LANDWIRTSCHAFT 4.0 & DATENSCHUTZ

PRAXISLEITFADEN FÜR ANBIETER UND ANWENDER DIGITALER TECHNOLOGIEN IN DER LANDWIRTSCHAFT

© LFI/Ing. Gerald PFABIGAN

Mit Unterstützung von Bund, Ländern und Europäischer Union

Bundesministerium
Land- und Forstwirtschaft,
Regionen und Wasserwirtschaft

LE 14-20

Europäischer Landwirtschaftsfonds für die Entwicklung des ländlichen Raums: Hier investiert Europa in die ländlichen Gebiete.

Ihr Wissen wächst

IMPRESSUM

Herausgeber: LFI Österreich, Schauflergasse 6, 1015 Wien

Erste Auflage, September 2022, Eigenverlag

Redaktion / Mitwirkende:
Universität für Bodenkultur Wien, Inst. f. Rechtswissenschaften
Landwirtschaftskammer Österreich
Grafik/ Layout: AIZ, Erhardt

Bildernachweise: LFI/Ing. Gerald PFABIGAN, Pexels/ Canva-studio

VORWORT

Vertrauen ist gut, Kontrolle ist besser – Achten Sie auf ordnungsgemäßen Datenschutz

„Digitalisierung" ist längst kein leeres Schlagwort mehr, bei dem man nicht genau weiß, was damit eigentlich gemeint ist. In den letzten Jahren wurde uns bewusst, wie sehr neue Technologien unsere Lebens-, Arbeits- und Wirtschaftsweise beeinflussen.

Dieser „Megatrend" Digitalisierung hat auch in der Landwirtschaft längst Einzug gehalten: Seien es die immer zahlreicher werdenden Agrar-Apps für's Smartphone, Precision Farming-Technologien für Ackerbau und Grünland, die zunehmende Automatisierung im Stall oder die digital abgewickelte, betriebliche Dokumentation: Die „Landwirtschaft 4.0" wird auf bäuerlichen Betrieben immer öfters zur Realität.

Das Angebot an diesen Technologien ist in kontinuierlichem Wachstum begriffen, was dazu führt, dass auch die Menge der dabei generierten (Agrar-)Daten immer größer wird. Dadurch wächst auch das Bedürfnis nach dem bestmöglichen Schutz dieser betrieblichen und persönlichen Informationen – und das bei gleichzeitiger Gewährleistung eines weitestgehend ungehemmten, freien Datenverkehrs.

In den meisten Fällen entscheiden Hersteller oder Anbieter digitaler Technologien über Zwecke und Mittel der Verarbeitung generierter oder gesammelter Agrardaten. Dies geht auch mit einigen datenschutzrechtlichen Verpflichtungen im Sinne der Datenschutz-Grundverordnung (DSGVO)[1] einher.

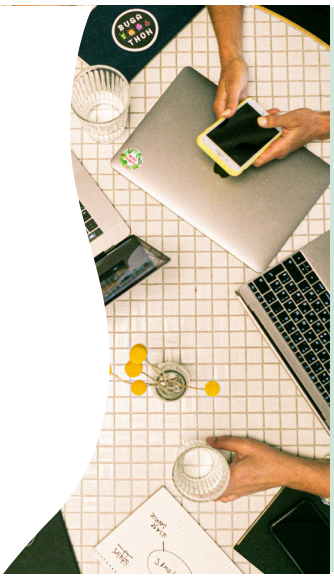
Der gegenständliche Leitfaden soll daher einen Überblick über die rechtlichen Vorgaben der DSGVO im Kontext der digitalen Landwirtschaft bieten und in komprimierter Form darstellen, wie aus der Sicht von Technologie-Anbietern bestmöglich damit umgegangen werden kann.[2]

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl L 2016/119, 1 (folgend kurz DSGVO).

[2] Der gegenständliche Leitfaden soll einen allgemeinen Überblick über die wichtigsten Rechte und Pflichten der DSGVO insbesondere im landwirtschaftlichen Kontext bieten. Es ist daher darauf hinzuweisen, dass der gegenständliche Leitfaden keinen Anspruch auf Vollständigkeit oder Aktualität erhebt und die entsprechenden Ausführungen immer im konkreten Einzelfall zu prüfen sind.

INHALTSVERZEICHNIS

1. WANN IST DIE DSGVO ANWENDBAR UND WO EMPFIEHLT SICH EINE REGELMÄSSIGE ÜBERPRÜFUNG IHRER ANWENDBARKEIT?



Shortcut: Anwendungsbereich der DSGVO

- ***Räumliche Anwendbarkeit:***
  - *Niederlassung des Verantwortlichen in EU/EWR oder*
  - *betroffene Person innerhalb EU/EWR + Datenverarbeitung zum Anbieten von Waren/Dienstleistungen oder zum Beobachten des Verhaltens der betroffenen Person*
- ***Sachliche Anwendbarkeit:***
  - *Personenbezogene Daten werden zumindest teilweise automatisiert verarbeitet oder*
  - *zwar nicht automatisiert verarbeitet, aber in einem Dateisystem gespeichert.*

1.1 WANN IST DIE DSGVO RÄUMLICH ANWENDBAR?

Die DSGVO gilt in räumlicher Hinsicht für sämtliche

- zumindest teilweise automatisierten Verarbeitungsvorgängen personenbezogener Daten,[3]
- wenn der dafür Verantwortliche (z. B. Technologie-Anbieter) bzw. die Auftragsverarbeiterin (z. B. Cloud-Anbieterin) in der Europäischen Union (EU) oder dem Europäischen Wirtschaftsraum (EWR) niedergelassen ist.[4]

Dasselbe gilt grundsätzlich auch für Verantwortliche bzw. Auftragsverarbeiter, die

- zwar nicht über eine Niederlassung in der EU bzw. dem EWR verfügen,
- sich jedoch die von der Datenverarbeitung betroffene Person, somit zumeist die einzelne Landwirtin als Technologie-Nutzerin, innerhalb der EU aufhält und
- die Datenverarbeitung
- mit dem Anbieten von Waren oder Dienstleistungen oder mit
- der Beobachtung des Verhaltens der betroffenen Person innerhalb der EU einhergeht.[5]

[3] Zum sachlichen Anwendungsbereich siehe Punkt 1.2.
[4] Art. 3 Abs. 1 DSGVO.
[5] Art. 3 Abs. 2 DSGVO.

Da digitale Agrar-Technologien ihrer Konzeption nach vor Ort in landwirtschaftlichen Betrieben eingesetzt werden und im Rahmen dieses Einsatzes Daten generieren, sammeln oder sonst verarbeiten, ist in den allermeisten dieser Anwendungsfälle von der räumlichen Anwendbarkeit der DSGVO auszugehen; eine räumliche Unanwendbarkeit kann daher als absoluter Ausnahmefall betrachtet werden bzw. ist praktisch so gut wie auszuschließen.

1.2 WANN IST DIE DSGVO SACHLICH ANWENDBAR?

1.2.1 Die vier Elemente des sachlichen DSGVO-Anwendungsbereiches

Zusätzlich zum räumlichen muss immer auch der sachliche Anwendungsbereich der DSGVO eröffnet sein, damit sie im konkreten Einzelfall anzuwenden ist. Dementsprechend ist die DSGVO sachlich anwendbar, wenn folgende vier Voraussetzungen kumulativ vorliegen:

- Es muss sich um Daten (im Sinne von Informationen) handeln;
- welche ganz oder teilweise automatisiert verarbeitet werden;
- Bezugspunkt der Daten muss eine natürliche Person sein; und
- die Daten müssen sich auf eine natürliche Person beziehen (Personenbezug samt Identifizierbarkeit).[6]

Der Begriff der Daten wird in diesem Zusammenhang weit ausgelegt und umfasst grundsätzlich sämtliche Informationen, die einer Sammlung und Verarbeitung zugänglich sind. Im Kontext der digitalen Landwirtschaft bedeutet dies, dass alle erdenklichen und vielleicht auch auf den ersten Blick unwesentlichen Informationen, die von Agrar-Technologien elektronisch verarbeitet werden können, als „Daten" im Sinne der DSGVO angesehen werden können.[7] In ähnlicher Weise ist auch das Kriterium der automatisierten Verarbeitung in einem weiten Sinn zu verstehen und umfasst jegliche elektronische, d. h. computer- bzw. softwarebasierte Datenverarbeitung.

Die DSGVO ist darüber hinaus nur auf die Verarbeitung von Daten anwendbar, die sich auf natürliche Personen beziehen. Daten juristischer Personen (z. B. GmbH, Vereine, Stiftungen etc.) fallen somit nicht in den DSGVO-Anwendungsbereich. In diesem Zusammenhang ist zu beachten, dass zwar Daten juristischer Personen selbst nicht unter die DSGVO fallen, diese allerdings im Einzelfall dann anwendbar sein kann, wenn sich die Daten auf die hinter der juristischen Person stehenden natürlichen Personen beziehen (z. B. Geschäftsführer*in, Gesellschafter*innen, Mitarbeiter*innen, Mitglieder,

[6] Art. 2 Abs. 1 DSGVO. Darüber hinaus ist die DSGVO auch auf die nicht automatisierte Verarbeitung personenbezogener Daten anwendbar, wenn die Daten in einem Dateisystem gespeichert sind oder in einem solchen gespeichert werden sollen (z. B. Karteisystem oder analoge Datenbank). Da sich der gegenständliche Leitfaden auf das Agrar-Datenschutzrecht in Zusammenhang mit digitalen Agrar-Technologien bezieht, ist diese Option für die sachliche Anwendbarkeit der DSGVO nicht einschlägig, weshalb in weiterer Folge nicht näher darauf eingegangen wird.

[7] Dies umfasst beispielsweise Tiersensor-Daten im gleichen Maße wie GPS-Daten selbstfahrender Landmaschinen oder Luftbildaufnahmen von mit Spektralkameras ausgestatteten Agrar-Drohnen.

Funktionär*innen etc.). Auf die Verarbeitung solcher Daten wäre die DSGVO voll anwendbar.

Während die Auslegung der ersten drei Elemente des sachlichen Anwendungsbereiches vergleichsweise unproblematisch ist, ergeben sich hinsichtlich des „Personenbezuges", also der Beziehung zwischen den Daten und der natürlichen Person, regelmäßig komplexe Auslegungsfragen. Personenbezogene Daten sollen gemäß Art. 4 Z 1 DSGVO immer dann vorliegen, wenn sie sich auf eine identifizierte oder identifizierbare natürliche Person beziehen (Art. 4 Z 1 DSGVO). Dieses Begriffspaar ist wiederum wie folgt auszulegen:

- „identifiziert": Das Datum verweist in objektiv unverwechselbarer Weise auf die natürliche Person und die Identität dieser Person ergibt sich unmittelbar aus dem verarbeiteten Datum (z. B. eindeutig zuordenbare Namen, Fingerabdrücke oder Steuernummern, Adresse).
- „identifizierbar": Die natürliche Person kann „direkt oder indirekt, insbesondere mittels Zuordnung zu einer Kennung wie einem Namen, zu einer Kennnummer, zu Standortdaten, zu einer Online-Kennung oder zu einem oder mehreren besonderen Merkmalen, die Ausdruck der physischen, physiologischen, genetischen, psychischen, wirtschaftlichen, kulturellen oder sozialen Identität dieser natürlichen Person sind, identifiziert werden". [8]

Während es vergleichsweise einfach ist, festzustellen, ob eine natürliche Person durch die Datenverarbeitung identifiziert ist, tendiert die Auslegung des Begriffs der „Identifizierbarkeit" zuweilen dazu, auszuufern. In ErwGr 26 DSGVO wird dazu erläuternd festgehalten, dass für die Feststellung, ob eine Person identifizierbar ist, *„alle Mittel berücksichtigt werden [sollten], die von dem Verantwortlichen oder einer anderen Person nach allgemeinem Ermessen wahrscheinlich genutzt werden, um die natürliche Person direkt oder indirekt zu identifizieren".*[9] Da sowohl (Hilfs-)Mittel des Verantwortlichen als auch anderer Personen prinzipiell in die Beurteilung miteinzubeziehen sind, bedeutet dies – insbesondere vor dem Hintergrund immer häufiger eingesetzter Big-Data-Analyse-Systeme –, dass vor allem bei der gemeinsamen Verarbeitung einer Vielzahl unterschiedlicher Daten die Identifizierbarkeit natürlicher Personen nur in seltenen Fällen völlig ausgeschlossen werden kann.

[8] Siehe Art. 4 Z 1 DSVO (Hervorhebungen durch Verfasser).
[9] Siehe ErwGr 26 dritter Satz DSGVO.

Beispiel: DSGVO und Tiersensorik

Werden Milchkühe mit Pansen-Sensoren versehen, die ihre Vitalfunktionen in Echtzeit aufzeichnen, liegen auf den ersten Blick reine Sachdaten vor, da die Daten sich nicht auf eine natürliche Person beziehen, sondern auf ein Tier. Werden die Daten einer ganzen Herde mit einer bestimmten Anzahl an Nutztieren aufgezeichnet und weiterverarbeitet und diesen Daten weitere Daten wie z. B. Futter-Intervalle, Stalltemperatur oder Bewegungsabläufe hinzugefügt, tritt schrittweise der Personenbezug und die Identifizierbarkeit der Landwirtin ein, da einerseits auf die Zugehörigkeit der Herde zur Landwirtin und andererseits auf den Umgang mit ihren Nutztieren geschlossen werden kann. Werden die gesammelten Daten schließlich gemeinsam unter Verwendung eines Nutzer*innen-Profils verarbeitet, ist spätestens an diesem Zeitpunkt auch eine Identifizierbarkeit gegeben und es handelt sich um personenbezogene Daten.

Für Sie als Technologie-Anbieter*in handelt es sich daher bereits immer dann um personenbezogene Daten, wenn eine Information isoliert betrachtet zwar keine erkennbare Verbindung zu einer natürlichen Person aufweist, ein solcher Konnex jedoch durch die Mitberücksichtigung von Zusatzwissen Ihrerseits oder dritter Personen, durch (rechtmäßig verwendete) Hilfsmittel oder das Hinzutreten weiterer Verarbeitungsschritte hergestellt werden kann. Dem EuGH folgend kommt es insbesondere darauf an, ob solche Hilfsmittel, Zusatzwissen oder weitere Verarbeitungsschritte im Einzelfall „vernünftigerweise" zur Identifizierung einer Person eingesetzt werden könnten. Ausgeschlossen ist der Personenbezug demnach immer dann, wenn die eingesetzten Mittel gesetzlich verboten sind oder die Identifizierung einen unverhältnismäßigen Aufwand an Zeit, Kosten und Arbeitskräften erfordern würde.

Kann hingegen kein Personenbezug hergestellt werden (zur Anonymisierung von Daten siehe näher unter Punkt 2), ist der Verarbeitungsvorgang nicht von der DSGVO erfasst. Dies ist beispielsweise bei reinen Maschinen(funktions-)daten ohne Konnex zur natürlichen Person der Fall.[10]

[10] Auch bei Maschinendaten ist jedoch Vorsicht geboten, da diese unter Umständen Rückschlüsse auf die Arbeitstätigkeit oder den (sorglosen bzw. sorgsamen) Umgang mit den Maschinen durch Arbeitnehmer*innen oder dritte Personen zulassen.

1.2.2 Zweifelsregel und die regelmäßige Überprüfung des Personenbezugs

Beim Personenbezug von Daten handelt es sich vor diesem Hintergrund nicht um eine statische Größe, sondern vielmehr um eine dynamisch änderbare Eigenschaft, die über einen bestimmten Zeitraum hinweg sowohl „wegfallen" (z. B. bei Anonymisierung der Daten) als auch nachträglich eintreten[11] kann. Daher kann sich auch bei – im Zeitpunkt ihrer erstmaligen Erhebung – reinen Sachdaten durch das Hinzutreten zusätzlicher Informationen und deren gemeinsamer Verarbeitung „schleichend" ein Personenbezug ergeben. Je nach konkreter Lage des Einzelfalls können damit ein und dieselben Agrardaten als personenbezogene oder nicht-personenbezogene Daten einzustufen sein („Hybridcharakter" von Agrardaten). Dementsprechend empfiehlt sich eine regelmäßige Überprüfung der Daten bzw. Datenströme betreffend deren etwaig geänderten Charakter. Im Zweifelsfall ist die Behandlung als personenbezogene Daten und damit die Anwendung und Einhaltung der DSGVO anzuraten, um negativen Folgen wie insbesondere Geldbußen oder Schadenersatzforderungen von vornherein vorzubeugen. Insbesondere wenn die gesammelten Sach- und/oder Hybriddaten schließlich gemeinsam unter Verwendung eines Nutzer*innen-Profils verarbeitet werden, ist von personenbezogenen Daten auszugehen.

Beispiel: Zweifelsregel

Je nach Aufbau eines FMIS (Farmmanagement- und -informationssystems) kann über die Auswertung von Leistungs- und Maschinendaten ein relativ genaues Bild über die Arbeitsweise von Mitarbeiter*innen im landwirtschaftlichen Betrieb gezeichnet werden. Aufgrund der Datenverarbeitung und dem möglichen Abgleich mit Dienstplänen kann insbesondere auf deren Arbeitsleistung (Effizienz) oder auf den (sorgsamen/nachlässigen) Umgang mit Betriebsmitteln geschlossen werden. Es ist daher von personenbezogenen Daten auszugehen, weshalb die DSGVO vollumfänglich anwendbar und einzuhalten ist.

[11] Stichwort: Schleichender Personenbezug.

2. DIE ROLLENVERTEILUNG IM AGRAR-DATENSCHUTZRECHT

Shortcut: Rollenverteilung im Agrar-Datenschutzrecht
*Typischerweise sind Landwirt*innen (=Technologie-Nutzer*innen) als betroffene Personen und Agritech-Anbieter*innen (= entscheiden über Zwecke und Mittel der Datenverarbeitung) als Verantwortliche im Sinne der DSGVO anzusehen. Während als Verantwortliche sowohl juristische als auch natürliche Personen in Betracht kommen, können ausschließlich natürliche Personen die Rolle der betroffenen Person einnehmen. Darüber hinaus können auch Auftragsverarbeiter beigezogen werden, die auf Anweisung des jeweiligen Verantwortlichen Datenverarbeitungsprozesse durchführen, jedoch keine eigenständige Entscheidung über die Zwecke und Mittel der Datenverarbeitung treffen.*

Je nachdem, welche Rolle eine konkrete Person im Regelungssystem der DSGVO einnimmt, sind unterschiedliche Rechte und Pflichten der DSGVO anwendbar. Nach der Diktion der DSGVO gibt es im europäischen Datenschutzrecht drei unterschiedliche Rollen:

- den Verantwortlichen,
- die betroffene Person und
- den Auftragsverarbeiter.

Gemäß Art. 4 Z 7 DSGVO sind alle natürlichen oder juristischen Personen, Behörden, Einrichtungen oder andere Stellen als „Verantwortliche" anzusehen, die *„über die Zwecke und Mittel der Verarbeitung von personenbezogenen Daten entscheide[n]"*. [12] Dementsprechend ist immer diejenige Person als Verantwortlicher zu qualifizieren, die auf die Verarbeitung der personenbezogenen Daten sowohl rechtlich als auch tatsächlich Einfluss nehmen kann bzw nimmt. Im Kontext des Agrar-Datenschutzrechts ist dies regelmäßig der Agritech-Anbieter, da dieser die jeweilige Technologie zur Verfügung stellt und im Normalfall auch die Analyse, Auswertung und weitere Verarbeitung der generierten Daten durchführt. Grundsätzlich können aber auch Landwirt*innen in die Rolle des Verantwortlichen schlüpfen, wenn sie beispielsweise über die Modalitäten der Verarbeitung personenbezogener Daten von Mitarbeiter*innen im landwirtschaftlichen Betrieb entscheiden (Lohnverrechnung, Arbeitszeitenaufzeichnung). Werden die Zwecke und Mittel der Datenverarbeitung von mehreren Personen (z. B. Landwirtin gemeinsam mit Agritech-Anbieter) festgelegt, können diese auch „gemeinsame Verantwortliche" sein; die genaue Ausgestaltung dieser Beziehung richtet sich dann nach Art. 26 DSGVO.

[12] Vgl. Art. 4 Z 7 DSGVO.

Die gemeinsamen Verantwortlichen müssen demnach eine Vereinbarung schließen, in welcher genau die unterschiedlichen Zuständigkeiten festgelegt werden, so zum Beispiel wer die betroffene Person zu informieren hat.

Als „betroffene Personen" sind im Sinne des Art. 4 Z 1 DSGVO all jene natürlichen Personen anzusehen, deren personenbezogene Daten – durch einen oder mehrere Verantwortliche – verarbeitet werden. Die Betroffenenrechte der DSGVO stehen ausschließlich jenen natürlichen Personen zu, die als betroffene Personen zu qualifizieren sind. Je nach Fallkonstellation kann dieselbe natürliche Person in unterschiedlichen Beziehungen betroffene Person, Verantwortlicher und/oder Auftragsverarbeiter zugleich sein.

Als Auftragsverarbeiter sind nach Art. 4 Z 8 DSGVO wiederum natürliche oder juristische Personen, Behörden, Einrichtungen oder andere Stellen zu qualifizieren, *„die personenbezogene Daten im Auftrag des Verantwortlichen verarbeite[n]".*[13] Im Gegensatz zum Verantwortlichen entscheiden Auftragsverarbeiter somit nicht über die Zwecke und Mittel der Datenverarbeitung, sondern führen diese im Auftrag und auf Anweisung des Verantwortlichen aus. Agritech-Anbieter können, müssen aber nicht als Auftragsverarbeiter einzustufen sein; eine Beurteilung hat auf Grundlage des jeweiligen konkreten Einzelfalls zu erfolgen. Zu den typischen Auftragsverarbeiter*innen zählen insbesondere Cloud-Speicher-Anbieter*innen oder eine externe Lohnverrechnung, da diese ausschließlich auf Anfrage der Verantwortlichen externen Speicherplatz bzw. Serverkapazitäten zur Verfügung stellen.

Im Regelfall sind Technologie-Anbieter als Verantwortliche und Landwirt*innen als betroffene Personen im Sinne der DSGVO zu qualifizieren. Oftmals treten zu dieser bilateralen Beziehung Auftragsverarbeiter hinzu, die insbesondere Verarbeitungstätigkeiten für die Agritech-Anbieterin durchführen (z. B. Cloud-Speicher-Anbieter*innen). Nach § 28 DSGVO ist bei der Auswahl von Auftragsverarbeiter*innen ein besonderer Sorgfaltsmaßstab seitens des Verantwortlichen gefordert und die Datenverarbeitung darf nur auf Grundlage eines Auftragsverarbeitungsvertrages (oder einem damit vergleichbaren Rechtsinstrument) erfolgen. In dieser Vereinbarung sind verpflichtend

- der Gegenstand und die Dauer der Datenverarbeitung,
- Art und Zweck der Datenverarbeitung,
- die Art der verarbeiteten personenbezogenen Daten,
- die Kategorien der betroffenen Personen und
- die Pflichten und Rechte des Verantwortlichen

zu regeln. Darüber hinaus sind im Vertrag detaillierte Pflichten zum Umgang mit den verarbeiteten personenbezogenen Daten sowohl während der Vertragslaufzeit als auch für den Fall der Vertragsbeendigung zu regeln.

[13] Vgl. Art. 4 Z 8 DSGVO.

Im Bereich der Agrartechnologien kommen Auftragsverarbeiter meist als „verlängerter Arm" von Agritech-Anbieter*innen zum Einsatz. Oftmals kann dies zu Komplikationen bei der Feststellung der Rollenverteilung nach der DSGVO führen, insbesondere dann, wenn die Entscheidungsgewalt über die Datenverarbeitung zwischen Verantwortlichem und Auftragsverarbeiterin unklar geregelt wurde. Eine Auftragsverarbeiterin wird dabei ab jenem Zeitpunkt als Verantwortliche zu qualifizieren sein, in dem sie eigenständig über die Zwecke und Mittel der Datenverarbeitung entscheidet. Wann dies der Fall ist, ist vor dem Hintergrund des konkreten Einzelfalls zu eruieren.

Generell ist die Rollenverteilung regelmäßig zu evaluieren, da sie sich aufgrund verschiedener Gegebenheiten ändern kann. So ist es möglich, dass Personen Akteur*innen- ihre datenschutzrechtlichen Rollen über die Zeit hinweg ablegen und/oder eine neue Rolle einnehmen. So könnte es sein, dass ein Auftragsverarbeiter nach und nach mehr Entscheidungsbefugnis erhält und somit zu einem Verantwortlichen erwächst. Es könnte jedoch auch der Fall eintreten, dass durch Hinzutreten von Personen oder der Änderung ihrer Rechtsstellung ihre datenschutzrechtlichen Rollen neu bewertet werden müssen. Bei der Rollenverteilung nach der DSGVO handelt es sich daher um ein bewegliches System, innerhalb dessen die Qualifikation einer bestimmten Person immer unter Berücksichtigung aller Begleitumstände des konkreten Einzelfalls (neu) zu beurteilen ist.

3. ANONYMISIERUNG UND PSEUDONYMISIERUNG UND IHRE AUSWIRKUNGEN AUF DIE ANWENDBARKEIT DER DSGVO BZW. DATENSICHERHEIT

Shortcut: Anonymisierung und Pseudonymisierung

- Anonymisierung beschreibt ein Verfahren, durch das der Personenbezug von Daten entfernt wird, indem die Daten beispielsweise um sämtliche Elemente bereinigt werden, die zu einer Identifizierbarkeit einer natürlichen Person führen könnten. Ob eine absolute Anonymisierung von Daten vor dem Hintergrund von Big-Data-Analysesystemen und der dadurch erleichterten Re-Identifizierung noch möglich ist, ist fraglich.
- Bei der Pseudonymisierung von Daten werden die den Personenbezug begründenden Informationen von den Inhalten der Daten in einer Weise getrennt, dass diese Verbindung beispielsweise nur unter Verwendung eines Identifikationsschlüssels wiederhergestellt werden kann. Pseudonymisierte Daten gelten daher als personenbezogene Daten, jedoch ist der Zugang zu den die natürliche Person identifizierenden Informationen nur einem eingeschränkten Kreis von Personen zugänglich. Damit stellt die Daten-Pseudonymisierung selbst eine valide Datenschutzmaßnahme im Sinne der DSGVO dar.

Ebenso wie sich der Personenbezug von Daten über einen bestimmten Zeitraum hinweg einschleichen kann, ist es auch möglich, dass er wieder wegfällt. Der nachträgliche Entfall des Personenbezuges führt konsequenterweise dazu, dass die DSGVO ab dem Wegfallszeitpunkt nicht mehr anzuwenden ist. Gleiches gilt natürlich, wenn der Eintritt des Personenbezuges von vornherein (z. B. durch technische Mittel bzw. die Ausgestaltung der Verarbeitungsprozesse) verhindert wird. Ein solcher Ausschluss bzw. ein aktives Entfernen des Personenbezuges von Daten wird „Anonymisierung" genannt. Wird der Personenbezug nicht vollends ausgeschlossen, jedoch die Identifizierbarkeit natürlicher Personen durch Maßnahmen wie die Zuweisung einer Kennnummer, die nur mit einem Zugangsschlüssel entschlüsselt werden kann, erschwert, spricht man hingegen von „Pseudonymisierung". Solche Maßnahmen können einen wesentlichen Beitrag zur Datensicherheit in Ihrem Betrieb leisten.

Daten bzw. Datensätze sind in diesem Sinne anonym, wenn

- eine inhaltliche Aussage nicht mehr oder
- nur mit unverhältnismäßig großem Aufwand (Zeit, Kosten, Personalaufwand)
- auf eine bestimmte natürliche Person bezogen werden kann.

Grundlegendes Ziel von Anonymisierungsmaßnahmen ist es, die Identifizierbarkeit natürlicher Personen auszuschließen. Dazu eignen sich insbesondere technische Maßnahmen (z. B. Software-Lösungen), die bereits im Zeitpunkt der ersten Datenerhebung bzw. -generierung eingreifen und identifizierende Merkmale der Daten entfernen.

Beispiel: Agrar-Drohnen und Datenanonymisierung

Bei der Befliegung landwirtschaftlich genutzter Flächen durch mit bildgebender Technik ausgestatteter Agrar-Drohnen können beispielsweise Software-Anwendungen eingesetzt werden, die unmittelbar im Aufzeichnungszeitpunkt ansetzen und etwaige natürliche Personen, die von den Drohnen mitaufgezeichnet werden (z. B. Mitarbeiter*innen, Spaziergeher*innen, Nachbar*innen etc.), digital unkenntlich machen.

Ähnlich dem Phänomen des schleichenden Personenbezuges stellt sich bei einmal anonymisierten Daten allerdings die Frage, wie nachhaltig eine Anonymisierung insbesondere am Beginn des Zeitalters der Big-Data-Analysen noch ausführbar ist. Mithilfe moderner und intelligenter Algorithmen ist es nämlich bereits aktuell in vielen Fällen möglich, selbst durch die Verarbeitung anonymisierter Daten gemeinsam mit einer großen Menge anderer Daten die dahinterstehenden natürlichen Personen identifizierbar zu machen (Re-Identifizierbarkeit). Bestehen hinsichtlich der Nachhaltigkeit der Anonymisierung Zweifel, wäre daher die Anwendung bzw. Einhaltung der DSGVO anzuraten, um einen etwaigen Vorwurf der Rechtsverletzung vorzubeugen.

Im Gegensatz dazu geht es bei der Pseudonymisierung personenbezogener Daten um die Trennung von Identitäts- und Informationsdaten. Eine Verknüpfung der Informationsdaten mit der Identität der betroffenen Person kann im Falle der Pseudonymisierung nur über einen entsprechenden Schlüssel (z. B. Kennwort) (wieder-)hergestellt werden. Dadurch sollen insbesondere Datenschutzrisiken im Zusammenhang mit der Datenverarbeitung weitestgehend reduziert bzw. vermieden werden.[14] Aufgrund des bestehenbleibenden Personenbezuges der Daten bleibt die DSGVO weiterhin auf die pseudonymisierten Daten anwendbar, jedoch kann durch die Daten-Pseudonymisierung den hohen Schutzstandards der DSGVO entsprochen werden. [15]

4. ESSENZIELLE PFLICHTEN VON TECHNOLOGIE-ANBIETERN IM ZUSAMMENHANG MIT DER VERARBEITUNG PERSONENBEZOGENER DATEN

4.1 ALLGEMEINE DATENSICHERHEIT

Als Verantwortlicher müssen Sie die Einhaltung der DSGVO zwingend gewährleisten und ein entsprechendes Datenschutz-Managementsystem in Ihrem Unternehmen implementieren, da ohne (digitale) Überwachungsinstrumente ein Überblick über die durchgeführten und noch bevorstehenden Datenverarbeitungsvorgänge nicht möglich ist. Insbesondere muss dadurch sichergestellt werden, dass die Verarbeitung personenbezogener Daten unter Einhaltung der Grundsätze der Datenverarbeitung des Art. 5 DSGVO erfolgt und dass sämtliche dieser Grundsätze konkretisierenden Vorgaben der DSGVO eingehalten werden (z. B. Transparenz, Datenminimierung, Gewährleistung der Richtigkeit der Daten, Speicherbegrenzung etc.).[16]

[14] Stichwort: Erhöhung des Datenschutzstandards.
[15] Siehe dazu insbesondere Art. 25 und Art. 32 Abs. 1 lit. a DSGVO.
[16] Siehe Art. 24 ff DSGVO.

4.2 DATENSCHUTZBEAUFTRAGTE*R

Ein*e Datenschutzbeauftragte*r ist vom Verantwortlichen bzw. vom Auftragsverarbeiter immer dann zu bestellen, wenn[17]

- die Datenverarbeitung durch eine Behörde oder öffentliche Stelle durchgeführt wird (nicht jedoch Gerichte in Ausübung ihrer justiziellen Tätigkeit); oder
- die Kerntätigkeit[18] des Verantwortlichen oder des Auftragsverarbeiters in der Durchführung von Datenverarbeitungsprozessen besteht, die eine umfangreiche regelmäßige und systematische Überwachung von betroffenen Personen erfordern; oder
- die Kerntätigkeit des Verantwortlichen oder des Auftragsverarbeiters in der umfangreichen Verarbeitung besonderer Kategorien von Daten (Art. 9 DSGVO) oder von strafrechtlichen Verurteilungen und Straftaten (Art. 10 DSGVO) besteht. [19]

Einschlägig ist im Bereich der digitalisierten Landwirtschaft insbesondere der zweitgenannte Fall. Je nach Ausgestaltung der konkret eingesetzten Technologie ist eine umfangreiche regelmäßige und systematische Überwachung von Landwirt*innen grundsätzlich möglich, wobei die geforderte Intensität der Beobachtung wohl nur in der Minderzahl der Fälle erreicht werden wird. [20] Die Aufgaben des Datenschutzbeauftragten im Unternehmen sind in Art. 39 DSGVO nicht abschließend geregelt. Zu den wichtigsten Aufgaben des Datenschutzbeauftragten zählen dabei die Beratung des Verantwortlichen, des Auftragsverarbeiters und der datenverarbeitenden Mitarbeiter*innen im Betrieb bzgl. der sie treffenden datenschutzrechtlichen Verpflichtungen (vorwiegend aus der DSGVO), die Überwachung der Einhaltung dieser Pflichten, die Beratung im Zusammenhang mit der Datenschutzfolgenabschätzung sowie die Zusammenarbeit mit der Datenschutzbehörde, für die der Datenschutzbeauftragte die erste Anlaufstelle im Betrieb bilden soll. [21]

Darüber hinaus ist die freiwillige Bestellung eines Datenschutzbeauftragten auch ohne das Vorliegen der genannten Voraussetzungen jederzeit möglich. Zu beachten ist dabei allerdings, dass auch bei einer freiwilligen Bestellung sämtliche Voraussetzungen z. B. betreffend die Verantwortungsbereiche und die Stellung des Datenschutzbeauftragten im Unternehmen des Verantwortlichen einzuhalten sind. Nähere Informationen zu den Bestellungsvoraussetzungen, die eine Person für die Position des Datenschutzbeauftragten erfüllen muss, sowie zu den von diesem zu erfüllenden Aufgaben finden sich in Art. 37 bis 39 DSGVO.

[17] Vgl. Art. 37 Abs. 1 DSGVO.
[18] Kerntätigkeit ist im Sinne von „Haupttätigkeit" zu verstehen und meint z. B. nicht die Datenverarbeitung als Nebentätigkeit.; siehe dazu ErwGr 97 DSGVO.
[19] Eine solche Kerntätigkeit liegt jedenfalls vor, wenn Ihr Unternehmens- bzw. Produktzweck in der Analyse oder Bereitstellung von digitalen Inhalten liegt (z. B, FIMS, Tiersensorik etc.)
[20] Zu denken ist dabei insbesondere an Technologien, bei denen es zu Profilbildungen bzw. kontinuierlicher Überwachung von Vorgängen im landwirtschaftlichen Betrieb kommt.
[21] Vgl. Art. 39 Abs. 1 DSGVO.

4.3 SPEZIELLE MASSNAHMEN DES DATENSCHUTZES

Einen Beitrag zu der durch Sie zu gewährleisteten Datensicherheit können die oben bereits erwähnte Anonymisierung und/oder Pseudonymisierung der verarbeiteten Daten leisten. Insbesondere durch das Trennen und Verschlüsseln der erforderlichen Informationen zur Herstellung des Personenbezuges (Passwortsicherung, AES-Verschlüsselung) kann dem durch die DSGVO geforderten, hohen Datenschutzniveau in weiten Teilen bereits entsprochen werden. Darüber hinaus müssen Sie in der Lage sein, im Falle technischer Komplikationen die gespeicherten Daten rasch und vollständig wiederherzustellen.[22] Ebenso ist es durch die Einrichtung entsprechender Strukturen in Ihrem Unternehmen zu vermeiden, dass Mitarbeiter*innen jederzeit Zugang zu sämtlichen gespeicherten personenbezogenen Daten eingeräumt wird bzw. sie einen solchen leicht erlangen können. Mitarbeiter*innen sollten nur zu jenen personenbezogen Daten Zugriff haben, die für sie im Rahmen ihrer Tätigkeit(-en) relevant sind (Auftragsprinzip). Ob die getroffenen Maßnahmen ausreichen oder aufgrund einer Unternehmensveränderung zusätzliche Datensicherheitsvorkehrungen getroffen werden müssen, ist im Rahmen einer Selbstevaluierung zumindest einmal jährlich festzustellen.

4.4 DAS ANGEMESSENE SCHUTZNIVEAU UND DIE DATENSCHUTZFOLGENABSCHÄTZUNG

Ob die von Ihnen veranlassten Datenschutzmaßnahmen ausreichend sind, ist anhand des Maßstabs eines „angemessenen Schutzniveaus“ zu beurteilen. Hierbei sind all jene Risiken zu berücksichtigen, die in Ihrem Betrieb eintreten könnten, wie z. B. ein unrechtmäßiger Zugriff auf Daten, deren Vernichtung oder eine (unbeabsichtigte) Datenlöschung durch Mitarbeiter*innen. Die notwendige Reichweite der Datenschutzmaßnahmen können Sie als Verantwortlicher durch eine Datenschutzfolgenabschätzung ermitteln. Eine solche ist dann verpflichtend durchzuführen, wenn die geplante Datenverarbeitung aufgrund ihrer Art, ihres Umfangs, der (Begleit-)Umstände oder der Verarbeitungszwecke voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben wird.[23] Die Einschätzung, ob ein hohes Datenschutz-Risiko vorliegt, ist durch den Verantwortlichen selbst zu treffen, bejahendenfalls eine Datenschutzfolgenabschätzung durchzuführen ist. Konkretisierend führt Art. 35 Abs. 3 DSGVO aus, dass eine Datenschutzfolgenabschätzung insbesondere in folgenden Fällen erforderlich ist:

- bei einer systematischen und umfassenden Bewertung persönlicher Aspekte natürlicher Personen auf Grundlage automatisierter Datenverarbeitungsvorgänge, sofern diese die Grundlage von Entscheidungen bilden, die gegenüber natürlichen

[22] Beispielsweise durch den Einsatz von Backup-Servern und regelmäßiger Zwischenspeicherung der Daten.

[23] Vgl. Art. 35 Abs. 1 DSGVO.

Personen Rechtswirkungen entfalten;

- bei umfangreicher Verarbeitung sensibler Daten (Art. 9 Abs. 1 DSGVO) oder strafrechtlich relevanter Daten (Art. 10 DSGVO); und
- bei systematischer und umfangreicher Überwachung öffentlich zugänglicher Bereiche (Videoüberwachung).

Das Vorliegen dieser Voraussetzungen ist im Landwirtschaftsbereich eher unwahrscheinlich. Auch ohne das Vorliegen eines hohen Datenschutzrisikos ist die regelmäßige Durchführung einer Datenschutzfolgenabschätzung empfehlenswert, da auf diese Weise potenzielle Folgen der Datenverarbeitung für den Schutz personenbezogener Daten sichtbar werden und so rechtzeitig für den Eintritt von Ernstfällen vorgesorgt werden kann. Weiters kann dadurch die Einhaltung des entsprechenden Sorgfaltsmaßstabes im Umgang mit personenbezogenen Daten jederzeit nachgewiesen werden.

Zur besseren Orientierung, welche Datenverarbeitungsvorgänge eine Verpflichtung zur Durchführung einer Datenschutzfolgenabschätzung bewirken, wurden durch die Datenschutzbehörde zwei unterschiedliche Listen in Form von Verordnungen veröffentlicht. Auf der sogenannten „Black List" finden sich demnach Datenverarbeitungsvorgänge, bei deren Vorliegen jedenfalls eine Datenschutzfolgenabschätzung durchzuführen ist.[24] Demgegenüber enthält die veröffentlichte „White List" Verarbeitungsprozesse, die jedenfalls keine solche Verpflichtung hervorrufen.[25]

Im Zuge der Datenschutzfolgenabschätzung müssen Sie sich insbesondere die Frage stellen, welches Risiko besteht und wie schwerwiegend dieses für die Rechte natürlicher Personen ist, wenn neue Prozesse und Technologien eingesetzt werden. Werden auch Auftragsverarbeiter eingesetzt, um die angebotenen Dienstleistungen zu erfüllen, so ist auch deren Tätigkeit in die Risikobewertung bzw. in die Datenschutzfolgenabschätzung miteinzubeziehen. Da sich die Risikobeurteilung laufend ändern kann, ist zumindest eine jährliche Re-Evaluierung notwendig, um technologische Neuerungen einschätzen zu können.

Die genauen Anforderungen an die Durchführung einer Datenschutzfolgenabschätzung werden in Art. 35 DSGVO sowie in den ErwGr 84, 90, 91, 92 und 93 DSGVO genannt. Die Einhaltung einer strikten Vorgangsweise bzw. eines vorgegebenen Verfahrens ist nicht notwendig, sofern nur sämtliche Voraussetzungen erfüllt werden. Dabei sollte man sich insbesondere folgende Fragen stellen bzw. folgende Verfahrensschritte beachten:

[24] Siehe Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung durchzuführen ist (DSFA-V), BGBl II 278/2018.
[25] Siehe Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutzfolgenabschätzung (DSFA-AV), BGBl II 108/2018.

1. *Ist eine Datenschutzfolgenabschätzung erforderlich (Profiling-Maßnahmen, sensible Daten, Videoüberwachung, Black List, Verwendung neuer Technologien etc.)?*
2. *Welche Datenarten werden aufgrund welcher Rechtsgrundlage erhoben (Datenkategorie; Einwilligung; Vertragserfüllung; rechtliche Verpflichtung; lebenswichtige Interessen; öffentliches Interesse etc.)?*
3. *Werden die Grundsätze des Datenschutzes nach Art. 5 DSGVO eingehalten (Rechtmäßigkeit, Transparenz, Zweckbindung, Datenminimierung, Speicherbegrenzung, Richtigkeit, Integrität und Vertraulichkeit etc.)?*
4. *Welche Datenverarbeitungsvorgänge werden durchgeführt und sind diese notwendig und verhältnismäßig (z. B. Fingerabdruckscanner zum Starten einer Maschine)?*
5. *Welche Risiken bestehen für die Schutzziele der DSGVO (Datenverfügbarkeit, Vertraulichkeit, Zweckbindung, Richtigkeit, Datenminimierung)?*
6. *Risikoanalyse (unter Berücksichtigung z. B. des Schadens für betroffene Personen, des Kontrollverlusts, etwaiger Diskriminierung oder Rufschädigung, Identitätsdiebstahl etc.)*
7. *Ist-Stand Erhebung: Welche Datenschutzmaßnahmen sind bereits etabliert (z. B. Pseudonymisierung)?*
8. *Soll-Ist-Vergleich: Welche Maßnahmen sind über die bereits bestehenden hinaus erforderlich (z. B. personelle, technische, bauliche Maßnahmen)?*
9. *Benötigt man weitergehende Informationen von der betroffenen Person selbst (z. B. Befragung bezüglich der potenziellen Gefahr der Verletzung von Geheimhaltungspflichten)?*

Das Ergebnis dieses Prozesses sollte ein Dokument sein, in dem

- die beabsichtigten Zwecke der Datenverarbeitungsvorgänge dargestellt und
- sämtliche Datenflüsse beschrieben werden;
- das angibt, welche Risiken dadurch entstehen sowie
- welche Maßnahmen gesetzt und Vorkehrungen getroffen werden, um diese Risiken für die betroffenen Personen (bestmöglich) zu minimieren.

Wurde eine Datenschutzfolgenabschätzung korrekt durchgeführt, können die darin berücksichtigten Datenverarbeitungsvorgänge unter Einhaltung der zu ergreifenden Schutzvorkehrungen durchgeführt werden. Ergibt die Prüfung hingegen, dass weiterhin ein hohes Restrisiko besteht, dem auch mit den angedachten Maßnahmen nicht effektiv begegnet werden kann, muss die zuständige Aufsichtsbehörde[26] informiert werden. Diese hat je nach dem Ergebnis einer eingehenden Prüfung entweder eine entsprechende Erlaubnis zu erteilen oder ein Verbot der Datenverarbeitung auszusprechen.

4.5 PRIVACY BY DESIGN UND PRIVACY BY DEFAULT IM DATENSCHUTZRECHT

Als Verantwortlicher müssen Sie dem Risiko der Verarbeitung entsprechend Datenschutzmaßnahmen durch Technikgestaltung (privacy by design) sowie datenschutzfreundliche Software-Voreinstellungen (privacy by default) ergreifen. Dabei handelt es sich insbesondere um die bereits erwähnten Maßnahmen wie Pseudonymisierung, Verschlüsselung personenbezogener Daten oder die Einführung eines Verfahrens zur regelmäßigen Selbstevaluierung.

4.5.1 Privacy by design

Maßnahmen im Bereich des Datenschutzes durch Technikgestaltung sind geeignete technische und organisatorische Maßnahmen, um Datenschutzrisiken zu minimieren. Dies bedeutet, dass der Schutz personenbezogener Daten bereits ab der ersten Planungsphase und während des gesamten Entwicklungsprozesses Ihrer Produkte oder Dienstleistungen (mit)berücksichtigt werden muss. Dabei sind

- der Stand der Technik,
- die Implementierungskosten,
- die Art, der Umfang, die Umstände und die Zwecke der Verarbeitung
- sowie die Schwere und unterschiedlichen Eintrittswahrscheinlichkeiten von Risiken

zu berücksichtigen.

Zu den häufigsten „privacy by design"-Maßnahmen zählen beispielsweise die Pseudonymisierung der Daten oder die Verschlüsselung des (gesamten) Datenverkehrs sowie die entsprechende Ausgestaltung der Netzwerkserver.

[26] Vgl. Art. 58 DSGVO.

4.5.2 Privacy by default

Im Gegensatz zu „privacy by design"-Vorkehrungen sollen datenschutzfreundliche Voreinstellungen („privacy by default") sicherstellen, dass durch entsprechende Softwarekalibrierung nur solche personenbezogenen Daten verarbeitet werden, die für die konkrete Dienstleistung bzw. das gewünschte Ergebnis des Verarbeitungsprozesses erforderlich sind. Diese Verpflichtung hat daher Auswirkungen auf die zu erhebende Datenmenge, den Verarbeitungsumfang und die Speicherdauer. Die am häufigsten getroffene Maßnahme stellt die automatische Voreinstellung von Nutzer*innen-Profilen auf die höchstmögliche Privatsphäre-Einstellung dar, die in weiterer Folge durch die betroffenen Personen selbst geändert werden kann.

4.6 Die Dokumentation der Datenverarbeitungsvorgänge

Auf Grundlage der sogenannten Rechenschafts- bzw. Nachweispflicht im Sinne des Art. 5 Abs. 2 DSGVO obliegt Ihnen die ausführliche Dokumentation der von Ihnen getroffenen Datenschutz-Maßnahmen. In diesem Sinne haben Sie nachvollziehbar zu dokumentieren, dass die Verarbeitung im Einklang mit den Datenschutzgrundsätzen der DSGVO erfolgt (Dokumentationspflicht), um dies auf Verlangen gegenüber der zuständigen Behörde entsprechend nachweisen zu können (Nachweispflicht).

Um der Nachweispflicht nachzukommen, ist ein Verzeichnis über die Verarbeitungstätigkeit entweder elektronisch oder handschriftlich zu führen, wobei es gegenüber der Aufsichtsbehörde im Falle einer Überprüfung jedenfalls exportierbar sein muss. Werden Sie sowohl als Verantwortlicher als auch als Auftragsverarbeiter tätig, müssen grundsätzlich separate Verzeichnisse geführt werden.

Die Pflicht zur Verzeichnisführung besteht bereits ab jenem Zeitpunkt, ab dem die Verarbeitung der Daten mehr als nur gelegentlich erfolgt, worunter jedenfalls die kommerzielle Datenverarbeitung zu subsumieren ist.[27] Die wichtigsten Inhalte eines Verarbeitungsverzeichnisses sind:

- die Namen und Kontaktdaten des bzw. der Verantwortlichen;
- der Zweck der Datenverarbeitung und die entsprechenden Rechtsgrundlagen;
- eine Beschreibung der Kategorien betroffener Personen und der Kategorien der verarbeiteten personenbezogenen Daten (z. B. Kund*innen und Lieferant*innen; Rechnungsdaten, Adressdaten etc.);
- die Kategorien von Empfängern, gegenüber denen die personenbezogenen Daten

[27] Detaillierte Vorgaben zur Führung eines Verarbeitungsverzeichnisses enthält Art. 30 DSGVO.

offengelegt worden sind oder noch offengelegt werden (z. B. Sozialversicherung, Finanzamt, Steuerberater etc.), einschließlich Empfänger in Drittländern oder internationalen Organisationen (z. B. Joint Venture mit Partnern aus China);

- eine Auflistung der Übermittlungsvorgänge von personenbezogenen Daten in ein Drittland (z.B. USA);
- die vorgesehenen Fristen für die Löschung der verschiedenen Datenkategorien;
- eine allgemeine Beschreibung der technischen und organisatorischen Datensicherheitsmaßnahmen.

Darüber hinaus sind Sie verpflichtet, im Fall einer Datenpanne dem Ernst der Lage entsprechend zu handeln. Dabei ist innerhalb von 72 Stunden eine Meldung an die Datenschutzbehörde zu erstatten, die insbesondere folgende Inhalte aufzuweisen hat: [28]

- eine Beschreibung der Art der Verletzung des Schutzes personenbezogener Daten (unter Angabe der ungefähren Zahl und der Kategorien betroffener Personen und der ungefähren Zahl der betroffenen personenbezogenen Datensätze);
- den/die Namen und die Kontaktdaten des/der Datenschutzbeauftragten;
- eine Beschreibung der wahrscheinlichen Folgen der Datenschutzverletzung; sowie
- eine Beschreibung der ergriffenen oder vorgeschlagenen Maßnahmen zur Behebung des Zustands der Datenschutzverletzung.

Sollte die Datenpanne nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen geführt haben, kann eine Meldung an die Datenschutzbehörde entfallen. Dieser Entfall der Meldepflicht ist jedoch eingehend zu prüfen und muss zur späteren Überprüfbarkeit auch dementsprechend dokumentiert werden.

[28] Vgl. Art. 33 Abs. 2 DSGVO.

5. DIE VERANTWORTLICHENPFLICHTEN UND BETROFFENENRECHTE DER DSGVO[29]

Sofern Ihre Kund*innen bzw. Technologienutzer*innen als „betroffene Personen" iSd § 4 Z 1 DSGVO zu qualifizieren sind, kommen diesen zahlreiche Rechte zu, die wiederum spiegelbildlich für Sie als „Verantwortlicher" zu erfüllende Pflichten begründen. Während einige dieser Pflichten vom jeweiligen Verantwortlichen jederzeit selbstständig einzuhalten sind, ist wieder anderen nur auf Antrag der von der Datenverarbeitung betroffenen Person nachzukommen. Im Folgenden werden die im landwirtschaftlichen Bereich wichtigsten Betroffenenrechte und Verantwortlichenpflichten dargestellt und deren Inhalt näher erläutert.
Sofern in Zusammenhang mit den einzelnen Betroffenenrechten und Verantwortlichenpflichten durch die DSGVO keine Sonderregelungen getroffen werden, werden die funktionellen und organisatorischen Aspekte im Zusammenhang mit Begehren betroffener Personen als auch der erforderlichen Reaktionen durch den Verantwortlichen durch Art. 12 DSGVO geregelt. Demnach haben Verantwortliche in jedem Fall

- geeignete Maßnahmen zu treffen, um betroffenen Personen sowohl alle Informationen, die vom Verantwortlichen selbstständig zu erteilen sind,[30] als auch sämtliche Mitteilungen im Zusammenhang mit der Geltendmachung von Betroffenenrechten[31] in einfacher Sprache und leicht zugänglicher, transparenter und präziser Form zukommen lassen zu können;[32]
- den betroffenen Personen die Ausübung ihrer Betroffenenrechte zu erleichtern;[33]
- den betroffenen Personen konkrete Informationen über Maßnahmen, die hinsichtlich geltend gemachter Betroffenenrechte getroffen wurden, binnen eines Monats nach Antragseingang zur Verfügung zu stellen, wobei diese Frist bei sehr komplexen Anträgen um maximal zwei Monate – also auf insgesamt drei Monate – verlängert werden kann;[34]
- den betroffenen Personen Informationen und Mitteilungen unentgeltlich zur Verfügung zu stellen.[35]

[29] Als Hilfestellung zur Geltendmachung der Betroffenenrechte siehe: https://www.dsb.gv.at/download-links/dokumente.html.
[30] Siehe Art. 13 und 14 DSGVO.
[31] Siehe Art. 15 bis 22 und Art. 34 DSGVO.
[32] Vgl. Art. 12 Abs. 1 DSGVO.
[33] Vgl. Art. 12 Abs. 2 DSGVO.
[34] Vgl. Art. 12 Abs. 3 DSGVO; nach Art. 12 Abs. 4 DSGVO hat der Verantwortliche die betroffene Person innerhalb eines Monats ab Antragseingang über ein etwaiges Nicht-Tätigwerden zu unterrichten.
[35] Vgl. Art. 12 Abs. 5 DSGVO; bei offensichtlich unbegründeten oder exzessiven Anträgen kann hingegen entweder ein angemessenes Entgelt verlangt oder ein Tätigwerden verweigert werden.

5.1 INFORMATIONSPFLICHTEN

Als Verantwortlicher haben Sie die Pflicht, Landwirt*innen als (typischerweise) betroffene Personen selbstständig sämtliche Informationen nach Art. 13 und 14 DSGVO verständlich darzulegen. Die DSGVO unterscheidet im Zusammenhang dieser Informationspflicht grundlegend zwischen Fällen, in denen personenbezogene Daten unmittelbar bei der betroffenen Person selbst erhoben werden (z. B. durch den Einsatz von Agrar-Technologien und Sammlung/Generierung personenbezogener Daten direkt bei der betroffenen Landwirtin) und solchen, in denen personenbezogene Daten nicht bei der betroffenen Person selbst erhoben werden (z. B. können Daten über eine dritte Person erlangt oder aus einer Datenbank bzw. einem Profil abgerufen werden).

5.1.1 Daten werden direkt bei der betroffenen Person erhoben

Werden personenbezogene Daten direkt bei der betroffenen Person erhoben, trifft Sie als Verantwortlicher die Pflicht, der betroffenen Landwirtin folgende Informationen selbstständig vor bzw. spätestens im Zeitpunkt der Datenerhebung zukommen zu lassen:

- die Kontaktdaten des Verantwortlichen, seiner Vertreterin und – sofern ein solcher bestellt wurde – die Kontaktdaten des Datenschutzbeauftragten;
- die Zwecke der Datenverarbeitung sowie die entsprechende(n) Rechtsgrundlage(n);
- eine Nennung etwaiger dritter Datenempfänger bzw. Empfängerkategorien (z. B. Versicherungen);
- Information über die Absicht, Datenübermittlungen in ein Drittland oder an eine internationale Organisation durchzuführen samt Verweis auf geeignete bzw. angemessene Garantien;
- die Dauer der Datenspeicherung oder, sofern die Dauer selbst noch nicht abschätzbar ist, jene Kriterien, die für die Festlegung der Dauer relevant sind beispielsweise gesetzliche Aufbewahrungspflichten oder vertragliche Schadenersatz- bzw. Gewährleistungsfristen etc.;

- Informationen über bestehende Betroffenenrechte nach der DSGVO;
- eine Information über die Widerrufbarkeit einer Einwilligung in die Datenverarbeitung samt einem Hinweis, dass die Einwilligung nur ex nunc widerrufen werden kann und bis zum Widerrufszeitpunkt aufrecht bleibt; sowie
- eine Information über die Möglichkeit, eine Beschwerde bei der Datenschutzbehörde einzubringen, sofern Vorgaben der DSGVO verletzt wurden;
- Informationen über gesetzliche oder vertragliche Pflichten bzw. Notwendigkeiten der Zurverfügungstellung personenbezogener Daten durch die betroffene Person samt Aufklärung über etwaige Folgen eines Unterlassens der Zurverfügungstellung;
- Informationen über eingesetzte Systeme automatisierter Entscheidungsfindung bzw. Profiling.

Sollten Sie planen, Daten nach der erstmaligen Informationserteilung zu einem anderen als dem ursprünglich mitgeteilten bzw. vereinbarten Zweck weiterzuverarbeiten, müssen Sie die betroffene Person vor der Weiterverarbeitung auch über den neuen Zweck informieren und darüber hinaus auch alle anderen relevanten Informationen erneut erteilen.

Eine Informationspflicht besteht nach Art. 13 Abs. 4 DSGVO nicht, wenn und soweit die jeweilige Landwirtin als betroffene Person bereits über die entsprechenden Informationen verfügt (keine Doppel- oder Mehrfachinformation erforderlich).

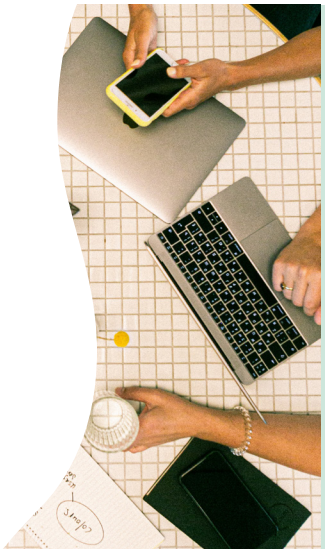
5.1.2 Daten werden nicht unmittelbar bei der betroffenen Person erhoben

Werden personenbezogene Daten nicht direkt beim Landwirt als betroffener Person erhoben (z. B. Datenerhebung über Dritte, Datenbanken, Profile etc.), sind diese nichtsdestotrotz davon in Kenntnis zu setzen. Auch in diesem Fall sind der betroffenen Person jene Informationen zukommen zu lassen, die auch im Falle der Erhebung der Daten direkt bei ihr zu erteilen wären. Zusätzlich dazu ist dem Landwirt allerdings auch offenzulegen, aus welcher Quelle die ihn betreffenden personenbezogenen Daten stammen, also wie diese erlangt wurden. Im Gegensatz zur Erhebung der personenbezogenen Daten direkt beim Landwirt muss die Informationserteilung innerhalb einer angemessenen Frist, jedoch in jedem Fall binnen eines Monats nach der Datenerlangung erfolgen.

Auch für die Datenerhebung nicht bei der betroffenen Person gilt, dass bei einer nachträglichen Änderung des Verarbeitungszweckes sämtliche relevanten Informationen erneut zu erteilen sind. Keine Informationspflicht besteht im Zusammenhang mit der Datenerlangung nicht direkt bei der betroffenen Person, wenn

- die betroffene Person bereits über sämtliche relevanten Informationen verfügt;
- die Informationserteilung unmöglich ist oder einen unverhältnismäßigen Aufwand für Sie als Verantwortlichen bedeuten würde;
- die Erlangung der Daten durch das Recht des jeweiligen Mitgliedstaates der EU bzw. durch das Recht der EU selbst vorgesehen bzw. geregelt wird; oder
- konkrete Geheimhaltungspflichten (z. B. Geschäftsgeheimnis, Berufsgeheimnis etc.) entgegenstehen.

5.2 ART. 15 DSGVO – RECHT AUF AUSKUNFT



Shortcut: Recht auf Auskunft
Betroffene Personen haben gegenüber dem Verantwortlichen das Recht, eine Auskunft darüber zu verlangen, ob sie betreffende personenbezogene Daten verarbeitet werden. Ist dies der Fall, hat der Verantwortliche der betroffenen Person weitere Informationen hinsichtlich der konkret verarbeiteten Daten zu erteilen. Die betroffene Person hat darüber hinaus das Recht auf eine Kopie der verarbeiteten Daten, wobei eine solche bei elektronischer Antragstellung in einem gängigen elektronischen Format zur erstellen ist. Im Gegensatz zum Recht auf Datenportabilität nach Art. 20 DSGVO muss die Kopie nur in einem gängigen Format (z. B. .pdf, .docx etc.) ausgefolgt werden; Strukturiertheit und Maschinenlesbarkeit der Daten ist hingegen nicht gefordert.

5.2.1 Allgemeines

Über die aktiven Informationspflichten des Verantwortlichen im Sinne der Art. 13 und 14 hinaus räumt die DSGVO betroffenen Personen ein Recht auf Auskunft ein. Das Auskunftsrecht nach Art. 15 DSGVO ist antragsbedürftig und von der jeweiligen Landwirtin geltend zu machen. Das bedeutet, dass der Verantwortliche die entsprechenden Informationen ausschließlich dann zu erteilen hat, wenn die betroffene Person einen diesbezüglichen Antrag bzw. eine darauf gerichtete Anfrage stellt.

5.2.2 Verpflichtete und Berechtigte

Das Recht auf Auskunft steht jeder natürlichen Person gegenüber jedem (potenziellen) Verantwortlichen zu, da vor einer einschlägigen Auskunft oft nicht beurteilt werden kann, ob überhaupt personenbezogene Daten verarbeitet werden. Das Auskunftsrecht nach Art. 15 DSGVO bildet daher in vielen Fällen die Grundlage für die (erfolgreiche) Gel-

tendmachung weiterer, darauf aufbauender Betroffenenrechte (z. B. Recht auf Löschung, Recht auf Datenportabilität etc.).

5.2.3 Die Auskunftserteilung und deren Inhalt

Gemäß Art. 15 Abs. 1 DSGVO haben Sie als Verantwortlicher auf Antrag bzw. Anfrage einer natürlichen Person eine Auskunft darüber zu erteilen, ob diese betreffende personenbezogene Daten verarbeitet werden, wobei bejahendenfalls auch weiterführende Informationen zu den konkret verarbeiteten Daten zu erteilen sind.

Als Verantwortlicher haben Sie das Recht und gegebenenfalls auch die Pflicht, die Identität der antragstellenden Person zu überprüfen, wenn berechtigte Zweifel daran bestehen. Dies soll vor allem dazu beitragen, eine Datenweitergabe an unbefugte Dritte und damit eine Verletzung der Vorschriften der DSGVO zu verhindern.

Ergibt eine anschließende Überprüfung, dass Sie keinerlei personenbezogene Daten der Antragstellerin verarbeiten, haben Sie dieser nichtsdestotrotz eine Negativauskunft zu erteilen, in der dieser Umstand kurz und prägnant mitgeteilt wird. Dadurch sind Sie Ihrer Auskunftspflicht bereits nachgekommen und die Rechte der Antragstellerin wurden gewahrt. Ebenso ist vorzugehen, wenn die angefragten Daten im Zeitpunkt der Antragstellung bereits gelöscht wurden.

Liegen hingegen personenbezogene Daten der antragstellenden Landwirtin vor und werden verarbeitet, hat die zu erteilende Auskunft im Sinne der Art. 15 DSGVO insbesondere folgende Informationen zu enthalten:

- den bzw. die Verarbeitungszweck(e);
- die Datenkategorie der verarbeiteten personenbezogenen Daten;
- etwaige Empfänger oder Kategorien von Empfängern der personenbezogenen Daten im Falle ihrer Offenlegung (Weiterleitung);
- die geplante Speicherdauer der Daten oder, falls die konkrete Dauer nicht eruiert werden kann, jene Kriterien, nach denen sich die Speicherdauer bestimmt;
- das Bestehen der weiterführenden Betroffenenrechte auf Löschung, auf Einschränkung der und Widerspruch gegen die Datenverarbeitung;
- Informationen über das Recht der betroffenen Person, eine Beschwerde an die Datenschutzbehörde zu erheben;
- sämtliche Informationen über die Herkunft der Daten, sofern diese nicht direkt bei der betroffenen Person erhoben werden; sowie
- Informationen über den Einsatz automatisierter Entscheidungsfindungssysteme bzw. von Profiling.

5.2.4 Voraussetzungen der Geltendmachung und Fristen

Die Geltendmachung des Auskunftsrechts ist an keinerlei Voraussetzungen geknüpft, da diese oft erst durch das Stellen eines Auskunftsbegehrens von ihrer Rolle als betroffene Person erfahren. Sofern Sie als Verantwortlicher eine große Menge an Daten verarbeiten, steht Ihnen im Falle sehr allgemein gehaltener Auskunftsanträge potenziell betroffener Personen die Möglichkeit offen, eine Präzisierung des Antrages zu verlangen. Beharrt die Betroffene allerdings auf ihrem weit formulierten Auskunftsersuchen, ist diesem vollumfänglich zu entsprechen; eine Verlängerung der Entsprechungsfrist im Sinne der Art. 12 Abs. 3 DSGVO kommt jedoch in Betracht. Die allgemeine Beantwortungsfrist beträgt einen Monat ab Eingang des Antrags und kann im erwähnten Fall umfangreicher Datenverarbeitungsvorgänge um bis zu zwei Monate verlängert werden.

5.2.5 Verweigerung der Auskunft und Kostenersatz

Gemäß Art. 12 Abs. 5 DSGVO besteht für den Verantwortlichen darüber hinaus die Möglichkeit, im Falle offenkundig unbegründeter oder exzessiver – z. B. häufig wiederholter – Antragstellung entweder ein angemessenes Entgelt für den dadurch verursachten Verwaltungsaufwand zu verlangen oder die Beantwortung der (missbräuchlich) exzessiven Anfrage zu verweigern. Die Gründe sowohl für die Auskunftsverweigerung als auch für einen etwaigen Kostenersatz sind jedoch eng auszulegen und beschränken sich in der Praxis im Wesentlichen auf die (absichtlich) „schikanöse" Rechtsausübung. Liegt eine solche nicht vor, hat die Auskunft die beantragten Informationen vollständig zu enthalten[36] und hat darüber hinaus kostenlos zu erfolgen.

5.2.6 Vorsicht beim Einsatz von Auftragsverarbeitern

Bedienen Sie sich als Verantwortlicher der Mitwirkung von Auftragsverarbeitern bzw. arbeiten Sie mit solchen zusammen, ist zu beachten, dass diese auf Grundlage der DSGVO weder zur Erfüllung des Auskunftsbegehrens noch zur Weiterleitung entsprechender Anträge an Sie verpflichtet sind. Diesbezügliche Verpflichtungen sollten daher jedenfalls in den iSd Art. 28 Abs. 3 DSGVO obligatorisch abzuschließenden Auftragsverarbeitungsvertrag aufgenommen und damit verbindlich vereinbart werden.

5.2.7 Das Recht der betroffenen Person auf eine Kopie der Daten

In Ergänzung des Auskunftsrechts gewährt Art. 15 Abs. 3 DSGVO der Landwirtin ein Recht auf Kopie aller sie betreffenden personenbezogenen Daten, die tatsächlich Gegenstand der Datenverarbeitung sind. Ein Recht auf Kopie ganzer Aktenstücke kann daraus jedoch nicht abgeleitet werden. Das bedeutet, dass nicht-personenbezogene

[36] Die Erteilung bloßer (verkürzter) „Differenzauskünfte" reicht nicht aus.

Daten sowie all jene personenbezogenen Daten, die ausschließlich von der Antragstellerin verschiedene Personen betreffen, nicht vom Recht auf Datenkopie umfasst sind und geschwärzt werden können bzw. werden müssen. Hinsichtlich der Form der Datenkopie kommt Ihnen als Verantwortlicher ein gewisser Entscheidungsspielraum zu; sofern die betroffene Person den Antrag allerdings elektronisch stellt, hat auch die Datenkopie elektronisch und in einem gängigen Format zu erfolgen. IdZ werden gängige Office-Dateiformate (wie z. B. .pdf oder .docx) ausreichen. Ein Recht des Landwirts auf eine maschinenlesbare und weiterverarbeitbare Kopie der Daten, wie sie durch das Recht auf Datenportabilität (Art. 20 DSGVO) vorgesehen ist, besteht hingegen nicht.

5.2.8 Folgen einer unrechtmäßigen Verweigerung

Landwirt*innen als betroffene Personen können zur Durchsetzung ihrer Auskunftsansprüche binnen eines Jahres ab Kenntnis des beschwerenden Ereignisses eine Beschwerde bei der Datenschutzbehörde einbringen. Diese kann einerseits die Auskunftserteilung anordnen und darüber hinaus im Falle der Feststellung einer Verletzung der DSGVO Geldbußen verhängen. Entsteht der betroffenen Person durch die Rechtsverletzung ein Schaden, kann auch ein entsprechender Schadenersatzanspruch gerichtlich geltend gemacht werden.

5.3 ART. 20 DSGVO – RECHT AUF DATENÜBERTRAGBARKEIT (DATENPORTABILITÄT)

Shortcut: Recht auf Datenportabilität
Durch das Recht auf Datenübertragbarkeit bzw. Datenportabilität wird der betroffenen Person die Möglichkeit eingeräumt, sie betreffende personenbezogene Daten, die sie dem Verantwortlichen bereitgestellt hat, herauszuverlangen und sie ohne Behinderung an einen neuen Verantwortlichen zu übertragen, sofern die Verarbeitung auf einer Einwilligung basiert oder aus der Erfüllung eines Vertrages resultiert. Zusätzlich kann die betroffene Person die direkte Übermittlung dieser bereitgestellten personenbezogenen Daten von einem Verantwortlichen an einen anderen (neuen) Verantwortlichen verlangen. Die Daten müssen dabei jeweils in einem strukturierten, gängigen und maschinenlesbaren Format bereitgestellt werden.

5.3.1 Allgemeines

Im Kern räumt Art. 20 Abs. 1 DSGVO betroffenen Personen das Recht ein, von ihnen selbst bereitgestellte Daten in einem strukturierten, gängigen und maschinenlesbaren Format vom Verantwortlichen herausverlangen zu können und diese anschließend ungehindert einem anderen Verantwortlichen zu übermitteln. Ergänzend dazu räumt Art. 20 Abs. 2 DSGVO betroffenen Personen das Recht ein, diese Daten direkt von einem Technologie-Anbieter an eine andere Technologie-Anbieterin übertragen zu lassen, ohne dass als „Zwischenschritt" eine Übertragung an die Landwirtin notwendig wird. In der Praxis spielt das Recht auf Datenportabilität eine immer gewichtigere Rolle, da aufgrund der stetig wachsenden Anzahl von Agritech-Anbieter*innen auch Anbieterwechsel immer häufiger werden.

5.3.2 Verpflichtete und Berechtigte

Als Verantwortlicher sind Sie Verpflichteter der Ansprüche nach Art. 20 DSGVO und müssen dem Antrag von Landwirt*innen als betroffenen Personen nachkommen. Wird der Antrag irrtümlich an einen Auftragsverarbeiter gerichtet, trifft diesen nach der DSGVO selbst keine ausdrückliche Pflicht, das Begehren an Sie als Verantwortlichen weiterzuleiten. Es ist daher ratsam, eine solche Verpflichtung in den obligatorisch abzuschließenden Auftragsverarbeitervertrag aufzunehmen.[37]

5.3.3 Umfang der Datenübertragung

Das Recht auf Datenportabilität erfasst ausschließlich personenbezogene Daten, die eine betroffene Person zumindest mitbetreffen; personenbezogene Daten Dritter, die keinerlei Bezug zur Antragstellerin aufweisen, können daher nicht von dieser, sehr wohl aber von der betroffenen dritten Person herausverlangt oder deren direkte Übertragung beantragt werden.

Eine weitere Grundvoraussetzung für die Ausübung des Rechts auf Datenportabilität ist, dass die Verarbeitung der personenbezogenen Daten durch den verpflichteten Verantwortlichen auf Grundlage einer Einwilligung oder in Erfüllung eines Vertrages im Sinne der Art. 6 Abs. 1 lit. a und b DSGVO erfolgt. Basiert die Datenverarbeitung auf einem oder mehreren anderen Rechtmäßigkeitstatbeständen des Art. 6 Abs. 1 DSGVO, ist diese zwar rechtmäßig, jedoch besteht kein Recht auf Datenübertragung. Da Agrar-Technologien in der landwirtschaftlichen Praxis in der Regel erworben werden und im Zuge dessen zumeist Dienstleistungsverträge abgeschlossen werden, wird eine Einwilligung bzw. ein zu erfüllender (Dienstleistungs-)Vertrag in den allermeisten dieser Fälle vorliegen.

[37] Vgl. Art. 28 Abs. 3 DSGVO.

Darüber hinaus umfasst das Datenportabilitätsrecht ausschließlich (von der betroffenen Person) „bereitgestellte" Daten. Das sind einerseits Daten, die Ihnen von der einzelnen Landwirtin wissentlich und aktiv übermittelt bzw. zur Verfügung gestellt wurden. Im Bereich der Agrar-Technologien sind daher insbesondere jene personenbezogenen (Roh-)Daten umfasst, die Ihnen die Landwirtin im Rahmen des Erwerbs der Technologie bzw. im Zeitpunkt des Abschlusses des Dienstleistungsvertrages aktiv zur Verfügung gestellt hat. Zusätzlich sollen aber auch solche personenbezogenen Daten erfasst sein, die durch die Nutzung eines entsprechenden Dienstes (z. B. GPS-Steuerung, Drohnen-Luftbilder, Boden- oder Tiersensordaten etc.), also durch sogenannte „Beobachtung", im Rahmen des Einsatzes der Technologie generiert werden. Dabei muss das einzelne erhobene Datum zumindest in irgendeiner Weise auf die Initiative der betroffenen Person zurückzuführen sein. Dies wird gerade im landwirtschaftlichen Kontext regelmäßig der Fall sein, da die Anwendung der jeweiligen Agrar-Technologien und die Auswertung der zur Verfügung gestellten Daten durch Sie als Agritech-Anbieter im Regelfall auf Grundlage eines Dienstleistungsvertrages (= Anweisung und damit Initiative der betroffenen Person) durchgeführt werden.

Vom Recht auf Datenübertragbarkeit erfasst sind daher zuallermeist Rohdaten. Nicht erfasst sind hingegen jene Daten, die durch die (Weiter-)Verarbeitung bzw. Auswertung der zur Verfügung gestellten Rohdaten generiert oder aus ihnen abgeleitet werden (z. B. Analysen, Statistiken, Pläne, Karteien etc.). Das Ergebnis der Dienstleistung des Verantwortlichen, das zumeist gerade in der Auswertung der zuvor erhobenen Rohdaten besteht, fällt daher nicht unter das Datenportabilitätsrecht; diese personenbezogenen Daten verbleiben daher beim bisherigen Verantwortlichen und sind, sofern kein Rechtmäßigkeitsgrund nach Art. 6 DSGVO (mehr) für ihre weitere Verarbeitung vorliegt, allenfalls aufgrund eines entsprechenden Löschungsbegehrens zu löschen. Obgleich ein Übertragungsrecht hinsichtlich solcher Daten nicht aus der DSGVO abgeleitet werden kann, kann ein solches vertraglich frei vereinbart werden. In diesem Fall würde sich das Datenportabilitätsrecht unmittelbar aus dem Dienstleistungsvertrag ableiten.

5.3.4 Geltendmachung und Fristen

Wie auch das Recht auf Auskunft (Art. 15 DSGVO) oder das Recht auf Löschung (Art. 17 DSGVO) muss das Recht auf Datenportabilität durch einen Antrag seitens der Landwirtin als betroffener Person aktiv geltend gemacht werden. Eine eigenmächtige Übertragung der Daten ohne eine entsprechende Vereinbarung mit bzw. nach Zustimmung oder auf Antrag der betroffenen Person würde gegen den Grundsatz der Zweckbindung der Datenverarbeitung verstoßen und wäre damit als rechtswidrig anzusehen.

Die Frist zur Durchführung der Datenübertragung beträgt einen Monat ab Eingang des Antrages und kann in Ausnahmefällen um bis zu zwei Monate verlängert werden. Die Erfüllung dieser Verpflichtung hat im Regelfall kostenlos zu erfolgen. Im Falle der offenkundig unbegründeten oder exzessiven Antragstellung kann die Übertragung verweigert oder ein angemessenes Entgelt dafür verlangt werden. [38]

5.3.5 Strukturiertes, gängiges und maschinenlesbares Format

Gemäß Art. 20 Abs. 1 DSGVO haben Sie als Technologie-Anbieter der Landwirtin als betroffener Person auf ihren Antrag hin sämtliche von ihr bereitgestellten personenbezogenen Daten in einem strukturierten, gängigen und maschinenlesbaren Format zur Verfügung zu stellen bzw. die Daten in einem solchen Format an einen bekanntgegebenen Dritten direkt zu übertragen.[39] Unter der Wendung des „strukturierten, gängigen und maschinenlesbaren" Formates ist eine Datenübertragung zwischen unterschiedlichen Systemen zu verstehen, ohne dass die Anwenderin bzw. Nutzerin des Systems hierfür spezielle Kenntnisse benötigt. Dies erfordert ein interoperables Format, wobei aktuell wohl Datenformate wie z. B. XML, JSON und CSV diese Kriterien erfüllen sollten. Das Recht auf Datenportabilität der betroffenen Person vermittelt dabei nur die Pflicht des Verantwortlichen, die Daten in „einem" solchen Format zu übertragen. Sofern allerdings mehrere am Markt verfügbare Formate die Kriterien der Strukturiertheit, Gängigkeit und Maschinenlesbarkeit erfüllen, trifft den Verantwortlichen keine Pflicht, die Daten in sämtlichen dieser Formate bereitzuhalten und zu übertragen. Ist das Format der Daten daher objektiv als strukturiert, gängig und maschinenlesbar zu qualifizieren, erfüllt die jeweilige Agritech-Anbieterin mit der Übertragung dieser Daten ihre aus Art. 20 Abs.1 bzw. 2 DSGVO entspringende Pflicht. Ob die neue, von der betroffenen Person ausgewählte Agritech-Anbieterin dieses Format auch tatsächlich verarbeiten kann, ist für die Pflichterfüllung der Altanbieterin hingegen nicht von Relevanz. Auch der Wunsch der Landwirtin als betroffener Person nach der Datenübertragung in einem ganz bestimmten strukturierten, gängigen und maschinenlesbaren Format kann, muss aber nicht erfüllt werden. Vorsicht ist allerdings geboten, wenn die Datenverarbeitung unter Verwendung eines speziell bzw. eigens entwickelten Datenformats erfolgt, das von keinem anderen Unternehmen verarbeitet werden kann. Sollten in einem solchen Fall strukturierte, gängige und maschinenlesbare Formate am Markt verfügbar sein und diese trotz bestehender Möglichkeit dazu – aufgrund von Technologie-Protektionismus – nicht verwendet werden und die Datenübertragung deshalb scheitern, wäre Art. 20 DSGVO als verletzt anzusehen und der betroffenen Person würden die entsprechenden Rechtsmittel offenstehen. Daher ist vom Einsatz von Monopolisierungsstrategien bzw. insbesondere von der Entwicklung spezieller Datenformate, die eine Verarbeitung bzw. ein Auslesen durch Konkurrenzanbieter offensichtlich erschweren oder verunmöglichen sollen, abzuraten.

[38] Siehe dazu näher unter Punkt 5.2.5.
[39] Vgl. Art. 20 Abs. 1 und 2 DSGVO.

5.3.6 Verweigerung des Datenübertragungsbegehrens

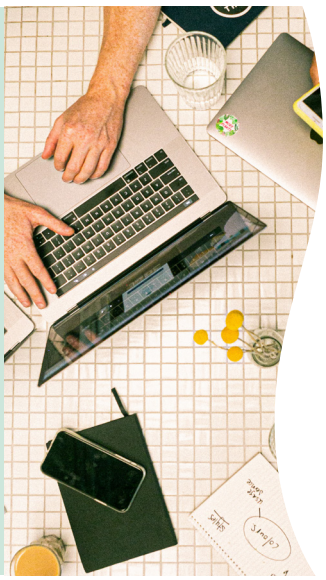
Datenübertragungsbegehren betroffener Personen können nur aus äußerst eingeschränkten Gründen verweigert werden. Diesbezüglich legt Art. 20 Abs. 4 DSGVO fest, dass durch die Ausübung des Rechts auf Datenportabilität die Rechte und Freiheiten anderer Personen nicht gefährdet werden dürfen. Kann eine solche Gefährdung nicht ausgeschlossen werden, darf die Datenübertragung nicht erfolgen. Rechte und Freiheiten Dritter können dabei sowohl Rechte im Sinne der DSGVO als auch Betriebs- und/oder Geschäftsgeheimnisse sein.Ganz allgemein kann eine Datenübertragung nach Art. 12 Abs. 5 DSGVO dann verweigert werden, wenn diesbezügliche Anträge offenkundig unbegründet oder exzessiv gestellt werden.[40]

5.3.7 Folgen einer unrechtmäßigen Verweigerung

Im Falle einer Verletzung des Rechts auf Datenübertragbarkeit nach Art. 20 DSGVO steht der Landwirtin binnen eines Jahres ab Kenntnis des beschwerenden Ereignisses (z. B. Verweigerung der Datenübertragung) die Erhebung einer Beschwerde an die Datenschutzbehörde offen. Diese kann – sofern die Voraussetzungen dafür vorliegen – die Datenübertragung anordnen und Geldbußen verhängen.[41] Sofern der betroffenen Person durch die Verweigerung der Datenübertragung ein Schaden entsteht, kann sie dessen Ersatz weiters potenziell im Wege einer Schadenersatzklage geltend machen.[42]

5.4 Art. 17 DSGVO – Recht auf Löschung

Shortcut: Recht auf Löschung
Betroffene Personen haben gegenüber dem jeweils Verantwortlichen das Recht, sie betreffende personenbezogene Daten dauerhaft und unwiederbringlich löschen zu lassen. Eine Löschung ist ausschließlich dann verpflichtend durchzuführen, wenn die betroffene Person einen entsprechenden Antrag an den Verantwortlichen stellt und zumindest einer der Löschungstatbestände des Art. 17 Abs. 1 DSGVO zum Zeitpunkt der Antragstellung erfüllt ist. Ausnahmen von der Löschungsverpflichtung bestehen nur aus bestimmten Gründen, z. B. wenn die Datenverarbeitung zur Erfüllung einer rechtlichen Verpflichtung des nationalen Rechts oder des Unionsrechts erforderlich ist.



[40] Siehe sinngemäß dazu näher unter Punkt 4.2.4.
[41] Siehe Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1, 4 DSG; Art. 83 DSGVO.
[42] Vgl. Art. 82 DSGVO und § 29 DSG.

5.4.1 Allgemeines

Das Recht auf Löschung versetzt die betroffene Person in die Position, die nicht DSGVO-konforme Verarbeitung personenbezogener Daten aktiv zu unterbinden und die rechtswidrig verarbeiteten Daten bzw. die Ergebnisse solcher Datenverarbeitungsvorgänge beim jeweiligen Verantwortlichen dauerhaft entfernen zu lassen. Dadurch soll insbesondere sichergestellt werden, dass rechtswidrig verarbeitete personenbezogene Daten bei jenen Personen oder Einrichtungen, die dafür verantwortlich sind, weiterhin gespeichert und einer weiteren (rechtswidrigen) Verarbeitung zugänglich bleiben. Die betroffene Person soll durch das Recht auf Löschung in die Lage versetzt werden, unter den entsprechenden Voraussetzungen selbst darüber entscheiden zu können, welche der sie betreffenden personenbezogenen Daten von wem (weiter-)verarbeitet werden. Art. 17 Abs. 1 DSGVO enthält diesbezüglich mehrere Löschungstatbestände. Eine Löschung personenbezogener Daten ist ausschließlich im Falle des Vorliegens zumindest eines dieser Gründe vorzunehmen.[43] Die einzelnen Löschungsgründe werden unter Punkt 5.4.4 näher behandelt.

5.4.1 Verpflichtete und Berechtigte

Als Verantwortlicher sind Sie gemäß Art. 17 Abs. 1 DSGVO bei Vorliegen der darin geregelten Voraussetzungen dazu verpflichtet, auf Antrag einer betroffenen Person (zumeist Landwirt*innen) die sie (mit-)betreffenden personenbezogenen Daten dauerhaft zu löschen. Wird der Antrag von der betroffenen Person irrtümlich an einen Auftragsverarbeiter gerichtet, trifft diesen nach der DSGVO keine explizite Pflicht, das Begehren an Sie als Verantwortlichen weiterzuleiten. Es ist daher anzuraten, eine solche Verpflichtung in den obligatorisch abzuschließenden Auftragsverarbeitervertrag aufzunehmen.

5.4.2 Voraussetzungen der Geltendmachung und Fristen

Der Antrag kann durch die betroffene Person formlos gestellt werden, jedoch muss das Vorliegen eines konkreten Löschungstatbestandes gemäß Art. 17 Abs. 1 DSGVO vorgebracht werden.[44] Am häufigsten werden im Rahmen der digitalen Landwirtschaft wohl der Löschungsgrund des Zweckwegfalls- bzw. der Zweckänderung sowie jener des Widerrufs der Einwilligung (beispielsweise aufgrund der Kündigung des Dienstleistungsvertrages im Zusammenhang mit einem Anbieter*innenwechsel) vorliegen.

Die Beantwortungs- bzw. Entsprechungsfrist beträgt einen Monat ab Eingang des Löschungsgesuches und kann in Ausnahmefällen um bis zu zwei Monate verlängert werden. Die Löschung hat im Regelfall kostenlos zu erfolgen; nur bei offenkundig unbegründeter oder exzessiver Rechtsausübung kann ein angemessenes Entgelt verlangt oder die Löschung verweigert werden. [45]

[43] Vgl. Art. 17 Abs. 1 lit. a-f DSGVO.
[44] Siehe dazu näher unter Punkt 4.4.1.
[45] Vgl. Art. 12 Abs. 5 DSGVO.

5.4.3 Die Mitteilungspflicht

Wurde die beantragte Löschung erfolgreich durchgeführt, haben Sie die betroffene Person darüber schriftlich und in einfacher, transparenter und verständlicher Form in Kenntnis zu setzen. Ebenso ist die betroffene Person im Fall eines negativen Ergebnisses, also einer Ablehnung des Antrags auf Löschung, darüber zu informieren.

Haben Sie die betroffenen personenbezogenen Daten dritten Empfänger*innen offengelegt, ist die Löschung der Daten auch diesen Personen mitzuteilen.[46] Gleichzeitig ist die antragstellende betroffene Person über sämtliche dritte Datenempfänger zu informieren, sofern sie dies in ihrem Antrag verlangt. Ist eine Information der Dritten unmöglich oder mit einem unverhältnismäßigen Aufwand verbunden, kann die Drittinformation auch unterbleiben.

Sofern Sie die personenbezogenen Daten öffentlich gemacht haben, trifft Sie darüber hinaus auch die Verpflichtung, sämtliche weiteren Verantwortlichen, die die zu löschenden Daten verarbeiten, von der Löschung selbst als auch davon zu verständigen, dass die betroffene Person auch die Löschung aller Links zu den personenbezogenen Daten sowie aller Datenkopien verlangt hat. Eine Ausnahme von dieser Informationspflicht besteht nur dann, wenn die Information sämtlicher Beteiligten für Sie unmöglich oder mit einem unverhältnismäßig hohen Aufwand verbunden wäre. Begehrt die betroffene Person die Auskunft über die Namen der informierten Verantwortlichen, ist auch diesem Ersuchen nachzukommen.[47]

5.4.4 Die Löschungsgründe

Personenbezogene Daten der Landwirtin (= betroffene Person) als Antragstellerin sind nach Art. 17 Abs. 1 DSGVO unverzüglich und unwiederbringlich zu löschen, wenn

- die verarbeiteten personenbezogenen Daten für jene Zwecke, für die sie ursprünglich erhoben oder verarbeitet wurden, nicht mehr gegeben sind und auch kein neuer bzw. anderer Zweck zwischen Verantwortlichem und betroffener Person vereinbart wurde. Liegen mehrere Verarbeitungszwecke vor, müssen sämtliche dieser Zwecke wegfallen, damit die Daten verpflichtend zu löschen sind.
- die Landwirtin als betroffene Person ihre Einwilligung in die Datenverarbeitung widerruft und diese auch auf keinen anderen Rechtmäßigkeitsgrund im Sinne der Art. 6 Abs. 1 DSGVO gestützt werden kann.
- nach Art. 21 Abs. 1 DSGVO unter den dort genannten Voraussetzungen durch die betroffene Person Widerspruch gegen die Datenverarbeitung eingelegt wurde und

[46] Vgl. Art. 19 DSGVO.
[47] Vgl. Art. 17 Abs. 2 DSGVO („Recht auf Vergessenwerden").

keine vorrangigen berechtigten Gründe für die (weitere) Verarbeitung vorliegen oder durch die betroffene Person Widerspruch gegen die Datenverarbeitung nach Art. 21 Abs. 2 DSGVO erhoben wurde.

- die Verarbeitung der personenbezogenen Daten unrechtmäßig erfolgt, wobei sämtliche Verstöße gegen die DSGVO und deren Verarbeitungsgrundsätze zu berücksichtigen sind.
- nationale Rechtsvorschriften oder solche der EU eine rechtliche Verpflichtung des Verantwortlichen zur Löschung der Daten vorsehen.
- die verarbeiteten personenbezogenen Daten in Bezug auf angebotene Dienste einer Informationsgesellschaft nach Art. 8 DSGVO (betrifft die Einwilligung von Kindern in die Verarbeitung personenbezogener Daten) erhoben wurden.

Der Zweck der Datenverarbeitung wird üblicherweise im Rahmen des Erwerbs einer konkreten Agrar-Technologie im Dienstleistungsvertrag festgelegt, wobei die Festlegung sehr allgemeiner Zwecke (z. B. zur Verbesserung der Kundenerfahrung) unzulässig ist. Eine konkrete Benennung des Verarbeitungszwecks ist zwingend erforderlich (= Grundsatz der Zweckbindung). Wird der Datenverarbeitungszweck erreicht oder werden bestimmte personenbezogene Agrardaten nicht (mehr) für die Zweckerfüllung benötigt, sind diese grundsätzlich unverzüglich zu löschen. Der Löschungsgrund des Zweckwegfalls kommt allerdings nur dann zur Anwendung, wenn kein anderer legitimer Verarbeitungszweck mehr vorliegt. Wird die Datenverarbeitung auf mehrere Verarbeitungszwecke gestützt, müssen daher sämtliche Zwecke wegfallen, damit eine Löschung durchzuführen ist.

Hinsichtlich des praxisrelevanten Löschungsgrundes der rechtswidrigen Datenverarbeitung ist zu beachten, dass die Rechtswidrigkeit, auf die sich der Löschungsanspruch stützt, im Zeitpunkt der Beantragung der Löschung durch den Betroffenen noch vorliegen muss. Rechtswidrigkeiten, die eine Datenlöschung rechtfertigen, können sich insbesondere aus Verstößen gegen die Art. 5, 6 und 9 DSGVO ergeben. Darüber hinaus kommen aufgrund der offenen Formulierung der Bestimmung auch andere Rechtswidrigkeiten der Datenverarbeitung, die über die DSGVO hinausgehen (z. B. in Materiengesetzen begründete Verpflichtungen), als Grund für einen Löschungsanspruch infrage.

5.4.5 Inhalt der Löschungsverpflichtung

Als Verantwortlicher haben Sie die Verpflichtung, die betreffenden Daten unwiderruflich zu löschen, was aber nicht mit der endgültigen Zerstörung der Daten bzw. der Datenträger gleichzusetzen ist. Dem Löschungsanspruch der betroffenen Person kann beispielsweise auch durch eine unumkehrbare Anonymisierung der Daten entsprochen werden. Zur Anonymisierung und den damit zusammenhängenden Problemstellungen siehe oben unter Punkt 3.

5.4.6 Verweigerung der Datenlöschung

Die Verweigerung des Begehrens darf grundsätzlich nur im allgemeinen Fall des Art. 12 Abs. 5 DSGVO (offenkundig unbegründete oder exzessive Rechtsausübung) sowie bei fehlender Erfüllung von Löschungstatbeständen erfolgen.
Darüber hinaus soll das Recht auf Löschung gemäß Art. 17 Abs. 3 DSGVO nicht bestehen, wenn die weitere Datenverarbeitung z. B. erforderlich ist

- zur Ausübung des Rechts auf freie Meinungsäußerung und Information,
- zur Erfüllung einer rechtlichen Verpflichtung, für die die weitere Datenverarbeitung erforderlich ist (z. B. steuerrechtliche Aufbewahrungspflichten),
- für im öffentlichen Interesse liegende Archivzwecke, wissenschaftliche oder statistische Zwecke, oder
- zur Verteidigung von Rechtsansprüchen (z. B. ausstehende Zahlungen der betroffenen Person).

5.4.7 Folgen einer unrechtmäßigen Verweigerung

Im Falle einer Verletzung des Rechts auf Löschung nach Art. 17 DSGVO steht der Landwirtin als betroffener Person binnen eines Jahres ab Kenntnis des beschwerenden Ereignisses (z. B. Verweigerung der Datenübertragung) die Erhebung einer Beschwerde an die Datenschutzbehörde offen. Diese kann – sofern die Voraussetzungen dafür vorliegen – die Datenübertragung anordnen und Geldbußen verhängen.[48] Sofern der betroffenen Person durch die Verweigerung der Datenübertragung ein Schaden entsteht, kann sie dessen Ersatz weiters potenziell im Wege einer Schadenersatzklage gegen den jeweils Verantwortlichen geltend machen.[49]

6. ALLGEMEINE RECHTSFOLGEN EINER VERLETZUNG DER DSGVO

Verletzen Sie als Verantwortlicher allgemeine oder konkrete Verpflichtungen im Sinne der DSGVO, steht der betroffenen Person grundsätzlich die Möglichkeit der Erhebung einer Beschwerde an die Datenschutzbehörde (DSB) offen.[50] Sofern die Beschwerde berechtigt ist, hat die Datenschutzbehörde Ihnen als Verantwortlichem die Beseitigung der Rechtsverletzung bescheidmäßig aufzutragen.[51] Darüber hinaus drohen bei schwerwiegender Verletzung von Vorgaben der DSGVO bzw. Rechten der betroffenen Person Geldbußen in der Höhe bis zu 20 Millionen Euro oder 4% des Jahresumsatzes.[52] Ebenso kann die betroffene Person bei Vorliegen der Voraussetzungen im Einzelfall potenziell Schadenersatzansprüche geltend machen, wobei dazu primär ein konkret entstandener materieller oder immaterieller Schaden nachzuweisen ist.[53]

[48] Siehe Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1, 4 DSG; Art. 83 DSGVO.
[49] Vgl. Art. 82 DSGVO und § 29 DSG.
[50] Vgl. Art. 77 DSGVO iVm § 24 Abs. 1 und 4 DSG.
[51] Vgl. § 24 Abs. 5 und § 26 Abs. 4 DSG. Gilt nur für Verantwortliche des privaten Bereichs. Bei Verantwortlichen des öffentlichen Bereichs hat die Datenschutzbehörde die jeweilige Rechtsverletzung lediglich mit Bescheid festzustellen; siehe § 26 Abs. 1 DSG.
[52] Vgl. Art. 83 Abs. 5 lit. b DSGVO.
[53] Vgl. Art. 82 DSGVO iVm § 29 DSG.

VERWEISE

[1] Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG (Datenschutz-Grundverordnung), Abl L 2016/119, 1 (folgend kurz DSGVO).

[2] Der gegenständliche Leitfaden soll einen allgemeinen Überblick über die wichtigsten Rechte und Pflichten der DSGVO insbesondere im landwirtschaftlichen Kontext bieten. Es ist daher darauf hinzuweisen, dass der gegenständliche Leitfaden keinen Anspruch auf Vollständigkeit oder Aktualität erhebt und die entsprechenden Ausführungen immer im konkreten Einzelfall zu prüfen sind.

[3] Zum sachlichen Anwendungsbereich siehe sogleich unter Punkt 1.2.

[4] Art. 3 Abs. 1 DSGVO.

[5] Art. 3 Abs. 2 DSGVO.

[6] Art. 2 Abs. 1 DSGVO. Darüber hinaus ist die DSGVO auch auf die nicht automatisierte Verarbeitung personenbezogener Daten anwendbar, wenn die Daten in einem Dateisystem gespeichert sind oder in einem solchen gespeichert werden sollen (z. B. Karteisystem oder analoge Datenbank). Da sich der gegenständliche Leitfaden auf das Agrar-Datenschutzrecht in Zusammenhang mit digitalen Agrar-Technologien bezieht, ist diese Option für die sachliche Anwendbarkeit der DSGVO nicht einschlägig, weshalb in weiterer Folge nicht näher darauf eingegangen wird.

[7] Dies umfasst beispielsweise Tiersensor-Daten im gleichen Maße wie GPS-Daten selbstfahrender Landmaschinen oder Luftbildaufnahmen von mit Spektralkameras ausgestatteten Agrar-Drohnen.

[8] Siehe Art. 4 Z 1 DSVO (Hervorhebungen durch Verfasser).

[9] Siehe ErwGr 26 dritter Satz DSGVO.

[10] Auch bei Maschinendaten ist jedoch Vorsicht geboten, da diese unter Umständen Rückschlüsse auf die Arbeitstätigkeit oder den (sorglosen bzw. sorgsamen) Umgang mit den Maschinen durch Arbeitnehmer*innen oder dritte Personen zulassen.

[11] Stichwort: Schleichender Personenbezug.

[12] Vgl. Art. 4 Z 7 DSGVO.

[13] Vgl. Art. 4 Z 8 DSGVO.

[14] Stichwort: Erhöhung des Datenschutzstandards.

[15] Siehe dazu insbesondere Art. 25 und Art. 32 Abs. 1 lit. a DSGVO.

[16] Siehe Art. 24 ff DSGVO.

[17] Vgl. Art. 37 Abs. 1 DSGVO.

[18] Kerntätigkeit ist im Sinne von „Haupttätigkeit" zu verstehen und meint z. B. nicht die Datenverarbeitung als Nebentätigkeit.; siehe dazu ErwGr 97 DSGVO.

[19] Eine solche Kerntätigkeit liegt jedenfalls vor, wenn Ihr Unternehmens- bzw. Produktzweck in der Analyse oder Bereitstellung von digitalen Inhalten liegt (z. B, FIMS, Tiersensorik etc.)

[20] Zu denken ist dabei insbesondere an Technologien, bei denen es zu Profilbildungen bzw. kontinuierlicher Überwachung von Vorgängen im landwirtschaftlichen Betrieb kommt.

[21] Vgl. Art. 39 Abs. 1 DSGVO.

[22] Beispielsweise durch den Einsatz von Backup-Servern und regelmäßiger Zwischenspeicherung der Daten.

[23] Vgl. Art. 35 Abs. 1 DSGVO.

[24] Siehe Verordnung der Datenschutzbehörde über Verarbeitungsvorgänge, für die eine Datenschutzfolgenabschätzung durchzuführen ist (DSFA-V), BGBl II 278/2018.

[25] Siehe Verordnung der Datenschutzbehörde über die Ausnahmen von der Datenschutzfolgenabschätzung (DSFA-AV), BGBl II 108/2018.

[26] Vgl. Art. 58 DSGVO.

[27] Detaillierte Vorgaben zur Führung eines Verarbeitungsverzeichnisses enthält Art. 30 DSGVO.

[28] Vgl. Art. 33 Abs. 2 DSGVO.

[29] Als Hilfestellung zur Geltendmachung der Betroffenenrechte siehe: https://www.dsb.gv.at/download-links/dokumente.html.

[30] Siehe Art. 13 und 14 DSGVO.

[31] Siehe Art. 15 bis 22 und Art. 34 DSGVO.

[32] Vgl. Art. 12 Abs. 1 DSGVO.

[33] Vgl. Art. 12 Abs. 2 DSGVO.

[34] Vgl. Art. 12 Abs. 3 DSGVO; nach Art. 12 Abs. 4 DSGVO hat der Verantwortliche die betroffene Person innerhalb eines Monats ab Antragseingang über ein etwaiges Nicht-Tätigwerden zu unterrichten.

[35] Vgl. Art. 12 Abs. 5 DSGVO; bei offensichtlich unbegründeten oder exzessiven Anträgen kann hingegen entweder ein angemessenes Entgelt verlangt oder ein Tätigwerden verweigert werden.

[36] Die Erteilung bloßer (verkürzter) „Differenzauskünfte" reicht nicht aus

[37] Vgl. Art. 28 Abs. 3 DSGVO.

[38] Siehe dazu näher unter Punkt 5.2.5.

[39] Vgl. Art. 20 Abs. 1 und 2 DSGVO.

[40] Siehe sinngemäß dazu näher unter Punkt 4.2.4.

[41] Siehe Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1, 4 DSG; Art. 83 DSGVO.

[42] Vgl. Art. 82 DSGVO und § 29 DSG.

[43] Vgl. Art. 17 Abs. 1 lit. a-f DSGVO.

[44] Siehe dazu näher unter Punkt 4.4.1.

[45] Vgl. Art. 12 Abs. 5 DSGVO.

[46] Vgl. Art. 19 DSGVO.

[47] Vgl. Art. 17 Abs. 2 DSGVO („Recht auf Vergessenwerden").

[48] Siehe Art. 77 Abs. 1 DSGVO iVm § 24 Abs. 1, 4 DSG; Art. 83 DSGVO.

[49] Vgl. Art. 82 DSGVO und § 29 DSG.

[50] Vgl. Art. 77 DSGVO iVm § 24 Abs. 1 und 4 DSG.

[51] Vgl. § 24 Abs. 5 und § 26 Abs. 4 DSG. Gilt nur für Verantwortliche des privaten Bereichs. Bei Verantwortlichen des öffentlichen Bereichs hat die Datenschutzbehörde die jeweilige Rechtsverletzung lediglich mit Bescheid festzustellen; siehe § 26 Abs. 1 DSG.

[52] Vgl. Art. 83 Abs. 5 lit. b DSGVO.

[53] Vgl. Art. 82 DSGVO iVm § 29 DSG.

Ländliches Fortbildungsinstitut (LFI) Österreich

Schauflergasse 6
1015 Wien

01/534 41-8566
01/534 41-5869
lfi@lk-oe.at
www.lfi.at

Ihr Wissen wächst