Rechtsanwältin Nina Diercks

Datenschutz im Beschäftigtenverhältnis – Teil 2

Zeit, mit den Mythen aufzuräumen und endlich das Notwendige zu tun!

I. Einleitung

Im ersten Teil dieser zweiteiligen Serie wurde mit gängigen Mythen aus dem Reich des Beschäftigtendatenschutzes aufgeräumt, erklärt, dass panische Schockstarre ob der DSGVO unnötig ist und damit aufgezeigt, dass selbstverständlich auch unter der DSGVO moderne und sachgerechte Personalarbeit möglich ist.[1]

Mit dem zweiten Teil wenden wir uns nun den wirklich notwendigen Maßnahmen zu, die die Personalabteilung ergreifen muss, um den Anforderungen der DSGVO gerecht zu werden.

Als Unternehmen im Ganzen, aber auch insbesondere als Personalabteilung[2] müssen Sie sich mit den folgenden acht Punkten beschäftigen:

- der Überblick I: das Verzeichnis von Verarbeitungstätigkeiten,
- die Aufklärung: Informationen zur Datenverarbeitung,
- die Verhältnisse zu „Dritten": CtC, JCC or DPA?,
- die konkreten Maßnahmen: technische und organisatorische Maßnahmen,
- die Schönheit: Privacy by Design & Default,
- die Risikoprüfung: Datenschutzfolgeabschätzung,
- die Datenpanne: Meldepflichten,
- der Überblick II: das Datenschutzmanagement-Handbuch.

Acht Punkte. Das ist machbar. Zudem sollten Sie sich mit diesen Themen unter der gedanklichen Prämisse beschäftigten, dass die DSGVO – allen Unkenrufen zum Trotz – nicht das gesetzgeberische Ziel hat, Unternehmen die unternehmerische und wirtschaftliche Tätigkeit zu erschweren,[3] sondern schlicht den Schutz von personenbezogenen Daten.[4] Blickt man darüber hinaus auf die Umsetzung der DSGVO nicht als bürokratisch erzwungene Auseinandersetzung mit dem Thema Datenverarbeitung und Datenschutz, sondern als guten Grund, die eigenen Prozesse im Unternehmen (endlich einmal?) zu evaluieren und zu analysieren, steht einem gut gelaunten Frühjahrsputz in Sachen Datenschutz nichts mehr im Weg. Und wenn Sie nun immer noch nicht überzeugt sind: die Komplexität von Steuern oder Sozialversicherungsabgaben bringt auch nur wenig Menschen wirklich Spaß – aber es muss nun einmal gemacht werden.

II. Prolog: Personenbezogene Daten und Datenverarbeitung – Was ist das eigentlich?

Um die nachfolgenden erläuterten Maßnahmen verstehen zu können, ist es wichtig zu wissen, was die Begriffe „personenbezogene Daten" und „Datenverarbeitung" eigentlich umfassen. An dieser Stelle ist der Gesetzgeber sehr konsequent und liefert mit Art. 4 Nr. 1 sowie Art. 4 Nr. 2 DSGVO die entsprechenden Definitionen:

„Personenbezogene Daten" sind „alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person beziehen". Damit sind natürlich Daten wie Namen, E-Mail-Adressen, Geburtsdaten personenbezogene Daten. Aber auch Online-Kennungen wie IP-Adressen, Cookies

[1] Zfm 2019, 97 ff.

[2] Warum Sie sich insbesondere als Personalverantwortliche mit diesen Themen auseinandersetzen müssen, wird sich im Verlauf der Lektüre verdeutlichen.

[3] Vgl. Erw.Gr. 4 der DSGVO, der einen Ausgleich mit der „unternehmerischen Freiheit" vorsieht; vgl. ferner Erw.Gr. 7 DSGVO, der als Zielsetzung der DSGVO Rechtssicherheit und Praktikabilität modernen Datenschutzes für Personen, Staat und Wirtschaft benennt. Im weiteren Sinne ist auch Art. 1 DSGVO in diesem Zusammenhang zu lesen, der neben dem Schutz personenbezogener Daten den freien Datenverkehr gesetzlich kodifiziert.

[4] Die dogmatische Diskussion um das genaue Schutzgut des Datenschutzes kann hier aus Platzgründen nicht wiedergegeben werden. Wenn Sie daran interessiert sind, sind die vielfältigen, auch kontroversen Debatten darüber auf Twitter unter den Hashtags #teamdatenschutz #Schutzgut insbesondere der KollegInnen @malteengeler, @privacyDE (Kirsten Bock) und @winfriedveil zu empfehlen.

oder Standortdaten sind Daten, die eine Person identifizierbar machen (können) und folglich als personenbezogene Daten einzuordnen sind.[5]

„Verarbeitung" ist „jeder … ausgeführten Vorgang … im Zusammenhang mit personenbezogenen Daten wie das Erheben, das Erfassen, die Organisation, das Ordnen, die Speicherung, die Anpassung oder Veränderung, das Auslesen, das Abfragen, die Verwendung, die Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung, den Abgleich oder die Verknüpfung, die Einschränkung, das Löschen oder die Vernichtung". Der Verarbeitungsbegriff ist sehr weit und erfasst faktisch jeden denkbaren Vorgang von Datenverarbeitungen.

Mit diesen Definitionen wird deutlich, warum sich jedes Unternehmen und insbesondere die Personalabteilung mit den Anforderungen der DSGVO auseinandersetzen muss: Gleich ob Karriere-Webseite, die guten alten Personalakten, der Einsatz von Bewerber- und Personalmanagement-Systemen oder die Beauftragung von Headhuntern – überall werden kontinuierlich personenbezogene Daten verarbeitet.

III. Die notwendigen Maßnahmen

Infolge der ständigen und allerorten stattfindenden Datenverarbeitungen ist es unabdingbar, sich zuerst einen Überblick über die Datenverarbeitungsprozesse im Unternehmen bzw. der jeweiligen Abteilung zu verschaffen. Und damit sind wir auch schon beim ersten Punkt des abzuarbeitenden Maßnahmenkataloges angekommen.

1. Der Überblick: Das Verzeichnis von Verarbeitungstätigkeiten

Gemäß Art. 30 DSGVO hat jeder Verantwortliche[6] ein „Verzeichnis von Verarbeitungstätigkeiten" zu erstellen. Der gesetzlich erforderliche Inhalt ergibt sich dabei aus Art. 30 Abs. 1 DSGVO, es muss enthalten:

- Namen und Kontaktdaten des Verantwortlichen,
- Kontaktdaten des/der Datenschutzbeauftragten, soweit bestellt,
- Zwecke der Verarbeitung,
- Beschreibung der betroffenen Personen- und Datenkategorien,
- Kategorien von Empfängern,[7]
- Datenübermittlungen in Drittländer, inkl. Dokumentation etwaiger Garantien zum Datenschutz,
- vorgesehene Fristen für die Löschung von Daten(-kategorien),
- allgemeine Beschreibung der technischen und organisatorischen Maßnahmen.

Das Verzeichnis von Verarbeitungstätigkeiten ist schriftlich zu führen (Abs. 3) und auf Verlangen der Aufsichtsbehörde vorzuzeigen (Abs. 4). Darüber hinaus gibt Art. 30 DSGVO keine Anforderungen bezüglich der Führung des Verzeichnisses vor.

Das könnte Unternehmensführungen nun dazu verleiten, das Verzeichnis von Verarbeitungstätigkeiten (VVT) tatsächlich sehr oberflächlich zu halten, um „einfach etwas zu Dokumentationszwecken da zu haben". Das kann man machen, wäre aber aus mehrfachen Gründen äußerst kurzsichtig. Zum einen würde ein solches VVT den Prüfern der Datenschutzbehörden kaum genügen, weil diese schnell erkennen können, ob das VVT tatsächlich halbwegs alle Verarbeitungsvorgänge im Unternehmen abbildet. Zum anderen erschwert sich das Unternehmen alle weitere Arbeit an der DSGVO-Compliance in unnötiger Weise. Es kann gar konstatiert werden, dass eine Erreichung der DSGVO-Compliance ohne ordentliches VVT scheitern muss.

Im VVT werden die Datenverarbeitungsprozesse des Unternehmens erfasst. Sind diese unbekannt, also auch die betroffenen Personen(-kategorien) sowie die jeweiligen Datenkategorien sowie ggf. Empfänger, können weder Informationen zur Datenverarbeitung noch Auftragsverarbeitungsverträge oder Verträge bzgl. der Übermittlung von Daten in unsichere Drittstaaten verfasst sowie sinnvoll Löschfristen[8] bestimmt werden. Kurz: die Umsetzung der DSGVO im Übrigen ist faktisch nicht möglich.

Anders ausgedrückt: Das VVT stellt das Datenschutz-Dashboard des Unternehmens und damit natürlich auch

[5] Siehe dazu weiter: Vollständiger Wortlaut des Art. 4 Nr. 1 DSGVO sowie EG 30; zum vorgehenden Meinungsstreit im Hinblick auf Personenbezogenheit von IP-Adressen abschließend: EuGH Urt. v. 19.10.2016 – C-582/14, BeckRS 2016, 82520 Rn 49 oder http://curia.europa.eu/juris/liste.jsf?language=de&num=C-582/14.

[6] So bezeichnet die DSGVO die natürlichen oder juristischen Personen, die für den Umgang mit den personenbezogenen Daten jeweils verantwortlich sind. Im Fall eines Unternehmens eben das Unternehmen.

[7] Auch Auftragsverarbeiter sind „Empfänger" personenbezogener Daten, vgl. Ernst, in: Paal/Pauly, 2. Aufl. 2018, Art. 4 Rn 57; währenddessen sind sie aber keine „Dritten" im Sinne des Art. 4 Nr. 10 DSGVO; das bedeutet, dass etwa der externe IT-Support oder der Anbieter des genutzten SaaS-Systems als Empfänger im VVT benannt werden müssen.

[8] Zu Löschfristen bei Personalauswahlverfahren: Diercks, Recruiting- und Personalauswahlverfahren unter DSGVO und BDSG, AuA, Heft 12/18.

der jeweiligen Abteilung dar. Um dieses optimal, d.h. vor allem auch als Grundinstrument für die effiziente Bildung der datenschutzrechtskonformen Unternehmensstruktur nutzen zu können, sollten für die Erstellung des VVT unbedingt Zeit und Ressourcen bereitgestellt werden.

a) Praxistipp: Aufnahme der Rechtsgrundlagen

Weiter sollten neben den gesetzlich geforderten Inhalten zur optimalen Nutzung des VTT auch sogleich die Rechtsgrundlagen der Datenverarbeitung benannt sowie – insbesondere in Fällen der Verarbeitung aufgrund von berechtigten Interessen nach Art. 6 Abs. 1 f) DSGVO – diese kurz begründet werden. Dies ist zwar an dieser Stelle nicht notwendig, jedoch benötigen Sie die Angabe der Rechtsgrundlage der Datenverarbeitung zum einen spätestens in den „Informationen zur Datenverarbeitung", zum anderen sollten Sie sich zwingend um die jeweiligen Rechtsgrundlagen der Verarbeitung Gedanken machen. Denn sicher kennen Sie den Grundsatz der Datenverarbeitung nach Art. 6 DSGVO, wonach eine Datenverarbeitung nur dann zulässig ist, wenn sie auf einer Rechtsgrundlage basiert. Übrigens, auch die Einwilligung ist eine Rechtsgrundlage (vgl. Art. 6 Abs. 1 a) DSGVO.[9]

Die Erfahrung zeigt: Je strukturierter und systematischer ein Unternehmen das VVT bzw. die Abbildung seiner Datenverarbeitungsvorgänge im Rahmen des Verzeichnisses angeht, desto leichter fällt es, die sonstigen Anforderungen der DSGVO zu erfüllen. Jede sorgfältige Arbeit hier spart an anderer Stelle Arbeit. So können bei sorgfältiger Arbeit zum Beispiel die Informationen zur Datenverarbeitung (dazu später mehr) quasi mit Copy & Paste aus dem VVT herausgezogen werden.

b) Praxistipp: Erstellen einer vollständigen Liste der Auftragsverarbeiter

Sie müssen an den entsprechenden Stellen im VVT jeweils die Empfänger der Daten benennen, auch die von Ihnen beauftragten Auftragsverarbeiter. Sinnvollerweise wird je Fachbereich bzw. den dort vorhandenen Datenverarbeitungsprozessen gleich eine Liste mit den Auftragnehmern beigefügt. Solche Listen müssen nämlich dann vorgehalten werden, wenn das Unternehmen selbst als Auftragnehmer agiert und im Rahmen eines Auftragsverarbeitungsvertrages seine Unterauftragnehmer benennen muss.

c) Praxistipp: Strukturieren nach Datenverarbeitungsprozessen

Ein VVT sollte unbedingt nach Datenverarbeitungsprozessen und nicht nach Systemprozessen strukturiert werden. Nehmen Sie hier nur das Beispiel von Personaldaten. Diese werden in der Regel über mehrere Systeme hinweg verarbeitet. Erfolgt nun eine Aufstellung nach System, geht der Blick für die Datenverarbeitungsvorgänge und wer daran beteiligt ist regelmäßig verloren bzw. muss unter großer Anstrengung aus verschiedensten Stellen des VVT zusammengesucht werden.

d) Praxisbeispiel: Aufbau eines VVT

Für den Aufbau und das Führen eines VVT gibt es keine verbindlichen Vorgaben. In der Kanzlei der Verfasserin wird regelmäßig so gearbeitet, dass zunächst die Datenverarbeitungen eines Unternehmens in einer Excel-Tabelle erfasst werden, um im Anschluss daraus das Verzeichnis zu erstellen. Am Anfang des VVT steht dabei ein Übersichts-Cluster wie folgt, in das aktive Verweisnormen eingearbeitet sind, so dass schnell zu den entsprechenden Stellen im VVT gesprungen werden kann:

Datenverarbeitung im Rahmen der	Zweck	Kategorien von Betroffenen und Daten	Rechtsgrundlagen	Empfänger (auch: Auftragsverarbeiter)	Löschfristen	Übermittlung an Dritte (inkl. Dritte in Drittstaaten)
Hauptleistung	4.1	5.1	6.1	7.1.	8.1	9.1.
Geschäftsverwaltung	4.2	5.2	6.2	7.2	8.2	9.2
Personalwesen	4.3	5.3.	6.3	7.3	8.3	9.3
Kandidaten- und Bewerberdaten	4.3.1	5.3.1	6.3.1	7.3.1	8.3.1	9.3.1
Personaldaten	4.3.2.	5.3.2.	6.3.2	7.3.2	8.3.2	9.3.2
Karriereseite	4.3.3	5.3.3	6.3.3	7.3.3	8.3.3	9.3.3
Finanz- und Lohnbuchhaltung	4.4	5.4	6.4	7.4	8.4	9.4
Unternehmensseite	4.5	5.5	6.5	7.5.	8.5	9.5

[9] Allerdings sollte diese nur gewählt werden, wenn tatsächlich keine andere Rechtsgrundlage wie die Verarbeitung aufgrund eines Vertragsverhältnisses (Art. 6 Abs. 1 b) DSGVO) oder aufgrund berechtigten Interesses (Art. 6 Abs. 1 f) DSGVO) zur Verfügung steht.

Das ist nun eine sehr einfache Übersicht über die möglichen Inhalte eines VVT. Dabei kann ein Unternehmen natürlich mehr als eine Hauptleistung erbringen und alle Kategorien können Unterabschnitte aufweisen. Das ist hier beispielhaft für den Bereich Personal gemacht.

2. Die Aufklärung: Informationen zur Datenverarbeitung

Ein wichtiges Ziel der DSGVO ist die Transparenz der Datenverarbeitung. Dies wird unter anderem durch die dem Verantwortlichen obliegenden Informationspflichten erreicht, welche in Art. 12–14 DSGVO niedergelegt sind. Die Betroffenen müssen demnach „Informationen zur Datenverarbeitung" erhalten können.

Bei „Informationen zur Datenverarbeitung" handelt es sich letztlich um nicht viel anderes als das, was bisher unter dem Begriff „Datenschutzerklärung" aufgrund der Vorgabe von § 13 TMG im Zusammenhang mit Webseiten bekannt war.

Nach der DSGVO ist nun nicht mehr nur im Internet über die Verarbeitung von personenbezogenen Daten aufzuklären, sondern stets und grundsätzlich. Das heißt, es muss nicht der Webseitenbesucher oder die Software-as-a-Service-NutzerIn über die Datenverarbeitung aufgeklärt werden, sondern auch Kunden, Lieferanten, Bewerber und Mitarbeiter.

Der Katalog der Informationen, die dem Betroffenen bereitgestellt werden müssen, ist dabei in Art. 13 Abs. 1 und 2 DSGVO[10] niedergelegt:

- Name und Kontaktdaten des Verantwortlichen,
- ggf. Kontaktdaten des Datenschutzbeauftragten,
- Zwecke der Verarbeitung und die Rechtsgrundlage,
- ggf. das berechtigte Interesse an der Verarbeitung,
- ggf. Kategorien von Empfängern der Daten,
- ggf. Übermittlung an Drittstaaten oder internationale Organisationen,
- Dauer der Speicherung bzw. Löschungskriterien,
- Aufklärung über Betroffenenrechte (Auskunft, Datenportabilität, Beschwerde, Widerruf und Widerspruch).

Hier zeigt sich nun das erste Mal, warum eine intensive Arbeit am VVT letztlich dem effektiven und effizienten Workflow im Datenschutzmanagement dient. Denn alle für die Informationen zur Datenverarbeitung notwendigen Informationen können dem VVT unmittelbar entnommen und bei guter Aufbereitung tatsächlich fast vollständig per Copy & Paste übernommen werden.

a) Praxistipp: regelmäßig notwendige IDV aus Sicht der Personalabteilung

Aus Sicht der Personalabteilung sind regelmäßig drei verschiedene Betroffenengruppen über deren Datenverarbeitungen zu informieren: die Besucher der (Karriere-) Webseite, die Kandidaten und Bewerber[11] sowie die Mitarbeiter des Unternehmens.

b) Praxistipp: Umsetzung der Informationspflicht

Wie in Teil 1 schon geklärt wurde, bedeutet das nun nicht, dass den Betroffenen Brieftauben übersendet werden und diese die Dokumente mit Siegelwachs gezeichnet per berittenem Boten zurückreichen müssten. Die Betroffenen müssen nur informiert werden, das heißt leichten Zugang zu den Informationen erhalten können.

Die Informationen zur Datenverarbeitung im Zusammenhang mit der Karrierewebseite und im Zusammenhang mit Kandidaten und Bewerbern können ganz einfach unter dem Punkt „Datenschutz" auf der Karrierewebseite selbst im Internet vorgehalten werden. Die Betroffenen können über den Ort der Abrufmöglichkeit sodann per Hinweis in Signaturen in E-Mails oder über Hinweise in (analogen wie digitalen) Stellenanzeigen informiert werden.[12]

Die Informationen zur Datenverarbeitung für Mitarbeiter können wiederum im Intranet vorgehalten und der Mitarbeiter hierüber bei Vertragsschluss informiert oder natürlich auch einfach jedem Mitarbeiter zum Vertragsschluss ausgehändigt werden.

[10] Informationspflichten gemäß Art. 13 Abs. 2 DSGVO sind zwar nach dem Wortlaut nur insoweit zu erteilen, als dies für eine faire und transparente Verarbeitung notwendig ist, angesichts der Unsicherheit der gesetzlichen Formulierung bietet es sich aber an, stets Informationen gemäß Art. 13 Abs. 2 DSGVO zu erteilen; vgl. auch Paal/Hennemann, in: Paal/Pauly, 2. Aufl. 2018, Art. 13 Rn 22.

[11] Siehe dazu ausführlich: Diercks, Active Sourcing und Talent Relationship Management (TRM) unter der Datenschutzgrundverordnung I – Teil 9 zur EU-DSGVO, Art. vom 21.6.2017, https://diercks-digital-recht.de/2017/06/active-sourcing-und-talent-relationship-management-trm-unter-der-datenschutzgrundverordnung-i-teil-9-zur-eu-dsgvo/.

[12] Vgl. Erw.-Gr. 58; Knyrim, in: Ehmann/Selmayr, 2. Aufl. 2018, Art. 13 Rn 22.

3. Die Verhältnisse zu „Dritten“: CtC, JCC or DPA[13]?

Als Unternehmen und vor allem als Personalabteilung arbeitet man datenschutztechnisch betrachtet heutzutage selten allein. Das Bewerbermanagementsystem ist in der Regel ein Software-as-a-Service-System, das Personalmanagementsystem ebenfalls und beide verfügen über Schnittstellen. Die Lohnbuchhaltung macht eventuell auch ein externer Dienstleister. Und angesichts des Arbeitsmarktes sind darüber hinaus auch drei Headhunter mit der Rekrutierung von Spezialisten beschäftigt.

In all diesen Konstellationen werden Daten verarbeitet. Wichtig ist hier zu klären, ob es sich um ein Auftragsverhältnis i.S.v. Art. 28 DSGVO, eine gemeinsame Verarbeitung i.S.v. Art. 26 DSGVO oder um eine Übermittlung zwischen zwei Verantwortlichen handelt, die die Daten jeweils zu eigenen Zwecken oder Mitteln verarbeiten.

Im Rahmen dieses Aufsatzes können diese drei verschiedenen Formen der Zusammenarbeit mit „Dritten“[14] nicht erläutert werden. Der Verantwortliche für eine Datenverarbeitung muss jedoch prüfen, ob eine Datenverarbeitung bei einem Dritten im Auftrag erfolgt oder ob die Daten mit gemeinsamen Mitteln und zu gemeinsamen Zwecken mit einem Dritten verarbeitet werden. In diesen Fällen sind nämlich gemäß der DSGVO nach Art. 28 bzw. Art. 26 DSGVO die dort vorgesehenen Verträge abzuschließen.[15]

Auch hier zeigt sich wieder die Effizienz eines guten VVT. Denn im Rahmen dessen sind diese Prüfungen und die notwendigen Zuordnungen letztlich schon erfolgt und aus den im VVT vorhandenen Daten können regelmäßig leicht die entsprechenden Verträge gestaltet werden.

4. Die konkreten Maßnahmen: technische und organisatorische Maßnahmen

Gemäß Art. 32 DSGVO müssen Verantwortliche

> *„... unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeiten und Schwere des Risikos ... geeignete technische und organisatorische Maßnahmen [treffen], um ein dem Risiko angemessenes Schutzniveau zu gewährleisten“.*

Dies bedeutet nichts anderes, als dass Verantwortliche durch technische wie organisatorische Maßnahmen eine ordentliche, sichere Verarbeitung von personenbezogenen Daten im Unternehmen sicherstellen können müssen. Personenbezogene Daten müssen also vor dem unbefugten Zugriff Dritter ebenso wie vor unbefugter Veränderung oder Löschung geschützt werden.

a) Technische Maßnahmen

Als mögliche technische Maßnahmen nennt Art. 32 Abs. 1 DSGVO

- die Pseudonymisierung,
- die Sicherstellung der Vertraulichkeit, Integrität, Verfügbarkeit und Belastbarkeit von Systemen und Diensten,
- die Wiederherstellbarkeit nach physischen und technischen Zwischenfällen sowie
- regelmäßige Überprüfungs-, Bewertungs- und Evaluierungsverfahren.

Diese Punkte mögen ein erster Anhaltspunkt sein, bei einer strukturierten Erstellung der eigenen technischen Maßnahmen hilft diese Auflistung jedoch kaum weiter.

Deswegen wenden wir uns in diesem Fall der Anlage zum § 9 BDSG-alt zu. Bei § 9 BDSG handelt es sich um die deutsche Vorgängernorm des Art. 32 DSGVO. In der Anlage dazu werden technische Maßnahmen aufgezählt und erläutert, darunter: Zutritts-, Zugangs-, Zugriffs-, Weitergabe-, Eingabe-, Auftrags-, Verfügbarkeits- und Trennungskontrolle. Wenn dieser Katalog durchgegangen und die in dem jeweiligen Unternehmen vorhandenen Maßnahmen nach diesem Katalog erfasst werden, etwa im Hinblick auf Zugriffskontrollen die Beschreibung der Zugriffsberechtigungen verschiedener Mitarbeitergruppen, existiert eine gute Grundlage für die technischen Maßnahmen – auch im Sinne der DSGVO.[16]

Auch hier wird wieder einmal die (IT-)Infrastruktur strukturiert und analysiert. Das Ergebnis ist unter „technische und organisatorische Maßnahmen“ im Verzeichnis von Verarbeitungstätigkeiten festzuhalten.

[13] Die Begriffe CtC, JCC und DPA sind gängige Kurzformen für die drei verschiedenen Formen der Datenverarbeitung mit „Dritten“ bzw. bezeichnet die dazugehörigen Verträge. Im Einzelnen: CtC meint die Datenverarbeitung von Controller-to-Controller oder Verantwortlicher zu Verantwortlichem; JCC meint die Datenverarbeitung im Rahmen eines Joint-Control-Contracts also die gemeinsame Verarbeitung nach Art. 26 DSGVO, DPA meint Data Protection Agreement und damit den Auftragsverarbeitungsvertrag nach Art. 28 DSGVO.

[14] „Dritte“ hier stets in Anführungsstrichen, da ein Auftragsverarbeiter – wie schon erläutert – im Sinne der DSGVO zwar einen Empfänger, aber keinen Dritten darstellt.

[15] Im Konzern sieht die Datenverarbeitung einerseits wesentlich einfacher, andererseits noch wesentlich komplexer aus.

[16] So i.E. auch: Martini, in: Paal/Pauly, 2. Aufl. 2018, Art. 32 Rn 29.

b) Organisatorische Maßnahmen

Der zweite Teil des Art. 32 DSGVO, der Inhalt der Verpflichtung zu organisatorischen Maßnahmen, erschließt sich hingegen nicht auf den ersten Blick. Sinn und Zweck von organisatorischen Maßnahmen erschließen sich jedoch schnell bei dem Gedanken daran, was System-Administratoren gerne als das Hauptproblem und das größte Risiko für die IT-Sicherheit identifizieren: den Anwender vor dem PC.

Die organisatorischen Maßnahmen sind also das Äquivalent zu technischen Maßnahmen im Hinblick auf die Mitarbeiter. So kann ein System unter technischen Gesichtspunkten aufgrund einer entsprechenden Zugriffskontrolle zwar als sehr sicher eingestuft werden,[17] aber diese Sicherheit kann durch einen Anwender unterlaufen werden, der das Passwort „123456" vergibt.

Damit wird deutlich, dass technische Maßnahmen allein dem Datenschutz und der Datensicherheit nicht Genüge tun können. Vielmehr müssen technische Maßnahmen von organisatorischen Maßnahmen gestützt werden. Organisatorische Maßnahmen sind insbesondere Richtlinien bzw. Betriebsvereinbarungen, in denen unter anderem verbindlich festgelegt wird,

- wie mit Passwörtern umzugehen ist (Länge, Sonderzeichen/Zahlen),
- dass Arbeitsgeräte beim Verlassen des Arbeitsplatzes zu sperren sind,
- dass an öffentlichen Orten nur mit Sichtschutzfolien zu arbeiten ist,
- dass Arbeitsgeräte an öffentlichen Orten nicht unbeobachtet gelassen werden (Klassiker: Laptop bleibt ungesperrt am Platz, während der Mitarbeiter Kaffee aus dem Zugrestaurant holt),
- dass unbekannte USB-Sticks nichts im Firmennetzwerk zu suchen haben.

Die Verbindlichkeit der Maßnahmen ist entscheidend. Zum einen bedeutet dies nämlich, dass Verstöße auch arbeitsrechtlich sanktioniert werden können und damit nicht nur die Warnfunktion erhöht ist, sondern auch die Durchsetzbarkeit der Maßnahmen gewährleistet werden kann.[18] Zum anderen werden mit derart verbindlichen Richtlinien auch zugleich die Dokumentationspflichten nach der DSGVO umfänglich erfüllt.[19] Nichtsdestotrotz sollten auch Schulungen der Mitarbeiter Teil der organisatorischen Maßnahmen sein, um die Bedeutung der Inhalte solcher Richtlinien zu transportieren und zu transferieren.

5. Privacy by Design and Default

Wie hier schon mehrfach erwähnt, setzen Unternehmen, insbesondere Personalabteilungen, eine Vielzahl von Software-Lösungen ein.

Hier stellt die DSGVO eine weitere Anforderung an die Verantwortlichen. Nämlich die Verpflichtung zum Datenschutz durch Technikgestaltung und Voreinstellung nach Art. 25 – wesentlich bekannter als „Privacy by Design & by Default".

a) Privacy by Design

Diese Verpflichtung trifft den verantwortlichen Anwender schon bei dem Gedanken an den Einsatz einer neuen Software-Lösung. Gemäß Art. 25 Abs. 1 DSGVO muss die entwickelte (bzw. angekaufte oder im Rahmen eines Software as a Service genutzte) Software „unter Berücksichtigung des Stands der Technik, der Implementierungskosten und der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der unterschiedlichen Eintrittswahrscheinlichkeit und Schwere der mit der Verarbeitung verbundenen Risiken für die Rechte und Freiheiten natürlicher Personen … dafür ausgelegt [sein], die Datenschutzgrundsätze wie etwa Datenminimierung wirksam umzusetzen".

Vereinfacht ausgedrückt bedeutet dies, dass die Technologie von vornherein so gestaltet sein muss, dass sie unter Beachtung der Grundsätze des Schutzes personenbezogener Daten operieren kann. Im Hinblick auf den Grundsatz der Datenminimierung muss eine Anwendung etwa so datenarm wie möglich funktionieren können. Im Hinblick auf die technische Datensicherheit muss eine Anwendung hingegen von vornherein ein technisches Schutzniveau aufweisen, das den verarbeiteten Daten gegenüber angemessen ist. Folglich müssen etwa Personalmanagementsysteme, die auch sensible Daten wie etwa Krankmeldungen enthalten, ein weit höheres Schutzniveau aufweisen als etwa der Urlaubskalender.

[17] Vgl. Anlage 1 Nr. 3 zu § 9 BDSG-alt.

[18] Vgl. zu Richtlinien und Betriebsvereinbarungen als organisatorischen Maßnahmen u.a.; Martini, in: Paal/Pauly, 2. Aufl. 2018, Art. 32 Rn 66.

[19] Ausführlich zu organisatorischen Maßnahmen insbesondere im Kontext von Arbeitsrecht und Compliance: Diercks, Was die DSGVO mit IT-Richtlinien, Arbeitsrecht und Compliance zu tun hat und warum das jetzt für Unternehmen wichtig ist, Art. v. 24.1.2017, https://diercks-digital-recht.de/2017/01/die-datenschutzgrundverordnung-macht-it-richtlinien-feuer-unter-dem-hintern-teil-7.

Diese Beispiele zeigen aber auf, dass die datenschutzkonforme Technikgestaltung keine manifeste Größe ist, sondern dass die Anforderungen im Einzelfall stark divergieren können.[20]

b) Privacy by Default

Nach Art. 25 Abs. 2 S. 1 DSGVO ist der Verantwortliche verpflichtet, die Voreinstellungen einer Anwendung in der datenschutzfreundlichsten Ausprägung vorzunehmen. Dies bedeutet: Kann der Nutzer einer Anwendung zwischen mehreren Optionen wählen, ist im Rahmen des Verarbeitungszweckes diejenige voreinzustellen, welche die „datenschonendste" ist. In einem Bewerbermanagementsystem ist etwa als Löschfrist für eingegangene Bewerbungen die nach dem Löschfristenkonzept des Unternehmens kürzeste als Voreinstellung einzutragen.[21] Hierdurch soll eine möglichst enge Zweckbindung sichergestellt und der Erforderlichkeitsgrundsatz der Datenverarbeitung gewahrt werden.[22]

c) Praxistipp: Prüfen Sie Anwendungen vor dem Erwerb!

Zusammenfassend lässt sich sagen, dass bei Privacy by Design die Frage „Benötige ich diese Daten wirklich?" und bei der Privacy by Default die „Gibt es eine datenschonendere Alternative?" zu stellen ist.

Dabei ist unbedingt darauf hinzuweisen, dass Anwendungen vor dem Erwerb im Hinblick auf die Technikgestaltung gemäß den vorstehenden Kriterien zu prüfen sind – und nicht nur auf die Wünsche der Fach- und IT-Abteilung. Die Erfahrung besagt, dass Unannehmlichkeiten äußerst groß werden können, wenn eine Software-Anwendung unternehmensweit erst (mit langen Lizenzzeiträumen) erworben und dann auf eine datenschutz- und arbeitsrechtliche Compliance unter deutschem bzw. europäischem Recht untersucht wird.

6. Die Risikoprüfung: Datenschutzfolgeabschätzung

Die sogenannte Datenschutzfolgeabschätzung gemäß Art. 35 DSGVO verpflichtet Verantwortliche dazu, besonders risikoreiche Verarbeitungsvorgänge vorab schon auf mögliche Gefahren für Rechte und Freiheiten der betroffenen Person zu überprüfen. Mit der Datenschutzfolgeabschätzung wird eine wichtige Grundannahme des Gesetzgebers statuiert, wonach die Bewertung der Angemessenheit von Datenschutzmaßnahmen vor allem davon abhängig ist, welches Risiko die Datenverarbeitung für den Grundrechtsträger mit sich bringt.[23]

Nach Art. 35 DSGVO muss eine Datenschutz-Folgeabschätzung vorgenommen werden, wenn

> *„... eine Form der Verarbeitung, insbesondere bei Verwendung neuer Technologien, aufgrund der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung voraussichtlich ein hohes Risiko für die Rechte und Freiheiten natürlicher Personen zur Folge hat."*

Nach Art. 35 Abs. 1 und 3 DSGVO liegt ein solches hohes Risiko insbesondere vor bei

- einer systematischen und umfassenden Bewertung persönlicher Aspekte,
- bei Verarbeitung von besonderen Datenkategorien (Art. 9 DSGVO) sowie
- bei systematischer umfangreicher Überwachung öffentlich zugänglicher Bereiche.

Diese relativ weiten und vagen Anwendungsfelder des Art. 35 DSGVO haben die Landesaufsichtsbehörden inzwischen jedoch konkretisiert und sogenannte „Positiv-Listen" herausgegeben, in denen Fallgestaltungen skizziert sind, bei denen die Aufsichtsbehörden eine Datenschutzfolgeabschätzung für zwingend notwendig halten.[24]

Für den Datenschutz im Beschäftigungsverhältnis wird dabei insbesondere folgender Auszug aus der Positiv-Liste des Hamburgischen Beauftragten für Datenschutz und Informationsfreiheit relevant:

> *„Verarbeitung von umfangreichen Angaben über das Verhalten von Beschäftigten, die zur Bewertung ihrer Arbeitstätigkeit derart eingesetzt werden können, dass sich Rechtsfolgen für die Betroffenen ergeben oder diese in anderer Weise erheblich beeinträchtigen."*[25]

Arbeitszeiterfassungssysteme und auch manch andere Personalmanagementanwendungen können regelmäßig theoretisch auch zur Bewertung von Beschäftigten im vorgenannten Rahmen eingesetzt werden. Dabei ist es wichtig zu wissen, dass es nicht darauf ankommt, ob der verantwortliche Unternehmer den Einsatz dieser Systeme tatsächlich auch zur Bewertung der Arbeitstätigkeit ge-

[20] Martini, in: Paal/Pauly, 2. Aufl. 2018, Art. 25 Rn 36.
[21] Siehe zu Löschfristen bei Personalauswahlverfahren: Diercks, Recruiting- und Personalauswahlverfahren unter DSGVO und BDSG, AuA, Heft 12/18.
[22] Hartung, in: Kühling/Buchner, 2. Aufl. 2018, Art. 25 Rn 25.
[23] Martini, in: Paal/Pauly, 2. Aufl. 2018, Art. 35 Rn 6.
[24] Eine Sammlung aller Positiv-Listen findet sich unter https://www.adorga-solutions.de/dsfa-art-35-ds-gvo-positivliste-der-aufsichtsbehoerden/.
[25] HmbBDI, Liste von Verarbeitungsvorgängen nach Art. 35 Abs. 4 DSGVO, S. 6, https://datenschutz-hamburg.de/dsgvo-information/art-35-mussliste/.

plant und gewollt hat, es kommt nur darauf an, ob das System eine solche Bewertung prinzipiell ermöglicht. Dies ergibt sich schon aus dem Gesetzeswortlaut („können").

Infolgedessen werden in diesem Rahmen regelmäßig Datenschutzfolgeabschätzungen notwendig sein. Jedenfalls ist aber die Prüfung zu dokumentieren, wenn bewusst keine Datenschutzfolgeabschätzung vorgenommen wurde.[26]

7. Die Datenpanne: Meldepflichten

Sie haben getan, was Sie konnten und trotzdem kann es sein, dass etwas passiert. „Etwas passiert" meint in diesem Fall eine Verletzung des Schutzes von personenbezogenen Daten im Sinne von Art. 4 Nr. 12 DSGVO.

Demnach liegt eine sogenannte Datenpanne vor bei einer

> *„... Verletzung, die, ob unbeabsichtigt oder unrechtmäßig, zur Vernichtung, zum Verlust, zur Veränderung oder zur unbefugten Offenlegung von beziehungsweise zum unbefugten Zugang zu personenbezogenen Daten führt".*

Das ist sehr abstrakt, aber einzuordnen sind darunter ebenso beispielhaft wie plastisch etwa die folgenden Fälle:

- ein Scriptkiddie mit zu viel Langeweile, der/die es versucht und geschafft hat, in das Bewerbermanagementsystem des Unternehmens einzudringen und Teile daraus zu löschen,
- der Fehler eines Programmierers, weswegen Personaldatensätze ungeschützt im Internet lagen,
- ein Mitarbeiter, der eine E-Mail statt in bcc an einen offenen Verteiler von 100 Personen versendete.[27]

In einem solchen Fall legt die DSGVO dem Verantwortlichen Melde- und ggf. Benachrichtigungspflichten nach Art. 33 und 34 DSGVO auf.

a) Meldepflicht nach Art. 33 DSGVO

Im Fall einer Datenpanne ist der Vorfall nach Art. 33 DSGVO binnen 72 Stunden nach Kenntnis des Vorfalls an die zuständige Behörde zu melden und der Vorfall zu dokumentieren.

Dies gilt nur dann nicht, wenn die Datenpanne voraussichtlich nicht zu einem Risiko für die Rechte und Freiheiten der Person führt. Dabei ist allerdings anzumerken, dass jeder Verletzung des Datenschutzes ein ebensolches Risiko inhärent ist. Schließlich ist im Gesetzestext nur von einem Risiko und nicht von einem „schweren" oder „überdurchschnittlichen" Risiko die Rede. Da die Prognoseentscheidung darüber, ob die Datenpanne zu einem „Risiko" führt, bei dem Verantwortlichen liegt, ist dieser gut beraten, der Behörde lieber eine Datenpanne zu viel als zu wenig zu melden.

Zum einen, da bei einer ordentliche Meldung nach Art. 33 Abs. 3 DSGVO unter

- Beschreibung der Art der Verletzung, Angabe der betroffenen Datenkategorien und soweit möglich der ungefähren Zahl der betroffenen Personen,
- Namen und Kontaktdaten des Datenschutzbeauftragten und einer sonstigen Anlaufstelle,
- Beschreibung der wahrscheinlichen Folgen der Verletzung,
- Beschreibung bereits ergriffener oder vorgeschlagener Gegenmaßnahmen, ggf. auch Abhilfemaßnahmen zur Schadensmilderung

die Chancen – jedenfalls bei leichten bis mittleren Datenpannen – gut stehen, dass die zuständige Behörde nicht viel mehr sagt als „Vielen Dank. Haben wir zur Kenntnis genommen". Zum anderen, da eine unterlassene, aber doch erforderliche Meldung in jedem Fall einen sanktionsfähigen Verstoß gegen die DSGVO darstellt.

aa) Praxistipp: Prozessanweisungen bereithalten

Art. 32 DSGVO sieht nur 72 Stunden zur Meldung der Datenpanne vor. Zwar muss die Meldung nicht vollständig binnen dieses Zeitraums geschehen, sondern es können auch nach Art. 33 Abs. 4 DSGVO einzelne Informationen nachgereicht werden, dies entbindet aber den Verantwortlichen nicht davon, die Meldung selbst innerhalb von 72 Stunden vorzunehmen und seiner Informationspflicht nach Abs. 3 schon soweit es möglich ist nachzukommen.[28]

Von daher ist es ratsam, Unternehmensprozesse für den Fall der Fälle vorzuhalten und alle Mitarbeiter mittels einer entsprechenden und leicht zugänglichen Prozessanweisung im Fall einer Datenpanne beim Einleiten der ersten Maßnahmen zu stützen, so dass kurzfristig binnen der genannten Fristen reagiert werden kann.

Derartige Prozessanweisungen für die Mitarbeiter sind nicht nur tatsächlich hilfreich bei der Begegnung von Datenpannen, sondern stellen zugleich wiederum organisatorische Maßnahmen im Sinne von Art. 32 DSGVO dar.

[26] Ausführlich zum Thema Datenschutzfolgeabschätzungen: Diercks, Die EU-DSGVO ist da! Teil 4 – Die Pflichten der Unternehmen, genau genommen: Dokumentationspflichten, Datensicherungspflichten und Meldepflichten, Ziffer 2 c), Art. vom 31.8.2016, https://diercks-digital-recht.de/2016/08/die-eu-datenschutzgrundverordnung-eu-dsgvo-ist-da-worauf-muessen-sich-unternehmen-einstellen-teil-4/.

[27] Vgl. hierz: Randt, in: Kühling/Buchner, 2. Aufl. 2018, Art. 4 Nr. 12 Rn 8a.

[28] Jandt, in: Kühling/Buchner, 2. Aufl. 2018, Art. 33 Rn 22 f.

bb) Praxistipp: Prozessanweisungen nicht nur für Datenpannen
Die Erstellung und das Vorhalten solcher Prozessanweisungen bieten sich übrigens auch für die Fälle von Auskunftsverlangen und den Wünschen einer Datenübertragbarkeit an.

b) Die Benachrichtigungspflicht
In den Fällen, in denen die Datenpanne „voraussichtlich ein hohes Risiko für die persönlichen Rechte und Freiheiten natürlicher Personen zur Folge hat", sieht Art. 34 DSGVO auch eine Benachrichtigungspflicht gegenüber den Betroffenen vor.

Während also eine Meldung bei der zuständigen Behörde nahezu immer zu erfolgen hat, besteht eine Benachrichtigungspflicht gegenüber den Betroffenen eher selten. Im Zweifel kann auch hier zunächst eine Absprache mit der Behörde stattfinden, denn diese kann einem Verantwortlichen auch aufgeben, die Betroffenen zu benachrichtigen.

8. Der Überblick II: Das Datenschutzmanagement-Handbuch

Ist das Unternehmen so weit gekommen, dass der hier aufgezeigte Grundstock an Maßnahmen und Dokumenten vorhanden ist, dann sollten diese in einem Datenschutzmanagement-Handbuch zusammengefasst werden.

Schließlich ist jedes Unternehmen aufgrund seiner Rechenschaftspflichten nach Art. 5 Abs. 2 DSGVO dazu verpflichtet, alle ihre Bemühungen auf dem Bereich des Datenschutzes zu dokumentieren und gegebenenfalls der Aufsichtsbehörde auf Anfrage Rechenschaft abzulegen. Nach Art. 58 DSGVO kann die Datenschutzbehörde dabei auch verlangen, dass der Verantwortliche ihr die entsprechenden Nachweise zur Verfügung stellt. Hat ein Unternehmen seine Bemühungen zum Datenschutz nun in einem Datenschutzmanagement-Handbuch zusammengetragen und kann diese Dokumentation bei Verlangen unmittelbar überreichen, wird der oder die BehördenvertreterIn voraussichtlich der weiteren Prüfung gegenüber schon einmal positiv eingestellt sein.

IV. Fazit – Oder: Wie bitte? Das müssen wir als Personalabteilung alles berücksichtigen?!

„Dafür ist doch Compliance zuständig!", lautet oft der entsetzte Ausruf aus der Personalabteilung, wenn ihr gewahr wird, welche Pflichten die DSGVO auferlegt. Die Antwort lautet an dieser Stelle „Ja, da haben Sie Recht und zugleich haben Sie Unrecht."

Natürlich ist Compliance oder konkret der Datenschutzbeauftragte dafür verantwortlich, die Umsetzung der DSGVO im Unternehmen zu begleiten und voranzutreiben. Doch woher sollte Compliance wissen, welche Datenverarbeitungsvorgänge konkret in der Personalabteilung vorgenommen werden? Wie soll der Datenschutzbeauftragte Kenntnis von den Sourcing-Verfahren, dem Talentpool oder dem Plan des Einsatzes einer neuen Software zur Personalauswahl erhalten? Natürlich gar nicht. Es sei denn, diese Informationen hat die Personalabteilung im Sinne des Verzeichnisses von Verarbeitungstätigkeiten aufgeführt. Ebenso kann die Personalabteilung keine den Art. 13 und 14 DSGVO entsprechenden Informationen zur Datenverarbeitung für die Karrierewebseite und die Bewerber erstellen, wenn keine Kenntnis darüber besteht, ob etwa die Webseite bei Fremdanbietern (ein Empfänger von Daten) gehostet wird oder die Bewerberdaten in externen Clouddatenbanken verarbeitet werden. Dies sind Informationen, die aus der IT kommen müssen und die ebenfalls in einem gut geführten Verzeichnis von Verarbeitungstätigkeiten erfasst sind. Dies sind nur einige wenige Beispiele dafür, dass ein Silo-Denken und -Arbeiten im Datenschutz nicht funktioniert.

Beschäftigtendatenschutz beginnt und endet nun einmal nicht damit, ob Sie einen Bewerber in die Datenschutzerklärung einwilligen lassen müssen.[29]

Beschäftigtendatenschutz kann nur dann funktionieren, wenn Sie sich auch als Personalabteilung mit den Grundlagen der Anforderungen an den Datenschutz nach der DSGVO vertraut machen und wenn Sie Ihre Datenverarbeitungsprozesse einmal gemeinsam mit Compliance, Datenschutz und der IT-Abteilung evaluieren und analysieren.

Beschäftigtendatenschutz ist zunächst einmal … Datenschutz.

Rechtsanwältin Nina Diercks, M. Litt (University of Aberdeen) führt die Anwaltskanzlei Diercks sowie den Blog Diercks Digital Recht (bis 2017: Social Media Recht Blog). In ihrer täglichen Arbeit beschäftigt sie sich mit all den juristischen Fragen, denen sich Unternehmen im Zusammenhang mit der fortlaufenden Verschränkung der analogen und digitalen Welt auseinandersetzen müssen. Ihre Tätigkeitsschwerpunkte liegen in der Beratung, Vertragsgestaltung und Vertretung auf dem Gebiet des IT-, Medien-, Datenschutz- und Arbeitsrechts. Daneben ist die Anwältin als Referentin sowie als Interviewpartnerin und (Gast-)Autorin gefragt und steht für alle diese Tätigkeiten gern zur Verfügung.

[29] Nein, müssen Sie nicht! Siehe Teil 1!