

Anhang zum Beitrag 10.1 Datenschutzprüfung von Energieversorgungsunternehmen

1. Allgemeine Informationen

- Name, Rechtsform, Anschrift Ihres Unternehmens:
- Ansprechpartner (Name, Funktion, Telefon, E-Mail)
- Datenschutzbeauftragter (Name, Telefon, E-Mail)

2. Datenschutzorganisation

- 2.1 Welche Unternehmensbereiche sind mit dem Thema Datenschutz betraut?
- 2.2 Beschreiben Sie bitte das Zusammenwirken der einzelnen Stellen in datenschutzrechtlichen Angelegenheiten unter Beifügung eines aussagekräftigen Organigramms
- 2.3 Sofern es einen Datenschutzbeauftragten gibt, wie und in welcher Häufigkeit berichtet er an die Geschäftsführung?

3. Umsetzung der DS-GVO

- 3.1 Welche Unternehmensbereiche waren oder sind maßgeblich in die Umsetzung der DS-GVO involviert?
- 3.2 Kreuzen Sie bitte die wesentlichen Maßnahmen an, die Sie im Rahmen der Umsetzung getroffen haben.
 - Sensibilisierungsmaßnahmen
 - interne Datenschutz-Richtlinie
 - Erstellung von Datenschutzhinweisen zur Erfüllung der Informationspflicht
 - Löschkonzept
 - Neuverhandlung Auftragsverarbeitungsverträge
 - Prozess Datenschutz-Folgenabschätzung
 - Anpassung und Erweiterung interner Vorgaben zur Dokumentation

- Dokumentation der Umsetzung der DS-GVO
- Überarbeitung/Erstellung von Betriebsvereinbarungen
- Benennung eines internen bzw. Beauftragung eines externen Datenschutzbeauftragten
- Prozesse für Betroffenenrechte
- Prozesse für Beschwerdebearbeitung
- Prüfung vertraglicher Grundlagen für internationalen Datentransfer
- Überprüfung/Neuverhandlung der Verträge mit externen Dienstleistern
- Dokumentation der internen Datenschutzorganisation
- Prozess für die Meldung von Datenpannen
- Sonstige:

3.3 Erläutern Sie bitte kurz den Umsetzungsstatus, falls noch nicht bzw. nicht vollständig umgesetzt. Benennen Sie bitte auch die Gründe.

3.4 Hat Ihre Interne Revision oder eine vergleichbare Einheit die Einführung und Umsetzung der DS-GVO in Ihrem Unternehmen geprüft?

4. Zulässigkeit der Datenverarbeitung

4.1 Bitte listen Sie die wesentlichen unternehmensspezifischen Datenverarbeitungen auf und ordnen Sie diesen die Rechtsgrundlagen zu, auf die Sie die Verarbeitung personenbezogener Daten stützen (Artikel 6, 9 DS-GVO inklusive Spezialnormen).

4.2 Sofern Sie auf Basis von Einwilligungen personenbezogene Daten verarbeiten, fügen Sie bitte exemplarisch Ihr(e) Muster bei.

5. Beschwerde-Bearbeitung

- 5.1 Listen Sie bitte die mit der Bearbeitung datenschutzrechtlicher Beschwerden befassten Stellen Ihres Unternehmens auf.
- 5.2 Anhand welcher Kriterien stuft Ihr Unternehmen die Rückmeldung eines Kunden als datenschutzrechtliche Beschwerde ein (Beschwerdedefinition)?
- 5.3 Wie unterscheidet sich die Bearbeitung einer datenschutzrechtlichen Beschwerde von der Bearbeitung einer sonstigen Beschwerde?

6. Betroffenenrechte

- 6.1 Wie stellen Sie sicher, dass den Betroffenenrechten auf Auskunft, Berichtigung, Löschung, Einschränkung der Verarbeitung, Nachberichtspflicht und Datenübertragbarkeit angemessen nachgekommen wird? Bitte kreuzen Sie zutreffendes an.
 - Regelungen der Verantwortlichkeiten, Zuständigkeiten und des Kommunikationsverlaufs im Unternehmen
 - Prozesse zur Beantwortung von Anfragen der Betroffenen (einschließlich Erkennen als Anfrage zu einem Betroffenenrecht z. B. durch Schlüsselwörter, Identifikation der Betroffenen, Bearbeitungsdauer, Rückmeldung an Betroffene u.a.)
 - Verwenden von Mustern für Antwortschreiben
 - Prozesse zur Sicherstellung der Einhaltung von Fristen
 - Prozesse zur Nachverfolgung des Fortschritts der Bearbeitung
 - Verfahren zur Reaktion, wenn ein(e) Betroffene(r) mit der Beantwortung nicht zufrieden ist
 - Sensibilisierung der Mitarbeiter

- 6.2 Skizzieren Sie bitte überblicksartig Ihre wesentlichen Prozesse zu den o.g. Betroffenenrechten. Legen Sie bitte möglichst Nachweise (z. B. Verfahrensbeschreibungen, Muster-texte etc.) bei, die eine Überprüfung Ihrer Angaben ermöglichen.
- 6.3 Wie kommen Sie Ihren Informationspflichten gegenüber Kunden gem. Art. 13 bzw. 14 DS-GVO nach (z.B. Homepage, Postversand, E-Mail-Link, Aushang)? Bitte fügen Sie exemplarisch Ihre Muster-Texte bei.
- 6.4 Zu welchem Zeitpunkt informieren Sie Ihre Kunden i.S.v. 6.3?
- 6.5 Wie werden Missstände und Schwachstellen im Umgang mit Betroffenenrechten kontinuierlich verbessert und die Verbesserungsmaßnahmen auf ihre Wirksamkeit hin überprüft?

7. Sensibilisierungsmaßnahmen

- 7.1 Stellen Sie sicher, dass Ihre Mitarbeiterinnen und Mitarbeiter für den Umgang mit personenbezogenen Daten hinreichend sensibilisiert sind?
- Ja
- Nein
- 7.2 Benennen Sie, wenn zutreffend, die wesentlichen Sensibilisierungsmaßnahmen und machen Sie Angaben zum Ausführungsturnus.

8. Rechenschaftspflicht

- 8.1 Wie können Sie die Einhaltung der Grundsätze der Datenverarbeitung nachweisen? Benennen Sie die Art der Dokumentation, die Sie für diesen Zweck vorhalten.
- 8.2 Welche Aspekte bereiten ggf. Schwierigkeiten?

9. Bereichsspezifische Fragen (Versorgungswirtschaft)

9.1 Werden Informationssysteme geführt, welche personenbezogene Hinweise zu den jeweiligen Kunden speichern, wie z.B. das Wechselverhalten der Kunden?

9.2 Findet ein Abgleich/Austausch von personenbezogenen Daten (wie z.B. Zahlungsverhalten, Vertragstreue) mit anderen Energieversorgungsunternehmen statt? Wenn ja, auf welche Rechtsgrundlage wird dieser Abgleich/Austausch gestützt?

10. Sonstiges

Haben Sie Anregungen an die Aufsicht?