Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2017/90

PVP 2017, 317
Heft 11 v. 27.11.2017
Themen-Special

Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag

Mag. Wolfram Hitz/Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Trotzdem er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565).

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf. Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht**: In diesem Heft informieren wir Sie über die ...
  - **Datenschutzrechtsgrundlagen** (ABGB, Datenschutzgesetz 2000, Datenschutz-Grundverordnung),
  - **arbeitsrechtlich** relevanten **Daten** und **Definitionen**,
  - konkreten **Datenschutzfragen** im **arbeitsrechtlichen Alltag** -> Datenschutz ... im Bewerbungsverfahren, ... bei Zeiterfassung, ... bei Videoüberwachung, ... bei der privaten Nutzung des betrieblichen Internets/E-Mails, ... nach dem Dienstvertragsende (Dienstzeugnis, Auskünfte über ehemaligen Dienstnehmer).

- **Teil 2: Datenschutz im Alltag des Personalverrechners**
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs**
- **Teil 4: Details zur neuen Datenschutz-Grundverordnung**

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** ... Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//**BR** ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ... Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung

A) Datenschutz-Grundverordnung

Seit 25. 5. 2018 ist die Verordnung des Europäischen Parlaments und des Rates zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, kurz die **Datenschutz-Grundverordnung (DSGVO)**, in **allen EU-Mitgliedstaaten anzuwenden**.

Hinweis

Eine **EU-Verordnung** ist rechtlich in den einzelnen Mitgliedstaaten **unmittelbar wirksam**. Sie muss nicht erst - wie dies bei einer **EU-Richtlinie** der Fall ist - durch nationale Rechtsakte umgesetzt werden.

Hitz/Schrenk, Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag, PVP 2017, Seite 317

a) Die DSGVO ist neben bereits bestehenden gesetzlichen Regelungen anzuwenden. Sie wirkt sich insbesondere hinsichtlich **Transparenz** und **Offenlegung** der **Datenverarbeitung** und der vom DG gesetzten Maßnahmen aus.
b) Die **Befugnisse** und Aufgaben der **Aufsichtsbehörden** werden **erweitert**, für **Verstöße** gegen die Bestimmungen der DSGVO können extrem **hohe Strafen** verhängt werden.

Hinweis

Schon **derzeit** gibt es eine **Vielzahl** an **Datenschutz-Bestimmungen**, die in der Praxis mangels Kenntnis der Rechtsanwender oftmals wenig beachtet werden. Auf diese Regelungen wollen wir im folgenden Punkt B) eingehen.

B) Wissenswerte Datenschutz-Rechtsgrundlagen

1. Allgemeines bürgerliches Gesetzbuch (ABGB)

Als **Zentralnorm** unserer Rechtsordnung gilt **§ 16 ABGB**, aus dem das jedermann angeborene **Persönlichkeitsrecht** auf **Achtung** seines **Privatbereichs** und seiner Geheimsphäre abgeleitet wird. Grundfreiheiten und Menschenrechte richten sich primär an den Staat, haben darüber hinaus aber auch Auswirkungen auf das Verhältnis der Bürger untereinander.

Die aus dem arbeitsrechtlichen Schutzprinzip abgeleitete **Fürsorgepflicht** des DG ist in § 1157 ABGB geregelt und umfasst den **Schutz** der gesamten **Persönlichkeitsrechte** des DN.

Für die **Angestellten** findet sich eine entsprechende Norm ergänzend in **§ 18 AngG** *("Fürsorgepflicht")*.

2. Datenschutzgesetz 2000: gilt bis 24. 5. 2018

Das **DSG 2000 setzt** die 1995 erlassene **Datenschutzrichtlinie** der (damals) Europäischen Gemeinschaft **um** und wurde seither mehrfach novelliert.

Es regelt bspw die **Verwendung sensibler Daten** zur Erfüllung der sich aus Arbeits- bzw Dienstrecht ergebenden DG-Verpflichtungen.

3. Datenschutzgesetz: gilt ab 25. 5. 2018

Die **DSGVO enthält** Regelungsspielräume (**"Öffnungsklauseln"**), die von den Mitgliedstaaten genutzt werden können. Das DSG 2000 wird novelliert und heißt künftig nur noch DSG, das auf die DSGVO abgestimmt ist.

4. Datenschutzbehörde und Verwaltungsstrafen gemäß DSG 2000

Die **Datenschutzbehörde** (DSB), vormals Datenschutzkommission (DSK), ist als **weisungsfreie** Behörde dafür zuständig, dass die **Datenschutzregeln eingehalten** werden.

Wird gegen die **datenschutzrechtlichen Bestimmungen verstoßen**, kann der Betroffene (zB DN) nach dem DSG 2000 zwischen **verschiedenen Verfahren** wählen.

a) Das sogenannte **Ombudsmann-Verfahren** gemäß § 3 DSG 2000 bewirkt, dass die DSB bloß tätig wird.
b) Es kann alternativ ein **Verfahren** eingeleitet werden, das von der DSB mit **Bescheid** abzuschließen ist (§ 31 DSG 2000), oder
c) es kann eine **datenschutzrechtliche Klage** - etwa auf Löschung von Daten - bei einem **Zivilgericht** eingebracht werden (§ 32 DSG 2000).

Hitz/Schrenk, Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag, PVP 2017, Seite 318

Hinweis

Im Arbeitsrecht maßgebliche **Verstöße**, bspw gegen das Recht auf **Löschung** von Daten, sind mit einer relativ geringen Verwaltungsstrafe von **bis zu EUR 500,00** zu ahnden (§ 52 Abs 2a DSG 2000).

Mögliche Strafen nach der DSGVO werden in einem späteren Artikel behandelt.

C) Was sind arbeitsrechtlich relevante Daten bzw Definitionen?

- **personenbezogene** Daten (§ 4 Z 1 DSG 2000) -> zB Name, Adresse, Geburtsdatum, Sozialversicherungsnummer, Geschlecht ...
- **sensible** Daten (§ 4 Z 2 DSG 2000) -> zB Religionszugehörigkeit, Gesundheit
- **Verwendung** von Daten (§§ 6 f DSG 2000) -> zB rechtmäßiger, arbeitsplatzbezogener Zweck
- **Publizität** der **Datenanwendung** (§§ 16 ff DSG 2000) -> Meldung an DSB, vormals DSK, ausgenommen: **Standardanwendungen** (§ 17 Abs 2 und 3 DSG 2000, zB Personalverrechnungs-Systeme)

D) Datenschutz im arbeitsrechtlichen Alltag

1. Vorvertragliche Verpflichtungen (Bewerbung)

Arbeitsrechtliche und datenschutzrechtliche Verpflichtungen sind bspw bei der **Auswahl** der **Fragen** bzw beim Anfordern und Verwenden von **Unterlagen** im **Bewerbungsgespräch** zu berücksichtigen.

Bezüglich **Datenschutz** ist insbesondere darauf zu **achten**,

a) ob übermittelte **Daten verwendet** bzw
b) wie lange diese Daten **aufbewahrt** werden dürfen und
c) **welche Daten** vom Bewerber **verlangt** werden können (zB Strafregisterauszug).

zu a) Werden **Bewerbungsunterlagen** aktiv **zugesendet** oder in einem entsprechenden Onlineportal einer Firma **hochgeladen**, ist es **zulässig**, dass der DG diesen Bewerbungsprozess **verwendet**.

zu b) Jedenfalls **zulässig** ist, dass der DG die übermittelten Bewerbungsunterlagen so lange **aufbewahrt**, als der **Bewerbungsprozess dauert**. **Danach** dürfen die Unterlagen nur dann weiterhin **aufbewahrt** werden, wenn der **Bewerber zustimmt**.

Zu c) Der DG darf vom Bewerber grundsätzlich jene **Unterlagen verlangen** und **Informationen** einholen, die für eine etwaige **Beschäftigung** von Bedeutung sind.

Bestimmte sensible Daten abzufragen und die erhaltenen Informationen zu verarbeiten ist nur dann zulässig, wenn es einen **Rechtfertigungsgrund** gemäß § 8 Abs 4 Z 3 DSG 2000 gibt.

Beispiele

[#10122] **Abfrage nach Vorstrafen**

Grundsätzlich ist der DN **nicht verpflichtet**, beim Einstellungsgespräch DG-Fragen nach allfälligen **Vorstrafen zu beantworten**.

Ausnahme: Aufgrund der angestrebten beruflichen Tätigkeit kann ein entsprechender **DSG-Rechtfertigungsgrund** vorliegen.

a) Bei bestimmten beruflichen Tätigkeiten sind **Fragen** nach **Vorstrafen wahrheitsgemäß** zu beantworten bzw der verlangte **Strafregisterauszug vorzulegen**. Dies gilt vor allem dann, wenn der Bewerber durch die der Vorstrafe zugrunde liegende **Verurteilung** für die **konkret angestrebte berufliche Tätigkeit** (objektiv) **ungeeignet** erscheint.

Hitz/Schrenk, Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag, PVP 2017, Seite 319

So wird jemand, der sich bspw für den Job als **Kassier** in einer **Bank** bewirbt, eine **Vorstrafe** wegen **Unterschlagung** oder **Veruntreuung** bekannt geben müssen.

b) Bewirbt sich eine Person für den **Außendienst**, sind entsprechende Unterlagen bzw Fragen, ob er bereits einen **Verkehrsunfall mit Personenschaden** verschuldet hat, **zulässig** und müssen **wahrheitsgemäß** beantwortet werden.

[#10123] **Fragen nach dem Gesundheitszustand und Verlangen eines Gesundheitsattestes**

Fragen zum Gesundheitszustand sind grundsätzlich **nicht zulässig**.

Ausnahmen: Aufgrund der angestrebten beruflichen Tätigkeit kann ein entsprechender **DSG-Rechtfertigungsgrund** vorliegen.

a) Das gilt bspw für **Tätigkeiten**, für die **vorgeschrieben** ist, dass anhand einer **ärztlichen Untersuchung** festzustellen ist, ob der Bewerber geeignet ist (zB Koch [hygienische Anforderungen], Linienpilot).

b) Hat der DN eine **ansteckende Krankheit**, kann der DG - aufgrund seiner **Fürsorgepflicht** gegenüber den übrigen DN (§ 82 lit h GewO 1859) -
   - entsprechende **Fragen** zur **Gesundheit** stellen, die der DN wahrheitsgemäß zu beantworten hat, bzw
   - den DN auffordern, ein entsprechendes **ärztliches Attest** vorzulegen.

Hinweis

Hat der DN eine **ansteckende Krankheit**, ist dies ein **Entlassungsgrund** bei **Arbeitern** gemäß § 82 lit h GewO.

c) Besteht aufgrund der beruflichen Tätigkeit die **Gefahr**, mit Körperflüssigkeiten in Kontakt zu kommen (zB Krankenschwester), kann der DG - aufgrund seiner **Fürsorgepflicht** gegenüber den übrigen DN (§

82 lit h GewO 1859) -

- entsprechende **Fragen** nach **AIDS** oder einer **HIV-Infektion** stellen, die der DN wahrheitsgemäß zu beantworten hat, bzw
- den DN auffordern, ein entsprechendes **ärztliches Attest** vorzulegen.

2. Zeiterfassungssysteme

Werden Zeiterfassungssysteme im Unternehmen eingesetzt, dann sind arbeits- und datenschutzrechtliche Regelungen zu beachten. Der datenschutzrechtliche **Rechtfertigungsgrund** gemäß § 8 Abs 4 Z 3 DSG 2000 besteht aufgrund **§ 26 AZG**.

Je nachdem, wie die Zeiterfassungssysteme konkret ausgestaltet sind, ist zu **unterscheiden** in Systeme, die ...

- ... die **Menschenwürde nicht berühren** (zB Zeiterfassung mittels Magnetkarte) -> Soll ein derartiges System eingeführt werden, muss der BR oder der DN **nicht zustimmen**;
- ... die **Menschenwürde berühren** (zB Fingerabdruck, Iris-Scan) -> Soll ein derartiges System eingeführt werden, muss der BR oder der DN **ausdrücklich zustimmen**. Da es sich hierbei um eine **zustimmungspflichtige Maßnahme** gemäß § 96 Abs 1 Z 3 ArbVG handelt, kann der BR verhindern, dass ein derartiges Zeiterfassungssystem eingeführt wird.

3. Videoüberwachung

Videoüberwachungen sind dann arbeitsrechtlich **zulässig** , wenn etwa **sensible** Unternehmensbereiche überwacht werden müssen, wie zB der Kassenbereich einer Bank.

Hitz/Schrenk, Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag, PVP 2017, Seite 320

Da eine derartige Videoüberwachung jedenfalls die **Menschenwürde berührt**, ist nach den Bestimmungen des § 96 Abs 1 Z 3 ArbVG eine (**zwingende**) **BV** bzw in Betrieben ohne Betriebsrat nach § 10 AVRAG eine **Einzelvereinbarung** notwendig.

Werden

a) **höchstpersönliche Lebensbereiche** iSd § 50a Abs 5 DSG 2000 videoüberwacht (zB Toilette oder Waschräume) oder
b) dient die **Videoüberwachung** dazu, DN hinsichtlich deren Leistung oder Verhalten zu **kontrollieren**,

dann sind diese Videoüberwachungen jedenfalls **unzulässig** .

4. (Privat-) Nutzung von Internet (Social Media)

a) Private Nutzung von Internet, E-Mail etc durch Dienstnehmer erlaubt?

Die **private Nutzung** von **Betriebsmitteln**, wie etwa von Firmen-PC, Internet, Firmen-WLAN mit einem Privatgerät, Telefon und Kopierer, muss **ausdrücklich genehmigt** oder schlüssig **vereinbart** sein.

Der BR kann verlangen, dass eine entsprechende, **erzwingbare BV** abgeschlossen wird (§ 97 Abs 1 Z 6 ArbVG: "*Maßnahmen zur zweckentsprechenden Benützung von Betriebseinrichtungen und Betriebsmitteln*").

Auch wenn der DG die private Nutzung von Internet und E-Mail erlaubt, hat der **DN** darauf zu **achten**, dass durch diese

Privatnutzung

- seine **Arbeit nicht beeinträchtigt** wird und
- die für betriebliche Zwecke vorgesehenen **Speichermöglichkeiten nicht** unzumutbar stark **belastet** werden sowie dass
- **keine Sicherheitsrisiken** (zB Gefahr eines Virenimports; siehe hierzu PVP 2016/80, 295, November-Heft: "*Dienstnehmer nutzt privat das betriebliche Internet/E-Mail: Wann und wie haftet er für eingeschleppte Viren?*") und
- **keine finanziellen Belastungen** für den Betrieb geschaffen werden dürfen.

Hat der DG ein ausdrückliches **Verbot** der privaten Internet- und E-Mail-Benützung durch den DN ausgesprochen, muss er gemäß bestehender Rechtsprechung **dennoch dulden**, dass der DN während der Arbeitszeit das Firmen-E-Mail für private E-Mails in geringem Umfang für kurze, unbedingt erforderliche Mitteilungen nutzt.

Die **übermäßige Privatnutzung** kann jedenfalls einen **Entlassungsgrund** darstellen ("*täglich mind. 1,5h Internetznutzung, privates Surfen und Download umfangreicher Film- und Musikdateien*"; OGH 8 ObA 52/11x).

b) Überwachung der Internet- und E-Mail-Nutzung durch den Dienstgeber

Wie der DG für die ordnungsgemäße Nutzung der Betriebsmittel sorgt bzw die Nutzung kontrolliert, muss er aufgrund arbeitsrechtlicher (zB BR-Zustimmung?) und datenschutzrechtlicher Aspekte festlegen.

Die **Überwachung** ist in Österreich **ohne BR-Zustimmung** oder ohne DN-Zustimmung (in Betrieben ohne BR) grundsätzlich **nicht möglich** (§§ 96, 96a, 97 ArbVG, § 10 AVRAG), außer es liegt ein konkreter **Verdacht** auf eine **strafbare Handlung** bzw sonstige mögliche **Schädigungen** des DG (Viren, extremes Datenvolumen, Versand von Kundendaten etc) vor.

Auch das **"Mit-Lesen" privater** E-Mails ist grundsätzlich **nicht** erlaubt. In **begründeten Einzelfällen** ist eine individuelle, **spontane Kontrolle** zulässig.

Hitz/Schrenk, Datenschutzserie Teil 1: Datenschutz im arbeitsrechtlichen Alltag, PVP 2017, Seite 321

5. Nachvertragliche Verpflichtungen (Dienstzeugnisse, Auskünfte)

Der DN kann **30 Jahre** lang verlangen, dass ihm der DG ein **Dienstzeugnis** ausstellt. Aufgrund dieser Verpflichtung darf der DG unzweifelhaft **datenschutzrechtlich** die hierfür erforderlichen **Daten 30 Jahre lang aufbewahren**.

Die arbeitsrechtliche DG-Fürsorgepflicht endet nicht mit dem DV-Ende. So darf der ehemalige DG **hinsichtlich** des **ehemaligen DN nicht** ...

a) ... **Auskünfte** einem potenziellen DG erteilen, bei dem sich der DN bewirbt, wenn diese die beruflichen **Chancen**, den Job zu bekommen, **negativ** beeinflussen (OGH 30. 4. 2012, 9 ObA 56/11t; ARD 6269/3/2012: "*Die **Ankündigung** des **früheren Arbeitgebers** einer Angestellten, die bestehende **Geschäftsbeziehung** mit ihrem **neuen Arbeitgeber** dann **einschränken** zu wollen, wenn dieser die frühere Angestellte **einstelle** und diese für seine Betreuung zuständig sein sollte, **verstößt** gegen die **nachwirkende Fürsorgepflicht** des Arbeitgebers")*;

b) ... - aus datenschutzrechtlichen Gründen - **personenbezogene** oder **sensible** Daten (wie etwa Informationen über die Krankenstandshäufigkeit) **weitergeben**.

E) Rechte des Arbeitnehmers nach DSG 2000 bzw DSGVO (Auszug)

- Informationspflicht (Art 12-14 DSGVO)
- Recht auf Auskunft (§ 26 DSG 2000, Art 15 DSGVO)
- Recht auf Richtigstellung oder Löschung (§ 27 DSG 2000, Art 16-17 DSGVO)
- Recht auf Widerspruch (§ 28 DSG 2000, Art 21 DSGVO)

F) Zusammenfassung

Bereits jetzt sind **Datenschutz-Bestimmungen** zu beachten, bspw wenn

- **Zeiterfassungssysteme** mittels biometrischer Daten **eingerichtet** werden oder
- die **Privatnutzung** von Betriebsmitteln **kontrolliert** werden soll.

Durch die ab 25. 5. 2018 anzuwendende **DSGVO** und die damit verbundenen DN-Rechte wird das Thema **Datenschutz** jedenfalls **mehr** als bisher an **Bedeutung** gewinnen. Neu ab 25. 5. 2018 sind zunehmende Verpflichtungen hinsichtlich **Transparenz** und **Offenlegung** der **Datenverarbeitung** und der vom DG gesetzten Maßnahmen.

Wann und wie lange Daten der DN zulässigerweise **gespeichert** werden dürfen, wann diese **gelöscht** werden müssen, diese Themen regelt die **DSGVO präziser und strenger** als das bisher geltende DSG 2000.

Der DG hat künftig sehr genau zu **überlegen**, welche Daten des (ehemaligen) DN er noch **speichern** muss/darf und welche zu **vernichten** sind.

In der Praxis sind noch viele **Antworten offen**, etwa auf die Frage des **"Wie"** der **Datenvernichtung** sowie der grundsätzlichen Frage, ob sich das DN-Verhalten bezüglich ihrer Daten grundsätzlich ändern wird, dh, ob sie sensibler darauf achten, dass die Datenschutzbestimmungen vom DG beachtet werden.

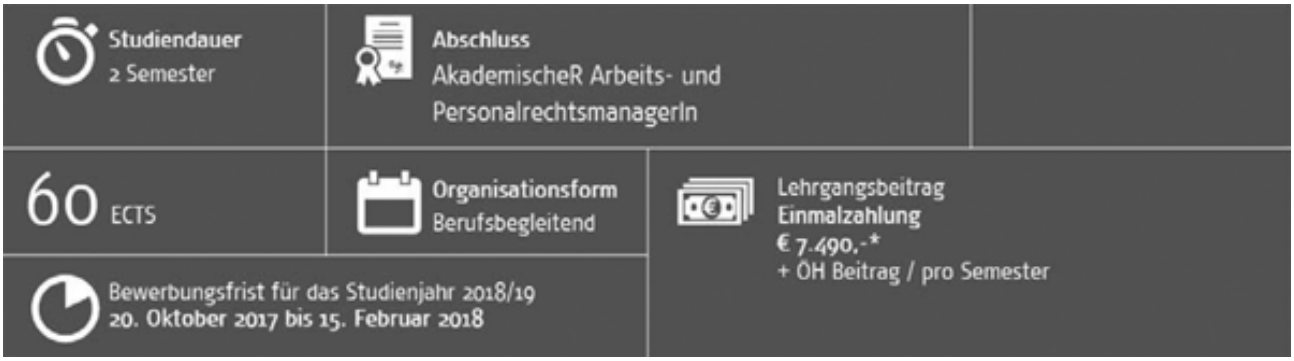
Hinweis der Redaktion

Der FH Campus Wien hat einen berufsbegleitenden **akademischen Lehrgang** mit dem Titel "*Arbeits- und Personalrechtsmanagement*" geschaffen, in dem die beiden Autoren vortragen.

Warum dieser Lehrgang eingerichtet wurde, beschreibt die FH Wien wie folgt:

"*Nationale Gesetze, EU-Recht, internationales Recht, Kollektivverträge oder Betriebsvereinbarungen regulieren das Personalwesen, begleitet von einer umfangreichen Rechtspre-*

chung. Der Lehrgang ***verknüpft*** *die Bereiche* ***Arbeits*** *-, Lohnsteuer- und* ***Sozialversicherungsrecht*** *mit Fragen des* ***Personalmanagements*** *. Er positioniert sich damit als interdisziplinäre Weiterbildung für PersonalverrechnerInnen, SteuerberaterInnen PersonalmanagerInnen und andere Berufsgruppen mit Personalagenden."*



Mehr **Details** finden Sie hier:
https://www.fh-campuswien.ac.at/studiengaenge/public-sector-akademische-lehrgaenge/arbeits-und-personalrechtsmanagement.html

Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2017/99

PVP 2017, 349
Heft 12 v. 22.12.2017
Themen-Special

Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners

Mag. Wolfram Hitz/Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Obwohl er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565). Die **ersten Schritte** für eine **innerbetriebliche Umsetzung** sollten unbedingt **zeitnah** gesetzt werden.

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf.

Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht**: In PVP 2017/90, 317 (November-Heft) informieren wir Sie über die **Datenschutzrechtsgrundlagen, arbeitsrechtlich** relevanten **Daten** und **Definitionen** und über konkrete **Datenschutzfragen** im **arbeitsrechtlichen Alltag**.
- **Teil 2: Datenschutz im Alltag des Personalverrechners:** In **diesem Heft** informieren wir Sie ua über die **Verwendung, Verarbeitung** und **Aufbewahrung sensibler Daten** und über die (**datenschutzrechtlichen) Pflichten** des Dienstleisters und seiner **Dienstnehmer**.
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs**
- **Teil 4: Details zur neuen Datenschutz-Grundverordnung**

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** ... Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//**BR** ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ... Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung//**WKO** ... Wirtschaftskammer Österreich

A) Warum ein entsprechender Aus- und Weiterbildungsbedarf bei Personalverrechnern besteht?

In einer kürzlich europaweit durchgeführten **Umfrage** eines internationalen HR- und Payroll-Dienstleisters gab mehr als die **Hälfte** der befragten **Personalisten** und **Personalverrechner** an, **"keine Ahnung"** zu haben, worum es sich bei der **DSGVO** handelt.[1)]

1) https://www.sdworx.at/de-at/presse/2017-11-28-hr-manager-ignorieren-dsgvo

Diese Umfrage zeigt - neben den Erfahrungen aus Aus- und Weiterbildungsveranstaltungen -, dass ein dringender Handlungsbedarf besteht und dass die **DSGVO** und die damit zusammenhängenden Änderungen des nationalen Datenschutzgesetzes bei Personalisten und Personalverrechnern **ganz oben** auf der **Agenda** für das Jahr **2018** stehen sollten/müssten.

Hitz/Schrenk, Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners, PVP 2017, Seite 349

Datenschutzverstöße [#10140] Konsequenzen

*"Verstoße gegen das Datenschutzrecht werden mit **hohen Geldstrafen** für Ihr Unternehmen geahndet und können auch für Sie **arbeitsrechtliche Konsequenzen** haben.*

*Zusätzlich können Geschädigte **Schadenersatz** einklagen. Dazu kommt noch der **Vertrauensverlust** bei Kunden und Geschäftspartnern, ..."* schreibt die **WKO** in einem "*IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter*" in der nunmehr 8. Auflage (https://www.wko.at/site/it-safe/mitarbeiter-handbuch.html).

B) Der Personalverrechner und die Verarbeitung personenbezogener Daten

1. Personenbezogene Daten: Übersendung an Dienstleister & Datenablage

Als Personalverrechner erhält man nahezu täglich - als **E-Mail Anhang** oder als **Ausdrucke** und **Kopien** - **personenbezogene Daten**. In erster Linie sind dies Daten, die benötigt werden, um

- die **Stammdaten** im PV-Abrechnungssystem **anzulegen**,
- die **Abrechnung korrekt durchführen** zu können (= abrechnungsrelevante Unterlagen, zB Meldezettel, Ausweiskopien oder die Kopien von Bankomatkarten und Aufenthaltstiteln).

Diese **Unterlagen** müssen entweder in **physischen** Ordnern, in **digitalen** Ordnern oder in **Dokumentenmanagementsystemen**, wie sie nahezu alle gängigen Softwarehersteller anbieten, abgelegt werden.

Das **Datenschutzrecht unterscheidet** dabei grundsätzlich **nicht**, ob die **Daten** nur **virtuell** am PC vorliegen oder physisch in **Papierform**. Solange es sich nicht um "Schmierzettel" handelt, die nicht systematisch geordnet oder abgelegt werden, sind die Daten immer gleich zu behandeln und zu schützen, egal in welcher Form sie vorliegen.

2. Verwendung und Verarbeitung sensibler Daten

a) Was sind (sensible) Daten?

Der **Begriff "*Daten*"** ist im Datenschutzrecht sehr **allgemein gehalten** und umfasst alle Angaben über Betroffene, deren Identität bestimmt oder bestimmbar ist. Bei diesen "Daten" gemäß § 4 DSG 2000 handelt es sich bspw um den Namen, das Geschlecht oder den Familienstand.

Bei " ***sensiblen Daten*** " handelt es sich bspw um Daten betreffend ethnische Herkunft, politische Meinung, religiöse Überzeugung oder die sexuelle Orientierung des Betroffenen.

b) Zustimmung des Dienstnehmers zur Datenverwendung?

Muss der **DN zustimmen**, wenn **notwendige** (**nicht sensible) Daten** für die Personalverrechnung verwendet werden? **Nein** , da sich die Rechtmäßigkeit, diese Daten zu verwenden, aus dem Gesetz ergibt. Dies allerdings unter der Voraussetzung, dass die Daten entsprechend den gesetzlichen Bestimmungen verwendet werden.

Der **Dienstleister** (Steuerberater, Bilanzbuchhalter, sonstiger Personaldienstleister) darf die Daten ausschließlich aufgrund der Aufträge des Auftraggebers verwenden (siehe § 6 DSG 2000).

Ja , eine **Zustimmung** zur Verwendung von Daten ist bspw dann **notwendig**, wenn die Daten **über** die gesetzliche **Aufbewahrungsfrist hinaus aufbewahrt** werden sollen. Dies spielt in der Personalverrechnung jedoch keine Rolle. Daher ist idR **weder** nach dem DSG 2000, **noch** nach den Bestimmungen der DSGVO oder nach dem "DSG neu" eine **DN-Zustimmung** für die Verwendung der für das DV relevanten Daten einzuholen.

Hitz/Schrenk, Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners, PVP 2017, Seite 350

C) So bewahren Sie Daten ordnungsgemäß iSd Datenschutzes auf

Neben dem Aspekt des Datenschutzes ist auch die **Datensicherheit** zu **berücksichtigen**. Der Wirtschaftstreuhänder, Bilanzbuchhalter oder ein sonstiger Dienstleister hat für die **technische Sicherung** und die **ordnungsgemäße Aufbewahrung** von personenbezogenen Daten zu sorgen.

Checkliste zur Aufbewahrung von personenbezogenen Daten (Empfehlung):

a) **Physische Dokumente** sind ...
- ... in **nicht einsehbaren**, verschließ- und/oder **versperrbaren** Kästen und
- in **Räumen aufzubewahren**, in denen grundsätzlich **kein Kundenverkehr** herrscht (nicht etwa in unverschlossenen Kästen im Empfangsraum oder in Archiven, in denen sich jemand unbemerkt Zutritt verschaffen kann);
- ... vom **Arbeitsplatz** zu **entfernen**, wenn sie nicht mehr verwendet werden;
- ... zu **vernichten** (einschließlich der Kopien), sobald die Dokumente aufgrund der Auftragserfüllung nicht mehr benötigt werden.

b) **Digitale Dokumente** sind ...
- ... auf **geschützten Speichermedien** (Firmenserver mit Firewall) und
- gegebenenfalls mit **Passwortschutz** zu speichern;
- ... zu **löschen** (einschließlich der Kopien), sobald die Dokumente aufgrund der Auftragserfüllung nicht mehr benötigt werden.

Hinweis

Eine (**ohne Rechtsgrund**) zeitlich **nicht befristete Speicherung** personenbezogener Daten **widerspricht** jedenfalls dem Grundsatz des **§ 6 Abs 1 Z 5 DSG 2000**.

D) Die (datenschutzrechtlichen) Pflichten des Dienstleisters

1. Pflichten des Dienstleisters nach § 11 DSG 2000

Pflichten des Dienstleisters nach § 11 DSG 2000 lassen sich wie folgt zusammenfassen:

- Daten sind ausschließlich aufgrund der Aufträge des Auftraggebers zu verwenden, insbesondere ist

verboten, die verwendeten **Daten ohne Auftrag** des Auftraggebers zu **übermitteln**.

- Es sind alle erforderlichen **Datensicherheitsmaßnahmen** zu **treffen**, zB betriebsinterne Festlegung der Aufgabenbereiche, Belehrung der betreffenden Mitarbeiter zu Datenschutzvorschriften, "Schutz" der Daten, etc.
- **Weitere Dienstleister** sind dann heranzuziehen, wenn der **Auftraggeber zustimmt**.
- Wird die **Dienstleistung beendet**, sind alle **Verarbeitungsergebnisse** und **Unterlagen**, die **Daten** enthalten, dem **Auftraggeber** zu **übergeben** oder **in dessen Auftrag** für ihn weiter aufzubewahren oder zu **vernichten.**

2. Verpflichtung der Dienstnehmer (Personalmanager, Personalverrechner etc) zur Geheimhaltung und Verschwiegenheit

DN unterliegen der **Treuepflicht** [#10140] Mitarbeiter sind daher grundsätzlich zur **Geheimhaltung** und **Verschwiegenheit** von Geschäfts- und Betriebsgeheimnissen **verpflichtet**.

Die **Pflicht** zu Verschwiegenheit und Geheimhaltung geht **über** das **DV-Ende** hinaus.

Hitz/Schrenk, Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners, PVP 2017, Seite 351

Empfehlung

Um die Verschwiegenheitsverpflichtung abzusichern, empfehlen wir, dass eine entsprechende **Regelung** in den **DV** (oder in einen **DV-Zusatz**) **aufgenommen** wird.

Auch in **privaten Gesprächen** dürfen die **Kunden-** bzw **Klientennamen** oder sonstige Informationen auch nach DV-Ende nicht erwähnt werden.

Verstößt der DN gegen diese Verpflichtung, kann er bei aufrechtem DV **entlassen** werden. Auch ein etwaiger **Schadenersatz** ist denkbar.

3. Datenschutzrechtliche Pflichten aufgrund der Korrespondenz mit Behörden, Klienten und Dritten

Grundsätzlich darf der Personalist oder Personalverrechner nur mit jenen Behörden und Dritten (zB Banken) in **Kontakt** treten, die in **Zusammenhang** stehen mit der laufenden **Personalverrechnung** oder etwaiger personalrechtlicher Beratung.

Finden Tätigkeiten im Auftrag des **Klienten** statt, wird idR eine **mündliche Vollmacht** diesbezüglich anzunehmen sein.

Nutzt der Personalverrechner die **Plattform WEBEKU**, wird er von dieser auf datenschutzrechtliche Bestimmungen hingewiesen.

Beispiel

Wird bspw die **SV-Nummer eines DN** benötigt, bietet die Plattform die Möglichkeit, diese mit Hilfe des Namens und des Geburtsdatums abzufragen. **Bevor** man diese Auskunft erhält, muss man folgenden **Hinweis bestätigen**:

"*Ich bestätige ausdrücklich, dass ich (allenfalls als **Vertreter**) **berechtigt** bin, diese Daten zu erhalten. Ihre **Abfrage** wird aufgezeichnet (**protokolliert**), es werden darüber Auskünfte nach dem Datenschutzgesetz gegeben."*

- **Korrespondenz und Kontakte mit GKK** [#10140] **Datenschutz-Infos**

Insgesamt gibt es bei allen **GKK interne Datenschutzrichtlinien**. So schreibt etwa die **Salzburger GKK**:

*"Jeder hat ein **Grundrecht** darauf, dass seine **Daten geschützt** werden. Zum Schutz Ihrer persönlichen Daten folgen wir innerhalb der Salzburger Gebietskrankenkasse sehr strengen Datenschutzrichtlinien. Unsere MitarbeiterInnen im Kundenservice dürfen daher **Auskünfte** zu **personenbezogenen Daten** nur unter **gewissen Voraussetzungen** und auf **gesicherten Kommunikationswegen** an Sie übermitteln."*

- **Korrespondenz und Kontakte mit Finanzbehörden** [#10140] **Datenschutz-Infos**

Beim Finanzamt erhält man online **kaum Informationen** zum Datenschutz.

- **Korrespondenz und Kontakte mit Magistrat der Stadt Wien** [#10140] **Datenschutz-Infos**

Beim Magistrat der Stadt Wien gibt es eine **umfassende Auskunft** über Datenschutz, Weitergabe personenbezogener Daten und Auskunftsrechte. (https://www.wien.gv.at/info/datenschutz/)

4. Pflichten des Dienstleisters bei der Auskunftserteilung

Den Personalisten oder Personalverrechner treffen aber auch Pflichten bei der Auskunftserteilung. So **kennt** nahezu jeder Personalverrechner bspw die **Anrufe** von **Bankmitarbeitern**, die sich anlässlich einer Kreditvergabe an die abrechnende Stelle wenden.

Hitz/Schrenk, Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners, PVP 2017, Seite 352

Eine solche **Auskunft telefonisch** zu erteilen ist **datenschutzrechtlich** höchst **problematisch**, da während eines Telefonats **nicht festgestellt** werden kann, ob der Gesprächspartner tatsächlich im **Auftrag** eines **DN** oder des **Klienten** anruft.

Empfehlungen

1. Fordern Sie eine **schriftliche Anfrage** an und holen Sie die **Zustimmung** des DN oder des Klienten ein, dass Sie die gewünschte Auskunft erteilen dürfen.
2. **Weitere Empfehlungen** für Personalisten, HR-Manager und Personalverrechner:
   - Erhaltene Daten müssen nach **datenschutzrechtlichen Bestimmungen verwahrt** werden. Physisch und digital sind entsprechende Anforderungen zu erfüllen.
   - Die **Verwendung** dieser Daten hat ausschließlich aufgrund der **Aufträge** des Auftraggebers zu erfolgen.
   - Die **Beschaffung** von Informationen bei Behörden oder Dritten darf nur für **abrechnungsrelevante** Unterlagen innerhalb der erteilten **Vollmacht** stattfinden.
   - **Auskünfte** über **personenbezogene Daten** an **Behörden** oder **Dritte** dürfen erteilt werden, wenn diese aufgrund der **Abrechnung** erforderlich sind und eine **Zustimmung** der betroffenen Person angenommen werden kann oder ausdrücklich gegeben wurde.
   - **Auskünfte** über **personenbezogene Daten** dürfen nur an den **Auftraggeber** oder dessen bevollmächtigten **Vertreter** gegeben werden. Holt etwa ein **DN** eines **Klienten Unterlagen** ab, ist uE die diesbezügliche **Zustimmung** des Auftraggebers (**Klienten**) zumindest mündlich einzuholen.
   - Für die Abrechnung **nicht mehr benötigte Unterlagen** sind dem Auftraggeber zu **retournieren**, wobei dieser **schriftlich bestätigen** soll, dass er die Unterlagen **erhalten** hat. Etwaige **Kopien** oder digitale Dokumente sind zu **vernichten**.

E) Datenschutzrechtliche Hinweise rund um die Privatnutzung von Firmeneigentum

Auch Personalisten und Personalverrechner nutzen oftmals Firmeneigentum (insbesondere Handy, Laptop etc) für Privatzwecke, zB um Nachrichten zu lesen, Überweisungen online durchzuführen oder über Facebook und Co zu chatten.

Ist eine solche **Nutzung** durch den DG - wie nachstehend erläutert - ausdrücklich **gestattet** oder geduldet, sind **datenschutzrechtliche** Aspekte zu **beachten**.

1. Erlaubte Privatnutzung bzw Privatnutzungsverbot

Wie bereits im 1. Teil der Artikelserie in PVP 2017/90, 317 (November-Heft) hingewiesen, ist für die **private Nutzung** von Betriebsmitteln eine ausdrückliche **Genehmigung** oder eine schlüssige **Vereinbarung** notwendig. Es ist umgekehrt aber **möglich**, dass der DG ein ausdrückliches **Privatnutzungsverbot** erteilt.

Allerdings muss der DG auch bei **Verbot** der privaten Nutzung von Betriebsmitteln nach der ständigen **Rechtsprechung** trotzdem **dulden**, dass der DN eine **Privatnutzung** in **geringem Umfang** vornimmt, etwa um kurze, unbedingt erforderliche E-Mail-Nachrichten zu versenden.

Hitz/Schrenk, Datenschutzserie Teil 2: Datenschutz im Alltag des Personalverrechners, PVP 2017, Seite 353

Beispiele aus der Rechtsprechung

a) Leitet ein DN **2-3 Spaß-E-Mails pro Woche** an Kollegen weiter, ist dies bei einer 20-jährigen unbeanstandeten Tätigkeit **kein Entlassungsgrund** (OGH 23. 6. 2004, 9 ObA 75/04a; ARD 5552/16/2004).
b) Wird jedoch der **Kopierer** über einen längeren Zeitraum in **exzessivem Ausmaß** und im bewussten Verstoß gegen DG-Weisungen **privat** genutzt, ist dies sehr wohl ein **Entlassungsgrund** (OGH 28. 2. 2012, 8 ObA 13/12p; ARD 6231/3/2012).
c) Details dazu werden im 3. Teil der Artikelserie aus DG-Sicht beleuchtet werden.

2. Personenbezogene Daten auf privaten Geräten: Was ist hierbei datenschutzrechtlich zu beachten?

Im Zeitalter von **mobile working** (home office) ist es durchaus üblich, dass private Geräte für betriebliche Zwecke genutzt werden. Dies kann etwa die Einrichtung der **Firmen-E-Mail-Adresse am Smartphone** oder **Tablet** sein oder der **Fernzugang** zum **Firmen PC** am **privaten Computer** oder Laptop.

Empfehlungen

Treffen Sie in diesen Fällen unbedingt entsprechende **Sicherungsmaßnahmen**:[2)]

- Sorgen Sie für eine **diebstahlsichere Aufbewahrung** des Geräts.
- **Sichern** Sie Ihre Geräte mit geeigneten **Passwörtern**.
- Geben Sie das Gerät **nicht unbeaufsichtigt** an Dritte weiter.
- **Schützen** Sie Ihr Gerät vor **unbefugten Blicken.**
- Nutzen Sie nur **sichere Internetverbindungen**, dies kann bspw ein privater, passwortgeschützter Internetzugang oder eine gesicherte Verbindung über Ihr Smartphone sein.
- DN sollen möglichst **kein öffentliches Netzwerk** nutzen, wie etwa jene in einem Kaffeehaus, einem Hotel oder im öffentlichen Verkehrsmittel (ÖBB).

2) **Quelle**: WKO "IT Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter", 8. Auflage

Hinweis

Private Cloud-Speicherdienste sollten für **Firmendaten** nicht oder nur nach **Rücksprache** mit dem **IT-Verantwortlichen** verwendet werden.

F) Schlussfolgerung

Aufgrund der ab Mai 2018 geltenden neuen Rechtslage sollten viele **DG überprüfen** und **überdenken**, wie im Unternehmen **personenbezogene Daten verwendet**, **aufbewahrt** und **verarbeitet** werden. Insbesondere Personalisten und Personalverrechner brauchen für ihre Arbeit tagtäglich personenbezogene Daten, für deren Verwendung es künftig eine **unternehmensinterne Richtlinie** geben sollte. Gerade in Zeiten

- von **"*mobile working*"**, **"*bring your own device*"**,
- aufgrund der oftmals erforderlichen - arbeitsrechtlich durchaus kritisch zu betrachtenden - **ständigen Erreichbarkeit** und
- aufgrund der allgemeinen raschen **technologischen Entwicklung**

sorgt eine solche Richtlinie dafür, dass die **datenschutzrechtlichen Bestimmungen eingehalten** und dadurch DN, Klienten und das eigene Unternehmen vor etwaigen **Schäden bewahrt** werden.

Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2018/8

PVP 2018, 28
Heft 1 v. 25.01.2018
Themen-Special

Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs

Mag. Wolfram Hitz/Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Obwohl er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565). Die **ersten Schritte** für eine **innerbetriebliche Umsetzung** sollten unbedingt **zeitnah** gesetzt werden.

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf. Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht:** In PVP 2017/90, 317 (November-Heft) informieren wir Sie über die **Datenschutzrechtsgrundlagen, arbeitsrechtlich** relevanten **Daten** und **Definitionen** und über konkrete **Datenschutzfragen** im **arbeitsrechtlichen Alltag**.
- **Teil 2: Datenschutz im Alltag des Personalverrechners:** In PVP 2017/99, 349 (Dezember-Heft) informieren wir Sie ua über die **Verwendung**, **Verarbeitung** und **Aufbewahrung sensibler Daten** und über die **(datenschutzrechtlichen) Pflichten** des Dienstleisters und seiner **Dienstnehmer**.
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs:** In diesem Heft informieren wir Sie ua darüber, welche **datenschutzrechtlichen Bestimmungen** während des **Bewerbungsprozesses**, des **laufenden Dienstverhältnisses** und nach **Beendigung** dessen zu beachten sind.

  Wir haben möglichst naheliegende und in der **Beratungspraxis** häufig auftauchende **Fragen** aufgegriffen und **beantworten** diese **praxisnah**. Der **Aufbau** des **Artikels** orientiert sich an der **Chronologie** eines Dienstverhältnisses (vom Bewerbungsprozess [#10140] laufende Dienstverhältnis [#10140] Beendigung des Dienstverhältnisses; beantwortet werden auch **Fragen** aus dem **Büroalltag**.
- **Teil 4: Details zur neuen Datenschutz-Grundverordnung**

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** ... Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//**BR** ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ...

Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**GlbG** ... Gleichbehandlungsgesetz//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung//**WKO** ... Wirtschaftskammer Österreich

A) Der Bewerbungsprozess: Welche Daten über einen Bewerber dürfen wie eingeholt werden?

1. Bewerberdaten und datenschutzrechtliche Grundsätze

Bereits im **Teil 1** dieser Serie (Datenschutz im Arbeitsrecht) haben wir im **Punkt D) 1.** (Vorvertragliche Verpflichtungen [Bewerbungen]) ua darauf hingewiesen, dass insbesondere ein **Rechtferti-**

gungsgrund für die Abfrage, die Verarbeitung bzw Aufbewahrung von (sensiblen) Daten vorliegen muss (weitere Details und Beispiele: siehe **PVP 2017/90, 317**; November-Heft).

Übermittelt der **Bewerber** seine **Unterlagen**, ist davon auszugehen, dass er **zustimmt**, dass seine Unterlagen/Daten entsprechend **verarbeitet** werden.

2. Informationen über den Bewerber einholen - (datenschutz)rechtliche Anmerkungen und Hinweise

In der Vergangenheit wurden **Informationen** über Bewerber eingeholt, indem der **frühere DG** oder **Personalchef kontaktiert** wurde, oder man war auf **Mundpropaganda** angewiesen.

Das **Internet** (Social Media-Plattformen, Postings, Blogs, Profile über Sportaktivitäten, Gemeinderatsprotokolle über Grundstückskäufe etc) schafft vielfältige **neue Info-Beschaffungs-Möglichkeiten**; es sind große Mengen an Informationen über Stellenwerber abrufbar. Die Frage ist, inwieweit deren **Nutzung** im Bewerbungsverfahren **rechtlich zulässig** ist.

Zu **unterscheiden** ist zunächst zwischen dem **faktischen** und dem **juristischen Problem**:

- **Faktisches Problem**

Selbst wenn der Personalist, auf welche Art auch immer, recherchiert, wird er dies in der Praxis sehr selten offenlegen, sondern eine Absage (aufgrund der Recherche) mit allgemeinen Aussagen begründen.

- **Rechtliches Problem**

Rein rechtlich ist aber darauf abzustellen, wo und auf welche Weise Daten recherchiert wurden.

Entgegen manch anderslautenden Aussagen sind jene **Daten**, die auf einem **Social Media-Profil öffentlich einsehbar** sind, vom Bewerber selbst öffentlich gemacht und unterliegen daher **nicht** mehr dem **Schutz** des Datenschutzrechtes. Es ist dabei egal, ob es sich um ein "freizeitorientiertes" oder ein "berufsorientiertes" Netzwerk handelt (zB Facebook vs Xing).

- **Arbeitsrechtliche Judikatur**

Die **arbeitsrechtliche Judikatur** geht ebenso in diese Richtung und sieht **beleidigende Postings** bzw ein Offenlegen von **Krankenstandsmissbrauch** via Facebook jedenfalls als **entlassungsrelevant** an (zB berechtigte Entlassung bei Beleidigungen als "*Arsch*", "*Arschloch*", dem Vorwurf der "*Blödheit*", OLG Linz 1. 3. 2017, 12 Ra 7/17m, ARD 6558/12/2017, bzw bei Bildern aus dem Urlaub oder bei Sportausübung während Krankenstand).

Hinweis

Achten Sie auf die **arbeitsrechtlichen Einschränkungen**, die sich aus der **Verwendung** (sensibler) **Daten** ergeben: Erfolgt etwa eine **Job-Absage** aufgrund eines **Diskriminierungstatbestandes**, können sich aus dem GlBG **Schadenersatzpflichten** ergeben (zB wird der Bewerber deshalb nicht engagiert, weil er laut seinem Profil gleichgeschlechtlich verpartnert ist oder Postings der Gewerkschaft teilt).

Hinweise der Redaktion

1 Im **nächsten Heft** setzen wir den Beitrag betreffend Datenschutz im Alltag des Firmeninhabers/Personalchefs fort und informieren über

- **datenschutzrechtliche Sonderfragen** *rund um das* **laufende Dienstverhältnis** ,
- *das* **Datenschutzrecht** *im* **Büroalltag** ,
- *die* **Aufgaben** *und* **Befugnisse** *der* **Datenschutzbehörde** ,
- *den Umgang mit* **Dienstnehmer-Daten** , *nachdem das* **Dienstverhältnis beendet** *wurde.*

Hitz/Schrenk, Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs, PVP 2018, Seite 29

2 Die Autoren bieten ein umfangreiches Info-Service rund um das neue Datenschutzrecht (© Wirtschaftskammer) an:

- **EU-Datenschutz-Grundverordnung** *(DSGVO):* **Kurzüberblick** *und Zeitplan (https://w.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html)*
- **EU-Datenschutz-Grundverordnung** *(DSGVO):* **Checkliste** *(https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html)*
- **Online-Ratgeber** *(http://dsgvo.wkoratgeber.at/), der Sie anhand verschiedener Fragen durch das Thema führt und nach einigen Klicks eine individuelle Auswertung empfohlener Maßnahmen liefert. Damit wissen Sie schnell, orts- und zeitunabhängig, was noch alles zu tun ist.*
- **Vereinbarung** *mit einem* **externen Dienstleister** *über eine Auftragsverarbeitung nach Art 28 DSGVO (https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html)*

3 Der FH Campus Wien hat in Kooperation mit der Akademie der WT einen berufsbegleitenden, 2-semestrigen **akademischen Lehrgang** mit dem Titel "*Arbeits- und Personalrechtsmanagement*" geschaffen. Dieser Lehrgang bietet eine **umfassende akademische Weiterbildung** zum Thema Arbeitsrecht, Personalrecht, Personalmanagement, SV-Recht und Lohnsteuerrecht.

Lehrgangsleitung: Mag. Friedrich Schrenk

Fachkonzept: entwickelt vom Autor dieses Beitrages, Florian Schrenk

Lehrgangsstart: 16. 3. 2018

Bewerbungsfrist: 15. 2. 2018

Die Vortragsblöcke finden alle 2 Wochen hauptsächlich am Freitag und Samstag statt.

Mehr **Details** finden Sie hier:
https://www.fh-campuswien.ac.at/studiengaenge/public-sector-akademische-lehrgaenge/arbeits-und-personalrechtsmanag

Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2018/14

PVP 2018, 49
Heft 2 v. 27.02.2018
Themen-Special

Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs

Mag. Wolfram Hitz/Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Obwohl er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565). Die **ersten Schritte** für eine **innerbetriebliche Umsetzung** sollten unbedingt **zeitnah** gesetzt werden.

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf.

Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht**: In PVP 2017/90, 317 (November-Heft) informieren wir Sie über die **Datenschutzrechtsgrundlagen, arbeitsrechtlich** relevanten **Daten** und **Definitionen** und über konkrete **Datenschutzfragen** im **arbeitsrechtlichen Alltag**.
- **Teil 2: Datenschutz im Alltag des Personalverrechners**: In PVP 2017/99, 349 (Dezember-Heft) informieren wir Sie ua über die **Verwendung**, **Verarbeitung** und **Aufbewahrung sensibler Daten** und über die (**datenschutzrechtlichen) Pflichten** des Dienstleisters und seiner **Dienstnehmer**.
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs**: In PVP 2018/8, 28 (Jänner-Heft) und in diesem Heft informieren wir Sie ua darüber, welche **datenschutzrechtlichen Bestimmungen** während des **Bewerbungsprozesses**, des **laufenden Dienstverhältnisses** und nach **Beendigung** dessen zu beachten sind.

  Wir haben möglichst naheliegende und in der **Beratungspraxis** häufig auftauchende **Fragen** aufgegriffen und **beantworten** diese **praxisnah**. Der **Aufbau** des **Artikels** orientiert sich an der **Chronologie** eines Dienstverhältnisses (Bewerbungsprozess [#10140] laufendes Dienstverhältnis [#10140] Beendigung des Dienstverhältnisses); beantwortet werden auch **Fragen** aus dem **Büroalltag**.
- **Teil 4: Details zur neuen Datenschutz-Grundverordnung**

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** ... Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//

BR ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ... Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**GlbG** ... Gleichbehandlungsgesetz//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung//**WKO** ... Wirtschaftskammer Österreich

Hitz/Schrenk, Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs, PVP 2018, Seite 49

B) Datenschutzrechtliche Sonderfragen rund um das laufende Dienstverhältnis

1. Belehrung und Unterweisung von Mitarbeitern

Nach derzeit geltender Rechtslage sind DN über die gesetzlichen und betrieblichen **Datenschutz**- und **Sicherheitsvorschriften** und die sich daraus ergebenden Pflichten zu **belehren**

Hinweis

Wie bereits im Teil 2, Punkt F (PVP 2017/99, 349 [Dezember-Heft] empfohlen, sollte es in jedem Unternehmen eine **interne Richtlinie** für die Einhaltung von **datenschutzrechtlichen Bestimmungen** geben.

2. Wann muss ein Datenschutzbeauftragter benannt werden?

Im DSG 2000 ist kein Datenschutzbeauftragter vorgesehen. Erst die **DSGVO** verlangt, dass vom Verantwortlichen oder Auftragsverarbeiter ein **Datenschutzbeauftragter** zu benennen ist, und zwar dann, wenn deren **Kerntätigkeit** darin besteht, dass

a) **Verarbeitungsvorgänge** durchgeführt werden, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine umfangreiche **regelmäßige** und **systematische Überwachung** von **betroffenen Personen** erforderlich machen, wie etwa bei Banken und Versicherungen;
b) besondere **Kategorien** von **Daten** (sensible Daten) oder von **personenbezogenen Daten** über strafrechtliche Verurteilungen und Straftaten umfangreich verarbeitet werden.

Wann genau diese Voraussetzung vorliegt, ist derzeit noch Gegenstand von Diskussionen. Die Möglichkeit, **freiwillig** einen **Datenschutzbeauftragten** zu bestellen, ist selbstverständlich gegeben.

3. Darauf hat das Unternehmen beim Datenschutzbeauftragten zu achten

a) Die **Kontaktdaten** des Datenschutzbeauftragten sind zu veröffentlichen und der **DSB** zu **melden**.
b) Der Datenschutzbeauftragte darf bei der Erfüllung seiner Aufgaben **keine Anweisungen** erhalten, wie er seine Aufgaben auszuüben hat, und
c) er darf aufgrund dessen, dass er als Datenschutzbeauftragter seine Aufgaben erfüllt, **nicht abberufen** oder **benachteiligt** werden (Art 37 DSGVO).

Hinweis

Die zuvor im Punkt 3. genannten Regeln stellen **keinen generellen Kündigungs**- und **Entlassungsschutz** dar.

Allerdings ist **Art 37 DSGVO** so formuliert, dass der Datenschutzbeauftragte die Möglichkeit hat, seine **Kündigung** (aufgrund seiner **Tätigkeit** als **Datenschutzbeauftragter**) wegen **Motivwidrigkeit** anzufechten.

4. Dürfen Dienstnehmer geortet und verfolgt werden (Tracking)?

Maßnahmen, die eine **Ortung** bzw das Tracking eines **Kfz** mittels **GPS** zulassen, sind in den meisten Fällen **Kontrollmaßnahmen**, die die **Menschenwürde** berühren. Dies bedeutet, dass entweder eine **BV** oder in Betrieben ohne BR eine **Einzelvereinbarung** abgeschlossen werden muss.

Hitz/Schrenk, Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs, PVP 2018, Seite 50

Im Einzelfall ist zu unterscheiden,

a) ob es sich etwa "nur" um die Ortung bzw das Tracking der Bewegung eines Lkw handelt, der idR **nur** für **dienstliche Zwecke** genutzt wird, oder
b) ob es den Pkw eines Außendienstmitarbeiters betrifft, der auch ein Recht auf **Privatnutzung** hat.

- **Grundsätze im Datenschutzrecht**

a) Der DG hat zu prüfen, ob er das verfolgte **Ziel** auch mit einem **gelinderen Mittel** erreichen kann.
b) **Ad-hoc-Kontrollen** aufgrund eines Verdachtsfalles oder wenn der DG die Ortungsmöglichkeit aufgrund eines Diebstahls aktiviert [#10140] diese Maßnahmen sind idR nicht zustimmungspflichtig.
c) Eine **heimliche Überwachung ohne** konkreten **Anlassfall** wird demgegenüber idR immer **rechtswidrig** sein.

- **Hinweise rund um die Fahrzeugüberwachung**

a) Im Fall des oben angeführten **Lkw** ist **denkbar**, dass **zulässigerweise** ein Zugriff bzw ein Tracking nur **außerhalb** der **Arbeitszeiten**/am **Wochenende** erfolgt, um **Missbrauch** zu **verhindern** bzw dokumentieren.
   - Zu diesem Zweck ist aus arbeitsrechtlicher Sicht **notwendig**:
   - **Entweder** eine **BV** nach § 96 ArbVG (bzw allenfalls die Zustimmung via Schlichtungsstelle gemäß § 96a ArbVG, wenn der BR die Zustimmung blockiert, aber eine "Selbstbindung" des DG auf bestimmte Fallkonstellationen vorliegt) **oder**

   in Betrieben ohne BR eine **Einzelvereinbarung**.
b) Bei **Pkw mit Privatnutzung** ist idR ein **Tracking ohne jegliche Einschränkung** bzw Begründung uE gänzlich **unzulässig**, da es sich idR um einen massiven Eingriff in die Privatsphäre des Dienstnehmers handelt.

   In bestimmten Fällen sind uE **begründete Ad-hoc-Zugriffe** bspw dann erlaubt, wenn Vorwürfe aus dem **Strafrecht** (Diebstahl), aus dem **Verwaltungsstrafrecht** (Organstrafmandate, Anonymverfügungen) oder sonstige Vorwürfe (zB **Nutzungs-Missbrauch**) vorliegen.

C) Das Datenschutzrecht im Büroalltag

1. Worauf ist im Umgang mit personenbezogenen Daten zu achten?

Im Vergleich zum derzeit gültigen § 13 DSG 2000 **regelt Art 32 DSVGO** die **Vorgaben zur Sicherheit** der Verarbeitung personenbezogener Daten konkreter.

Der Verantwortliche (vormals Auftraggeber) und der Auftragsverarbeiter (vormals Dienstleister) haben **geeignete technische** und **organisatorische Maßnahmen** zu treffen, um ein dem Risiko angemessenes Schutzniveau - gemäß dem aktuellen Stand der Technik - zu gewährleisten.

Als **Maßnahmen** werden in **Art 32 DSVGO** angeführt:

a) Die **Pseudonymisierung** und **Verschlüsselung** personenbezogener Daten und
b) **Verfahren** zur regelmäßigen **Überprüfung**, Bewertung und Evaluierung der **Wirksamkeit** der Maßnahmen.

2. Was bedeuten die datenschutzrechtlichen Vorgaben für den laufenden Bürobetrieb?

a) Wie in PVP 2017/99, 349 (Dezember-Heft) detailliert beschrieben, hat das **Unternehmen** für die **Datensicherheit** (ordnungsgemäße Aufbewahrung durch die technische Sicherung der Daten) zu **sorgen**.

Hitz/Schrenk, Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs, PVP 2018, Seite 51

b) **Hinweise** zum **digitalen Versand** (E-Mail) **personenbezogener Daten:**
- Die **generelle Verschlüsselung** beim **digitalen Versand** (E-Mail) von personenbezogenen Daten wird im laufenden Büroalltag aufgrund des Standes der Technik derzeit wohl **nicht möglich** sein.
- Es besteht zwar technisch die Möglichkeit, E-Mails und deren Anhänge zu verschlüsseln (zB Microsoft Outlook Trust Center oder sonstige Verschlüsselungssoftware), allerdings ist **nicht garantiert**, dass jeder **Empfänger verschlüsselte** Nachrichten ordnungsgemäß **öffnen** kann.

Hinweise

1) Da **Art 32 DSGVO** sehr **allgemein** formuliert ist und sich auf den **Stand der Technik** bezieht, sind die **Sicherungsmaßnahmen** stets der **technischen Entwicklung anzupassen**.
2) Es werden sich in den nächsten Jahren wohl aus der **Literatur** und **Rechtsprechung** entsprechende **Mindeststandards** für Sicherungsmaßnahmen und zur digitalen Übermittlung von personenbezogenen Daten entwickeln.
3) Wird etwa die **Lohnverrechnung** oder die **Bilanzerstellung extern** vergeben, ist darauf zu achten, dass ein **schriftlicher Auftragsverarbeitungsvertrag** mit dem externen Dienstleister (zB Bilanzbuchhalter, Steuerberater) abgeschlossen wird. In diesem **Vertrag** sind Punkte wie zB die Führung des **Verarbeitungsverzeichnisses** oder **Datensicherheitsmaßnahmen** zu regeln.
4) Ein entsprechendes **Muster** bieten wir in unserem **Info-Paket** (siehe Hinweise am Ende dieses Artikels) an.

3. Dürfen Geräte mittels Fingerabdruckscanner geschützt werden?

Die Gefahren der **Cyberkriminalität** bzw der Umstand, dass auf den **mobilen Endgeräten** immer mehr und immer **sensiblere Daten gespeichert** sind, erfordern ein **erhöhtes Ausmaß** an **Datensicherheit**. Eine **mögliche Strategie**, einen gestohlenen oder verlorenen Laptop vor raschem unerlaubtem Zugriff zu schützen, ist die Sperre des Geräts, die nur mittels **Fingerprint-Sensor** aufgehoben werden kann.

Durch die notwendige **Verarbeitung** von **biometrischen DN-Daten** (Fingerabdruck) werden jedoch sensible Daten iSd Datenschutzrechtes verarbeitet. Rechtlich **zulässig** ist dies nur dann, wenn

a) entweder der betroffene **Dienstnehmer ausdrücklich** diesem Verfahren **zustimmt** oder
b) ein entsprechender datenschutzrechtlicher **Rechtfertigungsgrund** vorliegt.

Zu a): Die **Zustimmung** ist im **Einzelfall** und vom DN **freiwillig** zu erteilen.

Zu b): Ein **Rechtfertigungsgrund** (der die Zustimmung ersetzen würde) liegt idR nur **selten** vor.

Hinweis

Ent-/Sperrung mittels **Biometrie** ist nur eine **mögliche Schutzmaßnahme** von vielen, um sensible oder für das Unternehmen sehr wichtige Daten zu schützen. **Ohne individuelle Zustimmung** ist idR eine solche Maßnahme (abseits von Einzelfällen) **datenschutzrechtlich unzulässig.**

Hitz/Schrenk, Datenschutzserie Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs, PVP 2018, Seite 52

D) Aufgaben und Befugnisse der Datenschutzbehörde

Die Aufgaben und Befugnisse der DSB sind im nationalen DSG geregelt. Sie kann bei einem **begründeten Verdacht**, dass datenschutzrechtliche Rechte und Pflichten verletzt werden,

- die Datenverarbeitungen überprüfen;
- vom Verantwortlichen oder Auftragsverarbeiter alle notwendigen Aufklärungen verlangen;
- Einschau in Datenverarbeitungen und diesbezügliche Unterlagen fordern.

Es ist grundsätzlich jedenfalls mit Kontrollen und Überprüfungen zu rechnen. Wie diese konkret ablaufen werden, ist noch nicht bekannt, dies hängt auch von der künftigen finanziellen sowie personellen Ausstattung der DSB ab.

In einem **aktuellen Leitfaden** zur DSGVO hat die **DSB** ihre **Befugnisse** kurz zusammengefasst:

- **Untersuchungsbefugnisse** (einschließlich des Betretungsrechts bestimmter Räumlichkeiten)
- **Abhilfebefugnisse** (das sind Befugnisse, die es der Aufsichtsbehörde ermöglichen, ein rechtswidriges Verhalten abzustellen, bspw durch konkrete Anordnungen oder indem **Geldstrafen** verhängt werden iHv bis zu 20 Mio EUR oder 4 % des gesamten weltweit erzielten Jahresumsatzes des vorangegangenen Geschäftsjahres)
- **Genehmigungs**- und **Beratungsbefugnisse**

Hinweis

Die DSB stellt auf ihrer Homepage klar, dass sie **keine inhaltliche Beratungsleistung** vornimmt. Eine etwaige Rechtsberatung muss bei einem Rechtanwalt oder einem sonstigen qualifizierten Dienstleister in Anspruch genommen werden.

E) Das Dienstverhältnis wurde beendet: Wie ist mit personenbezogenen Daten ehemaliger Dienstnehmer umzugehen?

1. Wovon hängt die Dauer der erlaubten Datenspeicherung ab?

Einer der **wesentlichen Grundsätze** des **Datenschutzrechtes** ist es, dass Daten **zeitlich** nur **begrenzt gespeichert** bzw

verarbeitet werden dürfen (dies schon bis dato auf Basis des DSG 2000 und noch mehr aufgrund der DSGVO [#10140] siehe hierzu im Detail die Ausführungen in Teil 4 der Serie).

Daten dürfen **so lange gespeichert** werden, als ein **Rechtfertigungsgrund** für die Verarbeitung der Daten vorliegt [#10140] Rechtfertigungsgründe können im Arbeits-, Sozialversicherung- bzw Steuerrecht **gesetzliche** Vorschriften, **KV-Regelungen** sowie **einzelvertragliche Verpflichtungen** sein.

Als Faustregel gilt, dass die **Dauer** davon abhängt, ob

a) es eine **gesetzliche Aufbewahrungspflicht** gibt oder
b) ein **gerechtfertigtes Aufbewahrungsinteresse** besteht, um mögliche DN-Forderungen abwehren zu können.

Beispiele für gerechtfertigtes Aufbewahrungsinteresse

In folgenden - in der Praxis häufiger vorkommenden - Fällen besteht ein **Aufbewahrungsinteresse**:

- mögliche Ansprüche des **abgelehnten Bewerbers** nach §§ 15 und 29 GIBG (**6 Monate**) abwehren zu können,
- Daten betreffend **Lohnsteuer**- und **Abgabenpflicht** nach § 132 BAO (**7 Jahre**),

- Daten betreffend **SV-Beiträge** nach § 68 ASVG (3 bzw 5 Jahre),
- Ansprüche auf Entgelt nach der **allgemeinen Verjährungsfrist** des § 1486 ABGB (**3 Jahre**)
- Anspruch auf **Ausstellung** eines **Dienstzeugnisses** nach § 1478 ABGB (**30 Jahre**)

2. In welcher konkreten Form sind die Daten zu löschen?

Hinsichtlich der "Löschung" jener Daten, die nicht mehr aufbewahrt bzw gespeichert werden dürfen, gibt es noch viele **ungelöste Praxisfragen**.

Insbesondere bei digital oder virtuell gespeicherten Daten war in der Vergangenheit ein "Löschen" bloß ein **Sperren** der **Zugriffsrechte**, wobei die Daten an sich noch in irgendeiner Form gespeichert blieben. Das wird künftig nicht ausreichen. Es ist sicherzustellen, dass die **Daten** auch **wirklich vernichtet** sind.

Abseits von diesen technischen Fragen sind in der **Praxis Vorgänge** zu beachten, die **selbstverständlich** erscheinen, aber bei der Vernichtung von Daten **oftmals übersehen** werden.[1)]

- Papierausdrucke mit Daten sollten immer nur **geschreddert** bzw bei größeren Mengen über **Spezialfirmen entsorgt** werden;
- Datenträger wie **Festplatten** dürfen **nicht bloß formatiert**, sondern müssen **professionell gelöscht** werden, bevor diese entsorgt werden;
- optische Datenträger wie CDs oder DVDs müssen **physisch zerstört** oder von Spezialfirmen entsorgt werden;
- **USB-Sticks** bergen oftmals eine Vielzahl an Daten und Informationen, die nicht oder **nicht ausreichend gelöscht** werden (USB-Sticks **niemals anderen Personen borgen**!);
- Ausdrucke bzw **Kopien aus** dem **Gerät** entfernen und bei **Fehldrucken/-kopien** sicherstellen, dass diese vernichtet (zB geschreddert) werden.

1) **Liste** abgeleitet *aus " IT-Sicherheitshandbuch für Mitarbeiterinnen und Mitarbeiter"* der BSIC/WKÖ, http://it-safe.at

F) Schlussfolgerung

Aufgrund bestehender Bestimmungen, vor allem jedoch mit Blick auf die bevorstehenden Neuerungen im Datenschutzrecht durch die DSGVO (und das Datenschutz-Anpassungsgesetz 2018) ist eine **zeitgerechte, unternehmensinterne Evaluierung** das Gebot der Stunde.

Die ersten Schritte sollten in naher Zukunft gemacht werden, zumal aus heutiger Sicht völlig **ungewiss** ist, wie sich die **Intensität** der **Kontrollen**, die Zahl der **Anzeigen** und die daraus resultierenden **Strafen** darstellen werden.

Praxistipps

Wir bieten ein **umfangreiches Info-Service** rund um das neue Datenschutzrecht (© Wirtschaftskammer) an:

- **EU-Datenschutz-Grundverordnung** (DSGVO): **Kurzüberblick und Zeitplan** (https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung.html)
- **EU-Datenschutz-Grundverordnung** (DSGVO): **Checkliste** (https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Checkliste.html)

- **Webinar**, die **Folien** zu diesem Webinar und **Fragen** und **Antworten** aus dem Chat zu diesem Webinar zur EU-Datenschutz-Grundverordnung finden Sie hier: https://www.wko.at/service/unternehmensfuehrung-finanzierung-foerderungen/webinar-datenschutz-jetzt-neu-angehen.ht
- **Onlineratgeber** (http://dsgvo.wkoratgeber.at/), der Sie anhand verschiedener Fragen durch das Thema führt und nach einigen Klicks eine individuelle Auswertung empfohlener Maßnahmen liefert. Damit wissen Sie schnell, orts- und zeitunabhängig, was noch alles zu tun ist.
- **Vereinbarung** mit einem externen Dienstleister über eine **Auftragsverarbeitung** nach Art 28 DSGVO (https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-mustervertrag.html)

Hinweis

Eine **Liste** von **Fachbüchern**, die zum neuen Datenschutzrecht erschienen sind, können Sie als kostenfreies **PVP-Leserservice** anfordern.

Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2018/22

PVP 2018, 83
Heft 3 v. 26.03.2018
Themen-Special

Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung

Mag. Wolfram Hitz

Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Obwohl er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565). Die **ersten Schritte** für eine **innerbetriebliche Umsetzung** sollten unbedingt **zeitnah** gesetzt werden.

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf.

Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht:** In PVP 2017/90, 317 (November-Heft) informieren wir Sie über die **Datenschutzrechtsgrundlagen, arbeitsrechtlich** relevanten **Daten** und **Definitionen** und über konkrete **Datenschutzfragen** im **arbeitsrechtlichen Alltag**.
- **Teil 2: Datenschutz im Alltag des Personalverrechners:** In PVP 2017/99, 349 (Dezember-Heft) informieren wir Sie ua über die **Verwendung**, **Verarbeitung** und **Aufbewahrung sensibler Daten** und über die (**datenschutzrechtlichen**) **Pflichten** des Dienstleisters und seiner **Dienstnehmer**.
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs:** In PVP 2018/8, 28 (Jänner-Heft) und PVP 2018/14, 49 (Februar-Heft) informieren wir Sie ua darüber, welche **datenschutzrechtlichen Bestimmungen** während des **Bewerbungsprozesses**, des **laufenden Dienstverhältnisses** und nach dessen **Beendigung** zu beachten sind.

  Wir haben möglichst naheliegende und in der **Beratungspraxis** häufig auftauchende **Fragen** aufgegriffen und **beantworten** diese **praxisnah**.
- **Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung:** Wir informieren in diesem Heft über die wichtigsten Grundbegriffe des neuen Datenschutzrechtes. Im nächsten Heft besprechen wir die uE **unabdingbar notwendigen Maßnahmen**, die aufgrund der DSGVO zu treffen

sind.

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung, PVP 2018, Seite 83

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** ... Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//**BR** ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ... Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**GlbG** ... Gleichbehandlungsgesetz//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**iZm** ... in Zusammenhang mit//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung//**WKO** ... Wirtschaftskammer Österreich

A) Vorbemerkungen

Wie im ersten Artikel unserer Serie erläutert, sind die **neuen Bestimmungen** im Datenschutzrecht (DSGVO und DSG in der Fassung des Datenschutzanpassungsgesetzes 2018) **ab 25. 5. 2018 anzuwenden.** Mit den gesetzlichen Bestimmungen und deren Auswirkung auf den Alltag des Personalverrechners und des Unternehmens haben wir uns bereits auseinandergesetzt.

Da das Datenschutzthema derart komplex und vielschichtig ist, ist es unumgänglich, jeden Einzelfall in jedem Unternehmen separat zu betrachten. **Auch wenn** die Umsetzung der notwendigen Maßnahmen durch **externe Dienstleister** erfolgen sollte, muss ein **Grundverständnis** für das Thema vorhanden sein. Dafür ist es notwendig, sich mit den **wichtigsten Begriffen** auseinanderzusetzen. Wir haben diese für Sie im vorliegenden Heft **zusammengefasst**.

Weiters informieren wir Sie im nächsten Heft über die uE **unabdingbar notwendigen Maßnahmen**, die aufgrund der DSGVO zu treffen sind.

Um sich einer gängigen Metapher zu bedienen: **Es ist 5 Minuten vor 12!**

B) Diese Datenschutzbegriffe sollten Sie unbedingt kennen

1. Verantwortlicher (vormals Auftraggeber; Art 4 Z 7 DSGVO)

"*Verantwortlicher*" ist die natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die allein oder gemeinsam mit anderen über die **Zwecke** und **Mittel** der **Verarbeitung** von personenbezogenen Daten **entscheidet**.

2. Auftragsverarbeiter (vormals Dienstleister; Art 4 Z 8 DSGVO)

"*Auftragsverarbeiter*" ist eine natürliche oder juristische Person, Behörde, Einrichtung oder andere Stelle, die **personenbezogene Daten** im Auftrag des Verantwortlichen **verarbeitet**.

3. Betroffener

Es gibt **keine eigene Definition** des Betroffenen in der DSGVO. Darunter wird eine von der **Datenanwendung betroffene Person** verstanden, die diverse Rechte hat (siehe auch die Ausführungen im Punkt C [Grundsätze für die Verarbeitung personenbezogener Daten]).

Welche Rolle hat der Steuerberater oder Bilanzbuchhalter?

a) Hinsichtlich der Verwaltung der **<u>eigenen</u> Klienten-** oder der **Mitarbeiterdaten** ist der

Steuerberater/Bilanzbuchhalter ein ***"Verantwortlicher"*** .

b) Als **externer Dienstleister** (etwa für Buchhaltung, Personalverrechnung oder Bilanzerstellung) ist der Steuerberater/Bilanzbuchhalter ein ***"Auftragsverarbeiter"*** .

c) Auch bei jenen Daten, die vom Auftragsverarbeiter aufgrund des Auftrages verarbeitet werden, muss der **Verantwortliche** weiterhin die **Informationspflichten** erfüllen oder die **Betroffenenrechte wahren**. Der Auftragsverarbeiter übernimmt diese Verpflichtungen gegenüber dem Betroffenen nicht.

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung, PVP 2018, Seite 84

4. Dateisystem (Art 4 Z 6 DSGVO)

Unter Dateisystem versteht man jede **strukturierte Sammlung personenbezogener Daten**, die nach bestimmten Kriterien zugänglich sind, unabhängig davon, ob diese Sammlung zentral, dezentral oder nach funktionalen oder geografischen Gesichtspunkten geordnet geführt wird.

Hinweise

a) Beispiele für Dateisysteme im Sinne der DSGVO sind die **Buchhaltung**, **Personalverrechnung**, **Spesenabrechnung**, **Adresslisten** udgl.

b) Eine **Ablage**, in die **unstrukturiert Notizzettel** von diversen Telefonaten mit Klienten gelegt werden, ist **kein Dateisystem**.

c) Es sind dabei **nicht nur elektronisch** geführte Dateisysteme erfasst, da die DSGVO in diesem Punkt technologieneutral ist. Unter die Definition fallen somit **sowohl automatisiert als auch manuell geführte Dateisysteme**.

C) Grundsätze für die Verarbeitung personenbezogener Daten (Artikel 5 DSGVO)

1. Generell einzuhaltende Verarbeitungsgrundsätze

Die **Verarbeitung** personenbezogener Daten muss auf

- **rechtmäßige** Weise,
- nach **Treu und Glauben** ([#10140] bezeichnet das Verhalten eines redlich und anständig handelnden Menschen) und
- in einer für die betroffene Person **nachvollziehbaren** Weise

erfolgen.

Alle **Informationen** und **Mitteilungen** zur Verarbeitung dieser personenbezogenen Daten müssen weiters

- **leicht zugänglich**,
- **verständlich** und
- in klarer und einfacher Sprache abgefasst sein (**Transparenz**).

Hinweis

Dieser **Transparenz-Grundsatz** betrifft jedwede mit der **Verarbeitung** zusammenhängenden **maßgeblichen Informationen**, wie insbesondere:

- **WER** ist der **Verantwortliche**?
- **WELCHEM Zwecke** dient die Verarbeitung?

2. Speziell einzuhaltende Verarbeitungsgrundsätze

Verarbeitungsgrundsätze	**Personenbezogene Daten müssen ...**
Zweckbindung 1)	... für festgelegte, eindeutige und **legitime Zwecke erhoben** werden und dürfen nicht in einer mit diesen Zwecken nicht zu vereinbarenden Weise weiterverarbeitet werden.
Datenminimierung 1)	... dem Zweck **angemessen** und **erforderlich** sowie auf das für die Zwecke der Verarbeitung **notwendige Maß beschränkt** sein. Dazu zählt auch, dass Verantwortliche durch technische Voreinstellungen sicherstellen müssen, dass grundsätzlich **nur personenbezogene Daten**, deren Verarbeitung für den jeweiligen bestimmten **Verarbeitungszweck erforderlich** ist, **verarbeitet** werden.
Richtigkeit 2)	... **sachlich richtig** und erforderlichenfalls auf dem **neuesten Stand** sein. Es sind alle angemessenen **Maßnahmen** zu treffen, damit **unrichtige** personenbezogene Daten **gelöscht** oder **berichtigt** werden.

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung, PVP 2018, Seite 85

Verarbeitungsgrundsätze	**Personenbezogene Daten müssen ...**
Speicherbegrenzung 3)	... in einer **Form gespeichert** werden, die die **Identifizierung** der betroffenen Personen nur so lange ermöglicht, wie es für die Zwecke, für die sie verarbeitet werden, **erforderlich** ist. Daher ist es unerlässlich, **regelmäßig** zu **evaluieren**, welche **Daten** sicher **gelöscht** werden müssen! Dies betrifft insbesondere (sensible) Daten der Personalverrechnung, aber auch alle anderen digitalen und physischen Daten und Unterlagen, die am Server und im Archiv existieren.

Ergänzende Anmerkungen zu den Verarbeitungsgrundsätzen:

1) Aufgrund dieser beiden Grundsätze ist es uE **notwendig**, **betriebsintern** und mit dem **Klienten festzulegen**, welche Daten bspw für eine **Anmeldung** rein rechtlich benötigt werden. Alle über die Erfüllung **gesetzlicher Verpflichtungen hinausgehenden Unterlagen** sollte man **ablehnen** oder **löschen**.
2) In der **Praxis** erlebt man häufig, dass Mitarbeiter von Klienten oder sonstige **Dritte Kontakt** mit der

steuerlichen Vertretung aufnehmen, um **Informationen** weiterzugeben oder zu erfragen [#10140] Unsere **Empfehlung** : Legen Sie in der Kommunikation mit Klienten künftig konkrete **Ansprechpartner** fest, die das **Datenmaterial** liefern. Damit kann der Steuerberater oder Bilanzbuchhalter von einer **Richtigkeit** und **Verifizierbarkeit** der Unterlagen ausgehen. Dies muss **auch** im **Interesse** des **Auftraggebers** in seiner Rolle als Verantwortlicher iSd DSGVO sein, um die gesetzlichen Verpflichtungen einhalten zu können.

3) Da in der DSGVO sowohl die Begriffe **"Löschen"** als auch **"Vernichten"** verwendet werden (Art 4 Z 2), wird auch in der Literatur zwischen diesen beiden Vorgängen **unterschieden**. Vorbehaltlich der Klärung durch Gerichte wird in der Literatur ua nachfolgende Meinung vertreten (nach *Schweiger* in Dako 2018/10):

   Das **"Löschen"** von Daten bedeutet, dass diese in einem **Backup** weiterhin vorhanden sein können. Dabei ist aber **sicherzustellen**, dass
   - nur ein **eingeschränkter Personenkreis** die Datensicherung durchführt,
   - jene **Personen**, die die **Daten** üblicherweise **verarbeiten**, **nicht mehr darauf zugreifen** können,
   - jedenfalls eine **räumlich getrennte Lagerung** erfolgt,
   - ein **Re-Store-Ablauf festgelegt** ist (keine direkte Wiederherstellung ohne Zwischenschritte) und
   - die **Sicherungskopien** regelmäßig überschrieben werden und somit ein **"Ablaufdatum"** haben.

Praxistipp

Die in der **Praxis** immer wieder feststellbare Vorgehensweise, **möglichst viele Daten möglichst lange aufzubewahren**, um bei einer GPLA-Prüfung für alle Eventualitäten gerüstet zu sein, war schon bis dato datenschutzrechtlich fraglich. Aufgrund der Bestimmungen der **DSGVO** kann diese **Praxis** jedenfalls **nicht mehr fortgeführt** werden!

Der **Betroffene** hat das **Recht**, dass jene **Daten gelöscht** werden, die **nicht** (mehr) **rechtmäßig verarbeitet** werden.

Hinweis zur Rechtmäßigkeit der Datenverarbeitung (Art 6 DSGVO)

Damit **personenbezogene Daten rechtmäßig** verarbeitet werden, ist notwendig, dass

a) entweder eine **rechtliche Grundlage** oder
b) eine **Einwilligungserklärung** des Betroffenen

vorliegt. Für **weitere Infos** hierzu siehe **PVP 2017/79, 277** (Oktober-Heft).

Hinweise

1. Im **nächsten Heft** setzen wir den Beitrag fort mit Infos zu uE **unabdingbar notwendigen** Maßnahmen, die aufgrund der DSGVO zu **treffen** sind. Dieser Beitrag beendet unsere Datenschutzserie.
2. Anschließend **beantworten** die beiden Autoren **ausgewählte Anfragen**, die PVP-Leserinnen und PVP-Leser an die Redaktion stellten und noch stellen können.
3. Eine **Liste** von **Fachbüchern**, die zum neuen Datenschutzrecht erschienen sind, können Sie als kostenfreies **PVP-Leserservice** anfordern.

4. Wir bieten ein **umfangreiches Info-Service** rund um das neue Datenschutzrecht (© Wirtschaftskammer) an, nähere Informationen dazu siehe **PVP 2018/14 (Februar-Heft)**.

Dokument 1 von 1

Personalverrechnung für die Praxis

PVP 2018/30

PVP 2018, 110
Heft 4 v. 26.04.2018
Themen-Special

Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung (Fortsetzung und Schluss der Serie)

Mag. Wolfram Hitz/Florian Schrenk

Der **Datenschutz** ist ein sehr **komplexes** Thema. Obwohl er in den vergangenen Jahren immer bedeutsamer geworden ist, wird er bis dato **kaum** in **Aus- und Weiterbildungen** im Bereich Personalverrechnung und Arbeitsrecht behandelt, obwohl es diesbezügliche Bestimmungen in Österreich seit den 70er-Jahren gibt (BGBl 1978/565). Die **ersten Schritte** für eine **innerbetriebliche Umsetzung** sollten unbedingt **zeitnah** gesetzt werden.

In einer **mehrteiligen, praxisorientierten Serie** bereiten wir übersichtlich und verständlich das für Personalverrechner und Personalisten **Wissenswerte** rund um den **Datenschutz** auf.

Die Serie gliedert sich wie folgt:

- **Teil 1: Datenschutz im Arbeitsrecht**: In PVP 2017/90, 317 (November-Heft) informieren wir Sie über die **Datenschutzrechtsgrundlagen, arbeitsrechtlich** relevanten **Daten** und **Definitionen** und über konkrete **Datenschutzfragen** im **arbeitsrechtlichen Alltag.**
- **Teil 2: Datenschutz im Alltag des Personalverrechners:** In PVP 2017/99, 349 (Dezember-Heft) informieren wir Sie ua über die **Verwendung**, **Verarbeitung** und **Aufbewahrung sensibler Daten** und über die (**datenschutzrechtlichen) Pflichten** des Dienstleisters und seiner **Dienstnehmer.**
- **Teil 3: Datenschutz im Alltag des Firmeninhabers/Personalchefs:** In PVP 2018/8, 28 (Jänner-Heft) und PVP 2018/14, 49 (Februar-Heft) informieren wir Sie ua darüber, welche **datenschutzrechtlichen Bestimmungen** während des **Bewerbungsprozesses**, des **laufenden Dienstverhältnisses** und nach dessen **Beendigung** zu beachten sind.

  Wir haben möglichst naheliegende und in der **Beratungspraxis** häufig auftauchende **Fragen** aufgegriffen und **beantworten** diese **praxisnah**..
- **Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung:** Wir informieren in PVP 2018/22, 83 (März-Heft) über die wichtigsten **Grundbegriffe** des neuen Datenschutzrechtes.

  In diesem Heft besprechen wir die uE **unabdingbar notwendigen Maßnahmen**, die aufgrund der DSGVO zu treffen sind, und **schließen** die **Kurzserie** mit einer **Checkliste** für **externe Dienstleister ab**.

Verwendete Abkürzungen in diesem Beitrag:

ArbVG ... Arbeitsverfassungsgesetz//**AVRAG** Arbeitsvertragsrechts-Anpassungsgesetz//**AZG** ... Arbeitszeitgesetz//**BR** ... Betriebsrat//**BV** ... Betriebsvereinbarung//**DG** ... Dienstgeber//**DN** ... Dienstnehmer//**ds** ... das sind//**DSB** ... Datenschutzbehörde//**DSBea** ... Datenschutzbeauftragter//**DSK** ... Datenschutzkommission//**DSG** ... Datenschutzgesetz//**DSGVO** ... Datenschutz-Grundverordnung//**DV** ... Dienstvertrag bzw Dienstverhältnis//**GKK** ... Gebietskrankenkasse//**GlbG** ... Gleichbehandlungsgesetz//**idR** ... in der Regel//**iHv** ... in Höhe von//**iSd** ... im Sinne des//**iZm** ... in Zusammenhang mit//**KV** ... Kollektivvertrag//**SV** ... Sozialversicherung//**WKO** ... Wirtschaftskammer Österreich

D) Diese Maßnahmen sollten hinsichtlich der neuen Datenschutz-Grundverordnung unbedingt getroffen werden

1. Technische Maßnahmen

In dieser Artikelserie haben wir uns bereits mit den technischen Maßnahmen auseinandergesetzt. **Zusammenfassend** ist nochmals festzuhalten, dass auch - oder vielleicht sogar insbesondere - der **Auftragsverarbeiter** (vormals Dienstleister) **geeignete** technische und organisatorische **Maßnahmen** zu treffen hat, um ein dem **Risiko angemessenes Schutzniveau** zu gewährleisten.

2. Datenschutzbeauftragter (Art 37 ff DSGVO; §§ 5, 57 DSG)

Der Verantwortliche und der Auftragsverarbeiter haben einen **Datenschutzbeauftragten** (DSBea) **dann** zu benennen, wenn

- die **Kerntätigkeit** des Verantwortlichen oder des Auftragsverarbeiters darin besteht, **Verarbeitungsvorgänge** durchzuführen, die aufgrund ihrer Art, ihres Umfangs und/oder ihrer Zwecke eine **umfangreiche regelmäßige** und **systematische Überwachung** von **betroffenen Personen** erforderlich machen, oder
- die **Kerntätigkeit** des Unternehmens in der **umfangreichen Verarbeitung sensibler Daten** (zB Krankenanstalten) oder von Daten über strafrechtliche Verurteilungen oder **Straftaten** besteht.

Müssen Steuerberater oder Bilanzbuchhalter einen Datenschutzbeauftragten bestellen?

Die **WKO** schreibt hierzu in einem eigens für **Personalverrechner** erarbeiteten Informationsschreiben (Hervorhebungen durch den Autor):

" ***Personalverrechner*** *arbeiten zwar oftmals auch mit* ***sensiblen Daten*** *(Gesundheitsdaten, Daten über religiöse Zugehörigkeit der Mitarbeiter eines Unternehmens), es ist jedoch sehr* ***fraglich*** *, ob sie das in einem* ***umfangreichen*** *Ausmaß (= große Anzahl der betroffenen Personen, umfassendes Datenvolumen,...) tun bzw ob diese konkrete Datenverarbeitung die* ***Kerntätigkeit*** *(= wichtigsten Arbeitsabläufe, Haupttätigkeit) dieses Unternehmens darstellt.*

Es ist zum ***jetzigen*** ***Stand*** *davon auszugehen, dass Personalverrechner standardmäßig* ***keinen*** ***Datenschutzbeauftragten*** *benötigen werden. Im Einzelfall könnte aber dennoch die Bestellung eines solchen notwendig werden (zB Spezialisierung im Unternehmen,...)."*

(Link:
https://www.wko.at/branchen/information-consulting/unternehmensberatung-buchhaltung-informationstechnologie/buchhaltung/leitfaden

oder google Suche: *dsgvo personalverrechner wko*)

Soweit absehbar, ist **im Regelfall kein DSBea** zu bestellen.

Hinweise

a) Ein **freiwillig bestellter** DSBea hat dieselben **Rechte** und **Pflichten** wie ein **zwingend** zu bestellender DSBea.
b) Aus arbeitsrechtlicher Sicht gilt, dass ein **DSBea** zwar **keinen generellen Kündigungs-** und **Entlassungsschutz** wie etwa ein Betriebsrat genießt, der nur mit Zustimmung des Gerichtes gekündigt oder entlassen werden darf.
c) Allerdings wäre eine Kündigung aufgrund der Tätigkeit als DSBea als **motivwidrige Kündigung anfechtbar**.

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung (Fortsetzung und Schluss der Serie), PVP 2018, Seite 111

3. Verzeichnis von Verarbeitungstätigkeiten (Verarbeitungs-verzeichni; Art 30 DSGVO, § 49 DSG)

Grundsätzlich müssen ein Verzeichnis führen ...

a) ... alle **Verantwortlichen** hinsichtlich der **Verarbeitungstätigkeiten**;
b) ... alle **Auftragsverarbeiter** hinsichtlich ihrer **Dienstleistungen**.

Diese Verzeichnisse sind **schriftlich** bzw in **elektronischer** Form zu führen.

Das Verarbeitungsverzeichnis ist ein **Kernelement** der DSGVO.

Ein Verzeichnis hat der **externe Dienstleister** zu führen ...

a) ... sowohl für Verarbeitungen, die den **eigenen Betrieb** betreffen, als auch
b) ... für jene, die für die **Klienten** durchgeführt werden.

Die Verarbeitungsverzeichnisse müssen **gegebenenfalls vorgelegt** werden.

Praxistipp

Vorlagen für ein Verarbeitungsverzeichnis finden Sie in der einschlägigen Literatur (siehe Hinweise am Ende dieses Artikels) und bspw unter folgendem **Link**:
https://www.wko.at/service/wirtschaftsrecht-gewerberecht/EU-Datenschutz-Grundverordnung:-Dokumentationspflicht.html

Hinweis

Die bis dato (rechtlich unrichtig) oftmals als "Freibrief" von datenschutzrechtlichen Verpflichtungen gehandhabte Standard- und Muster-Verordnung 2004 - **StMV 2004**, auf Basis derer etwa die **Personalverwaltung** für privatrechtliche Dienstverhältnisse (SA002) **nicht DVR-meldepflichtig** war, ist iZm der **DSGVO nicht mehr** anzuwenden.

Es sind daher künftig **auch** zB für die **Lohnverrechnung Verarbeitungsverzeichnisse** zu erstellen.

E) Informationspflicht (Art 13f DSGVO)

Der betroffenen Person sind durch den Verantwortlichen gewisse Informationen über die Verarbeitung von personenbezogenen Daten zur Verfügung zu stellen. Die Informationspflichten sind **sehr weitgehend** und reichen von

- den **Kontaktdaten** des **Verantwortlichen** über
- den **Verarbeitungszweck** und
- Angaben, ob die Daten **beim Betroffenen selbst** oder einem **Dritten erhoben** wurden, über
- die **Rechtsgrundlage** der Verarbeitung bis hin
- zur **Aufklärung** über **Betroffenenrechte** sowie
- zum allfälligen **Hinweis** auf die **Widerrufbarkeit** einer **Einwilligungserklärung**.

Auch ist zu **unterscheiden**, ob die Daten **vor** oder **nach** Inkrafttreten der **DSGVO** erhoben wurden. Handelt es sich um **"Altdaten"**, kann argumentiert werden, dass die in der DSGVO geregelten **Informationspflichten** für diese **noch nicht** anzuwenden sind.

Praxistipp

Die Informationen müssen **nicht jedem Betroffenen separat** zur Verfügung gestellt werden, sondern sie können etwa auch auf der **Website** oder (wenn DN betroffen sind) im **Intranet** bereitgestellt werden.

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung (Fortsetzung und Schluss der Serie), PVP 2018, Seite 112

F) Auskunftsrecht (Art 15 DSGVO)

Die betroffene Person hat ein Auskunftsrecht **gegenüber** dem **Verantwortlichen** über die verarbeiteten personenbezogenen Daten. Die Auskunft hat **schriftlich** zu erfolgen und kann nur dann abgelehnt werden, wenn

a) es sich um **offenkundig unbegründete** (zB tägliches Auskunftsbegehren) oder
b) **exzessive** Anträge handelt.

Die Auskunft darf weiters **nicht** in die **Rechte Dritter eingreifen** und kann aus diesem Grund (soweit berechtigt) **verweigert** oder **eingeschränkt** werden.

G) Datengeheimnis [#10140] Dienstnehmer müssen vom Dienstgeber belehrt werden

Eine Verpflichtung, die es bereits im DSG 2000 gab, wurde in § 6 DSG übernommen: Der **DG** ist **verpflichtet**, die **DN**

a) über das **Datengeheimnis** zu **belehren** und
b) sich schriftlich vom DN **bestätigen** zu lassen, dass dieser das **Datengeheimnis einhält**.

Inhaltlich geht es dabei darum, dass personenbezogene Daten nur dann übermittelt werden dürfen, wenn

a) eine **ausdrückliche Anordnung** vorliegt oder
b) **gesetzliche/vertragliche Verpflichtungen** erfüllt werden müssen.

Praxistipp

Ein (für die individuellen Bedürfnisse adaptierbares) **Muster** findet sich bspw unter

https://www.wko.at/service/wirtschaftsrecht-gewerberecht/eu-dsgvo-muster-verpflichtungserklaerung-datengeheimnis.html

H) Checkliste für Steuerberater und Bilanzbuchhalter

1) Analyse des Ist-Zustandes	• Welche **Rolle** habe ich als Steuerberater oder Bilanzbuchhalter? • Welche **(sensiblen) Daten** werden verarbeitet? • **Wie** werden die Daten **verarbeitet**? • **Wie** erfolgt die **Aufbewahrung** von Daten (elektronisch und Papierform)? • Wie erfolgt die **Löschung** und **Vernichtung** von Daten?
2) In welchen Bereichen besteht iZm der DSGVO Handlungsbedarf?	• Müssen **interne Abläufe optimiert** werden (insb durch Schulung der Mitarbeiter)? • Gibt es Handlungsbedarf bei den **technischen Voraussetzungen** (insb Sicherheit, Passwörter)? • Wird ein **Datenschutzbeauftragter** benötigt? • Muss ein **Verarbeitungsverzeichnis** angelegt werden?
3) Festlegung und Umsetzung von Maßnahmen	• Erstellung einer **Liste** von **Maßnahmen** (gereiht nach Priorität) • Erstellung eines **Zeitplanes** • Gegebenenfalls **Konsultation** eines **Experten** (Anwalt, WKO, sonstige Experten)

Hitz/Schrenk, Datenschutzserie Teil 4: Details zur und Auswirkungen der neuen Datenschutz-Grundverordnung (Fortsetzung und Schluss der Serie), PVP 2018, Seite 113

Hinweis

Falls **personenbezogene Daten** an Steuerberater oder Bilanzbuchhalter (Auftragsverarbeiter) **weitergegeben** werden, so ist ein **Vertrag** abzuschließen.

I) Abschließende Anmerkungen

- Unter dem Schlagwort **"Datenschutz"** verstand man bislang etwas Abstraktes, etwas mit dem sich "ja ohnehin nur große Unternehmen beschäftigen müssen". Spätestens jedoch, als das Thema medial aufgegriffen und in Fachzeitschriften umfassend behandelt wurde, war klar: Es ist im Wesentlichen **jedes Unternehmen betroffen**, unabhängig von Größe und Geschäftszweig.
- Aus dem äußerst umfassenden und komplexen Thema haben wir die personalrechtlichen Aspekte beleuchtet und sind zu dem Schluss gekommen, dass für **fast jedes Unternehmen Handlungsbedarf** besteht.
- In erster Linie geht es darum, ein **Grundverständnis** für das Thema zu **entwickeln** und grundlegende Prozesse des eigenen Unternehmens zu beleuchten. Zum einen werden die **technischen Voraussetzungen** auf dem **Prüfstand** stehen, aber auch **unternehmensinterne Abläufe**, die anhand individueller Richtlinien **optimiert** werden müssen.
- Bei Steuerberatern oder Bilanzbuchhaltern wird es wohl unerlässlich sein, **Mitarbeiter** - vor allem Personalverrechner - zu **sensibilisieren** und aufgrund der Verarbeitung von personenbezogenen Daten der Klienten zu **überlegen, freiwillig** einen **Datenschutzbeauftragten** zu bestellen.

- Es wird sich weisen, wie sich die DSGVO auswirken wird und wie die Unternehmer darauf vorbereitet sein werden, eines ist jedoch klar: **Datenschutz ist das Gebot der Stunde**.

Praxistipps

1. Die beiden Autoren **beantworten ausgewählte Anfragen** aus der Praxis für die Praxis, die an die Redaktion gemailt werden (pvp@lexisnexis.at). Die Antworten werden in einem der folgenden PVP-Hefte veröffentlicht.
2. Die Autoren haben gemeinsam mit der PVP-Redaktion **umfangreiche Buch-, Literatur- und Linktipps** zusammengestellt, die Sie als kostenfreies **PVP-Leserservice** anfordern können.