

PFLICHTEN ZUR INFORMATIONSSICHERHEIT UND ZUM DATENSCHUTZ FÜR AUFTRAGNEHMER

11.05.2026 / Version 1.0

INHALT

1.0	PRÄAMBEL	3
2.0	GELTUNGSBEREICH	3
3.0	GRUNDLEGENDE PFLICHTEN	3
3.1	Auskunfts- & Informationspflichten	3
3.2	Technische & Organisatorische Maßnahmen	4
3.3	Schulung des Personals	5
3.4	Umgang mit Vorfällen	5
3.5	Umgang mit Mängeln	6
3.6	Verpflichtung von Nachunternehmern	6
4.0	ERWEITERTE PFLICHTEN	7
4.1	Managementsystem für Informationssicherheit	7
4.2	Überprüfung durch TransnetBW	7

1.0 PRÄAMBEL

Als Betreiber kritischer Infrastruktur (KRITIS) trägt TransnetBW eine besondere Verantwortung für den Schutz von Informationen und Daten. Die Aufrechterhaltung eines angemessenen Informationssicherheitsniveaus ist daher fest in den Unternehmenszielen von TransnetBW verankert.

TransnetBW erwartet von seinen Dienstleistern und Lieferanten ein hohes Maß an Sorgfalt, Transparenz und Verantwortungsbewusstsein im Umgang mit geschäftlichen Informationen und personenbezogenen Daten. Um Risiken für TransnetBW, den Geschäftspartner und gegebenenfalls betroffene Dritte zu minimieren, verpflichtet TransnetBW seine Auftragnehmer zur Einhaltung der nachfolgenden Regelungen.

2.0 GELTUNGSBEREICH

Die folgenden Regelungen richten sich an alle Auftragnehmer (nachfolgend „AN“) der TransnetBW GmbH (nachfolgend „TransnetBW“), die mit TransnetBW-Informationen umgehen oder Zutritt zu TransnetBW-Standorten erhalten.

Der Begriff „Information“ schließt im Folgenden jede Art von geschäftlichen Informationen und personenbezogenen Daten ein, unabhängig davon, ob der AN mit diesen in digitaler oder analoger Form umgeht.

Weiterhin gelten die Regelungen unabhängig davon, ob der AN von TransnetBW bereitgestellte oder eigene Informationssysteme für den Umgang mit TransnetBW-Informationen einsetzt.

3.0 GRUNDLEGENDE PFLICHTEN

Die in dieser Ziffer 3.0 beschriebenen grundlegenden Pflichten gelten für den AN unabhängig von Art und Umfang der vertraglich geschuldeten Leistungen verbindlich.

3.1 AUSKUNFTS- & INFORMATIONSPFLICHTEN

- a. Der AN hat TransnetBW auf Anfrage einen qualifizierten Ansprechpartner zu benennen, der für die Beantwortung von Fragen und Anliegen im Bereich der Informationssicherheit und des Datenschutzes zur Verfügung steht.
- b. Dringende Auskünfte, die der Abwendung von akuten Gefahren oder der Aufklärung von Vorfällen gemäß Ziffer 3.4 dienen, hat der AN innerhalb einer durch TransnetBW gesetzten angemessenen Frist, spätestens jedoch binnen drei Werktagen nach Anfrage durch TransnetBW zu erteilen.
- c. Der AN ist verpflichtet, auf Anfrage von TransnetBW binnen vier Wochen seine Informationssicherheits- und Datenschutzmaßnahmen in Form eines von TransnetBW vorgegebenen Selbstauskunftsboogens darzulegen.
- d. TransnetBW wird bei Anfragen gemäß lit. b. und lit. c. Rücksicht auf den Schutz von Geschäftsgeheimnissen und die Sicherheitsinteressen des AN nehmen.
- e. Der AN hat TransnetBW vierzehn Tage im Voraus eines geplanten Wechsels oder Austritts von Personal zu informieren, welches der AN für die Erfüllung seiner Pflichten gegenüber TransnetBW einsetzt, über Zugang zu TransnetBW-

Informationssystemen verfügt oder zum Zutritt zu TransnetBW-Standorten berechtigt ist. Nicht geplante, kurzfristige Personalveränderungen sind TransnetBW unverzüglich, spätestens jedoch vor Inkrafttreten der Veränderung mitzuteilen.

3.2 TECHNISCHE & ORGANISATORISCHE MAßNAHMEN

- a. Der AN hat für den Umgang mit TransnetBW-Informationen angemessene technische und organisatorische Maßnahmen zu treffen, die deren Vertraulichkeit, Verfügbarkeit und Integrität während der gesamten Vertragsbeziehung bis zur Rückgabe und dauerhaften Löschung der Informationen durch den AN sicherstellen.
- b. Die technischen und organisatorischen Sicherheitsmaßnahmen müssen alle TransnetBW-Informationen sowie Informationssysteme des AN umfassen, die für die Erfüllung der vertraglichen Pflichten gegenüber TransnetBW erforderlich sind.
- c. Bei der Auswahl und Ausgestaltung der Sicherheitsmaßnahmen sind das Risiko sowie allgemein anerkannte Standards (ISO/IEC 27001, bei personenbezogenen Daten zusätzlich ISO/IEC 27701, oder gleichwertig) zu berücksichtigen, die anerkannte Regeln der Technik widerspiegeln.
- d. Der AN hat die ausgewählten und umgesetzten Sicherheitsmaßnahmen regelmäßig auf ihre fortwährende Angemessenheit und Wirksamkeit zu überprüfen.
- e. Die Maßnahmen des AN zum Schutz von TransnetBW-Informationen müssen mindestens umfassen:
 - / Verhaltensregeln für Personal zum sicheren Umgang mit Informationen
 - / Überprüfung der Vertrauenswürdigkeit des eingesetzten Personals, bevor Zugriff auf TransnetBW-Informationen gewährt wird
 - / Beschränkung des Zugangs zu Informationssystemen durch sichere Authentifizierungsverfahren, angemessene Berechtigungskonzepte und technische Maßnahmen
 - / Steuerung des Informationszugriffs (lesend, schreibend) auf Basis des Prinzips minimaler Rechte („Least Privilege“) und des Erforderlichkeitsprinzips („Need-To-Know“) sowie damit verbundener Freigabeprozesse
 - / Schwachstellen- & Patchmanagement für Informationssysteme
 - / Schutz vor Bedrohungen aus dem Internet (z. B. Schadsoftware, Phishing)
 - / Verschlüsselung von vertraulichen TransnetBW-Informationen, insbesondere bei Speicherung auf mobilen Datenträgern sowie beim Versand über öffentliche Netzwerke (z. B. das Internet)
 - / Schutz von internen Kommunikationsnetzwerken (z. B. durch Firewalls)

- / Physischer Schutz von Räumlichkeiten, in denen Informationsverarbeitung stattfindet, einschließlich darin befindlicher Unterlagen, Informationssysteme und Datenträger
- / Beschränkung des Zutritts zu Geschäftsräumen für Personal, Dienstleister und Besucher
- / Sicherung der Verfügbarkeit von Fachpersonal (z. B. durch Stellvertretung), Informationssystemen & Daten (z. B. durch Redundanzen, Backups, Monitoring & Wartung)
- / Protokollierung von administrativen Tätigkeiten an IT-Systemen sowie der Eingabe und Weitergabe personenbezogener Daten
- / Sichere Löschung & Entsorgung von Daten sowie Datenträgern (Löschkonzept)
- / Angemessene Trennung der Daten verschiedener Kunden (Mandantentrennung) sowie Trennung von Entwicklungs-, Test- und Produktivsystemen
- / Herstellung eines vergleichbaren, angemessenen Sicherheitsniveaus beim Arbeiten außerhalb der Geschäftsräume des AN (z. B. bei mobilem Arbeiten, Homeoffice oder Dienstreisen)
- / Geregelter Prozess zur Behandlung von Informationssicherheits- und Datenschutzvorfällen
- / Notfallvorsorge zur Aufrechterhaltung der Informationssicherheit, des Datenschutzes und des Geschäftsbetriebs in widrigen Situationen

3.3 SCHULUNG DES PERSONALS

- a. Der AN hat durch mindestens jährlich stattfindende Schulungsmaßnahmen sicherzustellen, dass sein Personal für aktuelle Bedrohungen im Bereich der Informationssicherheit und des Datenschutzes sensibilisiert ist, diese frühzeitig erkennen und ihnen durch geeignete Verhaltensweisen entgegenwirken kann.
- b. Der AN hat Personal, das er zur Erfüllung seiner vertraglichen Pflichten einsetzt und Zugriff auf TransnetBW-Informationssysteme erhält, vor Beginn der Tätigkeit in die Sicherheitsbestimmungen für externe Anwender von Informationssystemen einzuweisen. Diese sind auf der Website von TransnetBW unter <https://www.transnetbw.de/de/unternehmen/portraet/einkauf> abrufbar.
- c. Die Durchführung der Einweisung nach lit. b. hat der AN zu dokumentieren und auf Anfrage innerhalb von vierzehn Tagen gegenüber TransnetBW nachzuweisen.

3.4 UMGANG MIT VORFÄLLEN

- a. Ein Informationssicherheitsvorfall ist ein Ereignis, das die Verfügbarkeit, Vertraulichkeit oder Integrität von Informationen verletzt oder mit hoher Wahrscheinlichkeit zu einer Verletzung führen wird. Zusätzlich handelt es sich um einen Datenschutzvorfall, wenn personenbezogene Daten von dem Ereignis betroffen sind.

- b. Der AN hat Informationssicherheitsvorfälle, sofern konkrete Anhaltspunkte vorliegen, dass TransnetBW-Informationen betroffen sein könnten, innerhalb von 24 Stunden nach Kenntnisnahme an den Informationssicherheitsbeauftragten von TransnetBW (Informationssicherheit@transnetbw.de) zu melden. Datenschutzvorfälle sind mit gleicher Frist an die Datenschutzbeauftragte von TransnetBW (Datenschutz@transnetbw.de) zu melden.
- c. Die Meldung des AN muss mindestens Angaben zum Hergang des Vorfalls, zu Art und Umfang der betroffenen TransnetBW-Informationen sowie den ergriffenen Erstmaßnahmen enthalten. Sofern einzelne Angaben zum Zeitpunkt der Erstmeldung noch nicht bekannt sind, können diese innerhalb einer angemessenen Frist nachgereicht werden.
- d. Der AN ist verpflichtet, alle erforderlichen Maßnahmen zu treffen, um Schäden von TransnetBW infolge eines Vorfalls abzuwenden. Weiterhin hat er die Ursachen des Vorfalls zu analysieren. Die aus der Vorfallbehandlung gewonnenen Erkenntnisse muss der AN dazu nutzen, um Maßnahmen zur Vorbeugung zukünftiger Vorfälle zu treffen.
- e. Der AN hat TransnetBW über das Ergebnis der Ursachenanalyse und den Fortschritt der getroffenen Maßnahmen nach lit. c. bis zum vollständigen Abschluss der Vorfallbehandlung mindestens alle vier Wochen unaufgefordert zu informieren.

3.5 UMGANG MIT MÄNGELN

- a. Ein Mangel im Bereich der Informationssicherheit oder des Datenschutzes liegt vor, wenn der AN vertragliche Pflichten zum Schutz der Verfügbarkeit, Vertraulichkeit oder Integrität von TransnetBW-Informationen verletzt.
- b. Der AN hat Mängel gemäß lit. a. gegenüber TransnetBW unverzüglich, jedoch spätestens fünf Werktage nach deren Kenntnisnahme, anzuzeigen.
- c. Sofern von einer akuten Gefährdung von TransnetBW-Informationen aufgrund eines Mangels auszugehen ist, gilt eine Meldefrist von 24 Stunden ab Kenntnisnahme des Mangels durch den AN.
- d. Der AN ist verpflichtet, festgestellte Mängel innerhalb eines angemessenen Zeitraums zu beheben. Der AN hat TransnetBW die geplanten Abhilfemaßnahmen sowie den Zeitplan für deren Umsetzung mitzuteilen.
- e. Der AN hat TransnetBW über den Fortschritt der Abhilfemaßnahmen bis zur vollständigen Behebung des Mangels mindestens alle vier Wochen unaufgefordert zu informieren.

3.6 VERPFLICHTUNG VON NACHUNTERNEHMERN

Der AN hat vor dem Einsatz von Nachunternehmern alle vertraglichen Pflichten zum Schutz von TransnetBW-Informationen, einschließlich der Pflichten aus diesem Dokument, an die Nachunternehmer weiterzugeben, diese vertraglich zu verpflichten und die Einhaltung angemessen zu überwachen.

4.0 ERWEITERTE PFLICHTEN

Die in dieser Ziffer 4.0 beschriebenen erweiterten Pflichten sind zusätzlich für den AN verbindlich, sofern der Hauptvertrag ausdrücklich auf diese Ziffer verweist oder sofern die vertraglich vereinbarten Leistungen des AN für TransnetBW ganz oder wesentlich eine oder mehrere der folgenden Leistungen umfasst:

- / Betrieb, Wartung, Administration oder Monitoring von IT-Systemen, OT-Systemen oder Kommunikationseinrichtungen
- / Installation, Integration, Konfiguration oder Parametrierung von IT-Systemen, OT-Systemen oder Kommunikationseinrichtungen
- / Entwicklung, Anpassung oder Modifikation von Software oder Hardware

4.1 MANAGEMENTSYSTEM FÜR INFORMATIONSSICHERHEIT

- a. Der AN hat zur Steuerung, Überwachung und kontinuierlichen Verbesserung seiner technischen und organisatorischen Sicherheitsmaßnahmen ein Managementsystem für Informationssicherheit (ISMS) zu betreiben.
- b. Der Anwendungsbereich des ISMS muss alle Teile der Organisation des AN umfassen, in denen mit TransnetBW-Informationen umgegangen wird und die für die Erbringung der vertraglich vereinbarten Leistungen wesentlich sind.
- c. Der AN muss durch eine Zertifizierung oder ein vergleichbares Verfahren nachweisen, dass sein ISMS einem aktuellen, allgemein anerkannten Standard (ISO/IEC 27001 oder gleichwertig) entspricht. Das Nachweisverfahren muss eine regelmäßige, mindestens jährliche Überprüfung der Wirksamkeit des ISMS und der getroffenen Sicherheitsmaßnahmen durch fachkundige und unabhängige Prüfer umfassen.
- d. Die jeweils aktuellen Nachweise nach lit. c. sind TransnetBW auf Anfrage innerhalb von vierzehn Tagen zur Verfügung zu stellen.

4.2 ÜBERPRÜFUNG DURCH TRANSNETBW

- a. TransnetBW ist berechtigt, nach Ankündigung und mit angemessener Vorlaufzeit die Einhaltung der vertraglichen Pflichten des AN im Bereich der Informationssicherheit zu überprüfen. Dies kann Dokumentenprüfungen, Interviews oder Begehungen der Geschäftsräume des AN umfassen.
- b. Der AN hat an der Überprüfung mitzuwirken, indem er TransnetBW auf Verlangen Einsicht in Dokumente und Informationssysteme gibt, Auskünfte erteilt und während der üblichen Geschäftszeiten Zutritt zu seinen Geschäftsräumen gewährt.
- c. TransnetBW wird bei der Überprüfung die Beeinträchtigung von Betriebsabläufen des AN so gering wie möglich halten und Rücksicht auf den Schutz von Geschäftsgeheimnissen des AN nehmen.
- d. TransnetBW kann für die Überprüfung eigenes Personal oder unabhängige Dritte einsetzen, die vertraglich oder von Berufs wegen zur Verschwiegenheit verpflichtet sind und für die Durchführung der Überprüfung qualifiziert sind.

- e. Interne Aufwände, die dem AN aufgrund einer Überprüfung durch TransnetBW nachweislich entstanden sind, werden auf Anforderung des AN in angemessener Höhe separat vergütet. Der AN hat TransnetBW zu diesem Zweck den geschätzten Aufwand und damit verbundene Kosten mitzuteilen.
- f. Erfolgt die Überprüfung anlässlich eines Informationssicherheits- oder Datenschutzvorfalls (siehe Abschnitt 3.4) im Verantwortungsbereich des AN, hat dieser alle nachweislich entstandenen Kosten der Überprüfung, einschließlich der Aufwände für externe Prüfer und interner Aufwände bei TransnetBW, in angemessener Höhe zu übernehmen.