Datenschutz im Wald

Die EU-Datenschutz-Grundverordnung – kurz: DSGVO – gilt seit gut einem Jahr als europaweit zwingendes Recht. Unternehmen, die personenbezogene Daten verarbeiten, sind seitdem rechenschaftspflichtig und müssen die Einhaltung der datenschutzrechtlichen Vorschriften den Behörden gegenüber jederzeit nachweisen können. Auch die nunmehr um ein Vielfaches höheren Bußgelder bei Verstößen gegen die DSGVO beunruhigen viele Unternehmen. Diese Entwicklung macht auch vor Forstwirtschaftlichen Zusammenschlüssen nicht halt. Welche konkreten Pflichten sieht die DSGVO hier vor und wie können diese umgesetzt werden?

Gero Wilke, Malte Viergutz

Die Verarbeitung personenbezogener Daten ist allgegenwärtig. Auch bei Forstwirtschaftlichen Zusammenschlüssen (FWZ) fallen eine Vielzahl von Verarbeitungsvorgängen an, die datenschutzrelevant sind. Dies betrifft zum einen Mitgliederdaten wie Name, Anschrift und Kontaktdaten, aber auch alle sonstigen Daten, die einem bestimmten Mitglied zugeordnet werden können. Zum anderen können externe personenbezogene Daten wie z. B. von Mitarbeitern, Kunden, beauftragten Forstunternehmen und deren Mitarbeitern oder sonstigen Dienstleistern betroffen sein. Die datenschutzrechtlichen Pflichten treffen daher alle FWZ, unabhängig von Größe, Rechtsform oder technischer Ausstattung. Während der Datenschutz vor Inkrafttreten der DSGVO im Mai 2018 wenig bis keine Beachtung fand, kehrte es sich seither ins Gegenteil, mitunter mit fast hysterischen Zügen. Dabei ist ein angemessener, besonnener Umgang mit den Daten und den diesbezüglichen Pflichten für alle Unternehmen – und alle FWZ – mit machbarem Einsatz zu leisten. Zumal nicht jede gesetzliche Pflicht auch von jedem FWZ zu erfüllen ist.

Die Benennung eines (externen) Datenschutzbeauftragten ist grundsätzlich beispielsweise nur für solche FWZ verpflichtend, bei denen mindestens zehn Personen mit der Verarbeitung personenbezogener Daten befasst sind. Etwas anderes gilt nur für FWZ, die als Körperschaft des öffentlichen Rechts organisiert sind und daher nach dem deutschen Bundesdatenschutzgesetz (BDSG) stets einen Datenschutzbeauftragten bestellen müssen. Dessen Aufgabe ist die Überwachung und Koordination aller Datenschutzmaßnahmen in der FWZ. Zugleich ist er die zentrale Anlaufstelle für Betroffene, Aufsichtsbehörden, Mitarbeiter und für die Leitung der FWZ in datenschutzrechtlichen Belangen. Datenschutzbeauftragte sind daher auch für solche FWZ eine Überlegung wert, die nicht gesetzlich zur Bestellung verpflichtet sind.

Relevant für alle FWZ, die einen eigenen Internetauftritt vorhalten, ist eine Datenschutzerklärung. Wie das Impressum gehört diese zu den Kernpflichten eines Internetauftritts. Auch wenn die gefürchtete Abmahnwelle weitgehend ausgeblieben ist, besteht hier unbedingter Handlungsbedarf. Online gibt es zahlreiche Hilfestellungen und Datenschutzgeneratoren, von simpel und kostenlos bis kostenpflichtig, dauerhaft automatisch aktualisiert und mit Abmahnkostenschutz. Die Umsetzung ist meist innerhalb weniger Minuten erledigt.

Schneller Überblick

- Datenschutzrechtliche Pflichten treffen auch die FWZ
- Verpflichtend ist u. a. das Führen eines Verfahrensverzeichnisses sowie einer Liste technischer und organisatorischer Maßnahmen (TOM)
- Notwendig sind interne Richtlinien zum Umgang mit E-Mail, Home-Office und Social Media
- Wenn personenbezogene Daten ausgetauscht werden, müssen Auftragsverarbeitungsverträge (AVV) geschlossen werden
- Fazit: Datenschutz für FWZ ist machbar, Hilfestellungen sind verfügbar, die Umsetzung ist rechtlich verpflichtend

Pflicht: Verfahrensverzeichnis

Verpflichtend für ausnahmslos alle FWZ ist das Verzeichnis aller Verarbeitungstätigkeiten (Verfahrensverzeichnis). Dieses zwingend digital zu führende Verzeichnis beinhaltet eine systematische Auflistung aller Prozesse, bei denen personenbezogene Daten verarbeitet werden, vom Umgang mit etwaigen Bewerbungen über die Lohnbuchhaltung für Mitarbeiter bis hin zum Umgang mit Kundendaten. Anzugeben sind der jeweilige Zweck der Datenverarbeitung, die Betroffenen, die Empfänger der Daten, Löschfristen und einiges mehr. Muster dieser Verzeichnisse stellen zahlreiche Landesdatenschutzbehörden zur Verfügung [1].

Zum sogenannten Datenschutzmanagement gehört neben dem Verfahrensverzeichnis zwingend auch immer eine Auflistung aller technischen und organisatorischen Maßnahmen (TOM). Es gilt nachzuweisen, welche Maßnahmen seitens der FWZ ergriffen werden, um personenbezogene Daten vor Missbrauch, unbefugter Veröffentlichung, Löschung etc. zu schützen. Wie der Name schon sagt, beinhaltet diese Auflistung sowohl technische Maßnahmen wie Passwortschutz, Verschlüsselung und Anonymisierung als auch organisatorische Maßnahmen wie Festlegungen der Zugriffsrechte, Weisungen oder Notfallkonzepte.

Interne Richtlinien für Mitarbeiter

Vervollständigt wird das Datenschutzmanagement durch interne Richtlinien für Mitarbeiter und die FWZ selbst. Hier sind für FWZ vor allem Regelungen zur Nutzung von E-Mail, Social Media sowie Home-Office bzw. Mobile-Office und Fernwartungen/Fernzugriff relevant. Häufig bringt auch die Nutzung von eigenen Geräten der Mitarbeiter (bring your own device, byod) datenschutzrechtliche Probleme für die FWZ mit sich, da personenbezogene Daten der FWZ hierdurch ihrer Kontrolle entzogen werden können. Auch

DSGVO im Projekt KomSilva

In dem Projekt KomSilva („Entwicklung und Einsatz von Kommunikations- und Beratungshilfen für den Privat- und Kommunalwald zur Waldbesitzeransprache und zur Intensivierung der forstlichen Öffentlichkeitsarbeit") werden zahlreiche Kommunikationskanäle für FWZ getestet. Durch diese Technologien werden immer auch personenbezogene Daten gewonnen und verarbeitet. Damit unterstehen auch FWZ den Regelungen der DSGVO.

KomSilva ist ein mit Mitteln des Bundesministeriums für Ernährung und Landwirtschaft aufgrund eines Beschlusses des Deutschen Bundestages finanziertes Projektvorhaben (FKZ: 22011917). In dem Projektkonsortium arbeiten das KWF, UNIQUE, Cluster Forst und Holz Bayern und die Technische Universität München zusammen.

sollten (zumindest bei größeren FWZ) die Zuständigkeiten und Verantwortlichkeiten für bestimmte Datenverarbeitungen (und die damit einhergehenden Fragestellungen) klar geregelt werden. Hierunter fällt auch, wie mit Datenschutzanfragen umgegangen wird (gesetzliche Frist zur Beantwortung: 1 Monat) und vor allem, wie bei Datenschutzverstößen reagiert wird (gesetzliche Frist: 72 Stunden!). Dass es sich vor allem bei Letzterem (leider) nicht nur um eine hypothetische Fragestellung handelt, wird deutlich, wenn man sich vor Augen führt, dass bereits der Versand einer E-Mail mit offenem Verteiler (cc statt bcc) einen solchen Verstoß darstellen kann.

Auftragsverarbeitungsverträge

Auf vertraglicher Ebene müssen FWZ extern sogenannte Auftragsverarbeitungsverträge (AVV) mit allen Firmen schließen, mit denen personenbezogene Daten zur Verarbeitung ausgetauscht werden. Grund hierfür ist, dass so sichergestellt werden soll, dass derjenige (Verantwortliche), der personenbezogene Daten an einen Dritten (Auftragsverarbeiter) zur Verarbeitung weitergibt, dennoch die Kontrolle bzw. Kontrollmöglichkeiten behält und so die Einhaltung des Datenschutzniveaus sicherstellt. Beispiele für eine Auftragsverarbeitung sind externe IT-Dienstleister oder Cloud-Lösungen (z. B. für Backups) sowie externe Mitgliederverwaltungen. Auch für AVV finden sich online umfangreiche Hilfestellungen und Checklisten [2].

Daneben sollten grundsätzlich alle Verträge der FWZ, in denen auch datenschutzrechtliche Aspekte geregelt werden, auf Vereinbarkeit mit den Bestimmungen der DSGVO überprüft werden.

Auch intern gibt es vertraglichen Regelungsbedarf: von den Mitgliedern und Mitarbeitern sind Einwilligungserklärungen etwa bei Veröffentlichung von Fotos, bei Videoüberwachungen oder auch bei der Speicherung der Mitgliederdaten in einer Datenbank etc. einzuholen.

Schulungen

Zu guter Letzt sollten regelmäßig, d. h. mindestens jährlich, Schulungen aller Mitarbeiter eines FWZ in Datenschutzfragen erfolgen. Deren Umfang und inhaltliche Ausrichtung hängt sicherlich maßgeblich von der Größe des FWZ, dem Ausmaß der Datenverarbeitung sowie dem Kenntnisstand der Mitarbeiter ab. Es ist allerdings wichtig für die Verantwortlichen eines FWZ zu wissen, dass für Datenschutzverstöße der Mitarbeiter grundsätzlich die Verantwortlichen haften. Daher sollte schon aus eigenem (Haftungs-)Interesse einer Sensibilisierung und Aufklärung der Mitarbeiter in Datenschutzthemen eine hohe Priorität eingeräumt werden.

Im Ergebnis lässt sich festhalten: Datenschutz lässt sich sowohl für kleine als auch große FWZ dank verfügbarer Hilfestellungen gut umsetzen. Bereits mit einigen kleinen Maßnahmen und Dokumentationen kann hier viel erreicht werden. Wichtig ist, die Erforderlichkeit dieser Umsetzung zu erkennen und das Thema nicht länger aufzuschieben.

Literaturhinweise:

[1] https://www.datenschutz-bayern.de/datenschutzreform2018/verarbeitungsverzeichnis.html und https://www.ldi.nrw.de/mainmenu_Datenschutz/submenu_Verzeichnis-Verarbeitungstaetigkeiten.
[2] https://www.baden-wuerttemberg.datenschutz.de/wp-content/uploads/2018/01/muster_adv.pdf und https://www.datenschutz-bayern.de/technik/orient/oh_auftragsverarbeitung.pdf

Gero Wilke,
Rechtsanwalt, LL.M. ist Partner der Wirtschaftskanzlei SNP Schlawien und Fachanwalt für IT-Recht sowie externer Datenschutzbeauftragter. **Dr. Malte Viergutz** leitet die IT bei UNIQUE forestry and land use GmbH und ist interner Datenschutzkoordinator.