Verfahrensanweisung

Gestaltung von Leistungsvereinbarungen
und Anpassung der Beauftragungsprozesse
im Rahmen einer
Auftragsdatenverarbeitung
im Geltungsbereich des
Bundesdatenschutzgesetzes

Corporate Procurement

INHALTSVERZEICHNIS

1. Ziele und Hintergrund

Seit dem 01.09.2009 gelten erweiterte Regelungen im Bereich der Auftragsdatenverarbeitung. Dies betrifft insbesondere die Beauftragung von Dienstleistern mit der Verarbeitung von personenbezogenen Daten. Die Regelungen gelten sowohl für Neubeauftragungen als auch für bestehende Vertragsverhältnisse. Die Vereinbarung mit dem Auftragnehmer über die Auftragsdatenverarbeitung muss schriftlich dokumentiert werden und bestimmte Mindestinhalte zur Gewährleistung der Datensicherheit umfassen. Der Auftraggeber wird darüber hinaus dazu verpflichtet, sich vor Leistungsbeginn und in der weiteren Folge regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen Maßnahmen zur Gewährleistung der Datensicherheit zu überzeugen.

Die Nichtbefolgung von neuen Regelungen im Bereich der Auftragsdatenverarbeitung ist größtenteils bußgeldbewehrt. Wer vorsätzlich oder fahrlässig einen Auftrag nicht richtig, nicht vollständig oder nicht in der vorgeschriebenen Weise erteilt, handelt ordnungswidrig. Das gleiche gilt, wenn der Auftraggeber sich vor Beginn der Auftragsdatenverarbeitung nicht von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen überzeugt. In beiden Fällen kann ein Bußgeld bis zu € 50.000 (und bei Überschreitung dieses Betrages durch den erlangten wirtschaftlichen Vorteil sogar mehr) verhängt werden.

2. Geltungsbereich

Die vorliegende Verfahrensanweisung gilt für alle Mitarbeiter der beschaffenden Bereiche in den E.ON-Konzerngesellschaften im Geltungsbereich des BDSG. Die Market Units sind dafür verantwortlich, dass

a) die betroffenen Mitarbeiter informiert und entsprechend geschult werden,
b) die Verfahrensanweisung auch von den jeweiligen Business Units sowie deren Mehrheitsbeteiligungen eingehalten wird.

Wenn interne oder externe Dienstleister mit der Verarbeitung von personenbezogenen Daten beauftragt werden, muss der Auftraggeber die Einhaltung von Mindestanforderungen zur Gewährleistung der Datensicherheit durch geeignete vertragliche Vereinbarungen und durch Prüfung der Umsetzung der vereinbarten Maßnahmen sicherstellen.

a) Auftragsdatenverarbeitung (Definition)

Bei einer Auftragsdatenverarbeitung werden gemäß § 11 Abs. 1 S. 1 BDSG personenbezogene Daten im Auftrag durch andere Stellen erhoben, verarbeitet oder genutzt. Das bedeutet, dass bei allen Vertragsverhältnissen, bei denen E.ON-Gesellschaften Daten ihrer Mitarbeiter, Kunden oder anderer natürlicher Personen an Vertragspartner zur Verarbeitung und Nutzung zur Verfügung stellen, die E.ON-Gesellschaften als Auftraggeber und die Vertragspartner als Auftragnehmer agieren. Die konzerninternen Dienstleister agieren hingegen im Verhältnis zu den anderen E.ON-Gesellschaften als Auftragnehmer.

b) Betroffene Verträge (exemplarische Aufzählung)

Die unter 3. aufgeführten vertraglichen Vereinbarungen und die unter 4.a) aufgeführten zusätzlichen Maßnahmen werden insbesondere, jedoch nicht abschließend, für die Verträge mit den folgenden Vertragspartnern relevant:

- *IT-Dienstleister,*
- *Call Center,*
- *Buchhaltungs-Servicegesellschaften,*
- *Gehaltsabrechnungs-Dienstleister,*
- *Dienstleister, die Buchungen von Reiseleistungen durchführen (z. B. Reisebüros, Betreiber von Hotelbuchungs-Portalen, Mietwagengesellschaften),*
- *Dienstleister für Fahrzeug-Leasing (z. B. Dienstfahrzeuge im Rahmen der Gehaltsumwandlung),*
- *Lieferanten von sonstigen Gütern und Leistungen, die im Rahmen ihrer Leistungserbringung Kenntnis von Kunden- oder Mitarbeiterdaten erhalten; davon umfasst sind auch Leistungserbringer, die die Prüfung oder Wartung automatisierter Verfahren oder Datenverarbeitungsanlagen übernehmen, soweit ein Zugriff auf personenbezogene Daten nicht ausgeschlossen werden kann,*
- *Andere Konzerngesellschaften, an die personenbezogene Daten zum Zwecke der Verarbeitung oder Nutzung übermittelt werden, z. B. interne Dienstleister.*

Bei der Beauftragung von Dienstleistern gibt es Grenzfälle, in denen die Regelungen über die Auftragsdatenverarbeitung nicht zur Anwendung kommen. Bei diesen Fällen handelt es sich um sog. Funktionsübertragung, bei der nicht nur die Verarbeitung von Daten in Auftrag gegeben wird, sondern ganze Businessprozesse aus dem Unternehmen ausgegliedert werden und von dem Dienstleister ausgeführt werden. Die Verarbeitung personenbezogener Daten stellt dann nur einen Teil dieser Prozesse dar. Die Übermittlung der personenbezogenen Daten an den Dienstleister bedarf dann der Zustimmung der betroffenen Personen. Der Dienstleister ist bei der Verarbeitung personenbezogener Daten selbst für die Einhaltung der datenschutzrechtlichen Vorschriften, insb. der Maßnahmen zur Datensicherheit, verantwortlich. Die Zustimmung der betroffenen Personen ist dann nicht erforderlich, wenn eine gesetzliche Erlaubnis zur Übermittlung vorliegt; in diesem Fall sind die betroffenen Personen jedoch über die Übermittlung zu benachrichtigen.

3. Änderungsbedarf bei Vereinbarungen über die Auftragsdatenverarbeitung

Die im Folgenden dargestellten Mindestinhalte der Vereinbarungen über die Auftragsdatenverarbeitung sind als Konzernstandard zu verstehen, der die einheitliche Berücksichtigung bei allen Konzerngesellschaften im Geltungsbereich der neuen gesetzlichen Regelungen des BDSG sicherstellen soll.

Während sich das BDSG in der bisher geltenden Fassung auf allgemeine Rahmenvorgaben zur Gewährleistung der Datensicherheit beschränkte, enthält der geänderte § 11 BDSG detaillierte Vorgaben hierzu. Demnach sind in den vertraglichen Vereinbarungen mit Auftragsdatenverarbeitern *insbesondere* folgende Festlegungen schriftlich zu dokumentieren:

1. Der Gegenstand und die Dauer des Auftrags.
2. Der Umfang, die Art und der Zweck der vorgesehenen Erhebung, Verarbeitung oder Nutzung von Daten; die Art der Daten (z. B. Adressdaten, Rechnungsdaten) und der Kreis der Betroffenen (z. B. Privatkunden, Mitarbeiter, Lieferanten).
3. Die gemäß § 9 BDSG zu treffenden technischen und organisatorischen Maßnahmen.
4. Die Berichtigung, Löschung und Sperrung von Daten.
5. Die nach § 11 Abs. 4 BDSG bestehenden Pflichten des Auftragnehmers (insb. Verpflichtung der Mitarbeiter auf das Datengeheimnis, Ergreifen von technischen und organisatorischen Maßnahmen), insbesondere die von ihm vorzunehmenden Kontrollen.
6. Die etwaige Berechtigung zur Begründung von Unterauftragsverhältnissen.
7. Die Kontrollrechte des Auftraggebers und die entsprechenden Duldungs- und Mitwirkungspflichten des Auftragnehmers.

8. Mitzuteilende Verstöße des Auftragnehmers oder der bei ihm beschäftigten Personen gegen Vorschriften zum Schutz personenbezogener Daten oder gegen die im Auftrag getroffenen Festlegungen.
9. Der Umfang der Weisungsbefugnisse, die sich der Auftraggeber gegenüber dem Auftragnehmer vorbehält.
10. Die Rückgabe überlassener Datenträger und die Löschung beim Auftragnehmer gespeicherter Daten nach Beendigung des Auftrags.

Schließt eine Konzerngesellschaft einen Rahmenvertrag mit einem internen oder externen Dienstleister ab, unter dem mehrere Konzerngesellschaften Abrufe tätigen bzw. Einzelbestellungen auslösen können, ist in Bezug auf die oben dargestellten Mindestinhalte zwischen den sog. Basisregelungen zu unterscheiden, die für alle abrufberechtigten Gesellschaften gleichermaßen gelten sollen, und gesellschaftsspezifischen Regelungen, die die Anforderungen der einzelnen Gesellschaften widerspiegeln. Die Basisregelungen (dies werden in der Regel die Vereinbarungen gemäß Ziffer 4 bis 10 oben sein) können für alle abrufberechtigten Gesellschaften im Rahmenvertrag festgehalten werden. Die gesellschaftsspezifischen Regelungen (in der Regel die Ziffern 1 bis 3 oben sowie etwaige spezifische Abweichungen von oder Ergänzungen zu den Ziffern 4 bis 10) werden hingegen im Rahmen des jeweiligen Einzelabrufs vereinbart.

In der Anlage 1a dieser Verfahrensanweisung finden Sie das Muster für eine Datenschutzvereinbarung, die als Vertragsanlage zu einer Einzelleistungsvereinbarung verwendet werden kann oder in eine entsprechende vertragliche Vereinbarung eingearbeitet werden kann. Die Anlage 1b enthält das Muster für eine Datenschutzvereinbarung, die als Anlage zu einem Rahmendienstleistungsvertrag verwendet werden kann.

Wird zum Zwecke der Beauftragung eine SAP-Bestellung ausgelöst, sollte diese neben dem Verweis auf die AGB der auftraggebenden E.ON-Gesellschaft auch einen Verweis auf eine Anlage zur SAP-Bestellung enthalten, die die konkreten auftragsspezifischen Datenschutzregelungen enthält. Ein Muster für eine solche Anlage findet sich in Anlage 3 dieser Verfahrensanweisung. Der Abschluss der in Anlage 1a bzw. 1b beigefügten gesonderten Datenschutzvereinbarung ist im Falle der vorstehend beschriebenen SAP-Bestellung nicht erforderlich.

Alle bereits bestehenden vertraglichen Vereinbarungen mit konzerninternen und -externen Auftragsdatenverarbeitern sind zeitnah hinsichtlich deren Anpassungsbedarfs an die Neuregelung des § 11 BDSG zu überprüfen und gegebenenfalls sind erforderliche Ergänzungen vorzunehmen. Ebenso überprüft und ggf. angepasst werden müssen Vereinbarungen, bei denen eine oder mehrere Konzerngesellschaften die Rolle des Auftragnehmers übernommen haben, d. h. selbst personenbezogene Daten im Auftrag eines anderen Unternehmens verarbeiten.

4. Prüfungs-, Mitteilungs- und Auskunftspflichten

a) Prüfung der Angemessenheit der Maßnahmen zur Gewährleistung der Datensicherheit

Der Auftraggeber ist verpflichtet, den Auftragnehmer – unter Berücksichtigung der Eignung der von diesem getroffenen technischen und organisatorischen Maßnahmen – sorgfältig auszuwählen und sich (1) vor Beginn der Datenverarbeitung und sodann regelmäßig von der Einhaltung der beim Auftragnehmer getroffenen technischen und organisatorischen Maßnahmen zu überzeugen und (2) das Ergebnis schriftlich zu dokumentieren.

Der Auftraggeber kann sich dadurch von der Einhaltung der getroffenen technischen und organisatorischen Maßnahmen überzeugen, dass er sich vom Auftragnehmer zusammen mit dessen Dienstleistungsangebot und später in regelmäßigen Abständen eine Dokumentation der im Rahmen

der Verarbeitung und Nutzung von Daten des Auftraggebers bestehenden technischen und organisatorischen Maßnahmen zur Datensicherheit vorlegen lässt und diese dem für die Leistungen fachlich verantwortlichen Fachbereich zur Prüfung der Angemessenheit sowie zur schriftlichen Freigabe vorlegt.

In begründeten Fällen (z. B. im Zusammenhang mit der Verarbeitung von besonders sensiblen Daten oder von umfangreichen Datenbeständen) sollte darüber hinaus sichergestellt werden, dass der für die Leistungen fachlich verantwortliche Fachbereich vor der Erteilung des Auftrags durch den Einkaufsbereich und auf jeden Fall vor dem Beginn der Leistungserbringung durch den Auftragnehmer sowie auch später in regelmäßigen Abständen eine Besichtigung der Räumlichkeiten des Auftragnehmers vor Ort vornimmt, sich hierbei von der Angemessenheit der bestehenden Maßnahmen zur Gewährleistung der Datensicherheit überzeugt und dies in Form eines Prüfprotokolls schriftlich dokumentiert.

Der IT-Security Manager und/oder der Datenschutzbeauftragte der jeweiligen E.ON-Gesellschaft sind bei Bedarf gern dazu bereit, den fachlich verantwortlichen Fachbereich und den Einkaufsbereich beratend bei der Beurteilung der Angemessenheit von Maßnahmen zur Gewährleistung der Datensicherheit zu unterstützen.

Im Zusammenhang mit einer Konzern-Rahmenvereinbarung mit einem externen oder einem konzerninternen Dienstleister ist Folgendes zu beachten:

Auch wenn die Rahmenvereinbarung als solche in der Regel nur von einer Konzerngesellschaft mit dem Anbieter verhandelt und für den Gesamtkonzern abgeschlossen wird, ist jede Konzerngesellschaft, die einen konkreten Auftrag erteilt, selbst für die Einhaltung der datenschutzrechtlichen Vorschriften als Auftraggeber verantwortlich. Bezogen auf die in Ziffer 3 Absatz 3 oben beschriebene Konstellation bedeutet das, dass jede auftraggebende Gesellschaft nicht nur dafür verantwortlich ist, zu überprüfen, ob ihre gesellschaftsspezifischen Anforderungen vom Auftragnehmer umgesetzt werden, sondern auch, ob die Basisregelungen im Hinblick auf die personenbezogenen Daten ihrer Gesellschaft umgesetzt werden. Wird die Einhaltung der Basisregelungen von einer Konzerngesellschaft zentral für alle geprüft, bleibt die auftraggebende Gesellschaft gleichwohl für die Einhaltung verantwortlich, d. h., sie muss sich z. B. die Prüfungsergebnisse von der prüfenden Gesellschaft vorlegen lassen und sich anhand dieser Ergebnisse von der Einhaltung der Anforderungen überzeugen. Sollten diese Ergebnisse aus ihrer Sicht den Anforderungen nicht genügen, ist sie selbst dafür verantwortlich, die Einhaltung der Anforderungen zu veranlassen und zu überprüfen.

Um den Überblick über die Einhaltung der Anforderungen des § 11 BDSG zu behalten, sollte jeder Auftraggeber im Geltungsbereich des BDSG zeitnah zur Einführung der vorliegenden Verfahrensanweisung ein Verzeichnis ihrer bestehenden Vereinbarungen zur Auftragsdatenverarbeitung erstellen und laufend aktualisieren. In der Anlage 2 dieser Verfahrensanweisung finden Sie ein Muster für ein Verzeichnis der Auftragsdatenverarbeiter und der jeweils erteilten Auftragsdatenverarbeitungsaufträge.

Das Verzeichnis der Auftragsdatenverarbeiter und der an sie jeweils erteilten Aufträge kann in Dateiform geführt werden. Hingegen sind die jeweiligen vertraglichen Vereinbarungen mit den Auftragnehmern (und den Auftraggebern) schriftlich in Papierform festzuhalten; die Originale sind aufzubewahren. Ebenfalls sollte die Dokumentation der bei den Auftragnehmern durchgeführten Prüfungen der Maßnahmen zur Gewährleistung der Datensicherheit schriftlich geführt werden und im Original aufbewahrt werden, da diese dem Nachweis gegenüber den Aufsichtsbehörden dient.

b) Mitteilung bei Datenverlust

Gemäß § 42a BDSG, der nicht nur den Bereich der Auftragsdatenverarbeitung betrifft, sondern in jedem Fall der Verarbeitung personenbezogener Daten zu beachten ist, müssen auch nichtöffentliche

Stellen wie die E.ON-Konzernunternehmen der zuständigen Aufsichtsbehörde und den Betroffenen unverzüglich melden, wenn bestimmte bei ihnen gespeicherte personenbezogene Daten Dritten unrechtmäßig zur Kenntnis gelangt sind und schwerwiegende Beeinträchtigungen der Rechte oder schutzwürdigen Interessen der Betroffenen drohen.

Unter personenbezogenen Daten im obigen Sinn versteht man:

- Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder philosophische Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder Sexualleben,
- personenbezogene Daten, die einem Berufsgeheimnis (z. B. der ärztlichen oder anwaltlichen Schweigepflicht) unterliegen,
- personenbezogene Daten, die sich auf strafbare Handlungen oder Ordnungswidrigkeiten oder den Verdacht strafbarer Handlungen oder Ordnungswidrigkeiten beziehen, oder
- personenbezogene Daten zu Bank- oder Kreditkartenkonten.

Die Benachrichtigung der Betroffenen und der Behörde muss grundsätzlich unverzüglich (d. h. ohne schuldhaftes Zögern) erfolgen. Damit bei der Benachrichtigung das gesetzlich vorgesehene Verfahren und die gesetzlich vorgesehene Maßnahmenreihenfolge eingehalten werden, ist bei Eintritt der oben genannten Umstände unverzüglich die jeweils zuständige Rechtsabteilung einzubeziehen.

Erfolgt eine solche Benachrichtigung vorsätzlich oder fahrlässig nicht, nicht richtig, nicht vollständig oder nicht rechtzeitig, stellt dies eine Ordnungswidrigkeit dar, die mit empfindlichen Bußgeldzahlungen (bis 300.000,00 Euro und bei Überschreitung dieses Betrages durch den erlangten wirtschaftlichen Vorteil sogar mehr) belegt werden kann (§ 43 Abs. 2 Nr. 7 BDSG).

Damit die notwendigen Meldungen rechtzeitig und umfassend vorgenommen werden können, ist es empfehlenswert, innerhalb jeder Gesellschaft einen internen Meldeprozess festzulegen, in den auch der jeweilige Datenschutzbeauftragte eingebunden ist.

c) Erteilung der Auskunft an den Betroffenen gemäß § 34 BDSG

Die verantwortlichen Stellen sind gem. § 34 Abs.1 BDSG verpflichtet, einem Betroffenen auf dessen Verlangen hin grundsätzlich unentgeltlich Auskunft über

- die zu seiner Person gespeicherten Daten und die Herkunft dieser Daten
- den Empfänger dieser Daten bzw. die Kategorie von Empfängern und
- den Zweck der Speicherung

zu erteilen.

Hierzu soll der Betroffene die Art der personenbezogenen Daten, über die Auskunft erteilt werden soll, näher bezeichnen.

Die Auskunft ist auf Verlangen grundsätzlich in Textform zu erteilen.

In Ausnahmefällen besteht keine Auskunftspflicht der verantwortlichen Stelle. Inwiefern im jeweiligen Einzelfall ein Ausnahmefall vorliegt, ist jeweils unter Einbeziehung der zuständigen Rechtsabteilung zu klären.

Bei der Ablehnung des Auskunftsersuchens sollte intern dokumentiert werden, weshalb die Ablehnung stattgefunden hat. Ferner ist auch gegenüber dem Betroffenen die Ablehnung zu begründen.

Mit Bußgeld von bis zu 50.000,00 Euro (und bei Überschreitung dieses Betrages durch den erlangten wirtschaftlichen Vorteil sogar mehr) können vorsätzliche oder fahrlässige Verstöße gegen die Auskunftsvorschriften geahndet werden.

5. Inkrafttreten

Die Verfahrensanweisung tritt zum 20.11.2009 in Kraft.

6. Anlagen

Anlage 1a: Muster für eine „Datenschutzrechtliche Vereinbarung“ (Einzelvereinbarung)
Anlage 1b: Muster für eine „Datenschutzrechtliche Vereinbarung“ (bei Abschluss eines Rahmenvertrages)

Anlage 2: Muster für ein „Verzeichnis der Auftragsdatenverarbeiter“

Anlage 3: Muster für eine Anlage zu einer SAP-Bestellung mit auftragsspezifischen Regelungen