ECOVIS®

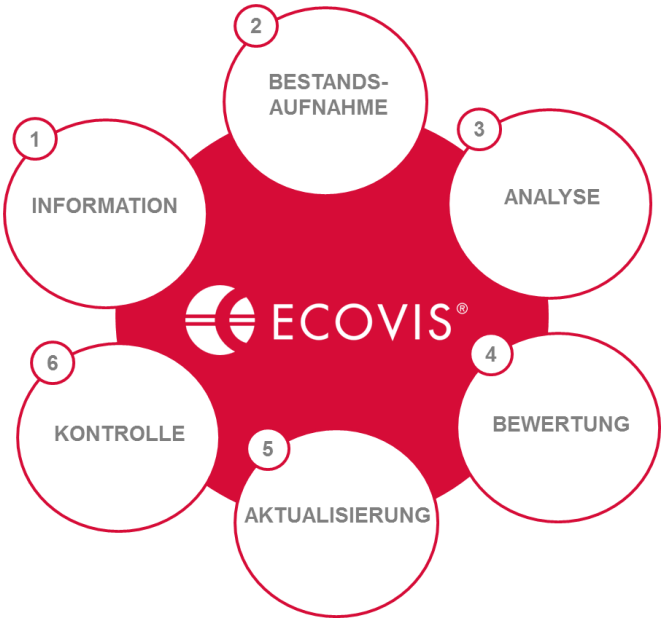
Datenschutz-Management-System

Wie wird die DSGVO mit Ihrem externen Datenschutzbeauftragten im Unternehmen eingeführt?

Die Anforderungen an den Datenschutz nehmen mit der neuen Datenschutzgrundverordnung (DSGVO) erneut zu. Ab dem 25. Mai 2018 tritt diese Verordnung vollends in Kraft. Viele Unternehmen achten bereits jetzt darauf, die Datenschutzregelungen nicht zu verletzen, haben dabei jedoch keine strukturierten Prozesse etabliert. Das kann bei der Komplexität der Verarbeitungstätigkeiten und durch die ausgeprägte Rechenschaftspflicht zu Problemen führen.

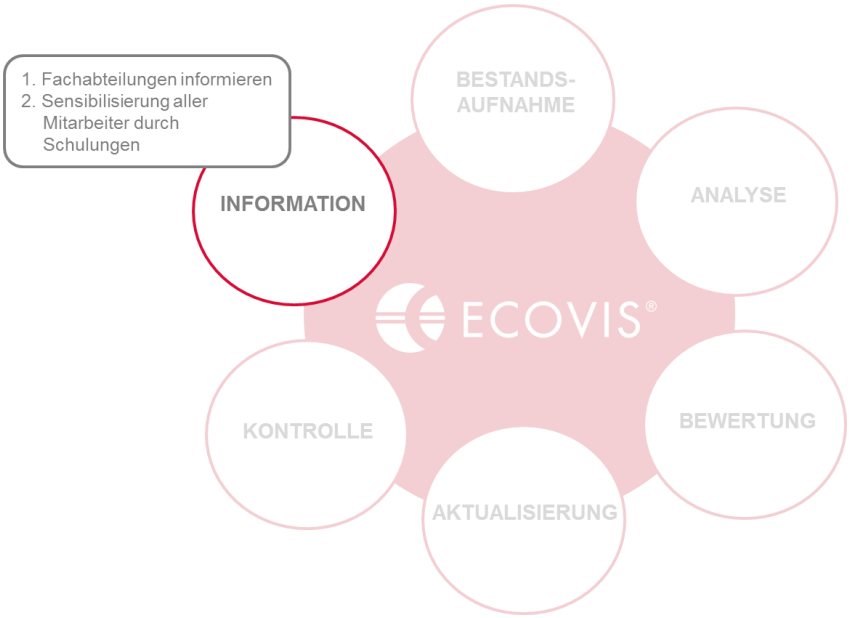
Jedes Unternehmen muss für sich selbst das optimale Datenschutz-Management-System entwickeln, nach dem es agiert. Ziel sollte es dabei immer sein, den Schutz der personenbezogenen Daten zu garantieren und in der Lage zu sein, dies nachzuweisen. Nachfolgend wird ein allgemeines Schema vorgestellt, anhand dessen jedes Unternehmen seinen systematischen Weg in ein gesetzeskonformes Datenschutz-Management findet.

Ihre Ecovis-Berater unterstützen bei allen Fragen von der Sensibilisierung der Mitarbeiter bis zur Kontrolle des Datenschutz-Management-Systems. Zur Dokumentation der Tätigkeiten wird die Spezialsoftware otris privacy eingesetzt. Weitere Informationen zum Datenschutz finden Sie auf https://www.ecovis.com/datenschutzberater/.



1. Information

Bevor mit der Bestandsaufnahme begonnen wird, ist es unabdingbar, die Fachbereiche im Unternehmen über die gesetzlichen Vorgaben und die daraus resultierenden Ziele des Unternehmens zu informieren. Dafür eignet sich beispielsweise ein internes Rundschreiben per E-Mail mit den zunächst wichtigsten Informationen über Beginn der Bestandsaufnahme und der Aufforderung zur Unterstützung.



Darüber hinaus sollten die näheren Projektschritte mit den Fachbereichsleitern besprochen werden. Dabei müssen die Ansprechpartner der entsprechenden Fachabteilungen festgelegt werden, die dem Datenschutzbeauftragten die relevanten Informationen für die Bestandsaufnahme bereitstellen und Raum schaffen, um ihm eigene Recherchen bzgl. internen Richtlinien, Verträgen, Vereinbarungen, Erklärungen usw. zu ermöglichen.

Die Sensibilisierung aller Mitarbeiter ist das A und O, um einen umfassenden, ganzheitlichen Datenschutz zu schaffen und langfristig zu erhalten. Der Datenschutzbeauftragte kann für einzelne Mitarbeiter oder ganze Fachabteilungen passende Datenschutz-Schulungen anbieten und durchführen. Ziel ist es, dass jeder Mitarbeiter zumindest ein Grundlagenwissen zum Datenschutz hat, wobei spezifisches Wissen nur selektiert den betroffenen Mitarbeitern vermittelt werden sollte.

2. Bestandsaufnahme

Sind die Fachbereiche über das Vorhaben in Kenntnis gesetzt, wird nun der IST-Zustand des Unternehmens aufgenommen. Dafür und für alle folgenden datenschutzrelevanten Vorhaben ist unter Umständen ein Datenschutzbeauftragter (intern oder extern) zu benennen. Dies muss vorab anhand des Art. 37 DSGVO geprüft werden.

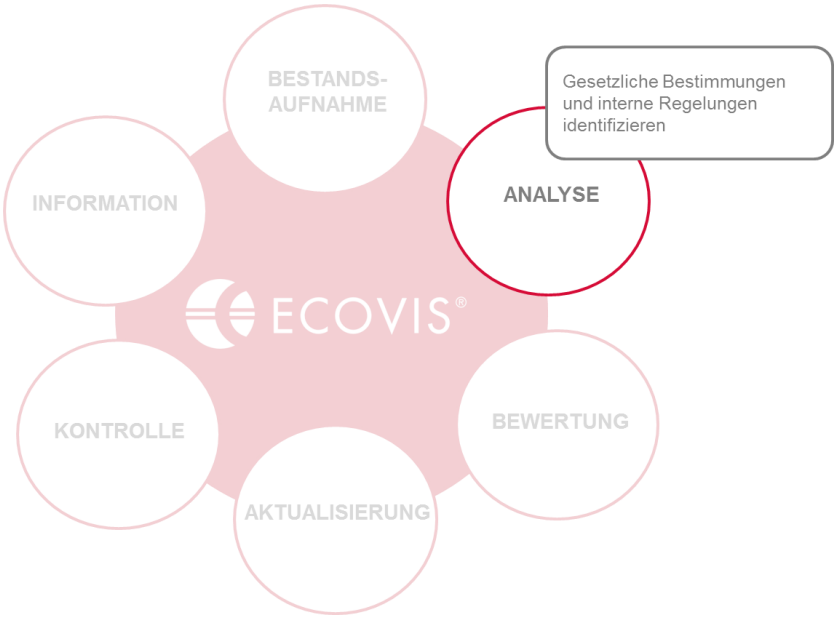
Wenn ein Datenschutzbeauftragter benannt wird, führt dieser eine Bestandsaufnahme im Unternehmen durch, die sämtliche Abläufe, bei denen personenbezogene Daten verarbeitet werden, dokumentiert. Dies geschieht anhand von Fragebögen bzw. Checklisten oder auch in persönlichen Gesprächen.

Diese Dokumentation der Prozesse muss vom Verantwortlichen fortlaufend anhand des Verzeichnisses von Verarbeitungstätigkeiten erfolgen. Folgendes Beispiel des Fuhrparkmanagement zeigt, wie umfangreich die Aufnahme der datenschutzrelevanten Verarbeitungen sein kann: Stamm- und Führerscheindaten, Versicherung, Unfälle/Schäden, Werkstatt, Zeit- und Orterfassung, (Leasing-) Verträge, Abrechnung usw.

Darüber hinaus muss sich der Datenschutzbeauftragte mit den gesetzlichen Bestimmungen nach DSGVO und BDSG intensiv auseinandersetzen und mit dem IST-Zustand im Unternehmen vergleichen. Dies kann bereits während der Bestandsaufnahme erfolgen.

3. Analyse

Für die internen Prozesse und Regelungen werden nun die entsprechenden gesetzlichen Bestimmungen identifiziert, um in der Lage zu sein, die Datenschutzkonformität der jeweiligen Verarbeitungen zu prüfen.



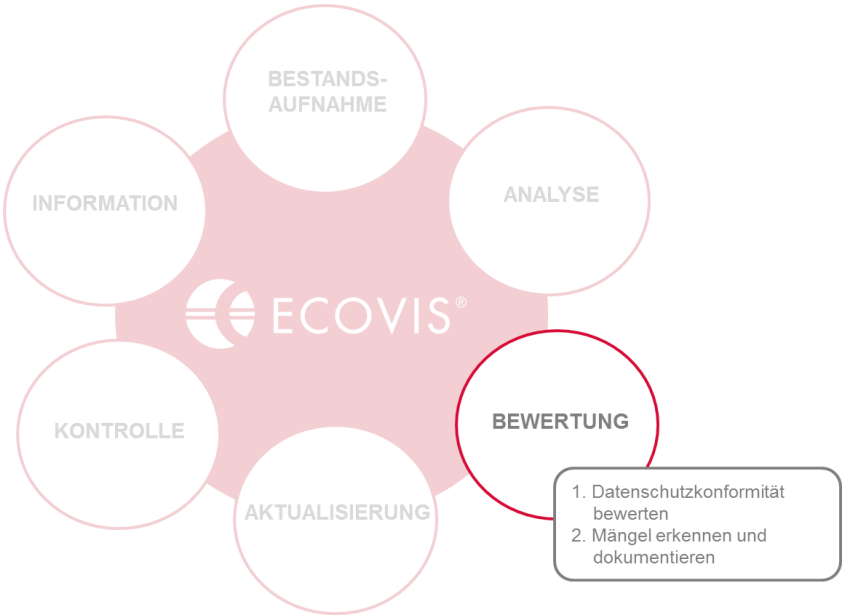
Um die jeweils geltenden gesetzlichen Vorschriften einfacher zu identifizieren, ist eine Kategorisierung der Verarbeitungstätigkeiten sinnvoll. Hier wird im Verzeichnis der Verarbeitungstätigkeiten zwischen Kategorien betroffener Daten, Personen und Empfängern unterschieden.

4. Bewertung

Das durch die Bestandsaufnahme und Analyse entstandene Verzeichnis der Verarbeitungstätigkeiten wird nun daraufhin geprüft und bewertet, ob datenschutzkonform agiert wird. Dies geschieht anhand des Abgleichs der Verarbeitungstätigkeiten mit den identifizierten gesetzlichen Bestimmungen. Werden Prozesse aufgedeckt, die nicht den gesetzlichen Vorgaben entsprechen und Risiken für Verlust oder Schädigung von personenbezogenen Daten darstellen, müssen Maßnahmen zur Beseitigung der Mängel eingeleitet werden.

Unter Umständen ist nach Art. 35 DSGVO eine Datenschutz-Folgenabschätzung durchzuführen, wenn Daten verarbeitet werden, die ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge haben. Diese Daten müssen einer gesonderten Zulässigkeitsprüfung unterzogen werden, bevor sie verarbeitet werden.

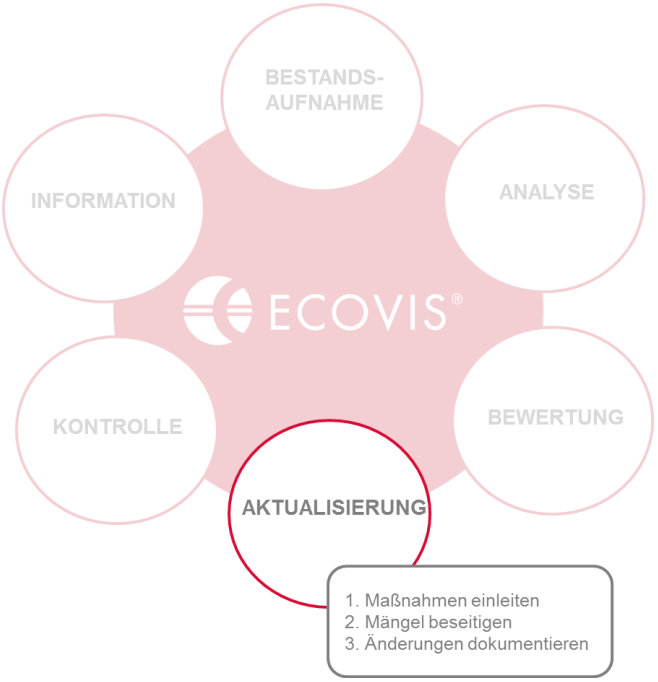
So wie die Bestandsaufnahme und Analyse teils parallel erfolgen, geschieht dies auch mit der Bewertung der dokumentierten Verarbeitungen. Bei der Komplexität an Dokumentationen gilt es nun, als besondere Herausforderung, den Überblick zu behalten.



5. Aktualisierung

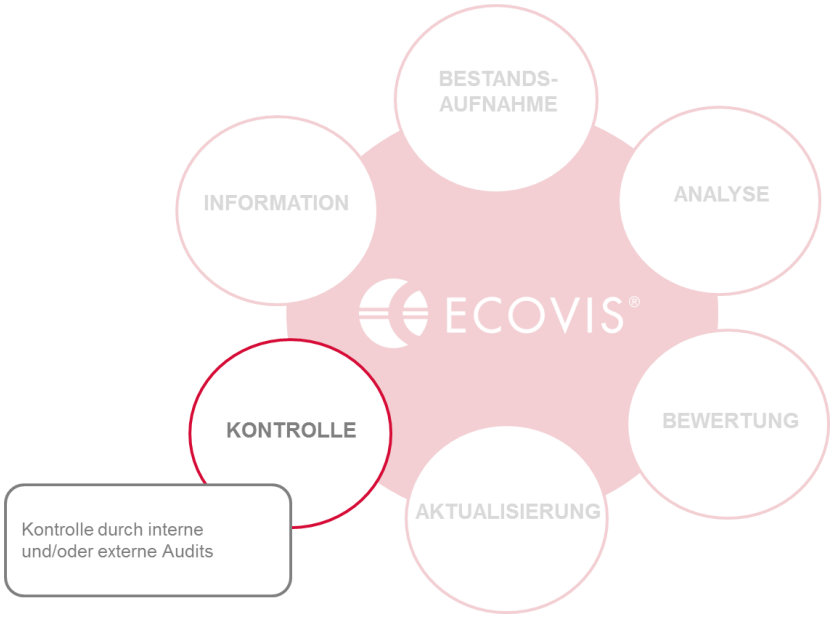
Die in der Bewertungsphase erkannten Mängel müssen nun mit entsprechenden technischen und organisatorischen Maßnahmen (bspw. Zutritts-, Zugangs-, Auftragskontrolle) behoben werden. Um den Überblick über alle Anpassungen zu behalten und der Rechenschaftspflicht nachzukommen, müssen alle Veränderungen dokumentiert werden.

Bevor jedoch die nicht-gesetzeskonformen Prozesse angepasst werden können, müssen die Verantwortlichen in den Fachbereichen erneut dahingehend sensibilisiert werden, dass die entsprechenden Prozessänderungen datenschutzrechtlich notwendig sind und das Unternehmen bei Nichtbeachtung mit hohen Strafen zu rechnen hat.



6. Kontrolle

Die vorangegangen Schritte sind ausschlaggebend für ein funktionierendes gesetzeskonformes Datenschutz-Management-System. Um langfristig einen umfassenden Schutz zu erhalten, muss dieses System in regelmäßigen Abständen kontrolliert und unter Umständen nachgebessert werden. Wie in den Schritten 1 bis 5 werden auch hier die Abläufe geprüft, analysiert, bewertet und aktualisiert sowie die Mitarbeiter informiert. Die Kontrolle (das Audit) kann intern durch das eigene Unternehmen oder extern durch Dritte durchgeführt werden.



IMPRESSUM

Herausgeber: ECOVIS Grieger Mallison Rechtsanwälte PartG mbB
Am Campus 1-11, 18182 Rostock-Bentwisch
Tel. +49 381 64 92-10, Fax +49 381 64 92-60