Mitarbeiterdaten nach EU-Datenschutz-Grundverordnung - FAQ

Antworten auf die wichtigsten Fragen

Achtung: Hier kommen nicht nur datenschutzrechtliche, sondern auch arbeits- und sozialrechtliche Bestimmungen zur Anwendung!

1. Was ist bei der Personalverwaltung intern zu beachten?
2. Muss ein Personalverrechner das Einverständnis zur Datenspeicherung vom jeweiligen Mitarbeiter des Auftraggebers einholen?
3. Gibt es Ausnahmen beim Schutz von Mitarbeiterdaten?
4. Wenn ich von meinen Mitarbeitern das Religionsbekenntnis und die Gewerkschaftszugehörigkeit für die Lohnverrechnung abspeichere und verarbeite. Habe ich dann bereits sensible Daten? Was sind die Folgen?
5. Bewerberunterlagen werden von Personalunternehmen geschickt - ist die Verschlüsselung hier nötig?
6. Gilt dieses Webinar auch als erste Einschulung für unsere Mitarbeiter?
7. Personenbezogene Daten betreffen ja auch Daten von Mitarbeitern. Reicht es aus, wenn ich z.B. im Anstellungsvertrag darauf hinweise, "dass Daten elektronisch verarbeitet werden" und der Mitarbeiter mit dem Vertrag dem zustimmt.
8. Wenn man Mitarbeitern zu Schulungen anmeldet und personenbezogene Daten bekannt geben muss; ist das noch erlaubt bzw. welche Maßnahmen muss ich im Sinne der DSGVO treffen?
9. Wir nutzen intern Fahrzeugtracking. Die Daten werden im Betrieb gespeichert. Es ist dadurch nachvollziehbar wann ein Mitarbeiter mit seinem Fahrzeug wo war. Fallen diese Daten unter "sensible" Daten?
10. Gibt es Vorschriften zur Archivierung der Personaldaten?
11. Was passiert wenn Mitarbeiter einen Privaten Ordner auf einem Firmen PC haben, muss der auch gesichtet werden?
12. Wie geht eine Personalvermittlungsfirma mit den Lebensläufen der BewerberInnen um?
13. Was kann/muss im Dienstvertrag datenschutzrechtlich berücksichtigt werden? Zustimmung zur Datenverarbeitung? Widerrufsrecht bzw Löschungsrecht (im Ausmaß der gesetzlichen Frist?)?
14. Wie ist mit Daten von Bewerbern, die nicht eingestellt wurden, umzugehen?
15. Wie lange dürfen Bewerberdaten in Evidenz gehalten werden? Wie sieht es bei (Blind)bewerbungen bezüglich Archivierung/Speicherung aus, um beispielsweise später darauf zugreifen zu können? Wie geht man mit datenschutzkonform mit Initiativbewerbungen um?
16. Ich bin eine HR Mitarbeiterin und arbeite mit allen Personaldaten (ua. Bankdaten etc) und gebe diese an ein externes Lohnbüro weiter, was muss ich hierbei beachten?
17. Ich erhalte Mitarbeiterdaten eines Klienten aus der EU zur Bearbeitung und Erledigung von verschiedenen Aufgaben. Was muss ich beachten?
18. Muss ich mir von meinen Mitarbeiterinnen schriftlich bestätigen lassen, dass sie zum Thema Datenschutz eingeschult wurden?
19. Wir wollen in unserem Intranet einen Geburtstagskalender unserer Mitarbeiter veröffentlichen. Brauchen wir dazu die Zustimmung der einzelnen Mitarbeiter?
20. Muss ich die Mitarbeiterdaten (Lohnzettel, Lebensläufe, Zeugnisse u.ä.) speziell schützen?
21. Müssen in Arbeitsverträgen von Mitarbeitern eigene Passi eingefügt werden, die die Zustimmung personenbezogener Daten einholen?
22. Muss ich die einzelnen Mitarbeiter fragen, ob ich ein Foto auf der Webseite unter den Ansprechpartnern veröffentlichen darf?
23. Wir haben als Unternehmer natürlich Kontakt mit Mitarbeitern von Kunden. Müssen wir mit jedem Mitarbeiter des Kunden Vereinbarungen treffen, dass seine Daten bei uns gespeichert werden (Mail, etc), oder reicht eine Vereinbarung mit dem Kunden, welcher Sie auf seine Mitarbeiter überbindet?
24. Wir sind Personalberater. Zählen Gehaltsangaben von Kandidaten zu den "sensiblen Daten"?
25. Ich bin eine EPU-Personalvermittlerin und bekomme viele Lebensläufe und Zeugnisse von Bewerbern (auf konkrete Jobs aber auch als Blindbewerbungen). Reicht es, wenn ich in meiner Signatur einen Passus habe, dass die Bewerber mir ihre Daten zur Verfügung stellen. Oder brauche ich da eine separate Email mit dem ausdrücklichen Einverständnis des Bewerbers?
26. Gibt es die gesetzliche Pflicht, die Mitarbeiter nachweislich zu schulen?

27. Ist bei der Verarbeitung von sensiblen Daten die Einverständnis der Betroffenen Person in jedem Fall gefordert oder kann zB ein auf biometrischen Daten basierendes Zutrittssystem durch eine Betriebsvereinbarung genehmigt werden?
28. Als Arbeitgeber habe ich ja auch Daten von Bewerbungen aufliegen, als Beispiel auch von meinen Mitarbeitern! Wie muss ich zum Beispiel mit Privat-Handynummern/Adressen/Daten umgehen?
29. Was mache ich mit dem Religionsverweis in den Zeugnissen?
30. Wie bzw. wann informiere ich einen Bewerber, der sich auf ein Inserat bewirbt, über seine Rechte (oder gilt das Zusenden von Bewerbungsunterlagen schon als Einwilligung)?
31. Wenn das Unternehmen eine Bewerbung zugesandt bekommt, die das religiöse Bekenntnis enthält, muss dann eine DSFA durchgeführt werden?
32. Muss man Bewerber darüber informieren, dass man deren Daten (6 Monate) aufbewahren möchte? Wenn ja, reicht eine automatische Antwort E-Mail?
33. Wenn auf einem Personalstammbogen die Frage nach Religionsbekenntnis gestellt wird und der Mitarbeiter füllt diese aus freien Stücken aus, gilt dies als Zustimmung für die Verarbeitung?
34. Wenn ein Bewerber der Evidenzhaltung seiner Unterlagen zustimmt, wie lange darf man diese Daten aufheben? Bis auf Widerruf?
35. Wir verlangen in einer Ausschreibung das Mitschicken eines Fotos. Brauche ich dafür eine Einwilligung?
36. Wenn eine Stelle an einem schwarzen Brett ausgehängt wird, muss ich dann am Ende der Ausschreibung einen Hinweis zur DSGVO vermerken?
37. Ist eine Einwilligung des Mitarbeiters wirklich freiwillig (Stichwort Kündigung)?
38. Was ist die Alternative für all die Punkte die mittels Betriebsvereinbarung zu regeln wären, wenn es im Unternehmen keinen Betriebsrat gibt?
39. Kann ich einmalige Zustimmungserklärung der Mitarbeiter einholen, die für alle zukünftigen Veröffentlichungen von Fotos im Internet, Intranet und Mitarbeiterzeitung gilt, oder muss ich fallbezogene Zustimmungserklärungen einholen?
40. Müssen alle bestehenden Mitarbeiter eine Einwilligungserklärung unterschreiben, dass ihre Daten verarbeitet werden?
41. Reicht bezüglich Videoaufzeichnung (zu Sicherheitszwecken) eine Vereinbarung im Dienstvertrag?
42. Wenn ein Mitarbeiter die Zustimmung für die Veröffentlichung von Fotos für Werbung gegeben hat, kann er diese Zustimmung nach Lust und Laune zurückziehen?
43. Wie kann ich den Betriebsrat mit ins Boot holen? Bin ich auch für seine Datenverarbeitungen verantwortlich?
44. Bewerber bei Arbeitskräfteüberlassern und damit eine Versendung des Profils von diesen, wie sieht es da aus? Benötige ich hier eine eigene Einwilligung, obwohl dem Bewerber bekannt ist, dass er sich bei einem Arbeitskräfteüberlasser bewirbt?
45. Bedarf die Zutrittskontrolle via Handscan einer BV?
46. Muss auch der E-Mail-Verkehr gelöscht werden, wenn der Mitarbeiter ausgeschieden ist? Bzw. wie lange darf ich diese Mail aufbewahren?
47. Sind E-Mails die ein Mitarbeiter verfasst als personenbezogene Daten einzustufen und müssen sämtliche E-Mails bei Ausübung des Auskunftsrechts bekannt geben werden?
48. Wie schaut es beim MA Firmenhandy aus? Benutzung von FB, WhatsApp bez. Fingerprint / Gesichtsscan etc. Welchen Datenschutzerklärungen werden hier benötigt seitens MA, Google, Apple, Facebook etc. diese Apps greifen ja auf die Kontaktdaten zu und das können ja auch Kundendaten/MA Daten sein. Ist dann ein MA Handy /Smartphone noch rechtlich "sicher"? Was gilt im Falle, wenn ein Firmenhandy auch privat verwendet werden kann?
49. Ist es zulässig, den Outlook-Kalender aller Mitarbeiter für alle anderen Mitarbeiter freizugeben, um eine Übersicht über die Abwesenheiten zu erhalten?
50. Wenn auf Firmenveranstaltungen Fotos/Videos gemacht werden, braucht man hiezu vom Personal beziehungsweise von der Kundschaft eine extra Einwilligung, wenn sie lediglich als Statisten auf dem Bild erscheinen und nicht als Hauptfigur?
51. Fotos vom Team – wenn ein Dienstnehmer aus der Firma ausscheidet, kann zwar das Einzelbild des Dienstnehmers aus der Webseite entfernt werden, doch existieren auch diverse Fotos, auf dem diese Dienstnehmer nicht alleine abgebildet ist. Muss man diese Fotos auf Verlangen des ehemaligen Dienstnehmers ebenfalls entfernen und wenn ja in welchem Zeitraum?
52. Wird der Datenschutz im Umgekehrten Sinne auch gewahrt bezüglich Betriebsgeheimnis oder muss man dazu den Arbeiter auch separat was unterschreiben lassen bzw muss es im Arbeitsvertrag stehen?

Weitergabe der Mitarbeiterdaten:

53. Brauche ich die Einwilligung der Mitarbeiter, wenn ich die Daten zur Lohnverrechnung an den zuständigen externen Dienstleister schicke? Was muss ich hier beachten? Gibt es hier Unterschiede zu Praktikanten zB unter 18-jährige Ferialpraktikanten?
54. Dürfen Steuerbüros bzw. der Personalverrechner die Stammdaten ausgeschiedener Mitarbeiter der Klienten in der EDV aufbewahren? Dies ist für Wiedereintritte relevant.
55. Darf ich personenbezogene Daten an ein Unternehmen im Unternehmen (Tochterunternehmen) ohne Zustimmung weiterleiten? Oder brauche ich eine Auftragsverarbeitungsvereinbarung?

56. Können Anzahl der Krankenstandstage an die Führungskraft übermittelt werden? Muss Führungskraft E-Mail nach angemessener Zeit löschen?
57. Wenn Lohnzettel per Post verschickt werden, muss ich diese eingeschrieben verschicken? Kann dieser per Mail verschickt werden?
58. Kann man in die Datenschutzerklärung für Mitarbeiter auch die Weitergabe der Personaldaten an die Konzernzentrale aufnehmen. Die Daten werden auch in der internationalen Cloudlösung Office 365 erfasst. Die Cloud befindet sich in Europa. Ich würde auch die Cloud in die Datenschutzerklärung aufnehmen.
59. Wie wirkt die DSGVO in internationalen Konzernen, wenn z.B. die Muttergesellschaft in den USA sitzt und Kopien aller Dienstverträge haben möchte oder z.B. ein zentrales Controlling wiederum in einem Schwesterunternehmen außerhalb der EU sitzt und ebenfalls Zugriff auf die DV benötigt? Muss man hier in der österr. Tochtergesellschaft von jedem Mitarbeiter vorher die schriftliche Zustimmung vor Weitergabe eine DV-Kopie einholen?
60. Wie sieht es bei der Verwendung von Google Docs oder Dropbox zur Verwaltung der Mitarbeiterdaten aus? Benötige ich hier eine Zustimmungserklärung des Mitarbeiters?
61. Wie soll ich den Mitarbeitern das Informationsblatt zur DSGVO zur Verfügung stellen? Einmalig per E-Mail?
62. Wie steht es um eine Informationspflicht von Gesellschaftern (die bei Beteiligung mit nicht mehr als 25% ja unbedingt als Dienstnehmer gelten)? Diese haben ja die Erfassung, Verarbeitung, Speicherung ihrer Daten mitbeschlossen.
63. Informationspflicht und Zustimmungen: Gilt dies für neue Mitarbeiter/Bewerber oder müssen alle im Unternehmen beschäftigten Mitarbeiter aktiv eine Information erhalten?
64. Informationspflicht erst bei Nachfrage des Mitarbeiters oder muss ich jetzt aktiv jeden informieren?
65. Wie gehe ich praktisch mit dem Informationsrecht um? Kopie des Personalaktes bei Auskunft notwendig?
66. Muss man die Informationspflicht bestätigen lassen oder wie kann man je nachweisen, dass man dieser nachgekommen ist?
67. Wie lange dürfen Arztbestätigungen/ Krankenstandsbestätigungen aufbewahrt werden?
68. Bzw. Daten von Mitarbeitern über Konkurse? Wie lange darf ich diese aufbehalten?
69. Wann endet die Verjährungsfrist für das Ausstellen eines Dienstzeugnisses? 30 Jahre? Können KV-Vereinbarungen kürzer sein?
70. Es gibt einige Vorschriften im Arbeitsrecht, wie lange Daten aufbewahrt werden müssen (zB Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: 30 Jahre).
71. Frage zur Speicherbegrenzung: eine Konzernrichtlinie legt viel längere (z.B. bei einem ehemaligen CEO 70 Jahre) Aufbewahrungsfristen vor. Sind generell solche internen Richtlinien gültig?
72. Müssen Daten gespeichert werden, damit z.B. Auskunft der Pensionsversicherungsanstalt gegeben werden kann, ob ein ehem. Mitarbeiter unter die Schwerarbeitsregelung fällt? Solche Anfragen gehen bei uns regelmäßig auch nach vielen Jahren ein.
73. Ist es möglich, den Namen von Bewerbern und die Stelle, auf die sie sich beworben haben, im Bewerbungsportal aufgrund des berechtigten Interesses des Verantwortlichen zu speichern (wenn noch keine Einwilligung im Hinblick auf die DSGVO vorliegt).
74. Darf ich der Polizei Auskunft geben, wenn diese Information über Mitarbeiter haben möchte, wie z.B. aktuelle Anwesenheit?
75. Wir machen jährlich Mitarbeitergespräche. Diese werden teilweise sehr persönlich, was an sich auch unsere Firmenphilosphie ist - mehr Familie als Firma. Müssen wir die Aufzeichnungen alle vernichten? Auch wenn es sich um bestehende Kollegen handelt?
76. Was passiert mit Lohnpfändungen die bereits abgeschlossen sind?
77. Was muss der Dienstgeber bei durch den Dienstnehmer verursachten Datenthemen, wie z.B. Lohnpfändung tun: ist der Dienstgeber für diese Daten ebenso verantwortlich?
78. Ist das Speichern von Daten (Namen, Geburtsdatum) zu Ehepartner und Kindern bei Neueintritten ein "unnötiges Datenhamstern?
79. Müssen im Verarbeitungsverzeichnis bzw. in der Information an den Beschäftigten alle Fälle angegeben werden, wo Mitarbeiterdaten verarbeitet werden? Also z.B. auch eine Liste, in der Dienstreisekosten aufgeführt werden oder eine Liste, in der die Ausgabe von Geräten an MA protokolliert wird, usw? Wie detailliert muss das gemacht werden? Kann eine zusammenfasende Formulierung verwendet werden?
80. Darf ich einen Kunden darüber informieren, dass sich ein Kollege im Krankenstand befindet, falls er anruft und mit diesem sprechen möchte?
81. Wir haben eine ICE-Liste für jeden Mitarbeiter (in case of emergeny - wer soll verständigt werden im Notfall). Sind dies "erforderliche Daten" oder darf ich diese Daten nicht haben (z. B. Lebensgefährte inkl. Handynummer, Mutter, etc. etc.) Dies kann ja - besonders beim Bereich "Lebensgemeinschaft" auch zu sensiblen Daten (sexueller Orientierung) führen. Darf ich so eine Liste führen?
82. Wir haben die privaten Telefonnummern aller Kollegen (wir sind 21) im Telefonsystem gespeichert. Wenn im Krankheitsfall ein Kollege ausfällt, muss ein Ersatz "besorgt" werden. Dazu braucht der Meister die Telefonnummern. Darf man das weiterhin so im System speichern?

---

1. Was ist bei der Personalverwaltung intern zu beachten?

Auch die Datenverarbeitung personenbezogener Daten von Mitarbeitern fällt unter die DSGVO. Es sollte hier geprüft werden, auf welcher Grundlage Daten verarbeitet werden (gesetzliche Verpflichtung, für die Dienstvertragserfüllung notwendig, Einwilligung?). Diese Verarbeitung ist genauso wie jede andere im Verarbeitungsverzeichnis auszuweisen.

2. Muss ein Personalverrechner das Einverständnis zur Datenspeicherung vom jeweiligen Mitarbeiter des Auftraggebers einholen?

Da der Personalverrechner üblicherweise auf Basis eines Auftragsverarbeitungsverhältnisses mit dem Auftraggeber (= Verantwortlichen) agiert und der Auftraggeber die Verpflichtung hat, aufgrund des Dienstverhältnisses auch entsprechend korrekt zu entlohnen, ist hierzu keine Einwilligung des jeweiligen Mitarbeiters des Auftraggebers nötig. Allerdings müssen Sie einen schriftlichen Auftragsverarbeitungsvertrag schließen, in welchem u.a. auch über diese Dinge abzusprechen ist. Muster finden Sie hier.

3. Gibt es Ausnahmen beim Schutz von Mitarbeiterdaten?

Ausnahmen iSv Ausnahmen von der DSGVO bestehen nur dann, wenn Daten anonymisiert verarbeitet werden, dh kein Personenbezug zum konkreten Mitarbeiter herstellbar ist.

4. Wenn ich von meinen Mitarbeitern das Religionsbekenntnis und die Gewerkschaftszugehörigkeit für die Lohnverrechnung abspeichere und verarbeite. Habe ich dann bereits sensible Daten? Was sind die Folgen?

Das sind sensible Daten. Für die Verarbeitung derartiger Daten brauchen Sie entweder eine ausdrückliche Einwilligung vom betroffenen Mitarbeiter oder das Erfordernis der Erfüllung gesetzlicher Verpflichtungen. Ersucht etwa der AN den Gewerkschaftsbeitrag über die Lohnverrechnung abzurechnen, ist von einer Zustimmung zur Verarbeitung dieser Daten auszugehen.

5. Bewerberunterlagen werden von Personalunternehmen geschickt - ist die Verschlüsselung hier nötig?

Emails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Man kann sich aber aus Gründen der Datensicherheit dafür entschließen. Sinnvoll ist die Verschlüsselung jedenfalls bei der Handhabe mit heiklen Daten wie Bankverbindungen, Kreditkartendaten usw, aber natürlich auch bei der Handhabe mit sensiblen oder strafrechtlich relevanten Daten.

6. Gilt dieses Webinar auch als erste Einschulung für unsere Mitarbeiter?

Es ist ein erster Schritt, allerdings dauert das Webinar nur 30 Minuten und bietet nur einen ersten Einblick in datenschutz- und datensicherheitsrelevante Themenstellungen. Wir empfehlen auch, sich das Mitarbeiter-Handbuch auf www.it-safe.at zumindest herunter zu laden und den Mitarbeitern zur Verfügung zu stellen. Auch interne Regelungen wären sinnvoll (zB private Internetnutzung, wohin soll sich der Mitarbeiter mit datenschutzrechtlichen Fragen wenden, usw).

7. Personenbezogene Daten betreffen ja auch Daten von Mitarbeitern. Reicht es aus, wenn ich z.B. im Anstellungsvertrag darauf hinweise, "dass Daten elektronisch verarbeitet werden" und der Mitarbeiter mit dem Vertrag dem zustimmt.

Wohl eher nicht, allein schon deshalb, weil die Einwilligung sehr pauschal abgeholt wird und nicht auf konkrete Datenarten, Zwecke der Verarbeitung etc verwiesen wird. Viele der Verarbeitungsvorgänge im Zusammenhang mit Mitarbeiterndaten werden Ihnen durch Arbeits- und Sozialrecht bzw Kollektivverträge vorgegeben, sind somit „zur Erfüllung einer rechtlichen Verpflichtung erforderlich“ und rechtmäßig gemäß Art 6 DSGVO.

Weitere Verarbeitungen wie zB die Veröffentlichung der Fotos der Mitarbeiter im Intranet usw sollten Sie im Zweifel allerdings nochmals durch individuelle Einwilligungen absichern.

8. Wenn man Mitarbeitern zu Schulungen anmeldet und personenbezogene Daten bekannt geben muss; ist das noch erlaubt bzw. welche Maßnahmen muss ich im Sinne der DSGVO treffen?

Ja, das ist noch erlaubt. Es sollten nur so viele Daten weitergegeben werden, wie konkret für den Zweck notwendig (Anmeldung zur Schulungsmaßnahmen) und sichergestellt werden, dass Daten nicht weitergegeben werden.

9. Wir nutzen intern Fahrzeugtracking. Die Daten werden im Betrieb gespeichert. Es ist dadurch nachvollziehbar wann ein Mitarbeiter mit seinem Fahrzeug wo war. Fallen diese Daten unter "sensible" Daten?

Es sind personenbezogene Daten, allerdings keine sensiblen Datensätze.

Unabhängig davon ist im Einzelfall zu prüfen, ob ergänzend der Abschluss einer Betriebsvereinbarung bzw. die Zustimmung des einzelnen Arbeitnehmers notwendig ist.

10. Gibt es Vorschriften zur Archivierung der Personaldaten?

Es gibt einige Vorschriften im Arbeitsrecht, wie lange Daten aufbewahrt werden müssen (zB Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: 30 Jahre). Wie Daten archiviert werden, gibt das Gesetz allerdings nicht vor.

11. Was passiert wenn Mitarbeiter einen Privaten Ordner auf einem Firmen PC haben, muss der auch gesichtet werden?

Private Datenverarbeitungen von Mitarbeitern würden nicht in die DSGVO fallen, allerdings wäre es natürlich ein Problem, wenn der Arbeitgeber (IT oÄ) auf die Daten zugreifen kann. Bzgl. der Zulässigkeit privater Nutzung der Betriebs-EDV sollte es idealerweise klare Vereinbarungen und Vorgaben geben.

12. Wie geht eine Personalvermittlungsfirma mit den Lebensläufen der BewerberInnen um?

Lebensläufe sind personenbezogene Datensätze iSd DSGVO. Dh Sie haben diese Art der Datenverarbeitung im Verarbeitungsverzeichnis zu protokollieren, Sicherheitsmaßnahmen zu implementieren, etc. Es gibt keine Sondervorschriften für diese Art der Datenverarbeitung.

13. Was kann/muss im Dienstvertrag datenschutzrechtlich berücksichtigt werden? Zustimmung zur Datenverarbeitung? Widerrufsrecht bzw Löschungsrecht (im Ausmaß der gesetzlichen Frist?)?

In dieser Generalität nicht zu beantworten. Die wesentlichen Punkte der Datenverarbeitung, zB zu Zwecken der Personalverrechnung, sind gesetzlich legitimiert und bedürfen keiner weiteren Zustimmung.

Die allenfalls notwendigen Zustimmungserklärungen hängen von der Situation im Einzelfall ab.

14. Wie ist mit Daten von Bewerbern, die nicht eingestellt wurden, umzugehen?

Die „Speicherbegrenzung" (gemäß Art 5 Abs 1 lit e DSGVO) bedeutet, dass Daten nur solange gespeichert werden dürfen, als dies erforderlich ist. Wird ein Bewerber abgelehnt, können die personenbezogenen Daten in Form der Bewerbungsunterlagen jedenfalls noch 7 Monate nach der Ablehnung gespeichert werden.

In einer rechtskräftigen Entscheidung der Datenschutzbehörde wurde eine Speicherung für einen Zeitraum von 7 Monaten als zulässig erachtet. Argument dafür ist die Frist von 6 Monaten ab Ablehnung der Bewerbung zur Geltendmachung von Ansprüchen nach §§ 15 Abs 1 und 29 GlBG wegen Diskriminierung bei Bewerbungen zzgl eines Monats für den potentiellen Klageweg. Möchte man Bewerberdaten länger speichern, ist dazu die Zustimmung des Bewerbers einzuholen.

15. Wie lange dürfen Bewerberdaten in Evidenz gehalten werden? Wie sieht es bei (Blind)bewerbungen bezüglich Archivierung/Speicherung aus, um beispielsweise später darauf zugreifen zu können? Wie geht man mit datenschutzkonform mit Initiativbewerbungen um?

Die Frist zur Geltendmachung von Ansprüchen nach §§ 15 Abs 1 und 29 GlBG wegen Diskriminierung bei Bewerbungen beträgt 6 Monate ab Ablehnung der Beförderung bzw der Bewerbung. Nach rechtskräftiger Entscheidung der Datenschutzbehörde dürfen Bewerberdaten sogar 7 Monate ab Ablehnung gespeichert werden, da auch eine Frist von einem Monat für den potentiellen Klageweg berücksichtigt werden darf.

Sollte eine Evidenzhaltung danach geplant sein, muss das im Einzelfall mit einem „berechtigten Interesse" des Unternehmens begründet werden können oder man holt sich die Einwilligung ein. Bei einer Initiativbewerbung/ Blindbewerbung kann das Unternehmen/ der Personalvermittler wahrscheinlich sogar mit einer längeren Aufbewahrungsfrist argumentieren, da der Bewerber sich nicht auf einen konkreten Posten bewirbt, sondern wohl (zumindest schlüssig) die Evidenzhaltung wünscht.

16. Ich bin eine HR Mitarbeiterin und arbeite mit allen Personaldaten (ua. Bankdaten etc) und gebe diese an ein externes Lohnbüro weiter, was muss ich hierbei beachten?

Es muss hierbei ein schriftlicher Auftragsverarbeitervertrag mit dem externen Lohnbüro geschlossen werden. Muster finden Sie hier.

17. Ich erhalte Mitarbeiterdaten eines Klienten aus der EU zur Bearbeitung und Erledigung von verschiedenen Aufgaben. Was muss ich beachten?

Es muss hierbei ein schriftlicher Auftragsverarbeitervertrag mit dem externen Lohnbüro geschlossen werden. Muster finden Sie hier.

18. Muss ich mir von meinen Mitarbeiterinnen schriftlich bestätigen lassen, dass sie zum Thema Datenschutz eingeschult wurden?

Eine schriftliche Bestätigung ist wohl weniger sinnvoll, wie der tatsächliche Nachweis einer Schulung, wie zB Zeugnisse externer Anbieter, Anwesenheitsbestätigungen interner Schulungen etc.

19. Wir wollen in unserem Intranet einen Geburtstagskalender unserer Mitarbeiter veröffentlichen. Brauchen wir dazu die Zustimmung der einzelnen Mitarbeiter?

Ja, in diesem Fall sollten Sie sich eine Einwilligung einholen.

20. Muss ich die Mitarbeiterdaten (Lohnzettel, Lebensläufe, Zeugnisse u.ä.) speziell schützen?

Es sind keine speziellen Datenschutzmaßnahmen im Arbeitsrecht vorgeschrieben. Bei heiklen, aber v.a. sensiblen Daten wäre aber natürlich das Augenmerk auf die Sicherheit der Daten zu erhöhen.

21. Müssen in Arbeitsverträgen von Mitarbeitern eigene Klauseln eingefügt werden, die die Zustimmung personenbezogener Daten einholen?

Nein, es kann jedoch eine Möglichkeit sein, eine datenschutzrechtliche Einwilligung, sofern nötig, einzuholen. Dabei ist jedoch das „Kopplungsverbot" zu beachten. Es kann kritisch sein, die Zustimmungserklärung als Teil des Arbeitsvertrages aufzunehmen, da der Mitarbeiter somit nur den Job erhält, wenn er auch die Zustimmung erteilt. Es ist vermutlich sinnvoller, die Zustimmungserklärungen separat zu regeln.

22. Muss ich die einzelnen Mitarbeiter fragen, ob ich ein Foto auf der Webseite unter den Ansprechpartnern veröffentlichen darf?

Man könnte auch argumentieren, dass das Unternehmen ein berechtigtes Interesse hat, das Foto der Mitarbeiter hier zu veröffentlichen. Auf Nummer sicher gehen Sie allerdings, wenn Sie sich die Einwilligung hierzu einholen.

23. Wir haben als Unternehmer natürlich Kontakt mit Mitarbeitern von Kunden. Müssen wir mit jedem Mitarbeiter des Kunden Vereinbarungen treffen, dass seine Daten bei uns gespeichert werden (Mail, etc), oder reicht eine Vereinbarung mit dem Kunden, welcher Sie auf seine Mitarbeiter überbindet?

Es reicht eine Vereinbarung mit Ihrem Kunden.

24. Wir sind Personalberater. Zählen Gehaltsangaben von Kandidaten zu den "sensiblen Daten"?

Nein.

25. Ich bin eine EPU-Personalvermittlerin und bekomme viele Lebensläufe und Zeugnisse von Bewerbern (auf konkrete Jobs aber auch als Blindbewerbungen). Reicht es, wenn ich in meiner Signatur einen Passus habe, dass die Bewerber mir ihre Daten zur Verfügung stellen. Oder brauche ich da eine separate Email mit dem ausdrücklichen Einverständnis des Bewerbers?

Nein, in diesem Fall ist die Einwilligung wohl auch dadurch gegeben, dass die jeweiligen Personen Ihnen die Lebensläufe zuschicken. Allerdings haben Sie über die Datenverarbeitung (hier eben die Speicherung) zu informieren. Es würde sich ein Verweis in Ihrer E-Mail Signatur auf eine allfällige Datenschutzerklärung auf Ihrer Website anbieten (Muster im Online-Ratgeber).

26. Gibt es die gesetzliche Pflicht, die Mitarbeiter nachweislich zu schulen?

Die Belehrung von Mitarbeitern über das Datengeheimnis ist in § 6 des österreichischen Datenschutz-Anpassungsgesetzes konkret angesprochen. Wie diese Belehrung auszusehen hat, bzw welche Schulungsmaßnahmen sinnvoll sind, ergibt sich aus dem jeweiligen Unternehmen selbst. Tipps und Vergleiche können Sie sich unter www.it-safe.at holen!

27. Ist bei der Verarbeitung von sensiblen Daten das Einverständnis der Betroffenen Person in jedem Fall gefordert oder kann zB ein auf biometrischen Daten basierendes Zutrittssystem durch eine Betriebsvereinbarung genehmigt werden?

Die Frage der Zulässigkeit bzw die notwendigen Maßnahmen sind im Einzelfall von der Konstellation abhängig. Wenn ein legitimer Rechtfertigungsgrund vorliegen sollte (z.B. Zutritt zu Hochsicherheitstrakt/-labor etc), ist eine Umsetzung dieser Maßnahme auch ohne Zustimmung denkbar. Fehlt diese Legitimation (z.B. Zeiterfassung mittels Biometrie) liegt eine Kontrollmaßnahme vor, die die Menschenwürde berührt und wäre entweder eine Betriebsvereinbarung notwendig oder ohne Betriebsrat die Zustimmung des einzelnen Arbeitnehmers.

28. Als Arbeitgeber habe ich ja auch Daten von Bewerbungen aufliegen, als Beispiel auch von meinen Mitarbeitern! Wie muss ich zum Beispiel mit Privat-Handynummern/Adressen/Daten umgehen?

Die Rechtmäßigkeit der Datenverarbeitung wird sich hier aufgrund mehrerer Rechtfertigungsgründe ergeben (Durchführung vorvertraglicher Maßnahmen, berechtigtes Interesse und allenfalls Einwilligung zur Verarbeitung durch die freiwillige Übermittlung von Daten, vgl auch EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung).

Bleiben diese Daten im Unternehmen, müssen natürlich auch entsprechend Datensicherheitsmaßnahmen eingehalten werden (z.B. Handynummern nicht offen zugänglich am Tisch liegen lassen, möglicherweise „heikle" Daten in einem versperrbaren Schrank ablegen, etc).

29. Was mache ich mit dem Religionsverweis in den Zeugnissen?

Angaben über das Religionsbekenntnis sind in der Regel sensible bzw besondere Kategorien von Daten, für deren Verarbeitung es im Arbeitsverhältnis keinen allgemeinen Rechtfertigungsgrund gibt (ausgenommen allfällig noch vorhandene Fälle der Geltendmachung von arbeitsfreien Tagen aufgrund der Religionszugehörigkeit). Die entsprechenden Angaben in den Zeugnissen sollten daher unkenntlich gemacht werden oder der Bewerber sollte selbst gebeten werden, eine bereinigte Version der Unterlagen zu schicken (z.B. Lebenslauf ohne Religionsbekenntnis schicken, Religionsbekenntnis selbst ausschwärzen).

30. Wie bzw. wann informiere ich einen Bewerber, der sich auf ein Inserat bewirbt, über seine Rechte (oder gilt das Zusenden von Bewerbungsunterlagen schon als Einwilligung)?

Eine Einwilligung ist von der Informationspflicht im Datenschutz klar zu trennen. Eine Einwilligung brauchen Sie möglicherweise um Daten verarbeiten zu können – informieren müssen Sie immer dann, wenn Sie Daten verarbeiten. Für die Verarbeitung von Daten des Bewerbers im Bewerbungsverfahren benötigen Sie üblicherweise keine gesonderte Einwilligung, jedoch müssen Sie den Bewerber über die dem Bewerbungsverfahren zugrundeliegende Datenverarbeitung informieren. Es besteht die Möglichkeit, bereits auf der Firmen-Website der Informationspflicht in der Datenschutzerklärung nachzukommen oder nach Einlangen der Bewerbung eine automatische Zusendung dieser Information durchzuführen. Auch im Zuge der Ablehnung oder der Einladung zu einem Gespräch kann die Datenschutzerklärung erfolgen.

31. Wenn das Unternehmen eine Bewerbung zugesandt bekommt, die das religiöse Bekenntnis enthält, muss dann eine DSFA durchgeführt werden?

Bzgl der Datenschutzfolgeabschätzung (DSFA) wurde eine Verordnung erlassen, die Fälle aufzählt, im Rahmen derer keine DSFA durchzuführen ist („white list"). In der Anlage unter „DSFA-A02 Personalverwaltung" findet sich eine grundsätzliche Ausnahme für *„personenbezogene Daten von Bewerbern, wenn diese Daten vom Betroffenen angegeben wurden*".

Besondere Kategorien personenbezogener Daten (sensible Daten) iSd Art 9 DSGVO dürfen nur aufgrund einer gesetzlichen Ermächtigung oder aufgrund einer rechtlichen Verpflichtung verarbeitet werden.

Übermittelte Informationen über das religiöse Bekenntnis sollten daher gelöscht werden, da zu diesem Zeitpunkt noch keine entsprechende Verpflichtung zur Verarbeitung besteht (dies würde auch dem Grundsatz der Datenminimierung (= nur so viele Daten wie nötig) entsprechen). Wird der

Bewerber eingestellt und begehrt eine Freistellung zur Erfüllung religiöser Verpflichtungen aufgrund einer bestimmten Religion, können Sie das Religionsbekenntnis im Rahmen der Lohnverrechnung verarbeiten.

32. Muss man Bewerber darüber informieren, dass man deren Daten (6 Monate) aufbewahren möchte? Wenn ja, reicht eine automatische Antwort E-Mail?

Ja, grundsätzlich hat eine Information in allen Fällen der Verarbeitung und Speicherung von Daten zu erfolgen. Die (Schrift-)Form ist völlig frei, es wird also auch eine automatische E-Mail ausreichend sein.

33. Wenn auf einem Personalstammbogen die Frage nach Religionsbekenntnis gestellt wird und der Mitarbeiter füllt diese aus freien Stücken aus, gilt dies als Zustimmung für die Verarbeitung?

Zu hinterfragen ist, zu welchem Zweck das Religionsbekenntnis erhoben und in weiterer Folge verarbeitet wird. Auch aus arbeitsrechtlicher Sicht ist die (unbegründete) Abfrage kritisch zu sehen. Ein abgelehnter Bewerber könnte mit dem Argument der Diskriminierung aufgrund der Religion Schadenersatz begehren. Es ist daher von der (unbegründeten!) Abfrage abzuraten.

34. Wenn ein Bewerber der Evidenzhaltung seiner Unterlagen zustimmt, wie lange darf man diese Daten aufheben? Bis auf Widerruf?

Es gibt zu dieser Frage noch keine Judikatur. Es wird sicherlich möglich sein, die Daten durch Zustimmung des Arbeitnehmers für einige Monate, vermutlich sogar für einige Jahre aufzubewahren. Allerdings kann die Zustimmung jederzeit widerrufen werden. Eine zeitlich unbefristete Aufbewahrung „bis auf Widerruf" wird im arbeitsrechtlichen Kontext aber zu weitgehend sein.

35. Wir verlangen in einer Ausschreibung das Mitschicken eines Fotos. Brauche ich dafür eine Einwilligung?

Zu hinterfragen ist, warum das Foto verlangt wird. Eine Ablehnung eines Bewerbers nach Übermittlung eines explizit verlangten Fotos könnte zu Schadenersatzforderungen wegen Diskriminierung nach dem Gleichbehandlungsgesetz führen, wenn sich aus dem Foto ein bestimmtes Geschlecht (vermutlich immer), eine bestimmte Ethnie, religiöse Zugehörigkeit, Weltanschauung etc ergibt. Die Verarbeitung wäre grundsätzlich nach Einwilligung des Bewerbers/Arbeitnehmers zulässig.

36. Wenn eine Stelle an einem schwarzen Brett ausgehängt wird, muss ich dann am Ende der Ausschreibung einen Hinweis zur DSGVO vermerken?

Nein. An dieser Stelle erfolgt noch keine Verarbeitung von Daten. Erst im weiteren Bewerbungsprozess sind die Grundsätze über die Informationspflichten/Datenschutzerklärung bzw die rechtmäßige Verarbeitung der Daten zu beachten. Man könnte aber z.B. bereits auf eine bestehende Datenschutzerklärung, welche den Bewerber- bzw Ausschreibungsprozess abdeckt, verweisen/ verlinken um sicherzustellen, dass Bewerber auch an die datenschutzrechtlichen Informationen kommen, ohne diese nochmals separat auszuhändigen oder zuschicken zu müssen.

37. Ist eine Einwilligung des Mitarbeiters wirklich freiwillig (Stichwort Kündigung)?

Ja, diese Wertung muss es grundsätzlich geben, sonst wäre eine Einwilligung im Arbeitsverhältnis gänzlich unmöglich. Die Freiwilligkeit der Zustimmung ist aber umso weniger gegeben, als der Grund für die Verarbeitung der Daten nicht plausibel ist.

38. Was ist die Alternative für all die Punkte die mittels Betriebsvereinbarung zu regeln wären, wenn es im Unternehmen keinen Betriebsrat gibt?

Ohne Betriebsrat ist eine Zustimmung im Rahmen einer Einzelvereinbarung einzuholen. Für den Bereich der Kontrollmaßnahmen, die die Menschenwürde berühren (zB Videoüberwachung), ist eine Vereinbarung/ eine Zustimmung des Mitarbeiters(vgl § 10 AVRAG) abzugeben.

39. Kann ich einmalige Zustimmungserklärung der Mitarbeiter einholen, die für alle zukünftigen Veröffentlichungen von Fotos im Internet, Intranet und Mitarbeiterzeitung gilt, oder muss ich fallbezogene Zustimmungserklärungen einholen?

Es ist grundsätzlich nicht auszuschließen, dass man einmalige Zustimmungserklärungen einholt, soweit die Verwendung der Fotos absehbar und begrenzt ist (z.B. Fotos von MitarbeiterInnen bei der Firmenveranstaltung, die in Internet, Intranet und Mitarbeiterzeitung veröffentlicht werden).

Betrifft die Veröffentlichung aber Fotos, die auch in den persönlichen Bereich des Arbeitnehmers gehen (Fotos von Firmenfeiern, After Work, Betriebsausflüge) oder für Werbezwecke verwendet werden, sollten jedenfalls fallbezogene Einwilligungen eingeholt werden.

40. Müssen alle bestehenden Mitarbeiter eine Einwilligungserklärung unterschreiben, dass ihre Daten verarbeitet werden?

Nein. Grundsätzlich wird der Großteil der Daten aufgrund einer gesetzlichen Verpflichtung bzw zur Erfüllung dieser verarbeitet. Zu prüfen ist nur, ob von bestehenden Mitarbeitern Daten verarbeitet werden, für die (schon immer!) eine Einwilligung notwendig wäre. Zu beachten ist die Übermittlung/ Zurverfügungstellung einer Datenschutzerklärung (Muster).

41. Reicht bezüglich Videoaufzeichnung (zu Sicherheitszwecken) eine Vereinbarung im Dienstvertrag?

Diverse Antworten zu Fragen rund um die Videoüberwachung. Arbeitsrechtlich ist zu beachten, dass bei einer – zulässigen – Videoüberwachung entweder eine Betriebsvereinbarung (nach § 96 ArbVG) abzuschließen ist oder wenn kein BR vorhanden ist, eine Einzelvereinbarung nach (§ 10 AVRAG).

42. Wenn ein Mitarbeiter die Zustimmung für die Veröffentlichung von Fotos für Werbung gegeben hat, kann er diese Zustimmung nach Lust und Laune zurückziehen?

Jede datenschutzrechtliche Einwilligung kann grundsätzlich unbegründet und jederzeit widerrufen werden. Fraglich ist, ob eine datenschutzrechtliche Einwilligung eingeholt wurde oder mit anderen Rechtsgrundlagen, wie der Vertragsnotwendigkeit oder einem berechtigten Interesse argumentiert wurde. Wenn das der Fall ist und es wurde aus urheberrechtlichen Gründen eine Zustimmung eingeholt, muss weiter geprüft werden, ob diese urheberrechtliche Zustimmung widerrufen werden kann. Zu unterscheiden ist grundsätzlich, ob es sich allenfalls um Fotos handelt, die rein zu Werbezwecken gemacht wurden und für deren Verwendung auch eine Honorierung erfolgte (die Rechte zur Verwendung erworben wurden).

43. Wie kann ich den Betriebsrat mit ins Boot holen? Bin ich auch für seine Datenverarbeitungen verantwortlich?

Nein. Der Betriebsrat ist selbst für die Verarbeitung „seiner" Daten verantwortlich (er ist datenschutzrechtliche Verantwortlicher) . Es kann natürlich sinnvoll sein, dem Betriebsrat bei Erstellung eines Prozesses zum Umgang mit den MA-Daten behilflich zu sein.

44. Bewerber bei Arbeitskräfteüberlassern und damit eine Versendung des Profils von diesen, wie sieht es da aus? Benötige ich hier eine eigene Einwilligung, obwohl dem Bewerber bekannt ist, dass er sich bei einem Arbeitskräfteüberlasser bewirbt?

Hier werden üblicherweise keine sensiblen Daten übermittelt, weshalb von einer (vor-)vertraglichen Notwendigkeit der Übermittlung ausgegangen werden kann und es zulässig ist (vgl: EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung).

45. Bedarf die Zutrittskontrolle via Handscan einer BV?

Die Frage der Zulässigkeit bzw die notwendigen Maßnahmen sind im Einzelfall von der Konstellation abhängig. Wenn ein legitimer Rechtfertigungsgrund vorliegen sollte (z.B. Zutritt zu Hochsicherheitstrakt/-labor etc), ist eine Umsetzung dieser Maßnahme auch ohne Zustimmung denkbar. Fehlt diese Legitimation (z.B. Zeiterfassung mittels Biometrie) liegt eine Kontrollmaßnahme vor, die die Menschenwürde berührt und wäre entweder eine Betriebsvereinbarung notwendig oder ohne Betriebsrat die Zustimmung des einzelnen Arbeitnehmers.

46. Muss auch der E-Mail-Verkehr gelöscht werden, wenn der Mitarbeiter ausgeschieden ist? Bzw. wie lange darf ich diese Mail aufbewahren?

Es sind zunächst Vorfragen hinsichtlich der Unterscheidung private und dienstliche E-Mails zu beantworten: Besteht in der Firma ein Privatnutzungsverbot? Gibt es allenfalls Vorgaben, dass private E-Mails zu kennzeichnen sind?

Wenn die Kategorien an E-Mails unterschieden werden können bzw aufgrund des Privatnutzungsverbotes davon auszugehen ist, dass nur dienstliche E-Mails vorhanden sind, wird man diese aufbewahren dürfen. Auch hier wiederum davon abhängig, ob ein Rechtfertigungsgrund besteht. Dieser kann bspw in vertraglichen Verpflichtungen mit Kunden (Kostenvoranschläge, Angebote, Gewährleistung, Schadenersatz, Aufträge etc) bestehen.

47. Sind E-Mails die ein Mitarbeiter verfasst als personenbezogene Daten einzustufen und müssen sämtliche E-Mails bei Ausübung des Auskunftsrechts bekannt geben werden?

Grundsätzlich beinhalten auch die vom Mitarbeiter verschickten E-Mails personenbezogene Daten und könnten daher theoretisch von einem Auskunftsbegehren erfasst sein. Allerding ist bei einem unbestimmten Auskunftsbegehren anzuraten, eine Konkretisierung zu verlangen. Werden große Mengen an Informationen über die betroffene Person verarbeitet, kann der Verantwortliche den Antragsteller ersuchen, dass er präzisiert, auf welche Informationen oder Verarbeitungsvorgänge sich der Antrag konkret bezieht.

48. Wie schaut es beim MA Firmenhandy aus? Benutzung von FB, WhatsApp bez. Fingerprint / Gesichtsscan etc. Welchen Datenschutzerklärungen werden hier benötigt seitens MA, Google, Apple, Facebook etc. diese Apps greifen ja auf die Kontaktdaten zu und das können ja auch Kundendaten/MA Daten sein. Ist dann ein MA Handy /Smartphone noch rechtlich "sicher"? Was gilt im Falle, wenn ein Firmenhandy auch privat verwendet werden kann?

Bzgl der Benutzung sozialer Medien am Diensthandy bitte die jeweils aktuelle Rechtslage beachten. Zum Thema Einsatz von Firmenhandy allgemein.

49. Ist es zulässig, den Outlook-Kalender aller Mitarbeiter für alle anderen Mitarbeiter freizugeben, um eine Übersicht über die Abwesenheiten zu erhalten?

Gegen diese Vorgehensweise spricht grundsätzlich nichts, solange damit ausschließlich berufliche Termine bzw An-/Abwesenheiten ersichtlich sind. Eine Einsichtnahme in Informationen über z.B. Krankenstand wäre kritischer zu sehen und könnte im Einzelfall einer Zustimmung durch die Betroffenen bedürfen. Eine pauschale Angabe „abwesend“ wird keiner separaten Zustimmung bedürfen.

50. Wenn auf Firmenveranstaltungen Fotos/Videos gemacht werden, braucht man hiezu vom Personal beziehungsweise von der Kundschaft eine extra Einwilligung, wenn sie lediglich als Statisten auf dem Bild erscheinen und nicht als Hauptfigur?

Die Frage ist, ob Personen auf dem Bild erkennbar sind. Wenn sie lediglich als Statisten im Bild aufscheinen, könnte man auch mit einem berechtigten Dokumentationsinteresse des Veranstalters sprechen (vgl: EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung). Allerdings muss vorab (bei der Einladung, beim Empfang) über die Video- bzw Fotoaufnahme informiert werden und entsprechend gekennzeichnet werden.

51. Fotos vom Team – wenn ein Dienstnehmer aus der Firma ausscheidet, kann zwar das Einzelbild des Dienstnehmers aus der Webseite entfernt werden, doch existieren auch diverse Fotos, auf dem diese Dienstnehmer nicht alleine abgebildet ist. Muss man diese Fotos auf Verlangen des ehemaligen Dienstnehmers ebenfalls entfernen und wenn ja in welchem Zeitraum?

Die Veröffentlichung von Fotos einzelner Mitarbeiter wird in der Regel auf Basis einer Einwilligungserklärung erfolgen. Wird diese widerrufen bzw verlangt der Mitarbeiter explizit die Löschung, ist diesem Löschbegehren nachzukommen.

Bei Gruppen-Fotos etc wird man als Dienstgeber besser mit einem berechtigten Interesse argumentieren können (vgl EU-Datenschutz-Grundverordnung (DSGVO): Grundsätze und Rechtmäßigkeit der Verarbeitung). Allerdings könnte es sein, dass ein Mitarbeiter im Rahmen eines Widerspruchsrechts (nicht zu verwechseln mit dem Widerruf einer allfälligen Einwilligung) höherwertige Interessen im Einzelfall geltend machen kann, dass das Foto nicht mehr veröffentlicht werden darf (vgl EU-Datenschutz-Grundverordnung (DSGVO): Datenschutzrechtliche Pflicht zur Umsetzung eines Widerspruches). Das ist von Fall zu Fall zu prüfen und kann im Ergebnis entsprechend abweichen.

52. Wird der Datenschutz im Umgekehrten Sinne auch gewahrt bezüglich Betriebsgeheimnis oder muss man dazu den Arbeiter auch separat was unterschreiben lassen bzw muss es im Arbeitsvertrag stehen?

Zu empfehlen ist der Abschluss einer entsprechenden Erklärung, siehe Muster.

53. Brauche ich die Einwilligung der Mitarbeiter, wenn ich die Daten zur Lohnverrechnung an den zuständigen externen Dienstleister schicke? Was muss ich hier beachten? Gibt es hier Unterschiede zu Praktikanten zB unter 18-jährige Ferialpraktikanten?

Nein, es ist ausreichend, den Arbeitnehmer bloß darüber zu informieren. Dies erfolgt im Rahmen der Datenschutzerklärung (Muster).

54. Dürfen Steuerbüros bzw. der Personalverrechner die Stammdaten ausgeschiedener Mitarbeiter der Klienten in der EDV aufbewahren? Dies ist für Wiedereintritte relevant.

Eine Aufbewahrung ist auch dort nur solange möglich, als dies rechtlich zulässig ist. Zu beachten sind daher gesetzliche Rechtfertigungsgründe wie Speicher- und Aufbewahrungsfristen.

55. Darf ich personenbezogene Daten an ein Unternehmen im Unternehmen (Tochterunternehmen) ohne Zustimmung weiterleiten? Oder brauche ich eine Auftragsverarbeitungsvereinbarung?

Zu hinterfragen ist, zu welchem Zweck die Daten weitergegeben werden sollen. Wird z.B. die Lohnverrechnung zentral von einem Tochterunternehmen durchgeführt, wird die Übermittlung der relevanten Daten – ohne Zustimmung des Mitarbeiters - rechtlich zulässig sein. Zu beachten ist, dass nicht pauschal sämtliche Daten im Konzern ohne rechtliche Begründung zusammengeführt und übermittelt werden dürfen.

56. Können Anzahl der Krankenstandstage an die Führungskraft übermittelt werden? Muss Führungskraft E-Mail nach angemessener Zeit löschen?

Auch hier ist der Zweck der Übermittlung und Verarbeitung zu hinterfragen. Eine Einsicht in die Anzahl der Krankenstandstage ist rechtlich zulässig, da dies zur Beurteilung von Entgeltfortzahlungsansprüchen relevant ist. Natürlich ist auch hier die Speicherbegrenzung zu beachten, sodass die Daten (das E-Mail) zu löschen sind, sobald die Erforderlichkeit für die Datenverarbeitung nicht mehr gegeben ist (vgl EU-Datenschutz-Grundverordnung (DSGVO): Aufbewahrungs- und Verjährungsfristen).

57. Wenn Lohnzettel per Post verschickt werden, muss ich diese eingeschrieben verschicken? Kann dieser per Mail verschickt werden?

E-Mails müssen auf Basis der DSGVO nicht zwingend verschlüsselt werden, das ist so nirgends ausgewiesen. Unverschlüsselte E-Mails bieten keine Datensicherheit und können von Unbefugten leicht „mitgelesen" werden. Unbedingt anzuraten ist daher die Verschlüsselung bei der Handhabe mit heiklen Daten wie Bankverbindungen und jedenfalls bei der Übermittlung von sensiblen Daten wie zB Gesundheitsdaten, aber natürlich auch bei der Handhabe mit strafrechtlich relevanten Daten.

Ein Lohnzettel beinhaltet in der Regel keine sensiblen Daten, weshalb der Versand per „normaler" Post ausreichend sein wird. Hier gibt es allerdings noch keine gesicherte Rechtsprechung.

58. Kann man in die Datenschutzerklärung für Mitarbeiter auch die Weitergabe der Personaldaten an die Konzernzentrale aufnehmen. Die Daten werden auch in der internationalen Cloudlösung Office 365 erfasst. Die Cloud befindet sich in Europa. Ich würde auch die Cloud in die Datenschutzerklärung aufnehmen.

Ja, diese Datenübermittlung sollte aufgenommen werden. Einerseits eben die Übermittlung an die Konzernzentrale und andererseits die Datenweitergabe an Auftragsverarbeiter (Office 365). Beispiele, wie man eine Datenschutzerklärung zusammenstellen kann, finden Sie in unserem Online-Ratgeber zu den Informationsverpflichtungen .

59. Wie wirkt die DSGVO in internationalen Konzernen, wenn z.B. die Muttergesellschaft in den USA sitzt und Kopien aller Dienstverträge haben möchte oder z.B. ein zentrales Controlling wiederum in einem Schwesterunternehmen außerhalb der EU sitzt und ebenfalls Zugriff auf die DV benötigt? Muss man hier in der österr. Tochtergesellschaft von jedem Mitarbeiter vorher die schriftliche Zustimmung vor Weitergabe eine DV-Kopie einholen?

Verantwortliche, die Teil einer Unternehmensgruppe sind, die einer zentralen Stelle zugeordnet sind können gem. Erwägungsgrund 48 der DSGVO ein berechtigtes Interesse haben, personenbezogene Daten innerhalb der Unternehmensgruppe für interne Verwaltungszwecke, einschließlich der Verarbeitung personenbezogener Daten von Kunden und Beschäftigten, zu übermitteln.

Der Rechtfertigungsgrund für die Übermittlung der Dienstverträge wäre zu hinterfragen, ebenso, welche Daten im Zuge der Controlling-Tätigkeit übermittelt werden dürfen. Handelt es sich um (anonymisierte) Zahlen, wird dies jedenfalls zulässig sein.

Für die Datenübermittlung innerhalb der EU wären keine zusätzlichen Erfordernisse zu beachten.

Für den Datenverkehr mit Drittstaaten sind folgende Regelungen zu beachten. Eine Einwilligung des einzelnen Betroffenen kann je nach Fallkonstellation notwendig sein.

60. Wie sieht es bei der Verwendung von Google Docs oder Dropbox zur Verwaltung der Mitarbeiterdaten aus? Benötige ich hier eine Zustimmungserklärung des Mitarbeiters?

Zu hinterfragen ist, ob die genannten Produkte als zuverlässige Auftragsverarbeiter gelten (siehe FAQ zu Sozialen Netzwerken).

61. Wie soll ich den Mitarbeitern das Informationsblatt zur DSGVO zur Verfügung stellen? Einmalig per E-Mail?

Die Art der Übermittlung bzw Zurverfügungstellung der Datenschutzerklärung kann selbst gewählt werden. Es ist also möglich, ein Mail zu übermitteln, die Information im Intranet oder am Schwarzen Brett zur Verfügung zu stellen (wenn die MA dort entsprechenden Zugriff bzw Zutritt haben) oder das Papier physisch zu übergeben. Es sollte aber in irgendeiner Form nachweisbar sein, dass die Mitarbeiter davon Kenntnis erlangt haben bzw die Möglichkeit hatten, davon Kenntnis zu erlangen.

62. Wie steht es um eine Informationspflicht von Gesellschaftern (die bei Beteiligung mit nicht mehr als 25% ja unbedingt als Dienstnehmer gelten)? Diese haben ja die Erfassung, Verarbeitung, Speicherung ihrer Daten mitbeschlossen.

Das ist davon unabhängig. Als Verantwortliche im datenschutzrechtlichen Sinn gilt das Unternehmen selbst, nicht die dahinterstehenden Personen. Sie sind dennoch von einer Datenverarbeitung betroffene Personen und müssen hierüber informiert werden. In diesem Fall könnte es nur möglich sein, dass diese Gesellschafter über die notwendigen Informationen bereits verfügen (weil sie selbst darüber beschlossen haben und in Zuge dessen informiert wurden oÄ). Vgl hierzu: EU-Datenschutz-Grundverordnung (DSGVO): Informationspflichten.

63. Informationspflicht und Zustimmungen: Gilt dies für neue Mitarbeiter/Bewerber oder müssen alle im Unternehmen beschäftigten Mitarbeiter aktiv eine Information erhalten?

In der Literatur wird die Meinung vertreten, dass die Informationspflicht auf alte, bereits vor Geltungsbeginn der DSGVO abgeschlossene Datenerhebungen, keine Anwendung findet. Allerdings ist im Arbeitsverhältnis davon auszugehen, dass laufend Datenerhebungen stattfinden und somit die Informationsverpflichtung sowohl für die neuen Mitarbeiter, als auch für die bestehenden Mitarbeiter gelten wird.

Bzgl Zustimmungserklärungen ist zu prüfen, ob diese von bestehenden Mitarbeitern bereits vorliegen und auch der DSGVO entsprechend sind.

64. Informationspflicht erst bei Nachfrage des Mitarbeiters oder muss ich jetzt aktiv jeden informieren?

Die Informationsverpflichtung ist unabhängig von der Nachfrage selbstständig zu erfüllen/ anbieten.Ähnlich, wie Sie Mitarbeiter über Datensicherheitsmaßnahmen schulen bzw belehren sollten, ist auch die Information (nach Art 13 und 14 DSGVO) von Ihnen als Dienstgeber selbstständig zur Verfügung zu stellen.

65. Wie gehe ich praktisch mit dem Informationsrecht um? Kopie des Personalaktes bei Auskunft notwendig?

Hier wurden offenbar Informationspflicht und Auskunftsrecht verwechselt. Informationen müssen dem Mitarbeiter von selbst zur Verfügung gestellt werden (vgl EU-Datenschutz-Grundverordnung (DSGVO): Informationspflichten). Auf ein Auskunftsbegehren eines Mitarbeiters muss innerhalb der Frist von einem Monat ordnungsgemäß reagiert werden (vgl EU-Datenschutz-Grundverordnung (DSGVO): Auskunftspflicht des Verantwortlichen). Werden

große Mengen an Informationen über die betroffene Person verarbeitet, kann der Verantwortliche den Antragsteller ersuchen, dass er präzisiert, auf welche Informationen oder Verarbeitungsvorgänge sich der Antrag konkret bezieht. Wird auch der Personalakt begehrt, ist dieser soweit zur Verfügung zu stellen, als personenbezogene Daten vorhanden sind.

66. Muss man die Informationspflicht bestätigen lassen oder wie kann man je nachweisen, dass man dieser nachgekommen ist?

Die Art der Übermittlung bzw Zurverfügungstellung der Datenschutzerklärung kann selbst gewählt werden. Es ist also möglich, ein Mail zu übermitteln, die Information im Intranet oder am Schwarzen Brett zur Verfügung zu stellen (wenn die MA dort entsprechenden Zugriff bzw Zutritt haben) oder das Papier physisch zu übergeben. Es sollte aber in irgendeiner Form nachweisbar sein, dass die Mitarbeiter davon Kenntnis erlangt haben bzw die Möglichkeit hatten, davon Kenntnis zu erlangen.

Eine tatsächliche Bestätigung der Ausfolgung der Datenschutzerklärung wäre der bestmögliche Nachweis. Die Datenschutzerklärung muss allerdings nicht „akzeptiert" oder „angenommen" werden. Sie ist lediglich zur Kenntnis zu nehmen.

67. Wie lange dürfen Arztbestätigungen/ Krankenstandsbestätigungen aufbewahrt werden?

Es kommt bei der max Speicherdauer immer darauf an, wie lange eine Speicherung notwendig ist, um einen bestimmten Zweck zu erfüllen. Da Krankenstandsbestätigungen (gemeint wohl Arbeitsunfähigkeitsbestätigungen) in unmittelbarem Zusammenhang mit der Frage der Entgeltfortzahlung und somit abrechnungstechnischen Fragen stehen, wird eine Frist von 7 Jahren zulässig sein.

68. Bzw. Daten von Mitarbeitern über Konkurse? Wie lange darf ich diese aufbehalten?

Die entsprechenden Daten können solange aufbewahrt werden, als es einen gesetzlichen Rechtfertigungsgrund dafür gibt. Da aufgrund der Pfändung ein direkter Abzug vom Lohn-/Gehaltskonto erfolgt ist, der Auswirkungen auf die Lohnverrechnung hat(te), werden 7 Jahre Aufbewahrungsfrist argumentierbar sein.

69. Wann endet die Verjährungsfrist für das Ausstellen eines Dienstzeugnisses? 30 Jahre? Können KV-Vereinbarungen kürzer sein?

Die Verjährungsfrist beträgt gem ABGB 30 Jahre. Nach der Judikatur könnte eine allgemeine und nicht auf bestimmte Fälle eingeschränkte KV-Verfallsbestimmung die Frist verkürzen. Die meisten KVs sehen aber keine derartig weiten Verfallsfristen vor.

70. Es gibt einige Vorschriften im Arbeitsrecht, wie lange Daten aufbewahrt werden müssen (zB Dienstzeugnisses nach § 1163 iVm § 1478 ABGB: 30 Jahre).

Unter folgendem Link finden Sie eine Auflistung potentieller Fristen.

71. Frage zur Speicherbegrenzung: eine Konzernrichtlinie legt viel längere (z.B. bei einem ehemaligen CEO 70 Jahre) Aufbewahrungsfristen vor. Sind generell solche internen Richtlinien gültig?

Wenn es sich bei diesen Fristen nur um interne Vorgaben handelt, wird eine derart lange Speicherung nicht zweckmäßig bzw erforderlich iSd DSGVO sein. Es wäre sonst auch von einer Umgehung auszugehen, da sonst jedes Unternehmen in den internen Compliance Vorschriften für sich andere Aufbewahrungsfristen festlegen könnte. Zu prüfen wäre nur, ob es entsprechende Haftungsbestimmungen oder (vertragliche) Regressverpflichtungen gibt, die das Aufbewahren der Daten notwendig machen.

72. Müssen Daten gespeichert werden, damit z.B. Auskunft der Pensionsversicherungsanstalt gegeben werden kann, ob ein ehem. Mitarbeiter unter die Schwerarbeitsregelung fällt? Solche Anfragen gehen bei uns regelmäßig auch nach vielen Jahren ein.

Eine pauschale Speicherung von Daten, um alle Eventualitäten abdecken zu können, ist nicht zulässig. Handelt es sich jedoch um Arbeitnehmer, die z.B. Tätigkeiten verrichten, die von der Schwerarbeitsverordnung erfasst sind – wodurch eine Nachfrage der PVA sehr wahrscheinlich ist – wird eine längere Speicherung möglich sein.

73. Ist es möglich, den Namen von Bewerbern und die Stelle, auf die sie sich beworben haben, im Bewerbungsportal aufgrund des berechtigten Interesses des Verantwortlichen zu speichern (wenn noch keine Einwilligung im Hinblick auf die DSGVO vorliegt).

Die vom Bewerber bereit gestellten (nicht-sensiblen) Daten dürfen jedenfalls rechtmäßig verarbeitet werden, dies auf Basis der Durchführung vorvertraglicher Maßnahmen bzw des berechtigten Interesses des Verantwortlichen.

74. Darf ich der Polizei Auskunft geben, wenn diese Information über Mitarbeiter haben möchte, wie z.B. aktuelle Anwesenheit?

Es sollte immer im Einzelfall geprüft werden, z.B. ob ein dringender Verdachtsfall dargelegt wird, sich die Polizei als solche auch entsprechend identifizieren kann und der Inhalt der Auskunft sich lediglich auf schlicht personenbezogene Daten (nicht sensible oder strafrechtlich relevante) bezieht.

75. Wir machen jährlich Mitarbeitergespräche. Diese werden teilweise sehr persönlich, was an sich auch unsere Firmenphilosphie ist - mehr Familie als Firma. Müssen wir die Aufzeichnungen alle vernichten? Auch wenn es sich um bestehende Kollegen handelt?

Auch hier ist zu hinterfragen, zu welchem Zweck die personenbezogenen Daten gespeichert und verarbeitet werden. Wird bspw von der Arbeitnehmerin bekanntgegeben, dass sie sich noch ein weiteres Kind wünscht oder informiert der Arbeitnehmer, dass er sich in der Freizeit vermehrt bei einer politischen Partei oder einer Religionsgemeinschaft engagiert, dürfen diese (zum Teil sensiblen) Daten nicht verarbeitet werden, da keine Rechtfertigung dafür besteht.

Um DSGVO-konform zu sein, sollte man die Aufzeichnung derartiger Informationen künftig vermeiden.

76. Was passiert mit Lohnpfändungen die bereits abgeschlossen sind?

Die entsprechenden Daten können solange aufbewahrt werden, als es einen gesetzlichen Rechtfertigungsgrund dafür gibt. Da aufgrund der Pfändung ein direkter Abzug vom Lohn-/Gehaltskonto erfolgt ist, der Auswirkungen auf die Lohnverrechnung hatte, werden 7 Jahre Aufbewahrungsfrist argumentierbar sein.

77. Was muss der Dienstgeber bei durch den Dienstnehmer verursachten Datenthemen, wie z.B. Lohnpfändung tun: ist der Dienstgeber für diese Daten ebenso verantwortlich?

Für die Daten, die in Zuge dessen durch den Dienstgeber verarbeitet werden, ist er auch verantwortlich.

78. Ist das Speichern von Daten (Namen, Geburtsdatum) zu Ehepartner und Kindern bei Neueintritten ein "unnötiges Datenhamstern?

Der Grundsatz der Datenminimierung besagt, dass nur so viele Daten erhoben und verarbeitet werden sollen, wie notwendig. Wozu werden die Daten benötigt? Kann keine Begründung gefunden werden, sollten die Daten auch nicht aufgenommen, sondern allenfalls in der Zukunft anlassfallbezogen abgefragt werden.

Mögliche Begründungen für eine zulässige Speicherung könnten die Gewährung einer Kinderzulage, die Abwicklung einer Krankenzusatzversicherung über den Arbeitgeber, die Inanspruchnahme einer Pflegefreistellung oder von Dienstverhinderungsgründen etc sein.

79. Müssen im Verarbeitungsverzeichnis bzw. in der Information an den Beschäftigten alle Fälle angegeben werden, wo Mitarbeiterdaten verarbeitet werden? Also z.B. auch eine Liste, in der Dienstreisekosten aufgeführt werden oder eine Liste, in der die Ausgabe von Geräten an MA protokolliert wird, usw? Wie detailliert muss das gemacht werden? Kann eine zusammenfasende Formulierung verwendet werden?

Grundsätzlich muss im Verarbeitungsverzeichnis jede Datenverarbeitung aufgenommen werden, das allerdings kann man auch etwas pauschaler gestaltet, iSv Zusammenführung von thematisch Verwandtem (z.B. Lohnverrechnung, Personalverwaltung, etc.). Beispiele für Verarbeitungsverzeichnisse

80. Darf ich einen Kunden darüber informieren, dass sich ein Kollege im Krankenstand befindet, falls er anruft und mit diesem sprechen möchte?

Bestenfalls informieren Sie darüber, dass der Kollege nicht im Büro ist und erst ab ... wieder erreichbar ist.

81. Wir haben eine ICE-Liste für jeden Mitarbeiter (in case of emergeny - wer soll verständigt werden im Notfall). Sind dies "erforderliche Daten" oder darf ich diese Daten nicht haben (z.B. Lebensgefährte inkl. Handynummer, Mutter, etc. etc.) Dies kann ja - besonders beim Bereich "Lebensgemeinschaft" auch zu sensiblen Daten (sexueller Orientierung) führen. Darf ich so eine Liste führen?

Eine derartige Liste kann mit Zustimmung des betroffenen Mitarbeiters geführt werden, da es sich um einen Aspekt der Fürsorgepflicht des Arbeitgebers handelt. Die ICE-Liste darf dann auch tatsächlich nur für die genannten Zwecke (Kontakt im Notfall) genützt werden. Auch bzgl der etwaig sensiblen Daten haben Sie, wenn die Daten vom Mitarbeiter selbst bekannt gegeben werden, seine ausdrückliche Zustimmung zur Verarbeitung als Notfallkontakt.

82. Wir haben die privaten Telefonnummern aller Kollegen (wir sind 21) im Telefonsystem gespeichert. Wenn im Krankheitsfall ein Kollege ausfällt, muss ein Ersatz "besorgt" werden. Dazu braucht der Meister die Telefonnummern. Darf man das weiterhin so im System speichern?

Die Verarbeitung persönlicher Daten ist für das „Leben" des Arbeitsverhältnisses notwendig. Somit ist auch die Verarbeitung der privaten Telefonnummer grundsätzlich zulässig. Zu hinterfragen ist, wer – und zu welchem Zweck - Zugriff auf diese Daten hat. Kann der Zugriff auch von KollegInnen abseits des Meisters erfolgen, sollte die Zustimmung der betroffenen Mitarbeiter eingeholt werden.

Stand: 21.09.2021