BfDI Der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit

Leitfaden zur Datenverarbeitung im Personalrat

Vorwort

Dieser Leitfaden soll den Personalvertretungen bei den öffentlichen Stellen des Bundes als Orientierung für den Umgang mit personenbezogenen Daten von Beschäftigten dienen. Er soll einen Überblick über die Rechtslage verschaffen und als Einstieg zu sich konkret stellenden Fragen zulässiger Datenverarbeitung in der Personalratsarbeit weiterhelfen. Zur vertiefenden Prüfung von Rechtsfragen wird die Lektüre der konkreten Rechtsvorschriften empfohlen.

Der Leitfaden gibt die Rechtsauffassung des Bundesbeauftragten für den Datenschutz und die Informationsfreiheit (BfDI) wieder, welche auch bei der Prüfung und Bewertung von Beschwerden der betroffenen Personen und bei datenschutzrechtlichen Kontrollen angesetzt wird.

Dieses Papier erhebt keinen Anspruch auf Vollständigkeit. Eine Anpassung an etwaige Leitlinien der Datenschutzkonferenz oder des Europäischen Datenschutzausschusses wird ausdrücklich vorbehalten. Es beschränkt sich im Übrigen auf das Bundespersonalvertretungsrecht. Soweit in einigen Stellen, die der Kontrolle des BfDI unterstehen, das Betriebsverfassungsgesetz gilt, soll dieser Leitfaden die sinngemäße Anwendung erleichtern.

1. Allgemeines

1.1 Rechtsgrundlagen

Rechtsgrundlage für die Datenverarbeitung in der Bundesrepublik Deutschland ist als unmittelbar geltendes Recht die Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz: die Datenschutzgrundverordnung (DSGVO). Diese EU-Verordnung lässt den nationalen Gesetzgebern noch gewisse Spielräume, so auch im Beschäftigungskontext. Hierzu erlaubt Artikel 88

DSGVO den Mitgliedstaaten durch Rechtsvorschriften oder Kollektivvereinbarungen spezifischere Vorschriften vorzusehen.

Auf dieser Ermächtigungsgrundlage beruht insbesondere § 26 Bundesdatenschutzgesetz (BDSG). Danach dürfen für Zwecke des Beschäftigungsverhältnisses personenbezogene Daten verarbeitet werden, wenn dies u.a. zur Ausübung oder Erfüllung von Rechten und Pflichten der Interessenvertretung der Beschäftigten erforderlich ist (§ 26 Abs. 1 Satz 1 BDSG).

Wer Beschäftigte im Sinne des BDSG sind, wird in § 26 Abs. 8 BDSG definiert (s.u. Nr. 1.3).

Zu den Interessenvertretungen zählen u.a. die Personalräte. Deren Rechte und Pflichten können sich aus einem Gesetz oder einem Tarifvertrag, einer Betriebs- oder Dienstvereinbarung (Kollektivvereinbarung) ergeben. Die Gesetze, aus denen sich Rechte und Pflichten der Interessenvertretungen ergeben, sind vielfältig. Das Arbeitsschutzgesetz, das Mutterschutzgesetz, das Allgemeine Gleichstellungsgesetz, das Sozialgesetzbuch Neuntes Buch oder das Entgelttransparenzgesetz und nicht zuletzt das Bundesbeamtengesetz oder das Bundespersonalvertretungsgesetz sind nur ein kleiner Ausschnitt der zahlreichen Rechtsgrundlagen, die im Beschäftigungskontext die Verarbeitung personenbezogener Daten mit sich bringen.

1.2 Grundsätze

Bei der Verarbeitung personenbezogener Daten sind die Grundsätze des Art. 5 DSGVO zu beachten.

Der Datenschutz ist geprägt von dem Grundrecht auf informationelle Selbstbestimmung. Danach ist zunächst jede Person Herr über ihre personenbezogenen Daten (Verbot der Datenverarbeitung mit Erlaubnisvorbehalt). Eine Datenverarbeitung ist deshalb nur zulässig, wenn die betroffene Person in die Verarbeitung ihrer personenbezogenen Daten eingewilligt hat oder wenn ein Gesetz die Datenverarbeitung erlaubt (Grundsatz der Rechtmäßigkeit). Liegt eines von beidem (Einwilligung oder Rechtsgrundlage) vor, ist die Verarbeitung aber auf den Zweck begrenzt, der vom Umfang der Einwilligung oder der Rechtsvorschrift erfasst wird.

Die unter diesen Bedingungen erfassten Daten dürfen – von bestimmten Ausnahmen abgesehen - nur für die Zwecke verarbeitet werden, für die sie erhoben wurden (Grundsatz der Zweckbindung). Dabei müssen die Daten geeignet sein, den Zweck zu erreichen. Das heißt, die Daten müssen dem Zweck angemessen sein und die Datenverarbeitung ist auf ein Maß zu beschränken, das zur Erreichung des Zwecks ausreicht (Grundsatz der Datenminimierung oder Grundsatz der Erforderlichkeit).

Für die Arbeit der Personalvertretung folgt aus diesen Grundsätzen, dass sie nicht nur eine Einwilligung oder eine Rechtsgrundlage für den jeweiligen Verarbeitungsvorgang braucht, sondern sie muss sich auch fragen, ob sie wirklich nur die Daten verarbeitet, die für den mit der Verarbeitung verfolgten Zweck nötig sind.

Für die Dauer der Datenverarbeitung müssen die Daten vor unbefugtem Zugriff, vor Verlust oder ungewollter Schädigung bis hin zur Zerstörung geschützt werden. Dies muss durch geeignete technische und organisatorische Maßnahmen (TOM) gewährleistet werden (Grundsatz der Integrität und Vertraulichkeit).

Schließlich dürfen Daten grundsätzlich nur solange verarbeitet werden, wie dies für den jeweiligen Zweck erforderlich ist (Grundsatz der Speicherbegrenzung). Daraus folgt, dass man sich schon bei der Verarbeitung bzw. schon bei der Verhandlung von Dienstvereinbarungen Gedanken machen muss, ab wann die Daten nicht mehr erforderlich sind und gelöscht werden müssen.

Zur Einhaltung dieser Grundsätze ist der Verantwortliche gem. Art.5 Abs. 2 DSGVO verpflichtet (Rechenschaftspflicht). Zur Verantwortung s. u. Nr. 3.1.

1.3 Definitionen

Art. 4 DSGVO enthält Begriffsbestimmungen. Danach sind u.a. (verkürzt)

personenbezogene Daten: alle Informationen, die sich auf eine identifizierte oder identifizierbare natürliche Person (= betroffene Person) beziehen, insbesondere Namen, Kennnummern, Standortdaten, besondere Merkmale;

Verarbeitung: u.a. automatisiertes oder nicht-automatisiertes Erheben, Ordnen, Speichern, Offenlegen, Löschen personenbezogener Daten;

Verantwortlicher: die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die Zwecke und Mittel der Verarbeitung entscheidet;

Dritter: eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, außer der betroffenen Person, dem Verantwortlichen oder dem Auftragsverarbeiter;

Einwilligung: jede freiwillig für den bestimmten Fall, in informierter Weise und unmissverständlich abgegebene Willenserklärung, mit der die betroffene Person zu verstehen gibt, dass sie mit der Verarbeitung der sie betreffenden personenbezogenen Daten einverstanden ist;

Gesundheitsdaten: personenbezogene Daten, die sich auf die körperliche oder geistige Gesundheit einer natürlichen Person beziehen und aus denen Informationen über deren Gesundheitszustand hervorgehen;

Besondere Kategorien personenbezogener Daten: Daten, aus denen u.a. ethnische Herkunft, politische Meinung, weltanschauliche Überzeugung, Gewerkschaftszugehörigkeit, Gesundheitsdaten, oder sexuelle Orientierung hervorgehen, Art. 9 DSGVO;

Beschäftigte: u.a. Tarifbeschäftigte, Beamtinnen und Beamte des Bundes, Richterinnen und Richter des Bundes, Soldatinnen und Soldaten, Zivildienstleistende, Auszubildende, Bewerberinnen und Bewerber sowie Personen, deren Beschäftigungsverhältnis beendet ist, § 26 Abs. 8 BDSG.

1.4 Datenschutzrechtliche Aspekte bei Dienstvereinbarungen

Dienstvereinbarungen sind Kollektivvereinbarungen im Sinne von Art. 88 DSGVO. Sie dürfen das Schutzniveau der DSGVO nicht unterschreiten. In Dienstvereinbarungen werden generelle Regelungen für eine Vielzahl von Einzelfällen getroffen. Soweit damit auch die Verarbeitung personenbezogener Daten verbunden ist, müssen sie Bestimmungen enthalten über die

- Zweckbestimmung,
- Art und Weise der Verarbeitung,
- Speicherdauer und Löschfristen.

In der Praxis spielen Kollektivvereinbarungen zum Beispiel bei Zeiterfassungssystemen, Videokameras, Personalinformationssystemen, Telefonanlagen oder Aktenverwaltungssystemen eine Rolle. Auch Dienstvereinbarungen zur privaten Nutzung von Internet und E-Mail am Arbeitsplatz können die Verarbeitung von Beschäftigtendaten regeln.

2. Datenverarbeitung in der Personalvertretung

2.1 Datenverarbeitung mit Rechtsgrundlage

Vielfach sind es Vorlagen der Dienststelle, die den Personalrat im Rahmen der Beteiligungsrechte im Einzelfall erreichen. Hier sind § 26 Abs. 1 S. 1 BDSG i. V. m. § 70 Abs. 2 Bundespersonalvertretungsgesetz (BPersVG) sowie die einschlägigen Mitbestimmungs-, Mitwirkungs- und Anhörungsvorschriften nach dem BPersVG die Rechtsgrundlage für eine zulässige Datenverarbeitung sowohl durch die Dienststelle als auch durch den Personalrat.

In vielen Fällen wird aber auch der Personalrat Informationen, die personenbezogene Daten enthalten, bei der Dienststelle anfordern, weil er sie für seine Arbeit benötigt. Rechtsgrundlage hierfür ist regelmäßig § 26 Abs. 1 S. 1 BDSG i. V. m. § 66 Abs. 1 BPersVG. Zulässig ist hiernach beispielsweise die Anforderung von Stellenbesetzungsübersichten mit weiteren Details zu den Beschäftigten wie Name, Funktion, Vergütungsgruppe, Datum der Einstellung, der letzten Beförderung, voraussichtlichem Eintritt in den Ruhestand usw.. Hier werden also sehr viele Daten zur Person verarbeitet. Diese Daten sind aber zur Ausübung und Erfüllung der Aufgaben des Personalrats erforderlich.

Denkbar ist auch die Informationsbeschaffung des Personalrats bei den Beschäftigten selbst, z.B. durch Befragung. Dabei ist zu beachten, dass nur solche personenbezogenen Daten erfragt werden dürfen, die für die Wahrnehmung personalvertretungsrechtlicher Aufgaben erforderlich sind.

2.2 Datenverarbeitung mit Einwilligung

Es wenden sich auch einzelne Beschäftigte an den Personalrat, sei es in Sprechstunden, Fragebogenaktionen oder mit Anregungen und Beschwerden im Sinne von § 62 Abs. 1 Nr. 3 BPersVG. In diesen Fällen muss der Personalrat prüfen, wie mit den ihm in diesem Rahmen übermittelten personenbezogenen Daten umzugehen ist und zwar nicht nur aus personalvertretungs- sondern auch aus datenschutzrechtlicher Sicht.

Ob die Datenverarbeitung durch den Personalrat in diesen Fällen immer einer Einwilligung der Beschäftigten bedarf, lässt sich allgemein nicht beantworten. Es ist aber problematisch, allein aus dem Umstand, dass sich die oder der Beschäftigte an den Personalrat gewandt hat, den Schluss zu ziehen, dass die betroffene Person mit der Verarbeitung ihrer personenbezogenen Daten im Personalrat einverstanden ist. Denn in Erwägungsgrund 32 zur DSGVO heißt es u.a., dass Stillschweigen keine Einwilligung

darstellen soll. Außerdem stellt die DSGVO einige Bedingungen auf, unter denen eine Einwilligung rechtsgültig ist, wie z.B. die Informiertheit (Näheres s. u. Nr. 2.2.1).

Aus Gründen der Rechtssicherheit wird daher empfohlen, eine ausdrückliche Einwilligung der Beschäftigten einzuholen. Denn die Einwilligung hilft allen Beteiligten, sich darüber klar zu werden, was wirklich gewollt ist. Sie sollten sich fragen, ob das Vorbringen der betroffenen Person tatsächlich eine Anregung oder Beschwerde im Sinne von § 62 Abs. 1 Nr. 3 BPersVG oder einem Spezialgesetz ist oder ob es sich um eine bloße Meinungs- oder Unmutsäußerung handelt.

Insbesondere wenn die Sache als eine berechtigt erscheinende Beschwerde aufgegriffen wird, zu deren Erledigung Verhandlungen mit der Dienststellenleitung aufgenommen werden sollen, muss vorher geklärt werden, ob die betroffene Person damit einverstanden ist.

Eine schriftliche Einwilligung empfiehlt sich auch, wenn Beschäftigte sich an ein einzelnes Personalratsmitglied wenden und dieses das Anliegen an das Gremium herantragen will oder ein Gespräch mit der Dienststelle gesucht werden soll.

2.2.1 Kriterien für eine rechtswirksame Einwilligung

Die Einwilligung muss einige Kriterien erfüllen, um rechtswirksam zu sein.

Die Einwilligung muss vor der Datenverarbeitung eingeholt werden. Eine rückwirkende Genehmigung ist nicht möglich.

Die betroffene Person muss wissen, in was sie einwilligt. Die Einwilligung muss deshalb erkennen lassen, welche Daten zu welchem Zweck verarbeitet werden. Als Daten kämen im Falle einer Beschwerde z.B. der Name der Person und der vorgetragene Sachverhalt in Betracht. Zweck der Verarbeitung dieser Daten wäre die Verhandlung in der Sache mit der Dienststelle. Falls Daten übermittelt werden sollen, muss auch aufgeführt werden, von wem sie wohin übermittelt werden.

Außerdem muss die Einwilligung freiwillig abgegeben werden. Die Freiwilligkeit im Beschäftigungsverhältnis wird grundsätzlich als problematisch angesehen, weil ein Abhängigkeitsverhältnis zum Dienstherrn besteht. Ob die tatsächliche Freiwilligkeit vorliegt, muss nach den Umständen des Einzelfalles beurteilt werden. Ein Indiz für Freiwilligkeit ist das Bestehen von Alternativen.

Zu beachten ist auch, dass eine Einwilligung jederzeit widerrufen werden kann. Darüber muss die betroffene Person belehrt werden.

Wenn eine Anregung oder Beschwerde weiterverfolgt werden soll, ohne dass die Beschwerdeführerin oder der Beschwerdeführer namentlich genannt wird, muss vorher überlegt werden, ob aus den Umständen des Einzelfalles Rückschlüsse auf die betroffene Person möglich sind. Dann wäre nämlich der Tatbestand der Identifizierbarkeit gem. Art. 4 Nr. 1 DSGVO erfüllt und es läge eine Datenverarbeitung vor. Rückschlüsse auf die betroffene Person sind auch möglich, wenn eine Bezugsgruppe aus fünf oder weniger Personen besteht.

Für weitere Details zur Einwilligung s. Art. 4 Nr. 11 und Art. 7 DSGVO sowie die Erwägungsgründe 32, 42, 43 und 171. Die unabhängigen Datenschutzbehörden des Bundes und der Länder (Datenschutzkonferenz - DSK) haben dazu das Kurzpapier Nr. 20 herausgegeben – abzurufen unter www.datenschutzkonferenz-online.de/media/kp/dsk_kpnr_20.pdf

2.3 Grenzen zulässiger Datenverarbeitung

Soweit das BPersVG die Beteiligungsrechte ausdrücklich aufzählt oder generell mit dem Informationsanspruch oder der Überwachungsaufgabe nach § 62 Abs. 1 Nr. 2 BPersVG allgemeine Rechtsgrundlagen formuliert, wird die damit in Zusammenhang stehende Datenverarbeitung zulässig sein.

Aber wie verhält es sich mit dem in § 2 BPersVG normierten Gebot der vertrauensvollen Zusammenarbeit? Nach diesem Gebot soll die Arbeit von Personalrat und Dienststelle durch gegenseitiges Vertrauen und gegenseitige Offenheit gekennzeichnet sein. Dies ist jedoch kein „Freifahrtschein" für die Offenlegung personenbezogener Daten über die vorgenannten Informationsrechte und –pflichten hinaus. Vielmehr müssen die Beteiligten hier auch das informationelle Selbstbestimmungsrecht der betroffenen Personen im Blick behalten.

2.4 Datenübermittlung an andere Interessenvertretungen

Die Datenübermittlung wird in Art. 4 Nr. 2DSGVO als Offenlegung durch Übermittlung, Verbreitung oder eine andere Form der Bereitstellung beschrieben. Dies ist auch als erfüllt anzusehen, wenn personenbezogene Daten vom Personalrat an andere Interessenvertretungen wie die Jugend- und Auszubildendenvertretung, an Stufenvertretungen, die Schwerbehindertenvertretung oder auch an die Gleichstellungsbeauftragte weitergegeben werden. Diese Interessenvertretungen sowie die Gleichstellungsbeauftragte haben regelmäßig eigene Informationsansprüche. Es gehört nicht zu den Aufgaben örtlicher Personalvertretungen diese mit Informationen zu versorgen. Für eine rechtmäßige Weitergabe personenbezogener Daten ist eine Einwilligung der betroffenen Person oder eine Rechtsgrundlage erforderlich, wie z.B. ein ausdrückliches Beteiligungsrecht nach dem BPersVG.

2.5 Datenübermittlung an Dritte

Für die zulässige Weitergabe von personenbezogenen Daten an einen Dritten, also an eine außenstehende Person, Behörde, Einrichtung oder Stelle (genaue Definition s. Art. 4 Nr. 10 DSGVO) ist eine Einwilligung der betroffenen Person oder eine Rechtsgrundlage erforderlich.

2.6 Sensible oder sensitive Daten

Personenbezogene Daten besonderer Kategorie werden oft als (besonders) sensible oder sensitive Daten bezeichnet. Nach Art. 9 Abs. 1 DSGVO sind das Daten, aus denen die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen oder die Gewerkschaftszugehörigkeit hervorgehen sowie genetische und biometrische Daten, Gesundheitsdaten oder Daten zum Sexualleben oder der sexuellen Orientierung.

Die Verarbeitung dieser Daten ist verboten (Art. 9 Abs. 1 DSGVO). Von diesem Verbot sind einige Fälle ausgenommen. Der Ausnahmekatalog ergibt sich aus Art. 9 Abs. 2

DSGVO. Als Ausnahme kommen neben der Einwilligung insbesondere die Erforderlichkeit im Rahmen des Arbeitsrechts (Art. 9 Abs. 2 lit. b) DSGVO) in Betracht. Jedoch spezifiziert § 26 Abs. 3 BDSG die Voraussetzungen für eine Verarbeitung besonderer Kategorien personenbezogener Daten im Beschäftigungskontext. Danach ist eine Verarbeitung zulässig, wenn eine der dort genannten Alternativen erfüllt ist:

- Ausübung von Rechten oder Erfüllung rechtlicher Pflichten aus dem Arbeitsrecht

oder

- Erforderlichkeit nach dem Recht der sozialen Sicherheit und des Sozialschutzes.

Zusätzlich zur Erfüllung der vorstehenden Alternativen muss auch das Interesse der betroffenen Beschäftigten beachtet werden. Es darf der Datenverarbeitung nicht entgegenstehen.

Zum Arbeitsrecht gehört auch das Personalvertretungsrecht. Durch die Spezifizierung in § 26 BDSG hat der nationale Gesetzgeber von der Regelungserlaubnis des Art. 88 DSGVO Gebrauch gemacht und für den Beschäftigungskontext die Anwendung von Art. 9 Abs. 2 DSGVO eingeschränkt.

Der häufigste Fall für die Verarbeitung sensitiver Daten im Personalrat dürfte die Verarbeitung von Gesundheitsdaten sein, etwa bei Beteiligungen im Rahmen von Dienst- und Arbeitsunfähigkeit oder im sogenannten BEM-Verfahren. Aus den vorstehenden Erläuterungen wird deutlich, dass die Verarbeitung zwar grundsätzlich datenschutzrechtlich zulässig ist, hier aber besondere Sorgfalt gefragt ist. Wer muss wieviel über den konkreten Fall wissen?

Soweit beim Personalrat überhaupt Einzelvorgänge mit Gesundheitsdaten entstehen, z.B. im Zusammenhang mit dem Arbeits- und Gesundheitsschutz, einem BEM-Verfahren oder sogar einer Kündigung sind diese Vorgänge besonders zu sichern, z.B. in einem Stahlschrank. Solange der Vorgang nicht abgeschlossen ist oder sich daraus noch Folgewirkungen ergeben, darf er aufbewahrt werden. Die Personalaktenrichtlinie des Bundesministeriums des Innern für Bau und Heimat sieht z.B. eine Aufbewahrungsfrist von bis zu 3 Jahren für die Sachakten im BEM-Verfahren vor. Personalräte sollten prüfen, ob für ihren Geschäftsbereich diese oder eine andere Personalaktenrichtlinie gilt und sich daran für die Aufbewahrungsdauer ihrer BEM-Vorgänge im Personalratsbüro orientieren. Dabei ist zu beachten, dass die eigentliche BEM-Sachakte bei der oder dem BEM-Beauftragten geführt wird.

Es ist deshalb stets kritisch zu fragen, ob eine Aufbewahrung des eventuell beim Personalrat entstandenen Vorgangs überhaupt erforderlich ist.

2.7 Grundstammdaten

Hinsichtlich des Vorhaltens sogenannter Grundstammdaten aller Beschäftigten wie z.B. Name, Alter, Familienstand, Arbeitsplatz usw. wird es in Dienststellen mit mehr als 100 Beschäftigten für zulässig erachtet, dass diese dauerhaft beim Personalrat vorliegen, weil diese Daten zur Wahrnehmung der Beteiligungsrechte immer wieder benötigt werden.

2.8 Tagesordnung und Protokoll

Die Tagesordnung für die Personalratssitzung soll es den Mitgliedern erlauben, sich auf die Sitzung sachgerecht vorzubereiten. Sie muss deshalb entsprechend detailliert sein. Demnach enthält bereits die Tagesordnung oftmals personenbezogene Daten. Da dies für die Sitzungsvorbereitung erforderlich ist, ist es datenschutzrechtlich zulässig.

Generell ist eine Aufbewahrung der Tagesordnung nach der Sitzung nicht mehr erforderlich, so dass sie zu vernichten ist, insbesondere auch bei den Personalratsmitgliedern. Über jede Verhandlung des Personalrats ist ein Protokoll zu fertigen, das mindestens den Wortlaut der Beschlüsse und die Stimmenmehrheit enthält (§ 43 Abs. 1 BPersVG). Das Protokoll ist der gesetzlich vorgesehene und wichtigste Nachweis für die Tatsache einer Beschlussfassung durch den Personalrat. Das Original ist als Bestandteil der Akten des Personalrats aufzubewahren, solange sein Inhalt von rechtlicher Bedeutung ist. Da diese in der Regel über die Amtszeit des Personalrats hinausgeht, ist es an den nachfolgenden Personalrat auszuhändigen und von diesem aufzubewahren. Aus datenschutzrechtlicher Sicht sollte bei Erstellung der Tagesordnung und Abfassung des Protokolls berücksichtigt werden, dass nicht mehr personenbezogene Daten darin aufgenommen werden, als dies für den jeweiligen Zweck erforderlich ist.

2.9 Technische und organisatorische Maßnahmen (TOM)

„Personenbezogene Daten sollen so verarbeitet werden, dass ihre Sicherheit und Vertraulichkeit hinreichend gewährleistet ist, wozu auch gehört, dass Unbefugte keinen Zugang zu den Daten haben und weder die Daten noch die Geräte, mit denen sie verarbeitet werden, benutzen können“ (Erwägungsgrund 38, Satz 12 zur DSGVO). Art. 25 und 32 DSGVO treffen die Regelungen zum Datenschutz durch Technikgestaltung und durch datenschutzrechtliche Voreinstellungen.

Da die Personalvertretungen in aller Regel die Hard- und Software nutzen, die in der Dienststelle zum Einsatz kommt, darf grundsätzlich angenommen werden, dass diese die notwendigen technischen und organisatorischen Maßnahmen zum Schutz der Datenverarbeitung ergriffen hat. Dies entbindet den Personalrat aber nicht von seiner Überwachungsfunktion in diesem Bereich.

Aber auch im Personalratsbüro muss man sich der Verpflichtung zum technischen und organisatorischen Datenschutz bewusst sein. Die Geschäftsräume des Personalrats sind vor unbefugtem Zutritt zu sichern. Darüber hinaus helfen abschließbare und abgeschlossene Schränke, unbefugte Zugriffe zu verhindern. Die PC sollten nach angemessener (kurzer) Zeit des Nicht-Gebrauchs kennwortgeschützt sein. Auch ein angemessener, geeigneter Schutz vor Mithören sollte gewährleistet sein, z.B. durch ausreichend starke Wände oder geschlossene Fenster und Türen während einer Sitzung oder eines Gesprächs.

2.10 E-Mail Nutzung, Soziale Netzwerke und What’s App-Gruppen beim Personalrat

Dass E-Mails wie eine von jedermann lesbare Postkarte sind, wenn sie über das weltweite Netz (www) verschickt werden, ist allgemein bekannt. Lässt sich der Versand über das Internet nicht vermeiden, ist eine Verschlüsselung zu empfehlen. Anderenfalls sollte auf den herkömmlichen Postweg zurückgegriffen werden.

Innerhalb einer Dienststelle oder innerhalb eines Behördennetzes sind E-Mails vor unbefugtem Mitlesen geschützt. Gleichwohl muss man beim Umgang mit E-Mails Sorgfalt walten lassen.

Dies trifft vor allem auf den Adressatenkreis zu. Wer muss wirklich Kenntnis von der Sache haben, um die es in der E-Mail geht? Gerade wenn es um den Umgang mit personenbezogenen Daten geht, sollte man sich vor dem Versand noch einmal die Frage nach der Erforderlichkeit der Weitergabe stellen. In diesem Zusammenhang ist ggf. auch zu prüfen, ob alle Adressaten offen aufgeführt werden dürfen oder ob ggf. Persönlichkeitsrechte verletzt werden, wenn auf diese Weise alle Adressaten einschließlich ihrer E-Mail-Adressen voneinander Kenntnis erlangen.

Nicht zuletzt sollte geprüft werden, ob alle Adressaten richtig erfasst sind. Kleine Tippfehler können schnell einen Fehlversand erzeugen.

Die Verarbeitung personenbezogener Daten durch den Personalrat via Sozialer Netzwerke ist zu unterlassen. Die Netzwerke sind vor unbefugtem Zugriff nicht hinreichend geschützt.

2.11 Dauer der Datenverarbeitung/Speicherfrist

Grundsätzlich dürfen personenbezogene Daten solange verarbeitet, d.h. gespeichert werden, wie sie für den Zweck, für den sie erhoben wurden, erforderlich sind (vgl. Art. 17 Abs. 1 lit. a) DSGVO). Ausnahmen von diesem Grundsatz sind in Art. 17 Abs. 3 DSGVO aufgezählt. Danach dürfen die Daten z.B. auch noch gespeichert werden, wenn dies zur Erfüllung einer rechtlichen Verpflichtung erforderlich ist (Art. 17 Abs. 3 lit. b) DSGVO). Das sind häufig Dokumentationszwecke, z.B. im Rahmen von Leistungsgewährungen oder für die Rechnungsprüfung. Die zulässige Speicherdauer muss im Einzelfall geprüft und festgelegt werden.

Häufig sind Aufbewahrungsfristen bereits in Rechtsgrundlagen oder den zugehörigen Verordnungen, Erlassen oder Richtlinien bestimmt, so z.B. dezidiert in § 113 Bundesbeamtengesetz für die Personalakte. Diese Bestimmungen richten sich an die Dienststelle.

Aber was ist mit den personenbezogenen Daten der Beschäftigten beim Personalrat?

Hier gilt der vorstehende Grundsatz: die personenbezogenen Daten dürfen solange aufbewahrt werden, wie sie erforderlich sind. Wenn also z.B. im Rahmen einer Mitbestimmung für eine Beförderung die entsprechenden personenbezogenen Daten der zu befördernden Person sowie etwaiger Konkurrentinnen und Konkurrenten dem Personalrat von der Dienststelle übermittelt werden, dann sind diese Daten bis zur Beschlussfassung des Gremiums erforderlich. Bis dahin können sich alle Personalratsmitglieder ein Bild von der zu entscheidenden Situation machen. Wird ein Beschluss gefasst und dieser der Dienststelle mitgeteilt, ist damit die ordnungsgemäße Beteiligung dokumentiert. Danach ist eine weitere Aufbewahrung der Unterlagen nicht mehr erforderlich.

Das gleiche gilt, wenn im Rahmen eines Beschwerdeverfahrens in einem Einzelfall personenbezogene Daten verarbeitet werden. Bis über die Beschwerde abschließend entschieden ist, sind die Daten als erforderlich zu betrachten und dürfen im Personalratsbüro aufbewahrt werden (elektronisch oder in Papier). Bei Beschwerdeverfahren

ist außerdem zu beachten, dass mit Ablauf der Amtszeit des Personalrats seine rechtliche Existenz und seine Befugnisse enden. Die im Rahmen des Beschwerdeverfahrens gespeicherten personenbezogenen Daten sind mit Ablauf der Amtszeit des Personalrats zu löschen und zwar auch dann, wenn das Beschwerdeverfahren zu diesem Zeitpunkt noch nicht abgeschlossen ist.

2.12 Datenlöschung

Über die vorstehend beschriebene Löschpflicht bei Wegfall der Erforderlichkeit hinaus bestehen weitere Löschpflichten. Diese sind in Art. 17 Abs. 1 DSGVO aufgeführt.

Für die Personalratsarbeit dürfte insbesondere der Widerruf einer Einwilligung von Bedeutung sein. Wird eine Einwilligung widerrufen, ist die damit zusammenhängende Datenverarbeitung einzustellen. Der Widerruf der Einwilligung wirkt für die Zukunft. Für die Vergangenheit war die Datenverarbeitung zulässig. Ob und wann die in der Vergangenheit verarbeiteten Daten zu löschen sind, muss anhand des konkreten Einzelfalls entschieden werden. Sofern Aufbewahrungsfristen greifen, sind diese zu beachten.

In der Personalratsarbeit werden personenbezogene Daten nicht nur in Beteiligungsangelegenheiten verarbeitet. Auch in anderem Zusammenhang fallen personenbezogene Daten an. Das dürfte häufig in Korrespondenz des Personalrats sein, wie z.B. in E-Mails der Mitglieder untereinander aber eventuell auch mit Rechtsanwälten.

Hierzu empfiehlt es sich, einmal genauer hinzuschauen und festzulegen, welche Kategorien von Dokumenten entstehen und für diese Löschfristen festzulegen. Während man vor einigen Jahren noch davon ausgehen konnte, dass E-Mails einen eher informellen Charakter hatten und eher „kurzlebig“ waren, ersetzen sie zwischenzeitlich oftmals den Schriftverkehr in Papierform völlig. Für die Festlegung einer Löschfrist hilft es, sich zu fragen, ob der Inhalt des Dokumentes eine rechtliche Folgewirkung hat, z.B. in einem noch laufenden Verfahren oder einem fortzuführenden Projekt. Dann sollte die Kommunikation auch dort abgelegt und z.B. aus dem E-Mail-Postfach gelöscht werden.

Soweit die Dienststelle ein Löschkonzept erstellt hat, ist dieses auch von der Personalvertretung zu beachten.

Die DSK hat zur Datenlöschung das Kurzpapier Nr. 11 herausgegeben.

Löschung bedeutet praktisch, dass die Daten unwiederbringlich verloren oder physikalisch zerstört sind. Für automatisiert verarbeitete Daten bedeutet dies, dass es nicht reicht, sie in einen virtuellen Papierkorb zu verschieben. Bitte informieren Sie sich in Ihrer Dienststelle, wie die tatsächliche Löschung sichergestellt wird. Auf Papier vorhandene Daten sind zu schreddern oder einem qualifizierten Entsorger zu übergeben, der sie nach DIN-Norm vernichtet.

3. Datenschutzvorschriften in der Dienststelle

Soweit die Dienststelle Datenschutzvorschriften erlassen hat, müssen diese auch vom Personalrat beachtet werden. Die Dienststelle ist „Verantwortlicher“ im Sinne von Art. 4 Nr. 7 DSGVO für die Einhaltung des Datenschutzes in der gesamten Dienststelle. Da es sich aber bei diesen Vorschriften regelmäßig um Regelungen zur Ordnung in der

Dienststelle und des Verhaltens der Beschäftigten gem. § 80 Abs. 1 Nr. 18 BPersVG handeln wird, hat der Personalrat ein Mitbestimmungs- also Mitgestaltungsrecht. Darüber hinaus helfen die Datenschutzvorschriften der Dienststelle auch dem Personalrat bei einer ordnungsgemäßen und regelkonformen Verarbeitung personenbezogener Daten.

Wenn der Personalrat meint, etwas anderes zu brauchen, als für die Dienststelle allgemein erlaubt ist, muss dies im Rahmen der personalvertretungsrechtlichen Möglichkeiten verfolgt werden. Das trifft insbesondere auf die Ausstattung mit Hard- und Software zu. Ist der Einsatz privater Ausstattung (Geräte, USB-Sticks usw.) in der Dienststelle oder im Home-Office verboten, gilt das auch für den Personalrat.

3.1 Datenschutzverantwortung und -kontrolle

§ 69 BPersVG stellt fest, dass die Dienststelle Verantwortlicher im Sinne der DSGVO bleibt und Personalrat und Dienststelle sich bei der Wahrung des Datenschutzes gegenseitig unterstützen.

In jedem Fall trifft den Personalrat als unabhängige Institution des Personalvertretungsrechts innerhalb der Dienststelle eine Verantwortung für eine rechtmäßige Verarbeitung der bei ihm aufkommenden personenbezogenen Daten. Der Personalrat muss keinen eigenen Datenschutzbeauftragten im Sinne von Abschnitt 4 DSGVO benennen. Entsprechend der Stellung und Aufgaben (Art. 38 und 39 DSGVO) obliegt es der/dem behördlichen Datenschutzbeauftragten, auch den Personalrat als Teil der verantwortlichen Stelle zu kontrollieren. Soweit erforderlich sollte der Personalrat die Beratung durch die/den behördlichen Datenschutzbeauftragten in Anspruch nehmen (Begründung zu § 69 BPersVG, BTDrs. 19/26820)

Das hindert den Personalrat nicht daran, ein Mitglied zur Datenschutzexpertin/zum Datenschutzexperten auszubilden – ebenso wie für andere Rechtsgebiete z.B. im Tarifrecht oder Arbeitsschutz. Das Mitglied könnte sich gezielt um alle Fragen zum Datenschutz sowohl im Einzelfall als auch bei generellen Regelungen kümmern sowie als Ansprechpartnerin/Ansprechpartner zur Verfügung stehen. Eine gute Zusammenarbeit mit der/dem behördlichen Datenschutzbeauftragten sollte angestrebt werden.

Im Übrigen unterstehen die Personalräte als Teil der Dienststelle der Datenschutzaufsicht des BfDI.

4. Datenschutzverstoß

Wenn eine Personalvertretung der Meinung ist, dass bei einem bestimmten Sachverhalt gegen datenschutzrechtliche Vorschriften verstoßen wurde, kann sie dies gegenüber der Dienststelle im Rahmen ihrer Überwachungsaufgabe nach § 62 Nr. 2 BPersVG geltend machen und auf Abstellung hinwirken. Denn auch die DSGVO und das BDSG gehören zu den dort genannten Rechtsvorschriften zugunsten der Beschäftigten.

Ein Beschwerderecht nach Art. 77 DSGVO steht nur betroffenen Personen zu. Nur diese können beim BfDI eine Beschwerde einreichen, womit sie auch gem. Art. 80 DSGVO eine Vertretung beauftragen können.

Jedoch kann sich eine Personalvertretung jederzeit mit einer allgemeinen Frage, die ggfs. auch nach Erörterung mit der/dem behördlichen Datenschutzbeauftragten nicht

beantwortet werden konnte, im Rahmen der allgemeinen Beratungs- und Sensibilisierungsfunktion an den BfDI wenden.

Sollte ein Datenschutzverstoß in der Personalvertretung festgestellt werden, kann die Aufsichtsbehörde nicht das Gremium zur Verantwortung ziehen, sondern nur die Dienststelle. Ob im Innenverhältnis die Dienststelle ggf. gegenüber dem einzelnen Personalratsmitglied dienstrechtliche Maßnahmen ergreift, wird stets vom Einzelfall abhängen.

Die Meldepflicht gem. Art. 33 und 34 DSGVO ist seitens der Dienststelle zu beachten.