Jonas Breyer

Die Datenschutz-Policy im Unternehmen

Seit dem 25.5.2018 wird das Datenschutzrecht für die meisten Unternehmen durch die DSGVO reguliert. Doch wie kann eine Umsetzung dieser Rechte und Pflichten in Unternehmen organisatorisch gelingen, in denen Experten verschiedenster Gebiete arbeiten und beinahe alle personenbezogene Daten verarbeiten? Ein wichtiger Baustein hierzu ist das Erstellen und das korrekte Anordnen einer Datenschutz-Policy im Unternehmen, die selbstverständlich auch Richtlinie, Leitlinie oder ähnlich genannt werden kann.

Rechtliche Grundlage der Datenschutz-Policy

Der Verantwortliche, zumeist also das Unternehmen, ist nach Art. 24 DSGVO verpflichtet, durch geeignete organisatorische Maßnahmen sicherzustellen und nachzuweisen, dass die Verarbeitung personenbezogener Daten gemäß den Bestimmungen der DSGVO erfolgt. Nach Art. 29 DSGVO muss der Verantwortliche ferner sicherstellen, dass ihm unterstellte Personen personenbezogene Daten ausschließlich auf Grundlage seiner Weisungen verarbeiten. Die Datenschutz-Policy kann sowohl eine solche organisatorische Maßnahme als auch eine Weisung an die Beschäftigten sein.

Zwar sind, insbesondere in größeren Unternehmen, datenschutzrechtliche Verstöße fast nie hundertprozentig vermeidbar. Mit einer wohlüberlegten Datenschutz-Policy kann aber ein strukturelles Fundament gelegt werden, um ihre Zahl und damit die Risiken für alle Beteiligten wesentlich zu reduzieren.

Formale Inhalte

Die Datenschutz-Policy sollte klar strukturiert sein. Sie sollte den Anordnenden (etwa die Geschäftsleitung) und den Adressatenkreis (etwa die Beschäftigten und die Geschäftsleitung) klar benennen und generell konkrete, durchdachte und realistische Handlungsanweisungen enthalten. Vage Gesinnungen und allgemeine Formulierungen helfen nicht weiter und werden in etwaigen Streitfällen wenig zur Klärung beitragen. Beim Aufführen des Verpflichtetenkreises ist zu bedenken, dass freie Mitarbeiter nicht vom Beschäftigtenbegriff des § 26 Abs. 8 BDSG erfasst werden, aber trotzdem häufig personenbezogene Daten verarbeiten; ähnliches gilt für Mitglieder der Geschäftsleitung, vor denen die DSGVO ebenfalls keinen Halt macht.

Die Datenschutz-Policy sollte den gesetzlichen Rechtsrahmen (typischerweise DSGVO und BDSG) benennen und bekanntgeben, wer im Außenverhältnis Verantwortlicher ist, was gerade bei größeren Unternehmen oder in Konzernstrukturen nicht immer offensichtlich ist. In Betracht kommt auch eine gemeinsame Verantwortlichkeit (Art. 4 Nr. 7 DSGVO, Art. 26 DSGVO), etwa in Gemeinschaftsbetrieben, wobei nach der Rechtsprechung des EuGH eine Verantwortlichenstellung auch durch faktische Verhältnisse begründet werden kann (EuGH, Urt. v. 5.6.2018 – C 210/16, Rn. 31). Zugleich ist zu regeln, wer im Innenverhältnis Verpflichteter ist und die Einhaltung der datenschutzrechtlichen Vorgaben in seiner Organisationseinheit überwacht (etwa der Leiter der geschäftsprozessverantwortlichen Organisationseinheit).

Zentrale Pflichten

Es ist nicht praktikabel, in der Datenschutz-Policy alle Regelungen der DSGVO wiederzugeben. Es empfiehlt sich aber, zumindest die zentralen Verarbeitungsgrundsätze nach Art. 5 DSGVO zur Orientierung als „allgemeinen Teil" wiederzugeben. Aus diesen lassen sich die meisten übrigen materiellen Pflichten ableiten. Als weitere zentrale Rechte und Pflichten sollten die Informationspflichten (Art. 12 DSGVO, Art. 13 DSGVO und Art. 14 DSGVO), die Datensicherheit (Art. 32 DSGVO), die Melde- und Benachrichtigungspflichten (Art. 33 DSGVO und Art. 34 DSGVO) und die Datenschutz-Folgenabschätzung (Art. 35 DSGVO) erwähnt werden.

Datenschutzbeauftragter

Ist der Verantwortliche zur Benennung eines Datenschutzbeauftragten verpflichtet (siehe Art. 38 DSGVO, § 38 BDSG), sollte dies in der Richtlinie aufgeführt sein und es sollten seine Kontaktdaten genannt werden. Eine Funktionsadresse genügt. Es sollte normiert werden, dass der Datenschutzbeauftragte weisungsfrei ist, über die erforderlichen Ressourcen verfügen muss und frühzeitig in Fragen der Verarbeitung personenbezogener Daten einzubinden ist. Es sollte ggf. auch geregelt werden, dass dem Datenschutzbeauftragten ein Budget bereitgestellt wird, das er eigenverantwortlich etwa für Fachliteratur und Fortbildungen einsetzen kann. Weitere lesenswerte Merkmale des Datenschutzbeauftragten, die aufgenommen werden können, ergeben sich aus den Leitlinien in Bezug auf Datenschutzbeauftragte der Art.-29-Gruppe (WP 243).

In der Datenschutz-Policy sollten kurz seine Aufgaben aufgeführt werden (Art. 39 DSGVO), insbesondere im Hinblick auf die Beratung, Schulungen der Beschäftigten und die Zusammenarbeit mit der Aufsichtsbehörde. Es sollte erwähnt werden, dass der Datenschutzbeauftragte zur Verschwiegenheit verpflichtet ist (§ 38 Abs. 2 BDSG), welche

Vertretungsregelung besteht und inwieweit er durch beauftragte Beschäftigte handeln kann. Geregelt werden sollte auch, inwieweit der Datenschutzbeauftragte Tätigkeitsberichte zu erstellen hat und inwieweit diese auszugsweise etwa dem Betriebsrat zur Verfügung gestellt werden. Zwar ist der Datenschutzbeauftragte unabhängig vom Betriebsrat; zumindest auf der Ebene des Beschäftigtendatenschutzes sind die Interessen aber oft ähnlich (etwa §§ 75 Abs. 2, 80 Abs. 1 Nr. 1, 87 Abs. 1 Nr. 6, 88 BetrVG) und es hat sich zur Vermeidung von Doppelarbeit daher eine gewisse Kooperation bewährt. Dafür spricht auch der neue § 79a BetrVG (hierzu Brink/Joos, NZA 2021, 1440).

Erlaubnistatbestände

Es sollten zumindest die allgemeinen Erlaubnistatbestände des Art. 6 Abs. 1 DSGVO wiedergegeben werden. Denn wegen des Verbots mit Erlaubnisvorbehalts sind sie von zentraler Bedeutung und sind nach wie vor nicht zwingend Allgemeinwissen.

Verpflichtung zur Vertraulichkeit

Es sollte klargestellt werden, dass alle Beschäftigten von der Personalabteilung zur Vertraulichkeit zu verpflichten sind. Zwar existiert das frühere Datengeheimnis des § 5 BDSG a. F. nicht mehr. Aus Art. 24 DSGVO und 32 Abs. 1 lit. b DSGVO folgt aber Ähnliches. Nach diesen Vorschriften muss der Verantwortliche durch geeignete organisatorische Maßnahmen die Vertraulichkeit personenbezogener Daten sicherstellen.

Schulungen

Die Datenschutz-Policy sollte regeln, innerhalb welcher Frist nach ihrer Einstellung neue Beschäftigte vom Datenschutzbeauftragten geschult werden. Auch sollten die übrigen Beschäftigten in einem bestimmten Turnus (etwa alle zwei Jahre) geschult werden. Dies kann mittels einer interaktiven Software durchgeführt werden. Dafür werden bei einer persönlichen Schulung, gegebenenfalls per Videokonferenz, oft interessante Rückfragen gestellt und es besteht so die Chance, häufige Fehlvorstellungen auszuräumen.

Verarbeitungsvorhaben

Zur Sicherstellung der DSGVO-Compliance sollte geregelt werden, dass neue Vorhaben zur Verarbeitung personenbezogener Daten (etwa die Inbetriebnahme einer neuen CRM-Software oder Mailingaktionen) oder deren Änderung einer vorherigen Freigabe durch den Datenschutzbeauftragten bedürfen. Dies umfasst auch Test- und Pilotverarbeitungen. Da häufig pseudonymisierte und anonymisierte Daten verwechselt werden und die Fehlvorstellung weit verbreitet ist, dass Unternehmerdaten von der DSGVO ausgenommen wären (wie etwa im kalifornischen CCPA vorgesehen), werden Verarbeitungsvorhaben ggf. erst gar nicht dem Datenschutzbeauftragten gemeldet. Deswegen kann sich eine kurze Information hierzu und zu ähnlichen branchen- oder unternehmenstypischen Datenschutzirrtümern empfehlen. Es ist zu regeln, wen die Pflicht zur Einbindung des Datenschutzbeauftragten trifft, etwa den Leiter der geschäftsprozessverantwortlichen Organisationseinheit, den Projektleiter oder bei agilen Strukturen den „Service Owner“ oder „Product Owner“.

Da in der Praxis eilige Vorhaben nicht ausbleiben, sollte klargestellt werden, dass die Einbindung des Datenschutzbeauftragten rechtzeitig zu erfolgen hat (er muss noch Einfluss nehmen können) und inhaltliche Mindestangaben zu machen sind, namentlich zum Zweck, zur Kategorien der Betroffenen, zu Datenarten, Empfängern, Löschfristen, Drittlandübermittlungen, individuellen Maßnahmen zur Datensicherheit, zugriffsberechtigten Personen und geplanten Auswertungen. Es kann geregelt werden, dass diese Informationen zugleich einem etwaigen Betriebsrat mitzuteilen sind. Der Praktikabilität wegen sollte geregelt werden, dass der Datenschutzbeauftragte bei einer aus seiner Sicht nötigen Datenschutz-Folgenabschätzung die dafür zuständige Abteilung darüber informiert und in sonstigen Fällen seine Einschätzung rückmeldet. Es ist wichtig klarzustellen, dass die Entscheidung, ob eine Verarbeitung gegen den Rat des Datenschutzbeauftragten durchgeführt wird, beim Anfragenden liegt.

Datenschutz-Folgenabschätzung

Je nach Geschäftstätigkeit des Unternehmens können Datenschutz-Folgenabschätzungen erforderlich werden, wenn eine Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat. Dies kann beispielsweise bei Software US-amerikanischer Herkunft auch namhafter Hersteller der Fall sein sein (vgl. Jungkind/Raspé/Schramm, NZG 2020, 1056, 1057). Für die Durchführung der Datenschutz-Folgenabschätzung ist nicht der Datenschutzbeauftragte zuständig, sodass eine zuständige Einheit im Unternehmen benannt werden sollte. Dem Datenschutzbeauftragten kommt aber eine beratende Rolle zu (Art. 35 Abs. 2 DSGVO). Zudem kann ihm die interne Zuständigkeit für eine Konsultation nach Art. 36 DSGVO übertragen werden.

Betroffenenrechte

Die Datenschutz-Policy sollte regeln, dass der Verantwortliche die Datenschutzinformationen nach Art. 13 DSGVO und Art. 14 DSGVO erfüllt und der Datenschutzbeauftragte ihn bei der Formulierung unterstützt. Hierbei ist zu bedenken, dass Datenschutzinformationen nicht nur in Bezug auf Kunden erstellt werden müssen, sondern auch Beschäftigte und Vertragspartner über Datenverarbeitungen informiert werden müssen. Entsprechendes gilt für Anfragen nach Art. 15 ff. DSGVO und Widersprüche nach Art. 21 DSGVO. Da der Datenschutzbeauftragte meist keinen regelmäßigen Zugriff auf sämtliche personenbezogenen Daten innehat und auch nicht benötigt, ist zu regeln,

dass ihm die zur Bearbeitung erforderlichen Informationen vollständig zur Verfügung zu stellen sind. Die Bearbeitung der vorgenannten Betroffenenanfragen kann die Datenschutz-Policy für bestimmte Teilbereiche der größeren Sachnähe wegen auch einer anderen Organisationseinheit übertragen, um den Datenschutzbeauftragten zu entlasten. Eine solche „Auslagerung" kann außerdem mittelbar bewirken, dass das Datenschutzbewusstsein der entsprechenden Einheit steigt und sie Prozesse aktiv so gestaltet, dass es zu weniger Betroffenenanfragen kommt. Jedenfalls sollte ein effizientes Verfahren etabliert werden, zumal die verspätete Bearbeitung von Betroffenenanfragen Schadensersatzforderungen auslösen kann (ArbG Neumünster, Urt. v. 11.8.2020 – 1 Ca 247 c/20).

Verarbeitungsverzeichnis

Die Datenschutz-Policy sollte vorsehen, dass der Verantwortliche das Verarbeitungsverzeichnis nach Art. 30 DSGVO führt und welche Datenkategorien einzupflegen sind, auch soweit der Verantwortliche als Auftragnehmer tätig wird. Es bedarf aus den vorgenannten Gründen einer klaren Regelung, wer die dazu erforderlichen Informationen dem Datenschutzbeauftragten zukommen lässt, etwa der Leiter der geschäftsprozessverantwortlichen Organisationseinheit.

Auftragsverarbeitung

Auftragsverarbeitungen sind gerade in größeren Unternehmen ein Dauerthema. Es sollte daher festgelegt werden, dass im Fall von Auftragsverarbeitungen die Vorgaben des Art. 28 DSGVO einzuhalten sind, insbesondere die dort genannten Mindestinhalte schriftlich zu vereinbaren und zu dokumentieren sind.

Meldungen von Verletzungen

Zur Einhaltung der Melde- und Benachrichtigungspflichten nach Art. 33 DSGVO und Art. 34 DSGVO ist zu normieren, dass bei Verdacht des Diebstahls von Hard- oder Software, des unbefugten Zugriffs auf personenbezogene Daten, Sabotage oder vergleichbaren Unregelmäßigkeiten der Datenschutzbeauftragte unverzüglich unter Angabe bestimmter Informationen zu informieren ist. Der Datenschutzbeauftragte sollte insbesondere über im Zusammenhang mit der Verletzung stehende Fakten, Auswirkungen und bereits getroffene Abhilfemaßnahmen informiert werden. Der Eilbedürftigkeit halber sollten nochmals dessen Kontaktdaten angegeben werden. An dieser Stelle kommt auch die oben erwähnte Vertretungsregelung zum Tragen. Optional kann eine zusätzliche Meldung an sonstige Funktionen wie den Compliance Officer, die Revision und den IT-Sicherheitsbeauftragten vorgesehen werden. Der Datenschutzbeauftragte sollte die Vorgänge dokumentieren.

Die Datenschutz-Policy sollte festlegen, dass eine etwaige Meldung an die Aufsichtsbehörde dem Datenschutzbeauftragten obliegt und er außerdem die etwaige Compliance-Funktion und die Revision, möglicherweise auch die Geschäftsleitung darüber informiert.

Die Erfahrung zeigt, dass viele Verdachtsmeldungen nicht meldepflichtig sind, etwa wenn es zu einzelnen Post-Irrläufern mit harmlosen Daten gekommen ist. Die Beurteilung hängt jedoch vom konkreten Einzelfall ab und das Artikulieren allgemeingültiger Kriterien gestaltet sich schwierig. Wenn schon eine allgemeingültige Erheblichkeitsschwelle für interne Meldungen an den Datenschutzbeauftragten geregelt wird, kann ein solches Vorgehen diesen einerseits entlasten, andererseits aber auch ein Compliance-Risiko für den Verantwortlichen darstellen.

Zugriff auf Daten durch den Arbeitgeber

Es ist ein immer wiederkehrendes Problem, dass der Arbeitgeber ein berechtigtes Interesse daran hat, etwa bei Krankheit, Urlaub oder Kündigung auf (geschäftliche) Daten eines Beschäftigten zuzugreifen. Die Datenschutz-Policy kann hier ein Prozedere anordnen, dass dies erst nach Prüfung und im Beisein des Datenschutzbeauftragten erfolgt, um Missbrauch zu verhindern. Können sich unter den eingesehenen Daten berechtigterweise auch Privatdaten des Beschäftigten befinden, muss der Arbeitgeber für deren Einsicht zuvor eine Rechtsgrundlage geschaffen haben. Dies ist etwa im Wege einer Einwilligung des Beschäftigte denkbar, ohne die eine Privatnutzung nicht zugelassen wird. Wurde der Beschäftigte zuvor auf mögliche Zugriffe des Arbeitgebers schon nicht hingewiesen, etwa im Wege einer Datenschutzerklärung, kann dies sogar gegen Art. 8 EMRK verstoßen (EGMR, Urt. v. 5.9.2017 – 61496/08 – Bărbulescu).

Die Policy kann auch vorsehen, dass der Zugriff zusätzlich im Beisein eines Betriebsratsmitglieds erfolgen muss, insbesondere, wenn die betroffene Person selbst ein Mitglied des Betriebsrats oder der Schwerbehindertenvertretung ist.

Anordnung der Datenschutz-Policy

Es obliegt dem Verantwortlichen, die Datenschutz-Policy im Unternehmen rechtlich korrekt zu verankern. Sie sollte nicht zum Bestandteil des Arbeitsvertrags gemacht werden, da dieser unter Umständen später nicht mehr einseitig geändert werden kann oder dies zumindest aufwändig wäre. Auch ist der Beschäftigte nicht verpflichtet, einer Vertragsänderung zuzustimmen.

Empfehlenswerter ist es, sie im Wege des Direktionsrechts nach § 106 GewO anzuweisen. Dazu muss die Datenschutz-Policy allen betroffenen Beschäftigten und etwa auch freien Mitarbeitern zugehen. Dies kann theoretisch per Intranet erfolgen, wo die Policy gegebenenfalls auch dauerhaft abrufbar sein sollte. Jedoch lässt sich so der einzelne Zugang im Streitfall kaum nachweisen. Auch die rechtliche Aussagekraft von auf zweifelhafter Rechts-

grundlage vorratsgespeicherten Server-Logfiles des Abrufvorgangs dürfte im Streitfall problematisch sein. In einem Rechtsstreit um Online-Einwilligungen in Telefonwerbung hat der Bundesgerichtshof IP-Adressen und ähnliche Logdaten insoweit jedenfalls keinen Beweiswert beigemessen (BGH, Urt. v. 10.2.2011 – I ZR 164/09).

Stattdessen sollte der Beschäftigte den Erhalt der Policy aktiv quittieren (§ 368 BGB), sodass der Arbeitgeber nachweisen kann, ihn vollständig informiert zu haben. Unwirksam ist hingegen die sinngemäße vorformulierte Bestätigung, die Datenschutz-Policy „gelesen zu haben und damit einverstanden zu sein". Zum einen kann ein solches Einverständnis wiederum zu einer unerwünschten Änderung des Arbeitsvertrags führen (siehe oben); zum anderen ist eine Klausel zum Gelesenhaben wegen Verstoßes gegen § 309 Nr. 12 b BGB (Bestätigung von Tatsachen) – insgesamt – unwirksam und damit wertlos. Die vorgenannten Grundsätze gelten auch für ähnliche Richtlinien wie die IT-Sicherheitsrichtlinie.

Eine öffentliche Bekanntgabe der Datenschutz-Policy ist nicht erforderlich. Allerdings kann es hilfreich sein, eine ggf. „abgespeckte" Fassung für Auftragsverarbeitungsverträge vorzuhalten, in denen der Verantwortliche als Auftragnehmer agiert. Denn in der Datenschutz-Policy liegt zugleich eine der – üblicherweise vom Auftragnehmer darzulegenden – organisatorischen Maßnahmen zur Datensicherheit gemäß Art. 28 Abs. 3 lit. c DSGVO. Entsprechendes gilt für eine mögliche IT-Sicherheitsrichtlinie.

Fazit

In Zeiten einer immer stärkeren datenschutzrechtlichen Regulierung leistet die Datenschutz-Policy im Unternehmen einen wichtigen Beitrag zur strukturellen DSGVO-Compliance, zur Rechtssicherheit sowie zur Enthaftung des Verantwortlichen. Ihre Erstellung bietet die Chance, die Interessen aller Beteiligten in einen Ausgleich zu bringen, Kooperationen zu begründen und maßgeschneiderte innerbetriebliche Verfahren zur Einhaltung des Datenschutzrechts zu gestalten.

Autor: **Jonas Breyer ist Rechtsanwalt in eigener Kanzlei in Wiesbaden und spezialisiert auf Datenschutz- und IT-Recht.**