es jedem Nutzer von Internetdiensten möglich sein muss zu wissen, welche personenbezogenen Daten über ihn an welcher Stelle verfügbar sind. Die datenschutzrechtlichen Bestimmungen von BDSG, TMG und TKG werden diesem Grundsatz insoweit gerecht, als sie Rechte für den Betroffenen und Pflichten für die verantwortliche Stelle, den Diensteanbietern von Telemedien bzw. Telekommunikationsdiensten enthalten. So sind in allen Gesetzen Auskunfts-, Löschungs- und Berichtigungsansprüche zu finden, die die Rechte der Betroffenen gewährleisten sollen. Demselben Zweck dienen bestimmte Informationspflichten der verantwortlichen Stellen.

Sollten im Agrarbereich Webinterfaces genutzt werden, so bedeutet dies, dass der Nutzer zu Beginn des Nutzungsvorgangs über Art, Umfang und Zweck der Erhebung und Verwendung der personenbezogenen Daten zu informieren ist (vgl. § 13 Abs. 1 TMG). Sofern das Interface der Landmaschine online direkt mit einem Webdienst verbundnen ist, gilt dieses ggf. auch hierfür. Werden die personenbezogenen Daten nicht direkt beim Nutzer erhoben, so ist dieser nachträglich darüber zu benachrichtigen, welche Daten zu welchem Zweck erhoben, verarbeitet und genutzt werden.

Dokumentationspflichten

Eine gesetzliche Dokumentationspflicht für Verfahren enthält § 4e BDSG; die Landesdatenschutzgesetze enthalten ähnliche Regelungen. Sie ist entweder in Form vom Meldungen der Verfahren gegenüber der zuständigen Datenschutzaufsichtsbehörde (§ 4d BDSG, siehe auch die Abschnitte „Generelle Regelungen“ zu Datenschutzbeauftragten und „Zuständigkeiten und Aufsichtsbehörden“ zu den Aufsichtsbehörden) umzusetzen, oder bei Bestellung eines internen betrieblichen oder behördlichen Datenschutzbeauftragten in Form eines Verfahrensverzeichnisses von diesem zu führen und auf Antrag jedermann bekannt zu geben (§ 4g Abs. 2 BDSG).

Die relevanten Angaben der Meldung der Verfahren bzw. der Inhalte der Verfahrensübersicht sind in § 4e BDSG dargestellt:

1. Name oder Firma der verantwortlichen Stelle,

2. Inhaber, Vorstände, Geschäftsführer oder sonstige gesetzliche oder nach der Verfassung des Unternehmens berufene Leiter und die mit der Leitung der Datenverarbeitung beauftragten Personen,
3. Anschrift der verantwortlichen Stelle,
4. Zweckbestimmungen der Datenerhebung, -verarbeitung oder -nutzung,
5. eine Beschreibung der betroffenen Personengruppen und der diesbezüglichen Daten oder Datenkategorien,
6. Empfänger oder Kategorien von Empfängern, denen die Daten mitgeteilt werden können,
7. Regelfristen für die Löschung der Daten,
8. eine geplante Datenübermittlung in Drittstaaten,
9. eine allgemeine Beschreibung, die es ermöglicht, vorläufig zu beurteilen, ob die Maßnahmen nach § 9 BDSG zur Gewährleistung der Sicherheit der Verarbeitung angemessen sind.

Üblicherweise werden durch eine verantwortliche Stelle mehrere Verfahren eingesetzt, so dass die Angaben nach den Nummern 1 bis 3 für diese Verfahren gleich sein dürften. Zum Punkt Nr. 9 siehe Abschnitt „Technisch-organisatorische Maßnahmen der Anlage zu §9 BDSG“.

Die Aufsichtsbehörden haben kommentierte Muster für Meldungen veröffentlicht, die als Template für eigene Verfahrensverzeichnisse dienen können. [z. B. https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verfahrensregister/Inhalt/Formulare/Formulare.php].

Zu beachten sind noch folgende Punkte:

1. Die in § 4e Satz 1 Nr. 9 dargestellten Angaben zu technisch-organisatorischen (Sicherheits-) Maßnahmen sind durch die betrieblichen bzw. behördlichen Datenschutzbeauftragten nicht zu veröffentlichen. Eine Befürchtung, durch die Öffentlichkeit der Verfahrensangaben würden Sicherheitsmaßnahmen und mögliche Angriffspunkte bekannt, muss nicht bestehen.
2. Die Sammlung der notwendigen Angaben für die Verfahrensverzeichnisse ist keine Holschuld der betrieblichen bzw. behördlichen Datenschutzbeauftragten, sondern eine Bringschuld der verantwortlichen Stellen (§ 4g Abs. 2. BDSG): Der Datenschutzbeauftragte hat nicht die Aufgabe, neue Verfahren oder Verfahrensänderungen (investigativ) aufzuspüren, sondern ist von der verantwortlichen Stelle aktiv zu informieren. Im Rahmen eines Datenschutzmanagements (siehe Kapitel „Datenschutzmanagement“ <3.2.7>) sollte ohnehin ein entsprechender Informationsfluss organisiert sein.
3. Dem Datenschutzbeauftragten sind über die oben genannten Angaben hinaus auch Angaben über zugriffsberechtigte Personen zur Verfügung zu stellen, also Angaben über das Berechtigungsmanagement (§ 4g Abs. 2. BDSG). Diese Angaben müssen ebenfalls nicht veröffentlicht werden.

Direkterhebungsgrundsatz

Nach § 4 Abs. 2 Satz 1 BDSG sind personenbezogene Daten beim Betroffenen zu erheben. Ausnahmen hiervon können nur aufgrund einer Rechtsvorschrift gemacht werden. Außerdem kann eine Ausnahme gemacht werden, wenn die Erhebung beim Betroffenen einen unverhältnismäßigen Aufwand erfordern

würde und keine Anhaltspunkte dafür bestehen, dass überwiegende schutzwürdige Interessen des Betroffenen beeinträchtigt werden (§ 4 Abs. 2 Satz 2 Nr. 2b BDSG).

Kurz gesagt, müssen personenbezogene Daten in der Regel bei demjenigen erhoben werden, den sie auch betreffen. Das bedeutet, dass etwa Informationen über ein Grundstück eines Landwirts, die einen Rückschluss auch auf den Landwirt selber zulassen, möglichst bei dem betroffenen Landwirt erhoben werden müssen. Nur in begründeten Ausnahmefällen kann auf andere Quellen zurückgegriffen werden.

Betroffenenrechte

Auskunftsrecht

Personen, die von Datenverarbeitung betroffen sind, haben in der Regel ein Auskunftsrecht gegenüber der datenverarbeitenden Stelle. Dies ist für die Auskunft bei privaten Stellen in § 34 BDSG geregelt (für öffentliche Stellen ist dieses Recht in § 19 BDSG zu finden). Diese Auskunft ist unentgeltlich und umfasst

- die zu einer Person gespeicherten Daten, auch soweit sie sich auf die Herkunft dieser Daten bezieht,
- den Empfänger oder die Kategorie von Empfängern, an die Daten weitergegeben werden, und
- den Zweck der Speicherung.

Ein solches Auskunftsrecht ist auch für den Bereich der Telemedien in § 13 Abs. 7 TMG geregelt.

Berichtigungsrecht

Personenbezogene Daten sind zu berichtigen, wenn sie unrichtig sind (vgl. § 35 Abs. 2 BDSG bzw. § 20 Abs. 1 BDSG).

Löschungsrecht

Personenbezogene Daten müssen gelöscht werden, wenn ihre Speicherung unzulässig ist bzw. wird oder sie für die Erfüllung des Speicher- bzw. Verarbeitungszwecks nicht mehr erforderlich sind (vgl. § 35 Abs. 2 BDSG bzw. § 20 Abs. 2 BDSG). Das bedeutet, dass auch wenn die Erhebung bzw. Speicherung von personenbezogenen Daten zunächst zulässig war, diese Zulässigkeit dann entfällt, wenn die Daten nicht mehr erforderlich sind. Die Daten sind dann umgehend zu löschen, sofern es für die Aufbewahrung keine weitere rechtliche Grundlage gibt und auch keine Einwilligung vom Betroffenen eingeholt wurde. Eine Speicherung auf Vorrat ist nicht zulässig. Die Speicherung jedes personenbezogenen Datums ist befristet. Die Umsetzung des Löschungsrechts muss von der datenverarbeitenden Stelle gewährleistet werden. Es ist nicht ausreichend, die Löschung erst auf Wunsch des Betroffenen vorzunehmen. Die datenverarbeitende Stelle muss selbst für die Einhaltung der Fristen und die dann erfolgende Löschung sorgen.

Sperrungsrecht

Die Löschung darf ausnahmsweise unterbleiben, wenn weitergehende Aufbewahrungsfristen gelten (z. B. im Rahmen der Abgabenordnung), Grund zu der Annahme besteht, dass durch eine Löschung

schutzwürdige Interessen des Betroffenen beeinträchtigt würden, oder eine Löschung wegen der besonderen Art der Speicherung nicht oder nur mit unverhältnismäßig hohem Aufwand möglich ist (vgl. § 35 Abs. 3 BDSG bzw. § 20 Abs. 3 BDSG). Die Daten sind auch zu sperren, wenn ihre Richtigkeit vom Betroffenen bestritten wird und sich weder die Richtigkeit noch die Unrichtigkeit feststellen lässt (vgl. § 35 Abs. Abs. 4 BDSG bzw. § 20 Abs. 4 BDSG).

Sperren bedeutet, dass die Daten nicht mehr im produktiven System erreichbar sind. Dies kann durch Aussondern in ein anderes System geschehen. Möglich ist auch die Markierung der gesperrten Daten etwa mit einem Flag, so dass gewährleistet ist, dass nur bestimmte Mitarbeiter (etwa im Rahmen der Revision beim Lohnunternehmer) Zugriff auf die gesperrten Daten bekommen.

Datenschutzmanagement

Die Implementierung und Sicherstellung des notwendigen und angemessenen Datenschutzniveaus ist, wie viele andere Aspekte (Beispielsweise Qualitätsmanagement, Arbeitssicherheit, Compliance) innerhalb einer Organisation, keine einmaliges Vorhaben, sondern eine Daueraufgabe, die Organisationen vorzugsweise mit Hilfe von Prozessen bearbeiten. Aus den gesetzlichen Vorschriften für betriebliche und behördliche Datenschutzbeauftragte ergeben sich einige Daueraufgaben für ein Datenschutzmanagement. Hinzu kommen organisatorische Aspekte, die sicherstellen, dass die Aufgaben mit dauerhaft hoher Qualität erfüllt werden. Gibt es bereits etablierte Managementsysteme, etwa für die Qualität der Produkte oder Dienstleistungen, IT-Sicherheit oder Risikomanagement, so haben diese Berührungspunkte mit dem Datenschutzmanagement, auf die man zurückgreifen sollte. Die folgende Darstellung orientiert sich an der Maßnahme M 7.1 (Datenschutzmanagement) des Bausteins „Datenschutz“ der IT-Grundschutzkataloge des BSI" [Abrufbar unter: https://www.bsi.bund.de/SharedDocs/Downloads/DE/BSI/Grundschutz/BaustDatenschutz/b01005_pdf.pdf?__blob=publicationFile].

Datenschutzprozess Herzstück des Datenschutzmanagements ist ein zyklischer Datenschutzprozess, der aus den drei Schritten „Erstellung des Datenschutzkonzeptes und Soll-Ist-Abgleich“ (M 7.3), „Umsetzung fehlender Maßnahmen“ und „Aufrechterhaltung des Datenschutzes im laufenden Betrieb“ besteht. Hinzu kommt eine Initialisierungsphase, in der die Aufbau- und Ablauforganisation festgelegt und beispielsweise eine Datenschutz-Leitlinie erstellt wird.

Teilprozess „Aufrechterhaltung des Datenschutzes im laufenden Betrieb“Der Teilprozess „Aufrechterhaltung des Datenschutzes im laufenden Betrieb“ hat die Aufgabe, auf Veränderungen im laufenden Betrieb zu reagieren. Diese können vielfältiger Natur sein, z. B. Änderungen an Verfahren und ihrer technischen Implementierung innerhalb der Organisation, an rechtlichen oder technischen Rahmenbedingungen (z. B. Änderung von Datenschutzgesetzen: Beispielsweise die Änderung des BDSG mit Wirkung vom 01.09.2009 (§ 47), 01.09.2010 (§ 47 Nr. 1) und 01.09.2012 (§ 47 Nr. 2), datenschutzrechtlich relevanten Rechtsgrundlagen, vertraglichen Regelungen oder Stärke von Verschlüsselungsverfahren) oder Sicherheitsvorfälle. Daher besteht dieser Teilprozess seinerseits aus fünf Teilprozessen:

- Management von IT-Sicherheitsvorfällen bei betroffenen Verfahren
- Management der Lebenszyklen von IT-Verfahren
- Monitoring und Management von Änderungen im Datenschutzrecht
- Technologie-Monitoring und -Management

- Monitoring und Management von Änderungen

Teilprozess „Management der Lebenszyklen von IT-Verfahren“Der Teilprozess „Management der Lebenszyklen von IT-Verfahren“ orientiert sich am Lebenszyklusmodell „Planung und Konzeption“, „Umsetzung des Konzeptes“, „laufender Betrieb“ und „Außerbetriebnahme und Löschung“. Hier finden sich die gesetzlich definierten Aufgaben eines Datenschutzbeauftragten wie das Führen von Verfahrensübersichten, ggf. Meldungen an die Aufsichtsbehörden, Schulung und Sensibilisierung, Vorabkontrollen und die Überwachung des laufenden Betriebes wieder. Der Baustein „Datenschutz“ der IT-Grundschutzkataloge stellt hierfür sogenannte Maßnahmen bereit, die die Umsetzung dieser Aufgaben beschreiben. Weitere Maßnahmen des Bausteins „Datenschutz“ betrachten Einzelaspekte der bzw. des datenschutzgerechten Konzeption und Betriebs, etwa die Verfahren zur Gewährleistung von Betroffenenrechten, Vorgaben für die Auftragsdatenverarbeitung und gemeinsame Verfahren, Voraussetzungen für die Freigabe und Aspekte bei der Auswertung von Datenbanken. Orientiert man sich an diesen Maßnahmen, hat man wichtige Voraussetzungen für die Aufrechterhaltung im laufenden Betrieb erfüllt.

Die übrigen vier Teilprozesse sind im Rahmen der Maßnahme M 7.1 (Datenschutzmanagement) dargestellt. Das Monitoring von Veränderungen im Datenschutzrecht und der Technologie sowie der Umgang mit diesen Veränderungen (Management) sind selbsterklärende Teilprozesse, die ihrerseits einen Neustart des Hauptprozesses auslösen können, wenn eine grundlegende Neugestaltung des Datenschutzkonzeptes erforderlich ist. Der Teilprozess „Monitoring und Management von Änderungen“ ist erforderlich, wenn das Datenschutzmanagement mit den Anforderungen und Formulierungen des IT-Grundschutzes (BSI-Standards und IT-Grundschutzkataloge) synchron gehalten werden.

Einige neuere Aufgaben des Datenschutzmanagements sind in der Darstellung des Bausteins „Datenschutz“ noch nicht explizit als Maßnahmentexte genannt. So gehört zu der Bearbeitung von Sicherheits- und Datenschutzvorfällen auch die Mitteilung an die Aufsichtsbehörde und ggf. an die Betroffenen gemäß § 42a BDSG, § 93 Abs. 3 TKG und § 15a TMG. Hinzu kommen Daueraufgaben des Datenschutzbeauftragten, etwa die Aufgabe, als Ansprechpartner für die Organisationsleitung und als vertraulicher Ansprechpartner für Betroffene (auch Beschäftigte) zu fungieren. Die Aufgaben eines Datenschutzbeauftragten sind im Maßnahmentext M 7.2 dargestellt.

Datenschutz im Agrarbereich

Geodaten und Standortdaten

Nach Artikel 3 Richtlinie 2007/2/EG des Europäischen Parlamentes und Rates v. 14. März 2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE-Richtlinie) gilt: Geodaten [sind] alle Daten mit direktem oder indirektem Bezug zu einem bestimmten Standort oder geografischen Gebiet […]. Diese Definition wurde auch von zahlreichen Geodateninfrastrukturgesetzen in den Bundesländern übernommen.

Hierbei ist zwischen Geobasisdaten und Geofachdaten zu unterscheiden. Geobasisdaten sind grundlegende amtliche Geodaten, welche die Landschaft (Topographie), die Flurstücke und die Gebäude im einheitlichen geodätischen Raumbezug anwendungsneutral beschreiben. Geofachdaten hingegen sind raumbezogene Daten aus einen Fachgebiet, z.B. Demographie, Epidemiologie,

Bodenkunde, Klimatologie, Wahlstatistik.

Standortdaten, die im Rahmen von Telekommunikationdiensten erhoben werden, sind in § 98 TKG geregelt. Dies betrifft insbesondere die Fälle, in denen Standortdaten mittels Mobilfunk erfasst werden und hiermit eine Lokalisierung des Mobilfunkgerätes erfolgt. Hierbei darf dieses nur mit Einwilligung des Betroffenen erfolgen und es sich Transparenzvorgaben einzuhalten, die gewährleisten, dass keine heimliche Standorterfassung erfolgen kann (s. o.).

Spezielle gesetzliche Datenschutzregelungen zu Geodaten im Sinne von Flächendaten gibt es für die im **Agrarbereich** zu vermutenden Konstellationen nicht. Zwar haben die Bundesländer (basierend auf EU-Recht) Geodateninfrastrukturgesetze erlassen. Jedoch richten sich diese Gesetze vor allem an öffentlich-rechtlich organisierte Stellen der Länder und nicht an die Privatwirtschaft. Dies gilt auch für das Geodatenzugangsgesetz des Bundes.

Somit muss im **Agrarbereich** auf die allgemeinen Grundsätze zurückgegriffen werden. Das Datenschutzrecht (insbesondere das BDSG) ist anwendbar, wenn es sich bei Geodaten um Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person handelt (vgl. § 3 Abs. 1 BDSG).

Es ist zu unterscheiden: Soweit die Standorterfassung im Rahmen von sog. „Diensten mit Zusatznutzen“ erfolgt (etwa zur Feststellung der aktuellen Position eines Fahrzeugs und damit auch des Maschinenbedieners), muss hierzu § 98 TKG beachtet werden. Die Regelung richtet sich dabei nicht nur an Mobilfunkprovider, sondern auch sonstige Anbieter von Telekommunikationsdiensten etwa über Apps oder auch sonstige Onlinedienste.

Werden die Daten für die Erfassung von Flurstücken (etwa die Abmessungen eines Feldes) genutzt, dann ist zu prüfen, inwieweit es sich hierbei um personenbezogene bzw. personenbeziehbare Daten handelt. So dürften sich oftmals hieraus auch Rückschlüsse auf den Eigentümer oder Pächter des landwirtschaftlichen Betriebs ziehen (etwa über die Art, in der er Landwirtschaft betreibt). Soweit sich auch Rückschlüsse auf den Wert des Grundstückes ziehen lassen, handelt es sich (auch) um Betriebs- und Geschäftsgeheimnisse, die hier nicht weiter behandelt werden.

Arbeitsbezogene Daten

Arbeitnehmer Stammdaten

Soweit Arbeitnehmerdaten (etwa bei angestellten Lohnunternehmern) verarbeitet werden, richtet sich dieses nach § 32 Abs. 1 Satz 1 BDSG: Personenbezogene Daten eines Beschäftigten dürfen für Zwecke des Beschäftigungsverhältnisses erhoben, verarbeitet oder genutzt werden, wenn dies für die Entscheidung über die Begründung eines Beschäftigungsverhältnisses oder nach Begründung des Beschäftigungsverhältnisses für dessen Durchführung oder Beendigung erforderlich ist. Dies gilt auch für die nicht automatisierte Datenverarbeitung (vgl. § 32 Abs. 2 BDSG).

Das bedeutet, dass Stammdaten der Arbeitnehmer (wie Name, Adresse, Kontodaten) verarbeitet werden dürfen.

Arbeitnehmer Tätigkeitsdaten

Auch Informationen über das Verhalten eines Arbeitnehmers dürfen nach § 32 Abs. 1 Satz 1 BDSG

verarbeitet werden. So ist es u. a. zulässig, eine Personalakte zu führen und Bewertungen des Arbeitnehmers über sein Arbeitsverhalten festzuhalten. Hierbei ist jedoch nach gängiger Rechtsprechung zu beachten, dass eine umfängliche Arbeitnehmerüberwachung nicht erfolgen darf. So hat 2003 das Bundesarbeitsgericht (BAG) entschieden [Urteil des BAG Az. 2 AZR 51/02]: „Das durch Art. 2 Abs. 1 i. V. m. Art. 1 Abs. 1 Grundgesetz gewährleistete allgemeine Persönlichkeitsrecht ist auch im Privatrechtsverkehr und damit auch im Arbeitsverhältnis zu beachten. […] Das allgemeine Persönlichkeitsrecht schützt den Arbeitnehmer vor einer lückenlosen technischen Überwachung am Arbeitsplatz durch heimliche Videoaufnahmen. Durch eine solche Kontrolle wird nicht lediglich eine Aufsichtsperson ersetzt. Vielmehr wird der Arbeitnehmer, der davon ausgehen muss, dass der Arbeitgeber bei bestimmten Gelegenheiten zum Mittel der heimlichen Videoaufzeichnung greift, einem ständigen Überwachungsdruck ausgesetzt, dem er sich während seiner Tätigkeit nicht entziehen kann.“

Diese Rechtsprechung bezieht sich zwar auf Videoüberwachung, kann aber auch auf andere Überwachungstechniken, wie die ständige Standortüberwachung eines Mitarbeiters, ausgeweitet werden.

Allgemeiner hat dann auch das Bundesarbeitsgericht 2008 entschieden [Beschluss des BAG Az. 1 ABR 16/07]: „Die mit der elektronischen Datenverarbeitung grundsätzlich verbundenen technischen Möglichkeiten, Einzelangaben über eine Person unbegrenzt zu speichern sowie jederzeit abzurufen, sind geeignet, bei den betroffenen Personen einen psychischen Anpassungsdruck zu erzeugen, durch den sie in ihrer Freiheit, ihr Handeln aus eigener Selbstbestimmung zu planen und zu gestalten, wesentlich gehemmt werden.“

Schon die Erhebung der entsprechenden Daten muss somit vom Datenschutzrecht gedeckt sein. Schon hierfür muss ein zulässiger Zweck vorliegen. Auch die Auswertung der Daten darf von diesem Zweck nicht abweichen, sofern keine der Ausnahmen in § 28 Abs. 2 BDSG vorliegt.

Im **Agrarbereich** ist dieses u. a. für die Erfassung der Tätigkeiten der Lohnunternehmer relevant. So ist es grundsätzlich zulässig, die Rahmendaten zu einer Tätigkeit (z. B. Beginn, Ende etc.) zu erfassen. Wird jedoch jede Bewegung eines Fahrzeugs erfasst und damit über längeren Zeitraum auch das Verhalten eines Angestellten, dann ist dieses eine unzulässige Arbeitnehmerüberwachung.

Eine Lösungsmöglichkeit wäre die Einbindung einer künstlichen Unschärfe in die erhobenen Geodaten, so dass etwa die konkrete Dauer einer Pause nicht mehr erkennbar ist, die Daten jedoch zur Abrechnung etwa anhand des Aufwands weiterhin geeignet sind. Beachtet werden muss auf jeden Fall auch die Zweckbindung der Daten. In der Regel dürfen die vollständigen Daten nicht für die Mitarbeiterüberwachung genutzt werden. Hiervon unabhängig ist die Nutzung für andere Zwecke (etwa für Abrechnungen oder statistische Auswertungen). Somit ist zur Festlegung der geeigneten Unschärfe zu prüfen, welche Genauigkeit der Daten für den zulässigen Zweck noch gerade erforderlich ist. Sind die Daten z. B. nur dafür erforderlich, um die Bearbeitung des Feldes an einem Tag zu dokumentieren, dann reicht ggf. eine sehr grobe Erfassung der Daten und nur stundengenaue Feststellung von Zeiten.

Soweit Daten über das Verhalten des Fahrers eines Fahrzeugs über SIM-Karten oder auch Speicherkarten etc. verarbeitet werden, kann § 6c BDSG einschlägig sein. Dies ist der Fall, wenn die automatisierte Datenverarbeitung direkt auf einer SIM- bzw. Speicherkarte in dem Fahrzeug erfolgt, ohne dass der Mitarbeiter hierauf Einfluss hat. Der Mitarbeiter muss dann u. a. in allgemein verständlicher Form über die Funktionsweise des Mediums einschließlich der Art der zu verarbeitenden personenbezogenen Daten aufgeklärt werde. Auch muss er erfahren, wie er sein Auskunftsrecht, Löschungsrecht etc. umsetzen kann und welche Maßnahmen bei Verlust der Zerstörung des Mediums

(der Karte) zu treffen sind. Kommunikationsvorgänge, die auf dem Medium eine Datenverarbeitung erfolgen, müssen für den Betroffenen eindeutig erkennbar sein.

Aber selbst wenn der § 6c BDSG nicht direkt anwendbar sein sollte, weil die Datenverarbeitung etwa nicht mittels eines Mediums erfolgt, sind diese Grundsätze anwendbar im Rahmen der allgemeine Datenschutzgesetze (vgl. Transparenz etc.).

Maschinendaten

Das Datenschutzrecht bezieht sich auf personenbezogene Daten im Sinne des § 3 Abs. 1 BDSG (Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbaren natürlichen Person). Maschinendaten werden hiervon nicht erfasst. Allerdings können diese zu personenbezogenen Daten werden, wenn sich aus den Maschinendaten Rückschlüsse auf etwas das Verhalten einer Person ziehen lassen. Werden z. B. über Sensoren Daten wie Beschleunigung, Geschwindigkeit, Spritverbrauch etc. erfasst, so sagen diese Daten auch etwas über den Führer der Maschine und seine Fahrweise aus, so dass es sich um zumindest personenbeziehbare Daten handeln kann.

Den Personenbezug und damit die Anwendung der Datenschutzgesetze kann man dadurch verhindern, dass die Maschinendaten nicht mit den Daten des Nutzers der Landmaschine verbunden werden oder nur statistische Daten verarbeitet werden. Beispielsweise wäre nur die Angabe zur Durchschnittsgeschwindigkeit oder zum Spritverbrauch pro 100 km zunächst nicht personenbezogen. Allerdings kann schon dann wieder ein Personenbezug entstehen, wenn die Maschine ausschließlich oder überwiegend von einer Person betrieben wird und diese Person etwa über Einsatzpläne identifizierbar wäre. Eine solche Identifizierung wäre auch in der Regel möglich, wenn die Daten mit einem Datum und einer Uhrzeit verbunden sind.

Auftragsbezogene Daten

Auftragserteilung

Die Verarbeitung von Daten, die für die Begründung, Durchführung oder Beendigung eines rechtsgeschäftlichen oder rechtsgeschäftsähnlichen Schuldverhältnisses mit dem Betroffenen erforderlich sind, ist in der Regel nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG zulässig. Das bedeutet, dass die Daten verarbeitet werden dürfen, die für die Erfüllung etwa eines Auftrags an den Lohnunternehmer erforderlich sind. Dies umfasst Informationen wie Name und Adresse des Auftraggebers, Informationen zum zu bearbeitenden Grundstück und Zahlungsangeben.

Auftragsdurchführung

Auch für die Datenverarbeitung im Rahmen der Auftragsdurchführung dient § 28 Abs. 1 Satz 1 Nr. 1 BDSG als Grundlage. So dürfen hierfür Informationen zum Grundstück verarbeitet und etwa zum Nachweis der Tätigkeit auch während der Tätigkeit etwa in Form von Geoinformationen erhoben werden. Hierbei gilt jedoch die Zweckbindung, so dass diese Informationen nur zur Auftragsdurchführung verwendet werden dürfen. Eine weitergehende Nutzung der Daten etwa zur Mitarbeiterüberwachung oder zur eigengeschäftlichen Bewertung eines Grundstücks oder gar zum Weiterverkauf der Daten ist nicht zulässig. Der Auftragnehmer darf die Daten nicht über die

Durchführung des Auftrags hinaus verwenden. Soll eine weitergehende Nutzung (etwa auch zur Speicherung für Folgeaufträge) erfolgen, ist hierfür in der Regel die ausdrückliche Einwilligung im Sinne des § 4a BDSG des Auftraggebers bzw. Betroffenen erforderlich.

Auftragsabrechnung und –abwicklung

Nach Erfüllung des Auftrags und Abrechnung der Leistung sind in der Regel die hierfür genutzten personenbezogenen Daten nicht mehr erforderlich. Da damit auch meist die Rechtsgrundlage für die weitere Nutzung der Daten entfällt, sind die Daten umgehend zu löschen bzw. dem Auftraggeber zu übergeben. Eine Ausnahme kann etwa nach der Abgabenordnung bestehen, die die Aufbewahrung von Geschäftsbriefen bzw. Rechnungen für eine bestimmte Zeit (in der Regel 10 Jahre) vorschreibt. Diese Geschäftsbriefe dürfen dann aufbewahrt werden. In der Regel umfasst diese Aufbewahrungsfrist jedoch nicht die übrigen bei der Auftragserfüllung angefallenen Daten. Diese müssen trotzdem gelöscht werden.

Aber auch die aufzubewahrenden Daten dürfen nicht in dem Produktivsystem vorgehalten werden, sondern müssen im Rahmen der Sperrung ausgesondert werden, so dass nur noch dann ein Zugriff erfolgen kann, wenn diese Daten etwa im Rahmen einer Kontrolle durch Behörden herausgegeben werden müssen.

Sollen personenbezogene Daten des Auftraggebers etwa für die Durchführung von Nachfolgeaufträgen aufbewahrt werden, dann muss der Auftraggeber hierin einwilligen.

Einbindung Dritter/Datenübermittlung

Eine Datenübermittlung von personenbezogenen Daten an Dritte bedarf einer Rechtsgrundlage oder der Einwilligung des Betroffenen. Liegt beides nicht vor, so kann es das Instrument der Auftragsdatenverarbeitung ermöglichen, Unterauftragnehmer etwa für die landwirtschaftliche Tätigkeit oder die Abrechnung einzusetzen. Nach § 3 Abs. 8 Satz 3 BDSG sind Auftragnehmer, die im Rahmen einer Auftragsdatenverarbeitung tätig werden, nicht als Dritte anzusehen, so dass auch keine Übermittlung vorliegt. Diese Auftragsdatenverarbeiter werden so angesehen, als wenn sie Mitarbeiter des beauftragenden Unternehmens wären. Hierzu ist jedoch ein besonderer Vertrag im Sinne des § 11 BDSG erforderlich. Dieser beinhaltet insbesondere ein Weisungsrecht des Auftraggebers. Der Auftragnehmer muss sich eng an die Weisungen halten. Somit kommt eine Auftragsdatenverarbeitung auch nur für Tätigkeiten infrage, bei denen der Auftragsdatenverarbeiter wenig bis keinen Gestaltungsspielraum über seine Tätigkeit hat. Auch darf er kein Eigeninteresse an den Daten haben (etwa zur Nutzung der Daten als Basis weitergehender Dienstleistungen). Des Weiteren muss der Auftragsdatenverarbeiter sorgfältig ausgewählt worden sein und regelmäßig überwacht werden. Ebenso muss er nachweisen, dass er die notwendigen technisch-organisatorischen Maßnahmen für seine Tätigkeit getroffen hat.

Protokolldaten

An vielen Stellen der Datenschutzgesetze gibt es direkte oder indirekte Vorschriften zur Protokollierung: Einige Landesgesetze enthalten explizit das Regelungsziel „Revisionsfähigkeit“; das BDSG gibt insbesondere in der Anlage zu § 9 BDSG technisch-organisatorische Maßnahmen vor, für deren Nachweisbarkeit typischerweise eine Protokollierung notwendig ist (z. B. für die Maßnahme „Eingabekontrolle“). Bei Abrufverfahren (§ 10 Abs. 4 BDSG) ist eine stichprobenartige Überprüfung

von Abrufen erforderlich, die ebenfalls typischerweise eine Protokollierung erfordert.

Daneben existieren für eine Reihe von (Verwaltungs-) Verfahren zudem bereichsspezifische (d. h. vom Datenschutzrecht des Bundes und der Länder abweichende Regelungen.), oft wesentlich konkretere Protokollierungsvorschriften, die sowohl öffentliche als auch private Stellen betreffen können. Beispiele hierfür sind Meldegesetze, Polizeigesetze, § 112 TKG oder § 97 SGB IV.

Für die typischen Anwendungsbereiche im **Agrarbereich** gibt es keine spezialgesetzlichen Protokollierungsvorgaben, so dass hier insbesondere die Anlage zu § 9 BDSG zu beachten ist.

Auch konkrete Vorgaben für die Ausgestaltung der Protokollierung gibt es nur in wenigen Vorschriften. Dennoch haben sich auf Basis der Anforderungen erprobte Vorgehensweisen entwickelt, die in diesem Text als grundlegende Empfehlungen dargestellt werden.

Zu unterscheiden sind Aufzeichnungen aufgrund fachlicher Anforderungen und Protokollierungen aufgrund datenschutzrechtlicher Anforderungen: So ist beispielsweise bei einer Tarifänderung für eine Dienstleistung eines Lohnunternehmers die Speicherung des Vortarifs für zurückliegende Abrechnungen erforderlich; ebenso dürfte bei einem Dauervertragsverhältnis nach einer Änderung der Postdresse des Auftraggebers auch die vorherige Adresse gespeichert bleiben, um auch während der Aufbewahrungsfrist der Rechnung den (schriftlichen) Vertrag zweifelsfrei dem Vertragsnehmer zuordnen zu können. In beiden Fällen handelt es sich um Aufzeichnungen aufgrund fachlicher Anforderungen.

Beispiele für Protokollierungen aufgrund datenschutzrechtlicher Vorschriften sind hingegen Zutrittsprotokolle zu Serverräumen, Protokolle von Anmeldungen (Log-Ins) an Betriebsystemen, oder Webanwendungen, Protokolle von Eingaben („Wer hat wann welchen Datensatz angelegt?“) oder Aufzeichnungen von übermittelten Daten (etwa Durchschriften bzw. Kopien von Meldungen von Lohnunternehmen an Sozialversicherungen)

Aus technischer Sicht gibt es häufig Gemeinsamkeiten zwischen der Protokollierung und der Aufzeichnung: Indem bei der Änderung auch Zeitpunkt und vornehmenden Person aufgezeichnet werden, kann gleichzeitig eine aus datenschutzrechtlichen Gründen erforderliche Protokollierung erfolgen. Zu beachten sind aber unterschiedliche Zwecke und damit Umfänge, Zugriffsrechte und Aufbewahrungsdauern der Protokollierung bzw. Aufzeichnung.

GrundsätzeFür Protokolldaten gelten die Grundsätze der Erforderlichkeit (Art, Umfang und Dauer der Protokollierung sowie die Dauer der Aufbewahrung sind auf das nötige Maß zu beschränken), der Datensparsamkeit und Datenvermeidung (Anonymisieren und Pseudonymisieren von Protokolldaten, z. B. durch Hashverfahren) sowie der Zweckbindung (alleiniger Zweck: Aufrechterhaltung von Datenschutz und Datensicherheit, nicht: Leistungs- und Verhaltenskontrolle).

AnforderungenDer Zweck der Protokollierung besteht darin, ein Verfahren so transparent zu machen, dass die Ordnungsmäßigkeit bzw. ein Verstoß gegen die Ordnungsmäßigkeit einer Verarbeitung personenbezogener Daten nachweisbar ist. Im Ergebnis soll ein Protokoll die Beantwortung der Frage erlauben, ob und warum bestimmte Daten in einem Datenverarbeitungssystem vorhanden sind oder nicht bzw. wie sie verarbeitet wurden.

Die Protokolldaten müssen darüber Auskunft geben können, wer wann welche personenbezogenen Daten in welcher Weise verarbeitet hat. Dazu müssen sie vollständig sein, dürfen nachträglich nicht veränderbar sein und dürfen nur Berechtigten zugänglich sein.

Es kann zwischen der Protokollierung administrativer Tätigkeiten und der Protokollierung der

Verfahrensnutzung unterschieden werden: Administrative Tätigkeiten (u. a. Änderung an Hardware, Software, Zugriffsrechten, Konfiguration oder Speicherung sowie Erstellung / Wiedereinspielen von Datensicherungen) sind zu protokollieren, um die Systemsicherheit zu überwachen. Eine solche Protokollierung kann auch der Entlastung von Administratoren bei ungerechtfertigten Vorwürfen dienen.

Die Protokollierung der Verfahrensnutzung (Eingabe und Veränderung von Daten, ggf. auch Lesezugriffe und Abrufe) dient der Verfahrensüberwachung auf inhaltlicher Ebene.

KonzeptionBei der Konzeption eines Protokollierungsverfahrens sollte man sich an den üblichen Lebenszyklusmodellen orientieren. Typische Phasen sind:

- Erzeugen (Festlegung von Art und Umfang der Protokollierung),
- Übertragen (ggf. Sicherung von Übertragungen, falls externe Protokollierungssysteme wie zentrale Syslog-Server verwendet werden),
- Speichern (Festlegung, ob eine Sofortauswertung möglich ist oder eine Speicherung erfolgen soll; Zugriffsschutz und Backup für Kontrolldaten, Manipulationsschutz),
- Auswerten (Beachtung von Mitbestimmungsrechten, Erstellung typischer Auswertungsszenarien),
- Löschen (Festlegung von Aufbewahrungsfristen, rückstandsfreie Löschung).

Ein Beispiel ist folgendes stichpunktartiges Konzept für Protokollierungsverfahren für administrative Zugriffe auf Windows-Server (z.B. bei Lohnunternehmern, Maschinenherstellern, Beratern und ihren Dienstleistern):

- Erzeugen (Ausschnitt):
  Protokollierung von
  - An/Abmeldungen mit administrativen Nutzerkonten (einschließlich erfolgloser Versuche),
  - Änderungen an Benutzerberechtigungen (neue Nutzer),
  - manuelle lesenden und schreibenden Zugriffen auf Datenbanken auf Dateiebene,
- Übertragen: keine Übertragung; lokale Speicherung in den serverinternen Sicherheitslogs
- Speichern: Wöchentliche Kopie der Dateien der Sicherheitslog auf einen zentralen Server; Löschung der lokalen Sicherheitslogs; tägliche Bandsicherungen des zentralen Servers (Aufbewahrung 1 Monat);
- Auswerten:
  - automatisierte Auswertung der Sicherheitslogs auf erfolglose Login-Versuche, Anlegen neuer Benutzerkonten und lesende Zugriffe auf Datenbankdateien
  - Aufklärung unklarer Aktivitäten durch Vorgesetzte der Administratoren
  - manuelle Auswertung der Logdateien bei „Verdachtsmomenten“
- Löschen:
  - automatisierte Löschung nach 2 Jahren

Technisch-organisatorische Maßnahmen

Der Fokus der folgenden Darstellung von technisch-organisatorischen Maßnahmen in diesem Abschnitt liegt auf der Nutzung im Agrarbereich, um personenbezogene Daten zu schützen und einen Personenbezug zu entfernen oder zumindest zu erschweren, um den Anforderungen an Datensparsamkeit und Datenvermeidung zu genügen und um die Durchsetzung der Zweckbindungsgrundsatzes zu erleichtern. Einige der Maßnahmen (insbesondere Verschlüsselungsverfahren) sind auch geeignet, Betriebs- und Geschäftgeheimnisse zu schützen.

Schutz von personenbezogenen Daten und von Betriebs- und Geschäftsgeheimnisse durch Anonymisierung, Pseudonymisierung und Aggregation

Die Maßnahmen Anonymisierung, Pseudonymisierung und Aggregation wurden bisher mit dem Ziel beschreiben, einen Bezug zu natürlichen Personen zu entfernen bzw. deren Identifizierbarkeit zu verhindern oder zu erschweren. Gleiches ist natürlich auch mit identifizierenden Angaben zu Betrieben oder ganz allgemein juristischen Personen möglich, in dem man beispielsweise Betriebsnamen entfernt. Zu beachten ist aber dabei, dass identifizierende Informationen, etwa Betriebsnummer oder Steuernummern, leichter öffentlich verfügbar sind als identifizierende Nummern natürlicher Personen.

Im Hinblick auf Betriebs- und Geschäftsgeheimnisse ist zu unterscheiden, ob der Schutz des Inhabers im Vordergrund steht oder der Schutz eines Verfahrens. Beispielsweise ist der Wert „Bilanzsumme von 430.000 Euro“ für sich genommen wenig schützenswert, so lange der dazugehörige Betrieb nicht bekannt ist. Hier würden die oben beschriebenen Maßnahmen der Anonymisierung, Pseudonymisierung und Aggregation dazu dienen können, den Zusammenhang der Daten zum fraglichen Betrieb zu entfernen.

Steht hingegen der Schutz eines Verfahrens im Vordergrund, etwa vorteilhafte Düngemaßnahmen in Zusammenhang mit Bodenbeschaffenheit und örtlichem Klima (oder als Extrembeispiel eine Rezeptur wie diejenige für Coca-Cola), und der zugehörige Betrieb im Hintergrund, so genügt es nicht, identifizierende Daten zu entfernen. Vielmehr muss auf Ebene der Verfahrensdaten selbst eingegriffen werden und ein Informationsverlust, etwa durch Aggregation oder Ausblenden einzelner Datenfelder, erzeugt werden.

Denkbar sind hier beispielsweise die Bildung von Summen oder Durchschnittswerten, die Zusammenfassung von Werten in Gruppen (siehe Beispiels oben: Größe bewirtschafteter Flächen).

Vorverarbeitung - Bereits während der Datenerhebung ist es denkbar, nicht erforderliche Details aus Datenerhebungen zu aggregieren, etwa durch Aufsummieren und Durchschnittsbildung, oder diese Details vor abschließenden der Speicherung zu entfernen. Gleiches gilt für die Filterung von identifizierenden Daten (etwa Fahrer- oder Maschinen-ID), die in dem entsprechenden Datensatz nicht benötigt werden.

Diese Überlegungen sind dann relevant, wenn entsprechend der Kommunikationsbeziehungen mehrere Datensätze oder Datei für unterschiedliche Adressaten erstellt werden, die möglicherweise zum Zeitpunkt der Speicherung bereits verschlüsselt werden. So ist es denkbar, anstelle eines umfassenden Datensatzes mit allen Detailinformationen den Beteiligten spezifische Datensätze bereitzustellen: Im Datensatz für den Landwirt/Bewirtschafter wären beispielsweise Fahrer- und Maschinen-ID nicht erforderlich, im Datensatz für den Lohnunternehmer wären ortsbezogene Details zu Erntemengen oder Saat- bzw. Düngerausbringungen nicht erforderlich, sofern nicht mit dem Bewirtschafter anderes

vereinbart wurde.

Zusammenfassendes Beispiel - Betrachtet man Beispiele für ISOXML-Datensätze, so können in diesen zahlreiche personen- und betriebsbezogene Daten enthalten sein, etwa Namen von Fahrer und Kunden („Customer“, wahrscheinlich Auftraggeber) und zeitspezifische, geolokalisierte Sensordaten (z. B. Ausbringungs- oder Erntemengen mit Ortskoordinaten und Zeitstempeln).

Während die ort- und zeitspezifischen Sensordaten durch die Sensoren der Maschinen „erzeugt“ werden, dürften Fahrer – und Kundennamen manuell oder mittels einer Steuerdatei (z. B. Auftragsliste eines Lohnunternehmers) als Tasks in das maschinenspezifische System eingegeben werden, das dann die ISOXML-Dateien mit Task-spezifischen Sensordaten erzeugt. Hier besteht zunächst die Möglichkeit, bei der Beschreibung der Aufgaben/Aufträge in Tasks die Klartextnamen von Personen (Fahrer, Kunden) gar nicht erst zu erfassen, so dass diese nicht auf die Maschinen übertragen werden.

Sind in den durch die Maschine erzeugten Dateien (etwa im ISOXML-Format) jedoch personenbezogene Daten enthalten und sollen diese Dateien (oder Teile davon) an Dritte weitergegeben werden (etwa an die Landwirte oder von diesen beauftragte Berater, an Organisationen wie Landwirtschaftskammern oder –verbände für regionale statistische Auswertungen), so ist der Personenbezug zu entfernen.

Dies kann wie oben dargestellt durch Anonymisierung, Pseudonymisierung und Vorverarbeitung erfolgen.

Als Beispiel wird ein Datensatz betrachtet, der aus einer Aufzeichnung von Maschinendaten stammt, einen kompletten Arbeitsauftrag umfasst und folgende Daten enthält:

- Maschinen-ID
- Datum
- Uhrzeit Beginn der Arbeit
- Uhrzeit Ende der Arbeit
- Geokoordinaten des Schlages (Grenzen)
- Geokoordinaten der Zufahrt zu einem Schlages
- Schlag-ID (einer internen Schlag-Kartei eines Landwirts oder Lohnunternehmers)
- Auftraggeber-ID und Auftraggebername
- Fahrer-ID und Fahrername
- geolokalisierte Sensordaten (ausgebrachte Düngemittelmenge) inklusive Zeitstempel

Unmittelbar identifizierende personenbezogene Daten sind in diesem Datensatz durch die Namen des Fahrers und des Auftraggebers enthalten. Diese sollten vor der Weitergabe an Dritte (etwa Berater von Landwirten) gelöscht werden.

Danach sind unmittelbar identifizierende Daten nicht mehr vorhanden – es bedürfte Zusatzinformationen, um diesen Datenbestand einer Person zuordnen zu können, etwa einer Liste „Fahrer-ID – Fahrername“, einer Schlagkartei mit Geokoordinaten oder einer Karte und des Wissens um Eigentumsverhältnisse, etwa im Kataster.

Die Entfernung eines direkten Personenbezugs im Hinblick auf den Fahrer ist durch Löschen der Fahrer-ID im Datensatz vergleichsweise einfach möglich. Dennoch ließe der restliche Datensatz in Zusammenhang mit einem Dienst- bzw. Einsatzplan bei einem Lohnunternehmer (Zuordnung Fahrer-Tag-Maschine) zum Beispiel zu, aus den zeit- und ortsabhängigen Sensordaten Rückschlüsse auf das Pausenverhalten des Fahrers oder auf eine Maschinenstillstand zu ziehen – auch noch nach Jahren. Solche Rückschlüsse sollten – wenn überhaupt – nur dem Betreiber der Maschine (Lohnunternehmer oder Eigentümer) möglich sein.

Um dies zu entschärfen, sollten Details entfernt werden, wenn sie für den Empfänger nicht erforderlich sind. So dürfte für eine statistische Auswertung von Maschinenflotten oder regionalen Saat-, Dünge oder Erntemengen kumulierte Zeitangaben, Strecken, Flächen oder Mengen ausreichend sein, die sich durch den Einsatz entsprechender Filter aus den Maschinendaten errechnen lassen.

Die Entfernung des Personenbezugs im Hinblick auf den Bewirtschafter bzw. Eigentümer kann nur gelingen, in dem die Geokoordinaten des Schlages (Grenzen, Anfahrten) und die Schlag-ID sowie die Geokoordinaten der zeit- und ortsabhängigen Sensordaten entfernt werden oder die Geokoordinaten so verändert werden, dass sich nicht mehr einzelne Schläge identifizieren lassen. Denkbar ist hier das Abschneiden von Nachkommastellen oder Normieren, indem die Koordinaten mehrere vergleichbarer Datensätze unterschiedlicher Schläge durch identische Koordinaten ersetzt werden („Dorfmittelpunkt“). Auf diese Weise wären regionale, aber nicht mehr schlaggenaue Informationen verfügbar.

Verschlüsselung

Eine gesetzliche Definition des Begriffs Verschlüsselung gibt es im Bundesdatenschutzgesetz nicht. Die Definitionen des Landesdatenschutzgesetzes Schleswig-Holstein lautet „Verschlüsseln das Verändern personenbezogener Daten derart, dass ohne Nutzung des Geheimnisses die Kenntnisnahme vom Inhalt der Daten nicht oder nur mit einem unverhältnismäßigen Aufwand möglich ist.“ (§ 2 Abs 1 Nr. 8). Die Definition lässt sich auf alle Arten von Daten erweitern. Die Geheimhaltung des (Entschlüsselungs-)Schlüssels, des „Geheimnis’“, bewirkt den Schutz der Informationen - ohne Kenntnis dieses Schlüssels ist kein Zugriff möglich.

Symmetrische Verschlüsselung

Symmetrische Verschlüsselungsverfahren nutzen für die Ver- und Entschlüsselung den gleichen Schlüssel. Moderne symmetrische Verschlüsselungsverfahren sind schnell und gelten (eine ausreichende Schlüssellänge vorausgesetzt) als sicher. Das bekannteste Beispiel ist der Algorithmus AES (Advanced Encryption Standard); empfohlene Schlüssellängen liegen bei 256 bit. Da für Ver- und Entschlüsselung der gleiche Schlüssel verwendet wird, muss zum Zeitpunkt des Verschlüsselns der Entschlüsselungsschlüssel bekannt sein.

Da von seinem Schutz der Schutz der verschlüsselten Daten abhängt, ist der Schlüssel geheim zu halten und zu transportieren. Dies hat zur Folge, dass er sicher zu speichern ist (etwa in Geräten) oder von Hand einzutragen ist (etwa als Passwort, aus dem er dann generiert wird) – sowohl bei der Verschlüsselung als auch bei der Entschlüsselung.

Weiter ist zwischen jedem Kommunikationspartner ein eigener Schlüssel zu vereinbaren, d.h. ein Schlüssel pro Kommunikationsbeziehung. Bezogen auf die Tätigkeit von mehreren Lohnunternehmern für einen Bewirtschafter bedeutet dies, dass pro Lohnunternehmer ein eigener Schlüssel mit dem

Bewirtschafter zu vereinbar ist.

Eine symmetrische Verschlüsselung kann zumindest in einem gewissen Maße zum Integritätsschutz von Nachrichten oder Daten verwendet werden: Einfache Manipulationen Unbefugter (d.h. von Personen, die sich nicht im Besitz des Schlüssels befinden) an verschlüsselten Daten lassen sich erkennen, denn durch die Manipulation wird die Struktur der verschlüsselten Daten verändert und eine Entschlüsselung ist nicht mehr möglich. Komplexe Manipulationen an verschlüsselten Daten, die den Inhalt der unverschlüsselten Daten manipulieren, sind nach heutigem Kenntnisstand bei modernen Verfahren ohne Kenntnis des Schlüssels nicht möglich. Der Empfänger verschlüsselter Daten kann sich daher relativ sicher sei, dass die entschlüsselten Daten diejenigen sind, die vom Absender verschlüsselt wurden, und auch tatsächlich vom Absender versandt wurden. Einen (gerichtsfesten) Nachweis kann er damit aber nicht führen, denn für eine vermeintliche Manipulation kommen als Urheber alle diejenigen infrage, die Zugang zum Schlüssel haben, mindestens Empfänger und Absender – folglich könnte ein Empfänger auch eigenständig Nachrichten manipulieren.

Asymmetrische Verschlüsselung

Asymmetrische Verschlüsselungsverfahren nutzen zwei verschiedene Schlüssel für Ver- und Entschlüsselung. Am häufigsten werden Public-Key-Verfahren verwendet, bei denen Schlüsselpaare bestehend aus Verschlüsselungsschlüssel und Entschlüsselungsschlüssel verwendet werden. Der Verschlüsselungsschlüssel erlaubt dabei keinen Zugriff auf verschlüsselte Daten und kann öffentlich bekannt sein kann. Er kann daher auch in Geräten ohne besonderen Zugriffsschutz für Lesezugriffe gespeichert werden. Gegen schreibende Zugriffe ist er zu schützen, da er andernfalls mutwillig gelöscht werden kann oder manipuliert werden kann (Ersetzung des Verschlüsselungsschlüssels durch ein Exemplar aus einem Schlüsselpaar, das dem Angreifer bekannt ist). Andernfalls ist auf andere Weise sicherzustellen, dass der öffentliche Schlüssel eines Empfängers tatsächlich zu dem Empfänger gehört, etwa mit Hilfe von Zertifikaten, die die Echtheit eines öffentlichen Schlüssels und die Identitätsdaten des Schlüsselinhabers bestätigen. Diese Verfahren sind bei Webservern weit verbreitet, müssten aber für Verschlüsselungsverfahren in Geräten (etwa in Landmaschinen) noch implementiert bzw. angepasst werden.

Der Entschlüsselungsschlüssel schützt wie symmetrischen Verfahren die verschlüsselten Daten und ist geheim zu halten.

Ein Vorteil beim Einsatz von Public-Key-Verfahren liegt darin, dass ein Schlüssel pro Kommunikationspartner benötigt wird – unabhängig davon, mit wie vielen Partnern kommuniziert wird. Bezogen auf die Tätigkeit von mehreren Lohnunternehmern für eine Bewirtschafter bedeutet dies, dass bei einer Einweg-Kommunikation von den Lohnunternehmern zum Bewirtschafter (etwa Daten über Erträge oder Düngemitteleinsatz) ein Schlüsselpaar für den Bewirtschafter ausreichend ist: alle Lohnunternehmen können den gleichen öffentlichen Schlüssel des dem Bewirtschafters verwenden, um Daten zu ihm senden zu können.

Eine asymmetrische Verschlüsselung kann ebenfalls in einem gewissen Maße zum Integritätsschutz von Nachrichten oder Daten verwendet werden: Einfache Manipulationen Unbefugter (d.h. von Personen, die keine Schlüssel verwenden) an verschlüsselten Daten lassen sich erkennen, denn durch die Manipulation wird die Struktur der verschlüsselten Daten verändert und eine Entschlüsselung ist nicht mehr möglich. Komplexe Manipulationen an verschlüsselten Daten, die sinnvoll den Inhalt der unverschlüsselten Daten manipulieren, sind nach heutigem Kenntnisstand bei modernen Verfahren

ohne Kenntnis des Entschlüsselungsschlüssels nicht möglich.

Es wäre aber für einen Angreifer möglich, eine korrekt verschlüsselte Nachricht zu erzeugen und dem Empfänger zuzuspielen, denn der zur Verschlüsselung verwendete Schlüssel ist öffentlich. Der Empfänger kann dies nicht feststellen, denn als Absender einer verschlüsselten Nachricht kommen wegen der Öffentlichkeit des Verschlüsselungsschlüssels eine Vielzahl von Personen infrage. Verfügt der Angreifer über den Entschlüsselungsschlüssel, so kann er Nachrichten bzw. Daten gezielt manipulieren, indem er sie zunächst entschlüsselt, an spezifischer Stelle eine Manipulation vornimmt (etwa Ertragsdaten ändert) und die manipulierten Daten mit dem öffentlichen Schlüssel erneut verschlüsselt. Auch dies kann der Empfänger nicht feststellen.

Daher verwenden viele asymmetrische Verfahren Signaturalgorithmen zum Integritätsschutz der Daten.

Einsatzszenarien und Schlüsselverwaltung

Für Verschlüsselungsverfahren gibt es mehrere Einsatzszenarien bei der Datenverarbeitung im **Agrarbereich**. Diese können die Vertraulichkeit von (personenbezogenen) Daten sowie in Teilen deren Integrität schützen.

Webbasierte Anwendungen

Für webbasierte Anwendungen kommen für verschlüsselte Datenübertragung Standard-Verschlüsselungsverfahren wie SSL/TLS (Secure Sockets Layer/Transport Layer Security) infrage. Sie implementierten mit Hilfe einer asymmetrischen Verschlüsselung eine Transportverschlüsselung für eine Kommunikation zwischen einem Browser und einem Webserver – unabhängig davon, welche Person den Browser nutzt bzw. an welche Datenverarbeitungssysteme die Informationen des Webservers weitergeleitet werden. Standardmäßig verwenden Webserver sogenannte Server-Zertifikate, die die Zugehörigkeit des Webserverschlüssels zum Servernamen bestätigen. Ein Nutzer kann sich also sicher sein, dass sein Browser mit dem „richtigen“ Webserver kommuniziert.

Mit Hilfe eines Server-Zertifikates ist es aber einem Webserver nicht möglich, die Identität eines Nutzers bzw. Browsers zu überprüfen. Hierzu muss eine entsprechende webbasierte Anwendung Nutzerkonto und Passwort abfragen (d.h. Authentisierung innerhalb der Anwendung). Alternativ können den Nutzern sogenannte Client-Zertifikate ausgestellt werden. Diese werden in einem speziellen Speicherbereich des Browsers gespeichert und beim Verbindungsaufbau zwischen Nutzerbrowser und Webserver an den Webserver übertragen. Auf diese Weise kann der Webserver verschiedene Clients unterscheiden und mit ihnen gesichert kommunizieren. Ein solches Vorgehen ist sinnvoll für die Verschlüsselung einer Maschine-zu-Maschine-Kommunikation, etwa um eine Kommunikation zwischen dem einem Server (etwa im bei einem Lohnunternehmer) und einer externen Datensicherung (bei einem Dienstleister) abzusichern.

Soll hingegen die Identität von menschlichen Nutzern gesichert werden, so wäre ein Client-Zertifikat nicht ausreichend, um unterschiedliche Nutzer eines Computers bzw. Browsers (etwa verschiedene Bearbeiter) sicher auseinander halten zu können. Hier sollten in jedem Fall Nutzernamen und Passworte verwendet werden. Dies ist auch erforderlich, da an die Nutzer unterschiedliche Zugriffsrechte an Daten geknüpft sein können.

Verschlüsselte Datenspeicherung in Endgeräten

Eine verschlüsselte Datenspeicherung in Endgeräten (etwa USB-Speichersticks, Tablets, Notebooks, USB-Festplatten, Speichermedien in Landmaschinen) verfolgt den Zweck, Information auch dann zu schützen, wenn ein unbefugter Zugriff auf den Datenträger im Endgerät nicht ausgeschlossen werden kann (z. B. Diebstahl, Verlieren, Liegenlassen): In diesem Fall könnten die Datenträger ausgebaut und direkt ausgelesen werden – Zugriffsschutzmechanismen wie Log-Ins, Passwörter oder auch Schlüsselschalter würden umgangen werden.

Um Daten ver- und entschlüsseln zu können, ist die Verwaltung von Schlüsseln notwendig. Diese werden häufig aus einem Passwort abgeleitet, das beim Start des Geräts einzugeben ist. Denkbar ist aber auch, Schlüssel auf SmartCards o.ä. zu speichern, die vor Benutzung einzulegen sind.

In beiden Fällen führt ein Verlust des Schlüssels (z.B. Passwort vergessen, SmartCard verloren oder unbrauchbar) zu einem Verfügbarkeitsverlust der gespeicherten Daten, so dass stets Alternativverfahren wie z. B. eine Hinterlegung des Passwortes, ein zweiter verschlüsselter Zugang (etwa für einen Administrator) oder Schlüsselkopien (etwa auf einer zweiten SmartCard) bedacht werden müssen. Ein solcher „Zweitschlüssel“ ist sorgfältig zu verwahren, denn andernfalls eröffnet er unbefugte Zugriffe.

Schlüsselmanagement

Ein typisches Einsatzszenario ist, dass ein Dienstleister für mehrere Kunden/Mandanten tätig ist und die jeweiligen Datenbestände verschlüsselt. Dabei sollten kundenindividuelle Schlüssel zum Einsatz kommen. Spätestens bei einer Verschlüsselung für die Kommunikation vom Dienstleister zu den Kunden sind kundenindividuelle Schlüssel erforderlich.

In der Praxis sind einfache Verfahren zur Auswahl des richtigen Kundenschlüssels erforderlich.

E-Mail

Handels es sich um E-Mailbasierte Kommunikation, so kommen zertifikatsbasierte asymmetrische Verschlüsselungsverfahren zum Einsatz. Hier sind vielfach die E-Mail-Clients in der Lage, passend zum Empfänger der Nachricht der richtigen Schlüssel zu wählen. Diese Verfahren sind zwar technisch ausgereift und werden im B2B (Business-to-Business)-Umfeld eingesetzt, haben sich aber in Bezug auf Endnutzer (noch) nicht durchgesetzt: Die Integration ist abhängig vom verwendeten E-Mail-Client (Outlook, Thunderbird, Webmail-Clients, et.) der Nutzer, die sehr vielfältig sein können. Für den **Agrarbereich** bedeutet dies, dass eine E-Mailverschlüsselung für die Kommunikation zu Beratern und Landwirten angeboten werden sollte, aber realistischerweise nicht erzwungen werden kann. Realistisch ist es aber, größere Dateien, die als Anhang an E-Mail ausgetauscht werden, mit Hilfe von Passwörtern zu verschlüsselt. An dieser Stelle dürfte der Inhalt der Anhänge (etwa Rechnungen, Ertragskarten, Erntemengen etc.) eine höhere Sensibilität als der Text der E-Mail haben. Dateien können manuell durch die Eingabe eines Passwortes (symmetrisch) verschlüsselt werden; der Empfänger nutzt das gleiche Programm und das gleiche Kennwort zur Entschlüsselung. Mit dem Programm 7zip steht ein kostenfreies Programm für verschiedene Betriebssysteme (Windows, Linux) zur Verfügung, das sich in die Betriebssystemstruktur einfach integrieren und einfach bedienen lässt (ähnlich wie die Windows-interne ZIP-Komprimierung von Dateien und Ordnern), den Verschlüsselungsstandard AES-256bit (Advanced Encryption Standard) unterstützt und auch einen Batchbetrieb für automatisierte Verschlüsselung und Versand zulässt.

Verschlüsselung bei Erhebung in Maschinen

Denkbar ist auch , dass Datenbestände direkt nach der Erhebung empfängerindividuell aufbereitet, verschlüsselt, gespeichert und bereitgestellt werden, etwa (ortbezogene) Details zu Erntemenge /Düngerausbringung verschlüsselt für den Bewirtschafter, Details der Auftragsbearbeitung (Maschinen- und FahrerID, Wegezeiten) für den Lohnunternehmer, maschinenspezifische Daten (Laufzeiten, Verschließparameter) für den Maschineneigentümer.

Während sich der Maschineneigentümer und der Lohnunternehmer in Bezug auf eine eingesetzte Maschine relativ selten ändern dürfte (mit der Konsequenz, dass eine manuelle Eingabe oder Auswahl eines maschinen- oder lohnunternehmerindividuellen Schlüssels eher selten vorkommt und damit eine realistische Möglichkeit ist), so dürfte für den Bediener/Fahrer einer Maschine eine manuelle Auswahl/Eingabe des „richtigen“ Schlüssels vor Arbeitsbeginn auf einem Schlag eher unrealistisch sein.

Zur Lösung sind mehrere Szenarien denkbar: Zum einen eine auftragsbezogene Schlüsselverwaltung, bei der die zu verwendenden Schlüssel zusammen mit einem „Arbeitsauftrag“ verwaltet wird. Startet oder quittiert der Fahrer einen solchen Auftrag (etwa bei Befahren eines Schlages zu Beginn der Bearbeitung), so könnte entsprechendes Schlüsselmaterial automatisiert zum Einsatz kommen. Voraussetzung dafür wäre, dass die Schlüssel zusammen mit den Aufträgen verwaltet und auf die Maschinen übertragen werden. Dies dürfte vorwiegend eine Aufgabe der Lohnunternehmer sein, die die Aufträge erstellen. Kurzfristige Auftragsänderungen bzw. Umdispositionen „auf Zuruf“, etwa per Telefonanruf, würden das Schlüsselmanagement erschweren.

Denkbar ist auch, georeferenzierte Schlüssel zu verwenden, um den Fahrer von manuellen Eingaben zu entlasten. Hierbei wäre die Verwendung eines Schlüssels abhängig vom Aufenthaltsort einer Maschine und würde von Schlag zu Schlag wechseln. Sinn würde dies machen für die Verschlüsselung von Daten für den Bewirtschafter oder Eigentümer einer Fläche. Auch hier müsste das Schlüsselmaterial in geeigneter Form auf die Maschinen übertragen werden. Dies könnte, neben einer auftragsbasierten Schlüsselverwaltung (siehe Vorabsatz) auch per Abruf (etwa GSM- oder UMTS-basiert) auf Basis der Schlag-Koordinaten geschehen, die zur „Identifizierung“ der Schlüssel unabhängig von einzelnen Lohnunternehmern verwendet werden. In Randbereichen von Schlägen wäre darauf zu achten, nicht aufgrund von GPS-Messfehlern unbeabsichtigt Schlüssel zu wechseln und Schlüssel, die benachbarten Schlägen zugeordnet sind, zu verwenden.

In beiden Fällen sollten asymmetrische Verfahren zum Einsatz kommen, damit bei der Verschlüsselung (anders als bei symmetrischen Verfahren) nicht auf die Vertraulichkeit des Schlüssels zu achten wäre. Die öffentlichen Schlüssel könnten auch zentral verwaltet und zum Abruf für Lohnunternehmer oder Maschinen(betreiber) bereitgestellt werden, etwa durch Verbände. Zur Identifizierung der Schlüssel könnten man an Namen, aber auch an Betriebsnummern oder Geokoordinaten denken. Letztes hätte allerdings zu Folge, dass Bewirtschafter, Pächter- und/oder Eigentümerwechsel einzelner Parzellen bei der Schlüsselverwaltung nachgezogen werden müssen.

Grenzen der Verschlüsselung

In allen Fällen liegen vor der Verschlüsselung von Daten diese Daten in unverschlüsselter Form vor und könnten unberechtigt kopiert werden. Will man dies verhindern, so wäre die Erhebung von Daten (etwa flächenspezifische Ertrags- oder Ausbringungsdaten oder maschinenspezifische Daten bei der Nutzung einer Maschine) zusammen mit einer unmittelbaren Verschlüsselung so zu kapseln, dass der Anwender keinen Zugang zu unverschlüsselten Daten hat.

Dies ist im Bereich der Maschinendaten zumindest für einige Datentypen denkbar, nicht hingegen im Bereich der Verwaltung von Daten und Aufträgen durch menschliche Bearbeiter: Diese könnten – vorsätzlich – vor der Verschlüsselung eine Kopie der Daten erzeugen und missbräuchlich verwenden. Ebenso wäre als Manipulationsszenario für Maschinendaten denkbar, in den Maschinen Daten von Sensoren (etwa laufende Erntemenge, Geschwindigkeit, etc.) bereits vor der Verschlüsselung „abzugreifen“ (Kopie der elektrischen Signale) und eigenständig zu speichern. Kommen „verschlüsselnde Sensoren“ zum Einsatz, so könnten durch einen böswilligen Maschinenbetreiber zusätzliche Sensoren für eigene Datenerhebungen verbaut werden.

In beiden Fällen bleibt als Resümee, dass eine Verschlüsselung vor Dritten schützt, nicht aber vor zweckfremder Nutzung durch Berechtigte.

Vertragsverhältnisse

Funktionsübertragung

Bei der Funktionsübertragung werden personenbezogene Daten an einen Dritten zur eigenverantwortlichen Datenverarbeitung übermittelt. Der Dienstleister wird dann selbst zur verantwortlichen datenverarbeitenden Stelle. Eine solche Übermittlung von Daten bedarf einer Rechtsgrundlage oder der Einwilligung des Betroffenen (vgl. § 4 Abs. 1 BDSG).

Auftragsdatenverarbeitung

Im Gegensatz zur Funktionsübertragung bietet die Auftragsdatenverarbeitung die Möglichkeit, externe Dienstleister in die Datenverarbeitung einzubinden, ohne dass hierbei eine Datenübermittlung im Sinne des § 3 Abs. 4 Nr. 3 BDSG vorliegt. Nach § 3 Abs. 8 Satz 3 BDSG sind bei einer Auftragsdatenverarbeitung die Auftragnehmer keine Dritten. Vielmehr werden sie behandelt, als wären sie Teil der datenverarbeitenden Stelle, die den Auftrag erteilt. Notwendig ist hierfür jedoch, dass der Auftragnehmer sorgfältig ausgewählt wird. Außerdem muss nach § 11 Abs. 2 BDSG eine schriftliche Vereinbarung getroffen werden, die folgende Punkt enthält:

- der Gegenstand und die Dauer des Auftrags,
- der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten, die Art der Daten und der Kreis der Betroffenen,
- die nach § 9 zu treffenden technischen und organisatorischen Maßnahmen,
- die Berichtigung, Löschung und Sperrung von Daten,
- die nach Absatz 4 bestehenden Pflichten des Auftragnehmers, insbesondere die von ihm vorzunehmenden Kontrollen,
- die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen,
- die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers,
- mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen,

- der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält,
- die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Wichtig ist insbesondere, dass der Auftragnehmer kein Eigeninteresse an den Daten haben darf und den Weisungen des Auftraggebers strikt folgt. Der Auftraggeber hat sich des Weiteren vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen (vgl. § 11 Abs. 2 Satz 4 BDSG).

Im **Agrarbereich** kann an verschiedenen Stellen eine Auftragsdatenverarbeitung vorkommen. So kann dieses der Fall sein, wenn Lohnunternehmer Unterauftragnehmern beschäftigen. Auch können Abrechnungsverfahren ausgelagert werden. Aber auch die Beauftragung von Serverdiensten oder gar Cloud-Anbietern kann eine Auftragsdatenverarbeitung darstellen, die die o. g. Anforderungen erfüllen muss. Und schließlich unterfallen auch die Prüfung oder Wartung automatisierter Verfahren oder von Datenverarbeitungsanlagen durch externe Stellen dem Recht der Auftragsdatenverarbeitung entsprechend (vgl. § 11 Abs. 5 BDSG).

Verhältnis Verpächter – Pächter

Hat ein Pächter landwirtschaftliche Nutzflächen von einem Verpächter gepachtet, dann ist in der Regel der Pächter der Auftraggeber gegenüber dem Lohnunternehmer. Der oben beschriebene Schutz der personenbezogenen Daten bezieht sich dann vor allem auf den Pächter. Aber auch personenbezogene Daten des Verpächters können relevant sein. Der Pächter darf die Daten des Verpächters nur weitergeben, wenn dieses für die Tätigkeiten im Rahmen des Pachtvertrages (z. B. Bewirtschaftung des Betriebs, Angaben gegenüber Behörden etc.) erforderlich ist. Ist die Weitergabe nicht durch den Pachtvertrag bzw. das Pachtverhältnis gedeckt und dient sie auch nicht zur Wahrung berechtigter Interessen des Verpächters, dann ist die Einwilligung des Verpächters für die Weitergab der Daten einzuholen.

Ein Lohnunternehmer ist in der Regel genauso wenig berechtigt, Daten des Verpächters für spätere weitere Aufträge aufzubewahren, wie er diese vom Pächter (Auftraggeber) vorhalten darf. Dies betrifft auch die Beschaffenheit des Betriebs bzw. der landwirtschaftlichen Fläche.

Allerdings hat der Verpächter in der Regel spätestens zum Ende der Pacht hin ein Auskunftsrecht gegenüber dem Pächter hinsichtlich der Daten, die für seine weitergehende Nutzung des Grundstücks relevant sind (z. B. Düngemittelnutzung, Fruchtfolgen etc.). Dies sollte sich möglichst schon aus dem Pachtvertrag ergeben. Ist dort keine Regelung getroffen, dann handelt es sich um eine Nebenpflicht des Pächters, damit der Verpächter seine rechtlichen Verpflichtungen zur Dokumentation erfüllen kann und er überhaupt in die Lage versetzt wird, das Pachtgrundstück weiterzuverpachten oder selber effektiv zu nutzen.

Sonderproblem Cloud-Computing

Das sog. „Cloud-Computing“ bezeichnet die verteilte Datenverarbeitung vernetzten Rechnern. Hierbei gibt es sehr unterschiedliche Ausprägungen der „Cloud“, die Auswirkungen auf die rechtlichen Grundlagen haben.

Nutzt im Rahmen der Datenverarbeitung in der Landwirtschaft einer der beteiligten Stellen einen

Cloud-Anbieter für Speicherung und Verarbeitung von personenbezogenen Daten, dann handelt es sich hierbei in der Regel um eine Auftragsdatenverarbeitung im Sinne des § 11 BDSG. Das bedeutet, dass mit dem Cloud-Anbieter ein Vertrag geschlossen werden muss, der den Anforderungen des § 11 Abs. 2 BDSG entspricht. An unproblematischsten dürfte dieses sein, wenn es sich um einen Anbieter innerhalb des Europäischen Wirtschaftsraums (EWR) handelt, der selber die Server betreibt. Rechtlich ergeben sich dann praktisch keine Unterschiede zu einem Anbieter, der seinen Auftraggebern geschlossene Systeme zur Verfügung stellt. Allerdings sind besondere Sicherheitsvorkehrungen zu treffen, so dass ausgeschlossen ist, dass unterschiedliche Mandanten des Cloud-Anbieters auf Accounts bzw. Speicherbereiche von anderen Kunden zugreifen können.

Der Auftraggeber ist verpflichtet, den Dienstleister sorgfältig auszuwählen. Neben Verfügbarkeit, Vertraulichkeit und Integrität muss die Umsetzung der Datenschutz-Schutzziele Transparenz, Intervenierbarkeit und Nicht-Verkettbarkeit nachgewiesen und kontrolliert werden.

Besondere Probleme ergeben sich beim Cloud-Computing, wenn verschiedene Anbieter zusammenarbeiten und auch über Ländergrenzen hinweg die Daten verarbeitet werden. Es muss gewährleistet werden, dass der Auftraggeber weiterhin die Kontrolle darüber hat, wie wo und von wem die personenbezogenen Daten verarbeitet werden. Dazu gehört, dass er im Rahmen des Auftragsdatenverarbeitungsvertrags i. S. d. § 11 Abs. 2 BDSG auch über Unterauftragnehmer seines Vertragspartners informiert wird. Er muss stets die Möglichkeit haben, die weitere Verarbeitung zu steuern bzw. auch zu unterbinden und die Daten restlos zu löschen. Die Übermittlung personenbezogener Daten in unsichere Drittstaaten außerhalb des EWR ist nur unter bestimmten Voraussetzungen zulässig. Diese können bei einer Verwendung sogenannter Standardvertragsklauseln oder verbindlicher Unternehmensregelungen erfüllt sein. Bei einer Datenübermittlung in die USA kann sich die verantwortliche Stelle grundsätzlich nicht allein auf eine Selbstzertifizierung nach den Safe-Harbor Prinzipien verlassen. Notwendig ist, dass der Auftraggeber die Zertifizierung und die Einhaltung der Prinzipien selbst überprüfen muss.

An diesen Grundsätzen ändert sich auch nichts, wenn es sich bei dem Auftraggeber etwa um ein kleines Unternehmen (z. B. Lohnunternehmer) handelt und der Cloud-Anbieter ein multinationaler Konzern ist. Auch hier müssen die o. g. Voraussetzungen erfüllt werden und u. a. das Weisungsrecht des Auftraggebers bestehen. Wie bei der Auftragsdatenverarbeitung beschrieben, ist der Auftragnehmer (hier der Cloud-Anbieter) dazu verpflichtet, die Daten nur im Rahmen des Auftrags zu nutzen. Eigene darüber hinausgehende Datenverarbeitungsvorgänge sind unzulässig. So wäre es unzulässig, Daten verschiedener Kunden miteinander zu verbinden, um hieraus eigene Erkenntnis zu erzielen. Vielmehr ist die Datentrennung zwischen verschiedenen Kunden zu gewährleisten.

Die Europäische Artikel 29-Datenschutzgruppe hat zu den besonderen Problemen beim Cloud-Computing eine Stellungnahme abgegeben, die auch die Voraussetzungen für deren Einsatz ausführlich beschreibt: http://ec.europa.eu/justice/data-protection/article-29/documentation/opinion-recommendation/files/2012/wp196_en.pdf.

Die Datenschutzbeauftragten von Bund und Ländern haben zum Cloud-Computing eine Orientierungshilfe veröffentlicht: http://www.datenschutz.hessen.de/download.php?download_ID=237.

4 Beispielszenarien

Im nächsten Abschnitt soll an beispielhaften Szenarien des Pflanzenbaus vorgestellt werden, an welchen Stellen zwischen verschiedenen Akteuren Geodaten ausgetauscht werden und welchem Zweck dieser Austausch dienen soll. Dabei wird sowohl auf die Sensibilität der Daten aus Perspektive der Landwirte eingegangen als auch auf welche kritischen Aspekte beim Datentransfer eingegangen werden muss.

Vor der Darstellung der einzelnen Szenarien wird auf die Rolle und Interessen der verschiedenen Akteure hinsichtlich der Geodaten eingegangen. Die Rollendarstellungen sind ergänzend zu den im iGreen-Deliverable 6.1, Kapitel 2, Abschnitt 2 zu sehen.

Gesondert wird in den Szenarien auf das Risiko im Umgang mit unverschlüsselten Daten hingewiesen.

Begriffe

- **Applikationskarte** - Karte der zu behandelnden Flache mit der positionsspezifischen Angabe der Mittelmenge
- **As applied Karte** - Karte, die die tatsächlich ausgebrachte Menge positionsspezifisch zeigt

Rollen und Ansprüche auf Daten

Landwirt - Ist für die Bewirtschaftung einer Fläche verantwortlich und entscheidet, welche Maßnahmen wann und in welcher Form auf dieser Fläche durchgeführt werden. Aus dieser Verantwortlichkeit ergibt sich sein Anspruch auf sämtliche an seine Fläche geknüpften Bewirtschaftungsdaten (insbesondere die Arbeitsdokumentation), die dem betriebseigenen Wissen zuzurechnen und damit vor der Einsichtnahme Dritter zu schützen ist.

In Einzelfällen muss er das Einverständnis des Grundstückseigentümers für die Aufzeichnung von Geodaten einholen, z.B. falls sich aus der Dokumentation Erkenntnisse ableiten lassen, die den Wert des Grundstücks beeinflussen. Hier wäre die einschlägige Rechtsprechung zu prüfen, in welchen Fällen dies der Fall ist.

Beratung - Unterstützt den Landwirt bei der Bewirtschaftung seiner Flächen durch die Interpretation bisheriger flächenbezogener Arbeitsdokumentationen (insbesondere die Auswertung von Ertragskarten) sowie Bereitstellung flächenbezogener Ausbringempfehlungen in Form von Applikationskarten insb. für Düngung und Pflanzenschutz. Zur Durchführung des Arbeitsauftrages hat die Offizialberatung Zugriff auf amtliche Geodaten, die zur Auswertung von Ertragskarten bzw. der Erstellung von Applikationskarten hinzugezogen werden können.

Die Daten des Landwirts, die seitens der Beratung zur Durchführung des Beratungsauftrages benötigt werden, dürfen von dieser während der Dauer der Erstellung der Beratungsleistung verwendet werden. Sollen die Daten darüber hinaus bei der Beratung verbleiben bzw. von dieser eine Verwendung für andere Zwecke beabsichtigt sein, sind dafür zwischen Landwirt und Beratung gesonderte Vereinbarungen zu treffen.

Lohnunternehmer - Unterstützt den Landwirt bei der Durchführung flächenbezogener Maßnahmen

mit eigenen geeigneten Maschinen. Zur Planung und Steuerung dieser Maßnahmen erhält er vom Landwirt ausgewählte Geodaten (Flächenkoordinaten / Vektordaten), anlassbezogen auch abzuarbeitende Applikationskarten.

Grundsätzlich darf er nicht ohne Zustimmung des Landwirts Geodaten der von ihm bearbeiteten Schläge erheben, bzw. auf Schlägen des Landwirts erhobene Daten müssten im gleichen Moment verschlüsselt werden und dürfen nur vom Landwirt oder in dessen explizitem Auftrag entschlüsselt werden.

> Im Rahmen der Arbeitsdokumentation werden von den Maschinen des Lohnunternehmers flächenbezogene Daten aufgezeichnet (as-applied-Karten bzw. Ertragskarten). Hier haben sowohl Lohnunternehmer als auch Landwirte Interesse, die für ihre jeweiligen Geschäftsprozesse relevanten Daten zu erhalten (s.A.: „Wem gehören die Geodaten?“ – Zeitschrift „Lohnunternehmen“ 1/2010, S. 6; Kopie erhältlich bei BLU oder DLR-RNH).

Fahrer - Führt an Lohnunternehmer statt pflanzenbauliche Maßnahmen für den Landwirt entsprechend der durch den Lohnunternehmer an ihn vergebenen Aufträge durch. Er hat keinerlei Anspruch an Geodaten des Landwirts. Er überwacht jedoch die Arbeitsdokumentation und ist für deren sichere Verwahrung verantwortlich.

Landtechnik - Die Landtechnik dient zur Umsetzung geodatenreferenzierter Aufträge bzw. erfasst Geodaten im Rahmen der Arbeitsdokumentation. Der Hersteller dieser Technik verbürgt sich, dass eine Steuerung der Landtechnik über Geodaten funktioniert, hat jedoch selbst keinerlei Rechte an den Geodaten, die auf die Maschine bzw. von der Maschine herunter transferiert werden.

Rahmenbedingungen

Für die betrachteten Szenarien wird unterstellt, dass alle Daten in einem elektronischen Format vorliegen. Den jeweiligen Teilnehmern stehen unterschiedliche Datenverarbeitungseinrichtungen zur Verfügung. Dies sind einzelne oder vernetzte Computer oder mobile Endgeräte. Es kann jedoch davon ausgegangen werden, dass jeweils lokale Speichermöglichkeiten gegeben sind und auch genutzt werden. Der Austausch kann über unterschiedlichste Medien erfolgen.

Konkrete Szenarien

1 Szenario „Ernte und Düngung“

Im Folgenden wird das Szenario „Ernte und Düngung“ beschrieben.

1.1 Auftragsausschreibung „Ernte“

Teilnehmer: Landwirt , Lohnunternehmer

Vorgang: Der LW fragt bei mehreren Lohnunternehmern die durchzuführende Maßnahme „Ernte“ an.

Ausgetauschte Daten:

LW->LU: ausgewählte Flächeninformationen (Anzahl Schläge, Gesamtumfang Ausschreibung in ha, grobe Lage nach Gemarkungen), Kultur, Zeitrahmen, einzusetzende Technik (Ertragskartierung, Strohmanagement)

LU->LW: Angebot

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

Risiko im Umgang mit Geodaten:

In diesem Szenario werden keine Daten ausgetauscht, aus denen Informationen zu konkreten Flächen hervorgehen.

1.2 LW beauftragt Lohnunternehmer

Teilnehmer: Landwirt , Lohnunternehmer

Vorgang: Ein konkreter Lohnunternehmer wird mit der Durchführung der Ernte beauftragt.

Ausgetauschte Daten:

LW->LU: Flächeninformationen , gewünschte Maßnahme, einzusetzende (Silierhilfs-) Mittel, Termin, einzusetzende Technik (Stroh häckseln ja/nein)

LU->LW: Auftragsbestätigung

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

Risiko im Umgang mit Geodaten:

In diesem Szenario übermittelt der Landwirt ausgewählte Informationen, aus denen die Umrisse, die Größen und die Lage der jeweiligen zu erntenden Flächen hervorgehen. Informationen zur Bewirtschaftung bzw. der Anbaustrategie des Landwirts bzw. der Wirtschaftlichkeit des Schlages sind daraus nicht ableitbar. Dabei gilt: Was der Landwirt dem Lohnunternehmer von sich aus nicht bereitstellt kann dieser nicht wissen.

1.3 Durchführung der Ernte

Teilnehmer: Landwirt , Lohnunternehmer, Fahrer

> Vorgang: Der Landwirt initiiert die konkrete Durchführung der Ernte. Der Lohnunternehmer leitet dies an den Fahrer weiter, der dann diese Arbeiten ausführt. Nach Durchführung erhält der Landwirt vom LU die Erntedokumentation soweit sie an seine

Flächen gebunden ist.

Erfasste Daten:

Datum der Ernte, (flächenspezifische) Ertragsdaten, ggf. Qualitätsdaten, Schlagzustand

Ausgetauschte Daten:

LW->LU->Fahrer: zu erntende Flächen, Kultur, Strohmanagement, Termin der Maßnahme

Fahrer->LU: (flächenspezifische) Erntemenge, Qualitäten, Verbrauch an Betriebsmitteln, Schlagzustand, Arbeitszeiten

LU->LW: Datum der Ernte, (flächenspezifische) Erntemenge, Qualitäten, Schlagzustand, Abrechnung

Dauerhaft gespeicherte Daten:

Bei Fahrer: Arbeitszeiten

Bei LU: Alle Daten soweit sie für eigene Geschäftsprozesse notwendig sind; **darunter fallen NICHT: (teilflächenspezifische) Erntemenge und Qualitäten**

Bei LW: (teilflächenspezifische) Erntemengen und Qualitäten, Schlagzustände; Daten die ihm durch den LU im Rahmen der Abrechnung übermittelt werden, werden in der eigenen Dokumentation gespeichert

Risiko im Umgang mit Geodaten:

Die im Ernteprozess erfassten georeferenzierten Sensordaten zum Ertrag sind hoch sensibel, da aus ihnen der wirtschaftliche Erfolg des bewirtschaftenden Landwirts über eine Fläche abgeleitet werden kann. Lohnunternehmer, die georeferenzierte Sensordaten als Arbeitsdokumentation erfassen, sind gehalten, dies nach Schlägen getrennt zu tun.

Es kommt in der Praxis häufig vor, dass Erntemaschinen an einem Tag mehrere Flächen unterschiedlicher Kunden bedienen, die Datenerfassung aber durchläuft. Da aber sowohl der Lohnunternehmer als auch seine Kunden ein Interesse daran haben, ausgewählte Daten auszuwerten, in die der jeweils andere keinen Einblick nehmen soll, muss an dieser Stelle eine technische Lösung gefunden werden, die dies gewährleistet, z.B. über eine Verschlüsselung der Daten, wobei sowohl Landwirt als auch Lohnunternehmer sich nur jeweils die Daten aufschließen können, auf die sie eine Zugriffsberechtigung haben. Dieses Verfahren wurde vom BLU bereits im Herbst 2010 vorgeschlagen (s.A.: „Wem gehören die Geodaten?“ – Zeitschrift „Lohnunternehmen“ 1/2010, S. 6; Kopie erhältlich bei BLU oder DLR-RNH).

Grundsätzlich ausgeschlossen muss sein, dass in zentralen Rechenzentren (z.B. von Dienstleistern oder Herstellern von Landtechnik) betriebs- und personenbezogene Sensor- und Dokumentationsdaten ohne schriftliche Zustimmung der Landwirte unverschlüsselt erfasst, verarbeitet und gespeichert werden. Da im Geschäftsfeld der Lohnunternehmen ein derartiger bürokratischer Aufwand nicht realisierbar ist, zumal deren Kunden ggf. die Zustimmung bei den Grundstücksbesitzern einholen müssten, sind technische Lösungen der „positionsbezogenen“

Verschlüsselung personenbezogener Daten auf Landmaschinen zu präferieren.

Ein weiteres Problem im Umgang mit sensiblen Daten bisher ist, dass diese Daten auch beim Arbeitsprozess nicht verschlüsselt werden. Daher muss ausgeschlossen werden, dass auf dem Datentransfer vom Landwirt (über den Lohnunternehmer und ggf. seinen Fahrer) zur Maschine und zurück unbefugte Dritte Einblick in die Daten erhalten können. Ein Speichern der Daten in einer „Cloud“ erscheint vor diesem Hintergrund höchst problematisch und wird daher von vielen Landwirten als zu unsicher abgelehnt.

1.4 Bedarfsermittlung / Erstellen Applikationskarte

Teilnehmer: Landwirt, ggf. Beratung, ggf. LU (Bodenbeprobung)

> Vorgang: Im Nachgang der Ernte der Vorfrucht ermittelt der LW für seine Schläge den Düngebedarf für die folgende Kultur. Eine teilflächenspezifische Bedarfsermittlung ist möglich, setzt jedoch das Vorliegen von (mehrjährigen) Ertragskarten für die zu planenden Flächen sowie eine nach Teilflächen getrennte Bodenbeprobung voraus.

Der Landwirt teilt dem Berater die zur Erstellung einer Applikationskarte notwendigen Informationen mit. Dieser ermittelt die teilflächenspezifischen Aufwandmengen. Die Beratung muss ggf. auch die Einhaltung der notwendigen Abstandsauflagen beachten. In diesem Fall ist das Ergebnis eine Applikationskarte, die diese Auflagen berücksichtigt. Andernfalls sind nur die unterschiedlichen Aufwandmengen berücksichtigt.

Erfasste / ermittelte Daten:

(Teil-) flächenspezifischer Düngebedarf

Ausgetauschte Daten:

LW -> Beratung: Flächenkoordinaten, Nährstoffabfuhr durch Ernte der geräumten Kultur (Ertragsdaten der vorigen Ernte, ggf. als Ertragskarte), folgende Kultur, Ertragserwartung, ggf. Ertragskarten der Vorjahre, ggf. Ergebnisse Bodenbeprobung

Beratung -> LW: Analyse der Ertragskarte; Darstellung des (flächenspezifischen) Düngebedarfs, Düngevorschläge in Form von Applikationskarten

Dauerhaft gespeicherte Daten:

Bei der Beratung: Daten des Landwirts werden ausschließlich zur Bearbeitung der Beratungsanfrage zwischengespeichert, es sei denn die Parteien treffen weitergehende Vereinbarungen.

Bei Landwirt: sämtliche dem Landwirt zur Verfügung gestellten schlagbezogenen Daten gehen (ggf. nach Bezahlung) in sein Eigentum über und werden von diesem gespeichert.

Risiko im Umgang mit Geodaten:

Auch hier stellt der Landwirt der Beratung freiwillig Geodaten zur Verfügung. Bei deren Analyse zieht

die Beratung eigene bzw. amtliche Geodaten hinzu. Sollte es im Interesse der Beratung liegen, ausgewählte Geodaten des Landwirts anonymisiert in den eigenen Datenbestand zur weiteren Verwendung aufzunehmen, sind hierfür vertragliche Regelungen zwischen Beratung und Landwirt zu treffen.

1.5 Durchführung der Maßnahme (teilflächenspezifisch)

Teilnehmer: Landwirt (ggf. Lohnunternehmer, Fahrer)

> Vorgang: Der Landwirt initiiert die konkrete Durchführung der Düngemaßnahme. Dazu überspielt er die Applikationskarte in sein Maschinenterminal und arbeitet sie mit seiner Düngetechnik ab. Ggf. wird ein Lohnunternehmer damit beauftragt, die Applikationskarte abzuarbeiten. In diesem Fall gelten die gleichen Abläufe wie bei der Beauftragung der Ernte.

Erfasste Daten:

Datum der Maßnahme, Arbeitszeiten, As-applied-Karte, ggf. Windgeschwindigkeit, Schlagzustand

Ausgetauschte Daten:

LW->LU: Applikationskarte, zu verwendender Dünger, Termin der Maßnahme, weitere Flächeninformationen

LU->Fahrer: Applikationskarte, zu verwendender Dünger, Termin der Maßnahme, Flächeninformationen

Fahrer->LU: As-applied-Karte, Datum der Maßnahme, Schlagzustand, Arbeitszeiten, Begründungen, warum und an welchen Stellen die Applikationskarte durch manuelle Eingriffe übersteuert wurde

LU->LW: As-applied-Karte, Datum der Maßnahme, Abrechnung, Schlagzustand, Begründungen, warum und an welchen Stellen die Applikationskarte durch manuelle Eingriffe übersteuert wurde

Bei Einsatz von maschinengestützten Telemetriesystemen zusätzlich:

Maschine->Maschinenhersteller: Prozess-/Maschinendaten

Maschinenhersteller->LU: (Aufbearbeitete) Prozessdaten, Wartungsinformationen etc.

Dauerhaft gespeicherte Daten:

Bei Fahrer: Arbeitszeiten

Bei LU: Alle Daten soweit sie für eigene Geschäftsprozesse notwendig sind; darunter fällt ggf. auch As-applied-Karte (wenn z.B. nach Pflanzenschutzgesetz der Fahrer bzw. der LU für eine ordnungsgemäße Applikation verantwortlich ist)

Bei LW: As-applied-Karte, Schlagzustände; Daten die ihm durch den LU im Rahmen der Abrechnung übermittelt werden, werden in der eigenen Dokumentation gespeichert

Risiko im Umgang mit Geodaten:

Aus einer einzelnen Applikationskarte, die der Landwirt dem Lohnunternehmer zur Abarbeitung überlässt, gehen nicht ausreichend Daten hervor als dass man aus diesen die Bewirtschaftungsstrategie des Landwirts (bzw. den wahrscheinlichen betriebswirtschaftlichen Erfolg) ableiten könnte. Sollte der Lohnunternehmer jedoch verschiedene Tätigkeiten für den Landwirt auf der gleichen Fläche durchführen, kann dieser durch Sammeln der Daten und deren Auswertung die Bewirtschaftungsstrategie des Landwirts ableiten.

Andererseits muss die als Arbeitsauftrag definierte Applikationskarte ggf. durch manuelles Eingreifen des Fahrers übersteuert werden (z.B. Senken der N-Düngeapplikationsmenge bei erkennbarer Überversorgung im Bestand). Dies kann jedoch nur erfolgen, wenn der Fahrer den Arbeitsauftrag selbst nachvollzieht und entsprechend in der Lage ist, diesen anzupassen.

Datenschutzrechtliche Bewertung der Szenarien „Ernte und Düngung“

Im Folgen werden die oben beschriebenen Einzelszenarien datenschutzrechtlich bewertet. Hierbei wird nur auf die o. g. Informationen Bezug genommen. Weitergehende Regelungen (etwa im Rahmen des allgemeinen Vertragsrechts, Wettbewerbsrecht, Recht am eingerichteten und ausgeübten Gewerbebetrieb, Schutz von Betriebs- und Geschäftsgeheimnissen etc.) bleiben außer Betracht.

Datenschutzrechtliche Bewertung „Auftragsausschreibung -Ernte-“

Die vom Landwirt bereitgestellten Informationen dürfen zum Zwecke der Angebotserstellung verarbeitet werden. Die Datenverarbeitung durch den Lohnunternehmer erfolgt für die Begründung eines rechtsgeschäftlichen Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG. Sollte es nicht zur Auftragserteilung kommen, so sind die übermittelten personenbezogenen Daten (u. a. Name und Adresse des Landwirts) umgehend wieder zu löschen, sofern keine Einwilligung des Landwirts für eine weitergehende Aufbewahrung (etwa für Ausschreibungen in Folgejahren) vorliegt.

Datenschutzrechtliche Bewertung „LW beauftragt Lohnunternehmer“

Die Daten des Landwirts darf der Lohnunternehmer zur Begründung und Durchführung des rechtsgeschäftlichen Schuldverhältnisses nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG verarbeiten. Diese Daten dürfen jedoch nicht an Dritte weitergegeben werden, sofern hierfür keine Einwilligung des Landwirts vorliegt.

Datenschutzrechtliche Bewertung „Durchführung der Ernte“

Die für die Aufgabenerfüllung notwendigen Daten dürfen nach § 28 Abs. 1 Satz 1 Nr. 1 BDSG durch den Lohnunternehmer und seine Mitarbeiter verarbeitet werden. Hierbei gilt eine strenge Zweckbindung, was bedeutet, dass die Daten für andere Zwecke (etwa eigene Recherchen über landwirtschaftliche Flächen) ohne die Einwilligung des Betroffenen nicht zulässig sind. Erfolgt eine Datenverarbeitung bzw. Speicherung bei einem Dienstleister (z. B. Datenbankprovider) und es kann über Verschlüsselung nicht sichergestellt werden, dass dieser keinen Zugriff auf die Daten hat, so muss mit diesem ein Auftragsdatenverarbeitungsvertrag geschlossen werden (s. o.) oder die Einwilligung des Betroffenen vorliegen. Im Rahmen der Auftragsdatenverarbeitung wird der Auftragnehmer dann so behandelt, als wäre er Mitarbeiter des Lohnunternehmers, so dass er nicht als Dritter im Sinne des

Datenschutzrechts anzusehen wäre. Allerdings ist hierbei zu beachten, dass der Auftragnehmer kein Eigeninteresse an den Daten haben darf bzw. diese nicht etwa mit Daten anderer Auftraggeber vermischen darf. So darf bzw. muss sogar der Lohnunternehmer natürlich ein Interesse daran haben, die Daten zur Erfüllung seines Auftrags zu nutzen. Darüber hinaus darf er jedoch die Daten nicht für eigene Zwecke (etwa Aufbauen einer eigenen Datenbank, Weiterverkauf etc.) verwenden. Dass ihn abstrakt die Daten interessieren könnten ist zunächst unbeachtlich. Relevant ist, was er dann mit den Daten macht. Es wäre somit unzulässig, wenn der Auftragnehmer als Dienstleister für unterschiedliche Lohnunternehmer tätig wäre und nicht gewährleistet ist, dass die Daten getrennt voneinander verarbeitet werden (Mandantentrennung).

Grundsätzlich ist auch die Nutzung der sog. Cloud für die Verarbeitung der Daten durch den Lohnunternehmer zulässig. Allerdings gelten auch hierbei in der Regel die Vorgaben der Auftragsdatenverarbeitung. Gerade im Rahmen der Datenverarbeitung in der Cloud muss auf die Datentrennung geachtet werden. Empfehlenswert ist eine Verschlüsselung der gespeicherten (personenbezogenen) Daten. Auch sollte sichergestellt sein, dass die Datenverarbeitung innerhalb der EU bzw. in Ländern mit einem vergleichbaren Datenschutzniveau geschieht. Ein Zugriff auf die Daten aus unsicheren Drittländern heraus (auch USA) muss verhindert werden. Das bedeutet, dass selbst wenn der Cloud-Anbieter eine Verarbeitung innerhalb der EU zusagt, jedoch Administratoren des Anbieters aus Drittländern Zugriff auf die Server haben, dieses problematisch ist.

Hinsichtlich der Verarbeitung von Daten des Fahrers der Landmaschine, also des Angestellten des Lohnunternehmers, muss sichergestellt sein, dass keine vollständige Arbeitnehmerüberwachung erfolgt. Der Angestellte darf keinem übermäßigen Überwachungsdruck ausgesetzt sein. Das bedeutet, dass die erfassten Daten über die Bewegungen und Pausen der Landmaschine nicht für die Mitarbeiterüberwachung ausgewertet werden dürfen. So weit wie möglich müssen diese anonymisiert werden oder Unschärfen etwa durch Aggregation erreicht werden. Mögliche Umsetzungen wären z. B. Aufsummierungen von Pausenzeiten und Arbeitszeiten pro Woche / Monat. Ebenso könnten Geoinformationen zusammengefasst bzw. Durchschnittswerte gebildet werden.

Nach Abschluss der Arbeiten und Abrechnung der Leistungen müssen die Daten wieder gelöscht werden, sofern keine Einwilligung des Landwirts für eine längerfristige Speicherung vorliegt. Nur die Geschäftsbriefe (in der Regel die Rechnungen) müssen nach der Abgabenordnung (AO) bzw. dem HGB ggf. für bis zu zehn Jahre aufbewahrt werden. Diese Daten müssen jedoch dann gesperrt werden, was bedeutet, dass hierauf nur noch zu Zwecken der AO bzw. des HGB durch den Lohnunternehmer zugegriffen werden kann.

Datenschutzrechtliche Bewertung „Bedarfsermittlung / Erstellen Applikationskarte“

Der Berater darf die vom Landwirt zur Verfügung gestellten Daten zur Auftragserfüllung verarbeiten (§ 28 Abs. 1 Satz 1 Nr. 1 BDSG). Auch hier gilt, dass die Daten nach Auftragserfüllung und Übergabe des Gutachtens zu löschen sind, sofern keine Einwilligung des Landwirts vorliegt, die eine längere Speicherung rechtfertigt. Auch eine Verwendung der Daten für eigene Zwecke ist dem Berater untersagt, sofern hierfür keine Einwilligung des Betroffenen vorliegt.

Datenschutzrechtliche Bewertung „Durchführung der Maßnahme (teilflächenspezifisch)“

Hierfür gilt grundsätzlich das Selbe wie bei „Durchführung der Ernte“ beschrieben. Die personenbeziehbaren Daten dürfen zur Aufgabenerfüllung genutzt werden und müssen nach Abschluss

der Arbeiten gelöscht werden, sofern keine Einwilligung des Landwirts für die längerfristige Aufbewahrung vorliegt und keine Aufbewahrungspflichten nach AO bzw. HGB gegeben sind.

Eine besondere Aufbewahrungspflicht über Informationen von verwendeten Pflanzenschutzmitteln ergibt sich aus § 11 Pflanzenschutzgesetz. Siehe hierzu die Szenarien „Pflanzenschutz“.

Hinsichtlich der Düngung ist u. a. das Düngegesetz (DüngG) zu beachten. Nach § 3 Abs. 3 DüngG ist das Bundesministerium für Ernährung, Landwirtschaft und Verbraucherschutz (Bundesministerium) ermächtigt, Vorschriften über die Aufzeichnung der Anwendung von Düngemitteln zu erlassen. Eine entsprechende Verordnung ist die „Verordnung über die Anwendung von Düngemitteln, Bodenhilfsstoffen, Kultursubstraten und Pflanzenhilfsmitteln nach den Grundsätzen der guten fachlichen Praxis beim Düngen“ (DüV). Nach § 7 DüV gilt:

„Betriebsinhaber haben bis zum 31. März des auf das jeweils abgelaufene Düngejahr folgenden Kalenderjahres aufzuzeichnen

1. die ermittelten Nährstoffmengen nach § 3 Abs. 3 einschließlich der zu ihrer Ermittlung angewendeten Verfahren,
2. die Werte nach § 4 Abs. 1 einschließlich der zu ihrer Ermittlung angewendeten Verfahren und
3. die Ausgangsdaten und Ergebnisse der Nährstoffvergleiche nach § 5 Abs. 1 nach den Anlagen 7 und 8.

Ausgenommen von Satz 1 Nr. 1 und 2 sind Flächen und Betriebe nach § 5 Abs. 4.

(2) Bei einer Zufuhr von Düngemitteln, Bodenhilfsstoffen, Kultursubstraten oder Pflanzenhilfsmitteln, die unter Verwendung von Fleischmehlen, Knochenmehlen oder Fleischknochenmehlen hergestellt wurden, auf landwirtschaftlich genutzte Flächen sind ferner innerhalb eines Monats nach der jeweiligen Düngungsmaßnahme aufzuzeichnen

1. der Schlag, auf den die Stoffe aufgebracht wurden, einschließlich der Bezeichnung und der Größe des Flurstücks sowie der darauf angebauten Kultur,
2. die Art und Menge des zugeführten Stoffes und das Datum der Aufbringung,
3. der Inverkehrbringer des Stoffes gemäß der Kennzeichnung nach der Düngemittelverordnung,
4. der enthaltene tierische Stoff gemäß der Kennzeichnung nach der Düngemittelverordnung,
5. bei Düngemitteln die Typenbezeichnung gemäß der Kennzeichnung nach der Düngemittelverordnung.

(3) Die Aufzeichnungen nach den Absätzen 1 und 2 sind sieben Jahre nach Ablauf des Düngejahres aufzubewahren.“

Diese Dokumentationspflichten betreffen den Betriebsinhaber. Besondere Aufbewahrungspflichten für den Lohnunternehmer ergeben sich hieraus nicht. Ggf. muss er die Daten und Aufzeichnungen an den Betriebsinhaber übergeben, die er für die o. g. Aufzeichnung und Dokumentation benötigt.

Handlungsempfehlungen – Möglichkeiten und Grenzen aus Sicht des Datenschutzes

- Es ist sicherzustellen, dass die für die Auftragsdurchführung erforderlichen Daten nach der

Erfüllung des Auftrags durch den Auftragnehmer (in der Regel der Lohnunternehmer) regelmäßig gelöscht werden. Die Software sollte so gestaltet werden, dass der Nutzer auf die Löschpflichten hingewiesen wird.

- Alternativ ist eine Einwilligung von dem Betroffenen durch den Lohnunternehmer über eine weitere Speicherung der Daten einzuholen. Diese muss jedoch losgelöst vom übrigen Vertrag für den Auftrag erfolgen und darf nicht in AGB oder einer allgemeinen Datenschutzerklärung etc. versteckt werden. Inhaltlich muss sie die zu speichernden Daten bzw. zumindest Datenarten (z. B. Logdaten) und die Zweckbestimmung beschreiben. Zu beachten ist, dass eine solche Einwilligung in der Regel jederzeit vom Betroffenen widerrufen werden kann. Der Lohnunternehmer muss dann die Daten löschen.
- Die Technik ist so zu gestalten, dass nach AO, HGB oder auch ‚Pflanzenschutzgesetz, Düngemittelverordnung etc. z aufzubewahrende Daten gesperrt werden, so dass ein Zugriff auf die Information aus dem Produktivsystem nicht möglich ist. Bei größeren Lohnunternehmern ist entsprechend ein Rollenkonzept zu entwickeln, das die Zugriffsrechte so gestaltet, dass nur befugte Personen auf diese gesperrten Daten Zugriff nehmen können.

2 Szenario „Pflanzenschutz“

Im Folgenden wird das Szenario „Pflanzenschutz“ beschrieben.

2.1 Auftragsausschreibung

Teilnehmer: Landwirt, Lohnunternehmer

Ausgetauschte Daten:

LW->LU: Flächeninformationen, gewünschte Maßnahme, einzusetzende Mittel, Zeitrahmen

LU->LW: Angebot

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

2.2 Beauftragung

Teilnehmer: Landwirt , Lohnunternehmer

Ausgetauschte Daten:

LW->LU: Flächeninformationen , gewünschte Maßnahme, einzusetzende Mittel, Termin

LU->LW: Auftragsbestätigung

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

2.3 Festlegung der Maßnahme

Teilnehmer: Landwirt , Beratung

Ausgetauschte Daten:

LW->Beratung: Flächeninformationen, Bestandsinformationen, gewünschte Maßnahme

Beratung->LW: Applikationskarte, Mittel, Termin der Maßnahme

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

2.4a Durchführung der Maßnahme (teilflächenspezifisch)

Teilnehmer: Landwirt , Lohnunternehmer, Fahrer

Erfasste Daten: Datum der Maßnahme, As-applied-Karte

Ausgetauschte Daten:

LW->LU: Applikationskarte, Mittel, Termin der Maßnahme

LU->Fahrer: Applikationskarte, Mittel, Termin der Maßnahme, Flächeninformationen

Fahrer->LU: As-applied-Karte, Datum der Maßnahme

LU->LW: As-applied-Karte, Datum der Maßnahme, Abrechnung

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

2.4b Durchführung der Maßnahme (nicht teilflächenspezifisch)

Teilnehmer: Landwirt , Lohnunternehmer, Fahrer

Erfasste Daten: Datum der Maßnahme

Ausgetauschte Daten:

LW->LU: Aufwandsmenge, Mittel, Termin der Maßnahme

LU->Fahrer: Aufwandsmenge, Mittel, Termin der Maßnahme, Flächeninformationen

Fahrer->LU: Datum der Maßnahme

LU->LW: Datum der Maßnahme, Abrechnung

Dauerhaft gespeicherte Daten:

Alle Daten bei den einzelnen Teilnehmern nach den jeweiligen Aufbewahrungspraktiken

Datenschutzrechtliche Bewertung des Szenarios

Diese Szenarien unterscheiden sich im grundsätzlichen Ablauf nicht von den Szenarien „Ernte und

Düngung“. Die Besonderheit liegt hier in den Vorgaben des Pflanzenschutzgesetzes. Eine besondere Aufbewahrungspflicht über Informationen von verwendeten Pflanzenschutzmitteln ergibt sich aus § 11 Pflanzenschutzgesetz. Danach gilt: Der Leiter eines landwirtschaftlichen, forstwirtschaftlichen oder gärtnerischen Betriebes ist verpflichtet, die Aufzeichnungen für die bewirtschafteten Flächen seines Betriebes unter Angabe des jeweiligen Anwenders zusammen zu führen. Es gilt eine drei jährige Aufbewahrungsfrist. Die Fristen zur Aufbewahrung der Aufzeichnungen rechnen ab dem Beginn des Jahres, das auf das Jahr des Entstehens der jeweiligen Aufzeichnung folgt.

Diese Frist gilt nach Artikel 67 Absatz 1 Satz 1 oder 2 der Verordnung (EG) Nr. 1107/200 auch für berufliche Verwender. Beruflicher Verwender wiederum ist nach der Richtlinie 2009/128/EG „jede Person, die im Zuge ihrer beruflichen Tätigkeit Pestizide verwendet, insbesondere Anwender, Techniker, Arbeitgeber sowie Selbständige in der Landwirtschaft und anderen Sektoren“. Das bedeutet, dass auch der Lohnunternehmer diesen Dokumentationspflichten unterliegt. Er muss somit die Informationen über die verwendeten Pflanzenschutzmittel für drei Jahre nach dem Jahr, indem das Mittel ausgebracht wurde, aufbewahren. Auch diese Daten sind zu sperren, so dass sie nur für Auskunftspflichten nach dem Pflanzenschutzgesetz (§ 63) verwendet werden können. Eine anderweitige Verwendung dieser Daten ist unzulässig.

Handlungsempfehlungen – Möglichkeiten und Grenzen aus Sicht des Datenschutzes

Es gelten dieselben Handlungsempfehlungen wie bei den Szenarien vorher:

- Es ist sicherzustellen, dass die für die Auftragsdurchführung erforderlichen Daten nach der Erfüllung des Auftrags regelmäßig gelöscht werden. Die Software sollte so gestaltet werden, dass der Nutzer auf die Löschpflichten hingewiesen wird.
- Alternativ ist eine Einwilligung von dem Betroffenen über eine weitere Speicherung der Daten einzuholen. Diese muss jedoch losgelöst vom übrigen Vertrag für den Auftrag erfolgen und darf nicht in AGB oder einer allgemeinen Datenschutzerklärung etc. versteckt werden.
- Die Technik ist so zu gestalten, dass nach AO, HGB, Pflanzenschutzgesetz, Düngemittelverordnung etc. aufzubewahrende Daten gesperrt werden, so dass ein Zugriff auf die Information aus dem Produktivsystem nicht möglich ist. Bei größeren Lohnunternehmern ist entsprechend ein Rollenkonzept zu entwickeln, das die Zugriffsrechte so gestaltet, dass nur befugte Personen auf diese gesperrten Daten Zugriff nehmen können.

3 Szenario „Datenverarbeitung durch Landmaschinen“

Telemetriesysteme sind schon heute auf den Großmaschinen einiger Landtechnikhersteller (AGCO, Claas, John Deere) im Einsatz. Andere Unternehmen (u. a. Case IH, New Holland, Deutz-Fahr) befinden sich z. Zt. in der Entwicklungsphase. Mit den Telemetriesystemen werden die von der Maschine selbst erhobenen Daten und die an die Maschine übermittelten Auftragsdaten erfasst und dann über Mobilfunklösungen an einen Datenserver des Herstellers übermittelt. Auf der einen Seite bietet die Telemetrie eine Reihe von nützlichen Funktionen, wie z. B. Übermittlung einer fälligen Wartung, Optimierung der Einstellung der Maschine, schnelles Finden der Maschine im Reparaturfall, Geofencing u. a. m. Auf der anderen Seite muss der Eigentümer der Maschine zustimmen und dafür bezahlen, dass seine Maschinendaten über die Telemetrie verschickt werden dürfen. Im Klartext heißt

dies, dass der Eigentümer ohne Einsatz des Telemetiesystems seine eigenen Daten nicht in sein Büro senden kann. Die Daten kann er nur über den kostenpflichtigen Umweg des Hersteller-Servers erhalten - und dies obwohl die einhellige Aussage der Hersteller lautet: "Die Daten gehören den Eigentümern der Maschine. Eine Einwilligung der Übertragung ist demnach erforderlich". Aber was nutzen erhobene Daten, an die der Eigentümer nicht kostenlos und ohne Umweg herankommen kann. Ein Hersteller von Radladern verweigert sogar Garantieansprüche des Eigentümers, wenn dieser die Telemetrie nicht zulässt.

Außerdem besteht die Frage, inwieweit Handydetektoren eingesetzt werden dürfen, um zu überprüfen, ob eine Landmaschine eine Mobilfunkverbindung aufbaut.

Datenschutzrechtliche Bewertung des Szenario

Hier wird ein Dritter (nämlich der Hersteller) für einen Teilschritt der Datenverarbeitung durch den Lohnunternehmer eingebunden. Auch dieser Dritte kommt mit personenbezogenen Daten des Landwirts ggf. in Berührung. Eine solche Datenübermittlung könnte der Lohnunternehmer durch eine ausdrückliche Einwilligung des Landwirts für diese Datenverarbeitung legitimieren. Neben den administrativen Problemen bei der Einholung dieser Einwilligung wäre ein Problem, dass sich die auch erfolgende Verarbeitung von Daten des Personals des Lohnunternehmers nur eingeschränkt über Einwilligungen regeln lässt. Dies liegt daran, dass im Arbeitsverhältnis hohe Anforderungen an die Freiwilligkeit der Einwilligung des Mitarbeiters zu stellen wären und auch der Fall beachtet werden muss, dass die Einwilligung nicht erteilt wird.

Daher dürfte in aller Regel hier das Instrument der Auftragsdatenverarbeitung im Sinne des § 11 BDSG zur Anwendung kommen. Neben der sorgfältigen Auswahl und regelmäßigen Prüfung des Auftragnehmers (hier des Herstellers) wäre hierfür ein Auftragsdatenverarbeitungsvertrag im Sinne des § 11 Abs. 2 BDSG erforderlich. Dieser muss ein Weisungsrecht des Auftraggebers (hier in der Regel der Lohnunternehmer) gegenüber dem Auftragnehmer (hier Hersteller) beinhalten.

Dass die in der Landmaschine gespeicherten Daten nur dann zur Verfügung gestellt werden, wenn ein (kostenpflichtiger) Vertrag geschlossen wird, wäre datenschutzrechtlich allenfalls zulässig, wenn der Eigentümer der Maschinen zumindest das ausschließliche Verfügungsrecht über die Daten hat. Er muss die Kontrolle darüber haben, dass die Daten ausschließlich in seiner Verfügungsmacht bleiben. Dies würde beinhalten, dass die Daten nicht ohne seine Zustimmung dem Hersteller zur Kenntnis gelangen können und er die Daten vollständig löschen kann, wenn er z. B. die Maschine veräußert.

Der Einsatz von Handydetektoren kann dann zulässig sein, wenn diese sich darauf beschränken, generelle Mobilfunkaktivitäten anzuzeigen. Dabei sollte die Reichweite so bemessen sein, dass nur dann Aktivitäten angezeigt werden, wenn Mobilfunkeinrichtungen tätig sind, die unter der Kontrolle der einsetzenden Person stehen (sollten). Unzulässig wäre jedoch der Einsatz von Systemen, die auch weitergehende Daten der Mobilfunknutzer (z. B. IMEI, Handynummer, IP-Adresse etc.) erfassen und nicht ausgeschlossen werden kann, dass Dritte in den Ortungsbereich des Systems gelangen können.

Handlungsempfehlungen – Möglichkeiten und Grenzen aus Sicht des Datenschutzes

Der Eigentümer der Landmaschinen muss die Kontrolle bzw. Verfügungsmacht über die dort verarbeiteten bzw. gespeicherten personenbezogenen Daten haben. Das beinhaltet auch, dass er diese

vollständig löschen können muss.

Nutzt der Eigentümer der Landmaschinen den Übermittlungsdienst des Herstellers für die Verarbeitung personenbezogener Daten (und sei es nur für die Aufbereitung bzw. Weiterleitung), dann ist in der Regel (sofern auch Daten von Kunden des Eigentümers der Maschinen bzw. seiner Mitarbeiter verarbeitet werden) ein Auftragsdatenverarbeitungsvertrag im Sinne des § 11 BDSG mit dem Hersteller zu schließen.

5 Fazit

Aus Datenschutzsicht muss bei jeder Verarbeitung personenbezogener Daten gewährleistet sein, dass hierfür eine Rechtsgrundlage vorliegt. Dies können Berechtigungen aus dem BDSG etwa zur Vertragserfüllung sein oder sie können auch aus Spezialnormen wie der Düngemittelverordnung oder dem Telekommunikationsgesetz / Telemediengesetz stammen. Liegt kein Gesetz vor, das die gewünschte Datenverarbeitung rechtfertigt, so ist die Einwilligung beim Betroffenen einzuholen. Diese muss die wesentlichen Punkte der Verarbeitung (etwa Datenarten, Beteiligte etc.) umfassen und freiwillig sein. Der Betroffene muss sie jederzeit widerrufen können.

Eine Datenverarbeitung darf auch nur erfolgen, wenn sich die verarbeitende Stelle vorher über den Zweck der Datenverarbeitung klar geworden ist und diesen auch dem Betroffenen kommuniziert. Dabei dürfen nur die personenbezogenen Daten verarbeitet werden, die für die Zweckerreichung erforderlich sind. Ist der Zweck erreicht, so sind die dann in der Regel nicht mehr erforderlichen Daten zu löschen, sofern keine gesetzlichen Aufbewahrungspflichten bestehen.

Die Datenverarbeitung muss sowohl intern als auch gegenüber Betroffenen transparent sein, wobei insbesondere Auskunftsrechte der Betroffenen zu beachten sind. Für ausreichende Datensicherheit muss gesorgt werden und regelmäßige Kontrollen (etwa durch den internen Datenschutzbeauftragten) gewährleistet sein.

Als besondere Problemstellung im Agrarbereich hat sich die Datenverarbeitung der eingesetzten Landmaschinen herausgestellt. Von diesen werden zahlreiche Daten etwa zur Position der Maschine, Verhalten des Fahrers etc. erfasst und ggf. an Dritte übermittelt. Auch dieses darf nur im Rahmen der Datenschutzgesetze erfolgen. Das bedeutet, dass der Besitzer der Landmaschine die Kontrolle darüber behalten muss, welche Daten an wen weiter gegeben werden. Insbesondere muss dabei ausgeschlossen werden, dass die Mitarbeiter vollständig überwacht werden und personenbezogene Daten (etwa die des Auftraggebers) unkontrolliert gespeichert und genutzt werden.

Datenhoheit der Landwirte

Die Erhebung georeferenzierter, d.h. raum-zeit-bezogener Daten in der Landwirtschaft mit modernen Ortungs- und Sensortechniken ist in besonderem Maße dazu geeignet, das Produktions- und Geschäftswissen von Landwirten und Lohnunternehmern abzubilden. Wie in anderen Branchen sind auch die Unternehmen in der Landwirtschaft darauf bedacht, ihre Datenhoheit zu wahren, d.h. Betriebs- und Geschäftsgeheimnisse zu schützen, um die eigene Wertschöpfung nicht zu gefährden. Letztlich ist es eine Akzeptanz- und Vertrauensfrage, ob ein Unternehmer bereit ist, seine Produktions- und Geschäftsdaten auf externe Server bei Dritten (z.B. in die "Cloud") auszulagern. Wie in der übrigen Wirtschaft wird dieses Thema auch von den Akteuren in der Landwirtschaft sehr kritisch diskutiert.

Speziell der Pflanzenbau ist betroffen, da das Produktions- und Geschäftswissen von Landwirten und Lohnunternehmern sehr effizient mit GPS-gestützten Dokumentations- und Sensortechniken der Landtechnik erfasst und auf zentrale Cloud-Dienste weitergeleitet werden kann.

Die Datenhoheit von Landwirten und Lohnunternehmern bedingt, dass sie bei Eigenmechanisierung auch zukünftig frei darüber entscheiden können, ob

- Maschinen eingesetzt werden, die Daten auf zentrale Cloud-Dienste weiterleiten, was vertraglich im Rahmen der Auftragsdatenverarbeitung zu regeln ist
- nur Maschinen eingesetzt werden, die sicherstellen, dass die Daten im Unternehmen verbleiben

Problematischer ist die Situation bei Maschinendienstleistungen durch Dritte. Es muss auch längerfristig davon ausgegangen werden, dass nicht alle Landwirte bereit sind, ihre Produktions- und Geschäftsdaten in die Cloud auszulagern. Andere lehnen den bürokratischen Aufwand ab, um die datenschutzrechtlichen Voraussetzungen für den Einsatz von Cloud-gebundenen Lohnmaschinen zu schaffen. Lohnunternehmer müssen auch zukünftig auf diese Kundeninteressen bezüglich der Datenhoheit eingehen können. Als Problemlösung bietet sich die Einführung einer sicheren End-to-End-Verschlüsselung von der Datenerfassung auf der Landmaschine bis zur Verarbeitung durch den Landwirt an. Dieser Schritt entlastet die Lohnunternehmer von datenschutzrechtlicher Bürokratie und führt zu Vertrauen bei den Landwirten als Kunden. Bei einer End-to-End-Verschlüsselung landwirtschaftlicher Produktionsdaten können weiterhin die Cloud-Infrastrukturen von Landmaschinenherstellern oder Dienstleistern genutzt werden. Damit wird der Datenhoheit des Landwirts entsprochen, der frei und ohne technische Zwänge entscheiden kann, ob er seine Daten selbst auswertet oder auf sicherem Weg an einen Dienstleister seiner Wahl weitergibt.

Sicht der Landwirte

Bei der Nutzung der im Rahmen des iGreen-Projekts beschriebenen Technologien sind drei Dinge für die Wahrung der Datenhoheit der Landwirte miteinander in Einklang zu bringen:

1. Aufbau und zur Stärkung des Vertrauens der Landwirte in die Wahrung der Datenhoheit durch seine Dienstleister

Um Vertrauen zu schaffen, sollte die Transparenz der Datenverwendung und die Rechte der Landwirte auf Auskunft, Berichtigung, Löschung und Sperrung immer gewahrt werden. Der Landwirt sollte stets darüber informiert werden, wenn eine Verwendung seiner Daten durch einen Dienstleister oder Dritte erfolgt.

Zudem können technische Lösungen helfen, Vertrauen zu schaffen. Hierfür bietet sich beispielsweise die Einführung einer sicheren End-to-End-Verschlüsselung von der Datenerfassung auf der Landmaschine bis zur Verarbeitung durch den Landwirt an. Dieser Schritt entlastet die Lohnunternehmer von datenschutzrechtlicher Bürokratie und führt zu Vertrauen bei den Landwirten als Kunden. Bei einer End-to-End-Verschlüsselung landwirtschaftlicher Produktionsdaten können weiterhin auch die Cloud-Infrastrukturen von Landmaschinenherstellern oder Dienstleistern genutzt werden. Damit wird der Datenhoheit des Landwirts entsprochen, der frei und ohne technische Zwänge entscheiden kann, ob er seine Daten selbst auswertet oder auf sicherem Weg an einen Dienstleister seiner Wahl weitergibt.

Jede technische oder organisatorische Datenschutzmaßnahme sollte darüber hinaus Lösungen dafür

bereithalten, Datenmissbrauch möglichst ganz auszuschließen.

2. Einhaltung des datenschutzrechtlichen Rahmens und darüber hinaus der Schutz von Betriebs- und Geschäftsgeheimnissen

Wichtig ist hierbei insbesondere der Aspekt der freiwilligen Einwilligung in die Weitergabe der Daten. Nicht alle Landwirte sind bereit, ihre Daten im Rahmen neuer Technologien weiterzugeben und sie beispielsweise in die Cloud auszulagern. Dieses wichtige Kundeninteresse muss auch unter dem Einsatz der "vernetzten" Landtechnik gewahrt bleiben. Die Datenhoheit von Landwirten und Lohnunternehmern bedingt, dass sie bei Eigenmechanisierung auch zukünftig frei über die Verwendung ihrer Daten entscheiden können, insbesondere darüber, ob

- Maschinen eingesetzt werden, die Daten auf zentrale Cloud-Dienste weiterleiten
- nur Maschinen eingesetzt werden, die sicherstellen, dass die Daten im Unternehmen verbleiben.

Die Erhebung georeferenzierter, d.h. raum-zeit-bezogener Daten in der Landwirtschaft mit modernen Ortungs- und Sensortechniken bezieht sich nicht nur auf personenbezogene Daten sondern ist außerdem in besonderem Maße dazu geeignet, das Produktions- und Geschäftswissen von Landwirten und Lohnunternehmern abzubilden. Wie in anderen Branchen sind auch die Unternehmen in der Landwirtschaft darauf bedacht, ihre Datenhoheit zu wahren, d.h. Betriebs- und Geschäftsgeheimnisse zu schützen, um die eigene Wertschöpfung nicht zu gefährden. Betriebs- und Geschäftsgeheimnisse sind jedoch vom Bundesdatenschutzgesetz nicht umfasst, sodass vertragliche Vereinbarungen zum Schutz dieser Informationen für den Landwirt von besonderer Bedeutung sind. Letztlich ist es aber auch eine Akzeptanz- und Vertrauensfrage, ob ein Unternehmer bereit ist, seine Produktions- und Geschäftsdaten auf externe Server bei Dritten (z.B. in die "Cloud") auszulagern. Dies betrifft speziell die im Pflanzenbau tätigen Landwirte, da Daten von Landwirten und Lohnunternehmern mit GPS-gestützten Dokumentations- und Sensortechniken der Landtechnik erfasst und auf zentrale Cloud-Dienste weitergeleitet werden können.

3. Entwicklung praktikabler Lösungen, die für die Anwender gut nachvollziehbar und mit möglichst geringem bürokratischem Aufwand verbunden sind

Häufig wird bei vertraglichen Vereinbarungen zum Datenschutz beim Einsatz von Cloud-gebundenen Maschinen oder anderen datenerfassenden Technologien der bürokratische Aufwand gescheut. Die Beteiligten sind hier gefordert, verständliche und gut nachvollziehbare Vereinbarungen zum Datenschutz zu entwickeln, die in der Praxis allgemein akzeptiert werden. Darüber hinaus sollten auch technische und organisatorische Lösungen praktikabel und für jeden Landwirt bezahlbar, zugänglich und technisch realisierbar sein. Hierfür bieten sich insbesondere die Methoden der Anonymisierung und Verschlüsselung von Daten und das Angebot dezentraler Speicherung an.

Vor dem Hintergrund dieser zentralen landwirtschaftlichen Datenschutzinteressen sind die im Rahmen der Datenschutz-Arbeitgruppe erarbeiteten Ergebnisse eine gute Grundlage für die Festlegung von Grundregeln für den Umgang mit sensiblen Daten in der Landwirtschaft. Für eine Verbindlichkeit zum zukünftigen generellen Umgang mit Daten im Rahmen von Vereinbarungen zwischen Landwirten mit ihren Dienstleistern und Lieferanten sind jedoch noch weitere Schritte notwendig. Beispielhaft seien an dieser Stelle von allen Beteiligten anerkannte Richtlinien zum Datenschutz und Musterverträge zur Datennnutzung genannt.

Sicht der Lohnunternehmer

Aus Sicht des Projektpartners Bundesverband Lohnunternehmen e.V. hat die Arbeitsgruppe "Task Force Rechte an Daten" im Rahmen des iGreen-Projekts ein sehr nützliches Dokument erstellt. Dadurch, dass an diesem Dokument alle mitgearbeitet haben, die im Dienstleistungsbereich Pflanzenbau tätig sind, wurden die datenschutzrechtlichen Belange der Landwirte, Berater, Lohnunternehmer, Landmaschinenhändler und -hersteller berücksichtigt. Es wird klar gestellt, dass die Maschinendaten dem Eigentümer der Maschine gehören und dass die persönlichen Daten sowie die Daten zur Bewirtschaftung der Schläge in die Datenhoheit des Landwirts fallen. Für die Lohnunternehmer, die sich auf zwei Seiten, Landwirt als Kunde und Landmaschinenhersteller, um den Datenschutz kümmern müssen, bietet dieses Papier eine gut lesbare und praxisrelevante Hilfestellung. Dies gilt auch für die besonders sensiblen Bereiche des Auslesens von Maschinendaten durch den Hersteller. Hier sollte sich der Lohnunternehmer als Kunde der Landmaschinenindustrie vertraglich zusichern lassen, dass die Maschinendaten nicht ohne seine Zustimmung durch den Hersteller gespeichert werden dürfen. Und falls der Lohnunternehmer diese Zustimmung erteilt, muss der Hersteller im Sinne der Transparenz darstellen, auf welchem Medium (Cloud-Server oder firmeneigener Server) die Daten gespeichert werden, wozu diese Daten genutzt werden und wer Zugriff auf die Daten hat sowie Zeitpunkt der Löschung der gespeicherten Daten. Der Lohnunternehmer kann dem Dokument auch entnehmen, welche Rechte und Pflichten bei der Erbringung von Dienstleistungen für ihn wichtig sind. Um sich auf rechtlicher Seite abzusichern, sollte der Dienstleister seinem Kunden erklären, welche Daten zu welchem Zweck gespeichert werden und sich die Speicherung durch eine schriftliche Vereinbarung ggf.im Bereich der allgemeinen Geschäftsbedingungen, erlauben lassen.

Transparente Handhabung von Datenflüssen

Neben den durch das Bundesdatenschutzgesetz bedingten Maßnahmen zum Schutze von personenbezogenen Daten ist im Agrarbereich eine transparente, nachvollziehbare und vertrauensvolle Behandlung auch nicht personenbezogener Daten von Seiten aller Parteien wünschenswert, da sich anders kaum eine enge Verzahnung der Daten der einzelnen Akteure erreichen lässt.

Die bestehenden technischen Ansätze zu diesen Themen sind noch ausbaufähig; die Austauschdatenformate wie z.B. ISOXML (zwischen FMIS und Landmaschinen) sind größtenteils mit der Problematik der Interoperabilität befasst, das Thema Datenhoheit wird jedoch kaum aufgegriffen.

Es erscheint sinnvoll, bereits auf technischer Ebene sowohl die Anforderungen durch das Bundesdatenschutzgesetz als auch die Wünsche der einzelnen Akteure im Agrarbereich aufzugreifen. Dieses ließe sich erreichen, indem zum Beispiel ausgetauschten Daten immer auch Metadaten angefügt würden, die intendierte Empfänger der Daten, den Zweck des Austauschs (Zweckbindung), Löschfristen und so weiter explizit darstellen, also Richtlinien bezüglich der Nutzung der Daten abbilden. Diese Metadaten müssen von den beteiligten Software-Komponenten verarbeitet und angezeigt werden. Während hierdurch ohne weitergehende Maßnahmen eine absichtliche missbräuchliche Nutzung durch z.B. manipulierte Software nicht ausgeschlossen werden könnte - dies würde recht komplexe Maßnahmen wie Verschlüsselung oder Treuhandservices benötigen - würde trotzdem geklärt, welche Nutzung welcher Daten grundsätzlich rechtmäßig ist und welches Datenschutzbedürfnis die einzelnen Teilnehmer jeweils haben. Im Vergleich zum Stand der Dinge, der durch Ad Hoc-Lösungen und weite Grauzonen geprägt ist, würde dies bereits eine große Verbesserung darstellen.

Literaturverzeichnis

- Bundesamt für Sicherheit in der Informationstechnik (BSI); IT-Grundschutzkataloge, Bonn.
- Bundestag; Gesetzentwurf der Bundesregierung Entwurf eines Gesetzes zur Vereinheitlichung von Vorschriften über bestimmte elektronische Informations- und Kommunikationsdienste (Elektronischer-Geschäftsverkehr-Vereinheitlichungsgesetz – ElGVG), BT-Drs. 16/3078, 23.10.2006.
- Bundesverfassungsgericht; Volkszählungsurteil, Urteil vom 15.12.1983, Az. 1 BvR 209/83, 1 BvR 269/83, 1 BvR 362/83, 1 BvR 420/83, 1 BvR 440/83, 1 BvR 484/83.
- Bundesarbeitsgericht; Urteil Az. 2 AZR 51/02, 27.03.2003
- Bundesarbeitsgericht; Beschluss 1 ABR 16/07, 26. 8. 2008
- Simitis, Spiros (Hrsg.); Bundesdatenschutzgesetz Kommentar, Baden-Baden, 6. Auflage 2006.
- Europäischer Gerichtshof; Urteil Rs. C-101/01 (Lindqvist), Slg. 2003, S. I-12971 ff.
- Europäischer Gerichtshof; Urteil Rs. C-275/06 (Promusicae), Slg. 2008, S. I-271 ff.
- Däubler, Wolfgang / Klebe, Thomas / Wedde, Peter / Weichert, Thilo (Hrsg.); Bundesdatenschutzgesetz Kompaktkommentar, Frankfurt am Main, 3. Auflage 2010.
- Entwurf Datenschutz-Grundverordnung; Vorschlag für eine Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten und zum freien Datenverkehr (Datenschutz-Grundverordnung), 25.01.2012.
- Heckmann, Dirk (Hrsg.); juris Praxiskommentar Internetrecht, Saarbrücken, 2007.
- Leisner, Walter; Das neue „Kommunikationsgrundrecht" – Nicht Alibi für mehr, sondern Mahnung zu weniger staatlicher Überwachung, in: NJW 2008, S. 2902 ff.
- Metschke, Rainer / Wellbrock, Rita; Datenschutz in Wissenschaft und Forschung, Berlin 2002.
- OECD Declaration on Transborder Data Flows; The OECD Observer, Nr. 135
- Richtlinie 2002/58/EG; Richtlinie 2002/58/EG des Europäischen Parlaments und des Rates vom 12. Juli 2002 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre in der elektronischen Kommunikation (Datenschutzrichtlinie für elektronische Kommunikation), ABl. EG Nr. L 201 vom 31.07.2002, S. 37-47
- Richtlinie 2006/24/EG; Richtlinie 2006/24/EG des Europäischen Parlaments und des Rates vom 15. März 2006 über die Vorratsspeicherung von Daten, die bei der Bereitstellung öffentlich zugänglicher elektronischer Kommunikationsdienste oder öffentlicher Kommunikationsnetze erzeugt oder verarbeitet werden, und zur Änderung der Richtlinie 2002/58/EG, ABl. EG Nr. L 105 vom 13.04.2006, S. 54-63
- Richtlinie 2007/2/EG; Richtlinie 2007/2/EG des Europäischen Parlaments und des Rates vom 14.03.2007 zur Schaffung einer Geodateninfrastruktur in der Europäischen Gemeinschaft (INSPIRE), ABl. EG Nr. L 108 vom 25.04.2007, S. 1-14

- Richtlinie 97/66/EG; Richtlinie 97/66/EG des Europäischen Parlaments und des Rates vom 15. Dezember 1997 über die Verarbeitung personenbezogener Daten und den Schutz der Privatsphäre im Bereich der Telekommunikation, ABl. EG Nr. L 24 vom 30.01.1998, S. 1-8
- Tinnefeld, Marie-Theres / Ehmann, Eugen / Gerling, Rainer W.; Einführung in das Datenschutzrecht, München, 4. Auflage 2005.
- UN Resolution 45/95; http://www.un.org/documents/ga/res/45/a45r095.htm