Unternehmensrichtlinie Datenschutz

Unternehmensrichtlinie Datenschutz

I. Allgemeines

1. Einleitung

1.1 Die im Unternehmen vorhandenen Daten sind für das Unternehmen und die reibungslosen Abläufe im Unternehmen von großem Wert. Diese Daten sind daher gegen unbefugte Zugriffe und andere Gefährdungen zu schützen.

1.2 Gleichzeitig erwarten die Kunden, Partner und Mitarbeiter des Unternehmens, dass die dem Unternehmen anvertrauten Daten besonders geschützt werden und ein sorgsamer Umgang mit ihnen erfolgt.

1.3 Das Unternehmen bekennt sich auch im Rahmen seines gesellschaftlichen Engagements zu seiner Verantwortung für den sorgsamen Umgang mit personenbezogenen Daten.

2. Ziel der Unternehmensrichtlinie

2.1 Mit dieser Unternehmensrichtlinie sollen einheitliche Standards für den Datenschutz im Unternehmen geschaffen werden.

2.2 Durch die Einhaltung der in dieser Unternehmensrichtlinie definierten Standards kommt das Unternehmen seinen datenschutzrechtlichen Verpflichtungen nach und sorgt für eine ausreichende Berücksichtigung der Interessen sowie Rechte der betroffenen Personen.

2.3 Die Beachtung dieser Unternehmensrichtlinie ist Voraussetzung für den sicheren Austausch von personenbezogenen Daten innerhalb des Unternehmens.

3. Anwendungsbereich der Unternehmensrichtlinie

3.1 Diese Unternehmensrichtlinie gilt für jegliche Verarbeitung von personenbezogenen Daten, wobei die erstmalige Erfassung von Daten, deren Speicherung und Verwendung sowie die Weitergabe innerhalb des Unternehmens und die Übermittlung an Dritte erfasst werden. Es werden umfassend alle datenschutzrechtlichen Aspekte geregelt, die sich im Rahmen der Datenverarbeitung ergeben können. Sie findet Anwendung auf sämtliche Arten von personenbezogenen Daten, insbesondere Daten von Mitarbeitern, Kunden, Lieferanten und anderen Geschäftspartnern.

3.2 Auch für alle Tochterunternehmen des Unternehmens ist diese Unternehmensrichtlinie verbindlich.

3.3 Die Herkunft der Daten ist für die Anwendbarkeit dieser Unternehmensrichtlinie nicht maßgeblich; entscheidend ist die Verwendung der Daten im Unternehmen.

3.4 Bestehende gesetzliche Verpflichtungen werden von dieser Unternehmensrichtlinie nicht berührt und sind somit zu erfüllen. Es ist daher stets zu prüfen, welche

gesetzlichen Regelungen einschlägig sind; deren Beachtung ist sicherzustellen. Sofern sich aus den gesetzlichen Bestimmungen geringere Anforderungen ergeben, gelten die Regelungen dieser Unternehmensrichtlinie.

4. Definitionen

4.1 **Personenbezogene Daten** im Sinne dieser Unternehmensrichtlinie sind Angaben über eine identifizierte oder identifizierbare natürliche Person. Daten, die ausschließlich Informationen über juristische Personen beinhalten, sind keine personenbezogenen Daten. Auch diese Daten sollen gleichermaßen geschützt werden. Der Personenbezug entfällt bei einer vollständigen Anonymisierung, nicht aber bereits bei der Verwendung von Pseudonymen.

4.2 **Betroffene Personen** sind diejenigen Personen, deren personenbezogene Daten im Unternehmen verarbeitet werden.

4.3 **Dritter** ist jede Stelle außerhalb des Unternehmens. Einzelne Stellen oder Abteilungen innerhalb des Unternehmens sind nicht Dritte, gleichwohl ist auch innerhalb des Unternehmens zu prüfen, inwieweit personenbezogene Daten unternehmensintern zur Verfügung gestellt werden müssen. Dienstleister, mit denen eine Vereinbarung zur Auftragsdatenverarbeitung besteht, gelten ebenfalls nicht als Dritte, da diese unter der Verantwortung des Unternehmens tätig werden.

II. Grundsätze der Datenverarbeitung

5. Zulässigkeit der Datenverarbeitung

5.1 Bei jedem Vorgang der Datenverarbeitung ist zu prüfen, ob die beabsichtigte Verarbeitung von Daten zulässig ist. Bestehen Zweifel an der Zulässigkeit, soll der Datenschutzbeauftragte kontaktiert werden.

5.2 Die Zulässigkeit der Datenverarbeitung kann sich aus verschiedenen Gesichtspunkten ergeben. Zunächst kann sich die Zulässigkeit daraus ergeben, dass der Betroffene in die Datenverarbeitung eingewilligt hat. Auch ohne Einwilligung des Betroffenen kann die Datenverarbeitung zulässig sein, wenn eine gesetzliche Ermächtigungsgrundlage einschlägig ist. Fehlt es an einer Einwilligung und einer gesetzlichen Ermächtigungsgrundlage, dann ist die Datenverarbeitung unzulässig.

5.3 Im Rahmen der Zulässigkeitsprüfung ist auch zu untersuchen, ob die Datenverarbeitung unter Berücksichtigung des Prinzips der Datenminimierung notwendig ist.

6. Gesetzliche Ermächtigungsgrundlagen

6.1 Die Verarbeitung personenbezogener Daten kann erforderlich sein für die Begründung oder Erfüllung eines Vertrags mit der betroffenen Person.

6.2 Eine Notwendigkeit und Ermächtigung zur Datenverarbeitung kann sich ergeben aufgrund einer rechtlichen Verpflichtung des Unternehmens, die beispielsweise unmittelbar resultiert aus einer gesetzlichen Regelung oder einer verbindlichen behördlichen Entscheidung. Als Ermächtigungsgrundlage kommt insoweit insbeson-

dere ein Auskunftsersuchen von Ermittlungsbehörden in Betracht.

6.3 Zulässig ist die Verarbeitung personenbezogener Daten auch, wenn sie zur Geltendmachung, Ausübung oder Verteidigung rechtlicher Ansprüche vor Gericht erforderlich ist. Gleiches gilt für die Wahrung lebenswichtiger Interessen.

6.4 Denkbar ist eine Datenverarbeitung schließlich in den Fällen, bei denen berechtigte Interessen des Unternehmens bestehen und gleichzeitig kein Grund zu der Annahme besteht, dass das schutzwürdige Interesse der betroffenen Person an dem Ausschluss der Datenverarbeitung überwiegt. Das Ergebnis einer solchen Interessenabwägung soll dabei schriftlich protokolliert werden.

7. Einwilligung und Protokollierung

7.1 Eine Einwilligung der betroffenen Person ist als Grundlage für die Datenverarbeitung ausreichend, wenn die betroffene Person zuvor ausreichend informiert wurde und ihre Einwilligung für die beabsichtigte Datenverarbeitung anschließend eindeutig und auf freiwilliger Basis erteilt hat.

7.2 Von einer ausreichenden Information ist auszugehen, wenn die wesentlichen Abläufe der Datenverarbeitung verständlich erläutert werden und insbesondere erklärt wird, zu welchem Zweck die Daten verarbeitet werden. Die betroffene Person soll darauf hingewiesen werden, dass ihre Einwilligung frei widerruflich ist. Außerdem ist darauf zu achten, dass Einwilligungserklärungen gegenüber anderen Erklärungen optisch hervorgehoben und abgegrenzt werden. Eine Kopplung der Einwilligung mit anderen Erklärungen soll vermieden werden.

7.3 Eine Einwilligung kann nur dann freiwillig abgegeben werden, wenn die betroffene Person im Falle einer Verweigerung der Einwilligung keine gravierenden Nachteile zu befürchten hat. Wird die Inanspruchnahme oder Erbringung von Leistungen von einer Einwilligung abhängig gemacht, ist die erteilte Einwilligung regelmäßig dann freiwillig, wenn sie der Vertragsbegründung oder Vertragserfüllung dient oder wenn die Inanspruchnahme von Leistungen auch in anderer zumutbarer Weise möglich wäre.

7.4 Die Einwilligungserklärung der betroffenen Person soll aus Nachweisgründen in Textform eingeholt werden. In jedem Fall ist darauf zu achten, dass eine eindeutige Erklärung der betroffenen Person vorliegt. Die entsprechenden Einwilligungserklärungen sind für den Fall einer späteren Überprüfung zu protokollieren.

7.5 Bei einer schriftlich erteilten Einwilligung kann es zulässig sein, die Erklärung einzuscannen und das Original anschließend zu vernichten. Sofern eine Einwilligung online eingeholt wird, ist darauf zu achten, dass eine Überprüfung erfolgt, bspw. über ein Double-Opt-in-Verfahren.

8. Zweckbindung

8.1 Personenbezogene Daten dürfen nur für den Zweck verarbeitet werden, für den sie ursprünglich erhoben wurden. Bei Einholung einer Einwilligung von der betroffenen Person ist auf den konkreten Zweck hinzuweisen. Es muss sich stets um einen

rechtmäßigen Zweck der Datenverarbeitung handeln.

8.2 Wenn später eine Datenverarbeitung zu einem anderen Zweck erfolgen soll, dann muss auch hierfür eine Einwilligung eingeholt werden oder eine gesetzliche Ermächtigungsgrundlage vorliegen, sofern der neue Zweck der Datenverarbeitung nicht bereits mit dem ursprünglichen Zweck vereinbar ist.

9. Verhältnismäßigkeit

9.1 Bei der Verarbeitung personenbezogener Daten ist der Grundsatz der Verhältnismäßigkeit zu beachten. Der Grundsatz der Verhältnismäßigkeit ist beachtet, wenn die Datenverarbeitung dazu geeignet ist, einen legitimen Zweck zu erreichen. Weiter darf kein milderes, gleichermaßen geeignetes Mittel zur Erreichung des vorgesehenen Zwecks zur Verfügung stehen. Schließlich ist zu prüfen, ob der Datenverarbeitung keine überwiegenden schutzwürdigen Interessen der betroffenen Person entgegenstehen.

9.2 Als milderes Mittel kann bspw. die Verarbeitung von aggregierten Daten oder sonstigen Daten ohne Personenbezug in Betracht kommen.

9.3 Bei der Prüfung der Verhältnismäßigkeit kann insbesondere der Ursprung der personenbezogenen Daten (geschäftlich, privat oder intim) zu berücksichtigen sein. Weiter ist das mit der Datenverarbeitung verbundene Risiko einer Beeinträchtigung von Persönlichkeitsrechten abzuschätzen.

9.4 Im Rahmen der Prüfung der Verhältnismäßigkeit ist auch zu untersuchen, inwieweit eine Datenverarbeitung nach den Grundsätzen von Treu und Glauben sowie in transparenter Weise erfolgt.

10. Datenminimierung

10.1 Die Datenverarbeitung im Unternehmen ist so zu organisieren, dass so wenig personenbezogene Daten wie möglich verarbeitet werden. Wenn personenbezogene Daten nicht mehr benötigt werden, sollen diese gelöscht werden.

10.2 Bereits bei der Datenerhebung ist darauf zu achten, dass als Voreinstellung nur die zwingend benötigen Daten verlangt und alle weiteren Daten auf freiwilliger Basis erhoben werden. Voreinstellungen und Vorgaben für betroffene Personen sollen möglichst datenschutzfreundlich gestaltet sein.

10.3 Für die im Unternehmen gespeicherten Daten ist festzulegen, für welchen Zeitraum eine Aufbewahrung bzw. Speicherung zu erfolgen hat. Gesetzliche Aufbewahrungspflichten sind hierbei zu beachten. Nach Ablauf der Aufbewahrungsfrist bzw. Speicherdauer ist für eine Löschung der Daten zu sorgen, idealerweise durch ein automatisiertes Verfahren.

10.4 Im Rahmen der Datenverarbeitung ist immer zu überprüfen, ob es zur Erfüllung der vorgesehenen Zwecke ausreichend ist, personenbezogene Daten zu anonymisieren oder zu pseudonymisieren. Bei entsprechenden Maßnahmen ist darauf zu achten, dass bei den entsprechend bearbeiteten Daten für den Empfänger der Daten jedenfalls kein Personenbezug mehr hergestellt werden kann, zumindest nicht mit

verhältnismäßigem Aufwand.

11. Direkterhebung und Information der betroffenen Person

11.1 Personenbezogene Daten sollen aus Transparenzgründen nach Möglichkeit bei der betroffenen Person direkt erhoben werden. Eine Erhebung bei Dritten ist dann in Erwägung zu ziehen, wenn hierfür berechtigte Gründe vorliegen, etwa das Vorgehen im Interesse der betroffenen Person ist oder eine Direkterhebung nur mit unverhältnismäßigem Aufwand möglich wäre.

11.2 Die betroffene Person ist grundsätzlich darüber zu informieren, wenn personenbezogene Daten über sie verarbeitet werden. Im Rahmen der Information sind alle relevanten Details mitzuteilen, die für die betroffene Person und die Ausübung ihrer Betroffenenrechte von Bedeutung sind. Eine gesonderte Information kann unterbleiben, wenn ihr die Datenverarbeitung bekannt ist. Hiervon ist bspw. auszugehen, wenn eine Einwilligung der betroffenen Person eingeholt wurde und die betroffene Person in diesem Zusammenhang vorab informiert wurde.

12. Datenqualität

12.1 Alle Mitarbeiter haben darauf zu achten, dass personenbezogene Daten richtig sind und auf dem neuesten Stand gehalten werden.

12.2 Unzutreffende oder unvollständige Daten sollen berichtigt oder gelöscht werden. Soweit eine betroffene Person die Berichtigung bzw. die Vervollständigung verlangt, ist ihrem berechtigten Verlangen unverzüglich zu entsprechen.

13. Datensicherheit

13.1 Für das Unternehmen ist von großer Bedeutung, dass die Sicherheit der Daten jederzeit gewährleistet ist. Vor diesem Hintergrund sind die Daten u.a. ausreichend gegen Verlust, gegen unbefugten Zugriff und vor anderen Gefahren zu schützen.

13.2 Es ist daher dafür zu sorgen, dass angemessene Maßnahmen getroffen werden, um personenbezogene Daten zu schützen. Der Schutz hat durch technische und organisatorische Maßnahmen zu erfolgen.

13.3 Für die einzelnen Vorgänge der Datenverarbeitung sind die konkreten Schutzmaßnahmen zu dokumentieren und auf ihre Angemessenheit zu überprüfen.

13.4 Die IT-Abteilung kann weitergehende Vorgaben im Interesse der Datensicherheit erlassen, insbesondere in Bezug auf die Nutzung von IT-Systemen im Unternehmen.

III. Spezielle Formen der Datenverarbeitung

14. Werbemaßnahmen

14.1 Im Vorfeld eines Vertrags ist es während der Phase der Vertragsanbahnung zulässig, Daten zur Erstellung von Angeboten, zur Vorbereitung von Vertragsunterlagen und zur Erfüllung sonstiger auf einen Vertragsabschluss gerichteter Wünsche zu verarbeiten.

14.2 Soweit potentielle Kunden eine Einwilligung erteilt haben, können sie auch unter Verwendung der Daten, die sie mitgeteilt haben, kontaktiert werden. Etwaige Einschränkungen des potentiellen Kunden sind hierbei zu beachten.

14.3 Für die Kommunikation während eines laufenden Vertragsverhältnisses mit einem Kunden ist dessen Einwilligung zur Datenverarbeitung nicht erforderlich, soweit die Datenverarbeitung zur Erfüllung der vertraglichen Verpflichtungen erforderlich ist.

15. Erstellung von Nutzerprofilen

15.1 Nutzerprofile mit Personenbezug dürfen nur mit Einwilligung der betroffenen Person oder bei Vorliegen einer gesetzlichen Ermächtigungsgrundlage erstellt werden. Andernfalls ist durch organisatorische und technische Maßnahmen sicherzustellen, dass Nutzerprofile nur ohne Personenbezug erstellt werden.

15.2 Ohne Einwilligung der betroffenen Person und ohne eine besondere Ermächtigungsgrundlage bleiben statistische Auswertungen und Untersuchungen auf Basis anonymisierter oder pseudonymisierter Daten möglich. Soweit jedoch pseudonymisierte Nutzerprofile angelegt werden, muss die betroffene Person hierüber informiert werden und eine Widerspruchsmöglichkeit haben.

16. Verarbeitung besonderer Arten von Daten

16.1 Bei der Verarbeitung von personenbezogenen Daten ist zu berücksichtigen, dass sensible Daten und Daten über besonders schützenswerte betroffene Personen nur bei Vorliegen von zusätzlichen Voraussetzungen und/oder bei Einhaltung besonderer Schutzmaßnahmen verarbeitet werden dürfen.

16.2 Ein besonderer Schutz besteht für Daten über die rassische und ethnische Herkunft, politische Meinungen, religiöse oder weltanschauliche Überzeugungen und die Gewerkschaftszugehörigkeit sowie für genetische Daten, biometrische Daten, Gesundheitsdaten, Daten zum Sexualleben und zur sexuellen Orientierung. Für die Verarbeitung der vorgenannten Kategorien von Daten bedarf es einer gesonderten Rechtfertigung, außerdem sind geeignete Sicherheitsvorkehrungen zu implementieren und zu dokumentieren.

16.3 Finanz- und Kreditinformationen über Mitarbeiter und Kunden sind ebenfalls als sensible Daten anzusehen und sollen den gleichen Schutz genießen. Die vorstehenden Regelungen sollen daher entsprechend für derartige Daten gelten.

16.4 Als besonders schutzbedürftig gelten weiter Daten über strafrechtliche Verurteilungen und Straftaten. Soweit derartige Daten im Unternehmen verarbeitet werden sollen, bedarf dies der vorherigen Prüfung und Freigabe durch den Datenschutzbeauftragten.

16.5 Zusätzlich ist zu beachten, dass auch Minderjährige im Hinblick auf sämtliche personenbezogene Daten besonders schutzbedürftig sind. Maßnahmen zur Datenverarbeitung dürfen sich daher ohne vorherige Prüfung und Freigabe durch den Datenschutzbeauftragten nicht gezielt an Minderjährige richten.

17. Auftragsverarbeitung

17.1 Wenn Dienstleister des Unternehmens in dessen Auftrag personenbezogene Daten verarbeiten, ist zu beachten, dass die gleichen Sorgfaltsanforderungen wie beim Unternehmen auch für den Dienstleister gelten.

17.2 Der Dienstleister wird im Auftrag und auch unter der Verantwortung des Unternehmens tätig. Trotz der Durchführung der Datenverarbeitung durch den Dienstleister bleibt das Unternehmen der Verantwortliche, so dass der Dienstleister sorgfältig auszuwählen ist.

17.3 Spätestens mit Beginn der Tätigkeit für das Unternehmen ist dafür Sorge zu tragen, dass mit dem Dienstleister eine gesonderte Vereinbarung zur Auftragsverarbeitung vereinbart wird und danach eine regelmäßige Kontrolle der Einhaltung der Pflichten aus der Vereinbarung zur Auftragsverarbeitung erfolgt. Abweichungen von der Standardvereinbarung zur Auftragsverarbeitung des Unternehmens sind mit dem Datenschutzbeauftragten abzustimmen.

18. Automatisierte Einzelentscheidungen

18.1 Entscheidungen, die für die betroffene Person rechtliche Folgen nach sich ziehen oder sie erheblich beeinträchtigen können, dürfen nicht ausschließlich auf eine automatisierte Verarbeitung von personenbezogenen Daten gestützt werden. Die automatisierte Datenverarbeitung darf nur als Hilfsmittel für die Entscheidung herangezogen werden, ohne dabei deren einzige Grundlage zu bilden.

18.2 Eine von dem vorstehenden Grundsatz abweichende Handhabung muss entweder für die Erfüllung eines Vertrages mit der betroffenen Person erforderlich oder von einer ausdrücklichen Einwilligung der betroffenen Person abgedeckt sein. Sofern auf dieser Grundlage automatisierte Einzelentscheidungen erfolgen, muss für die betroffene Person die Möglichkeit für eine Nachprüfung bestehen.

19. Übermittlung von Daten

19.1 Die Übermittlung personenbezogener Daten ist ein Fall der Verarbeitung von Daten im Sinne dieser Unternehmensrichtlinie. Auch die Übermittlung ist daher nur mit Einwilligung der betroffenen Person oder aufgrund einer anderen Ermächtigungsgrundlage zulässig.

19.2 Bei der Übermittlung in das Ausland ist zusätzlich zu prüfen, ob hierdurch die Interessen und Rechte der betroffenen Person beeinträchtigt werden. Unproblematisch ist insoweit die Übermittlung in einen Vertragsstaat der Europäischen Union. Bei allen anderen Staaten ist vorab zu prüfen, ob ein vergleichbarer Datenschutzstandard besteht. Ein vergleichbarer Standard kann unter anderem durch den Abschluss zusätzlicher vertraglicher Vereinbarungen erreicht werden, etwa durch Nutzung der EU-Standardvertragsklauseln. Jede Übermittlung von personenbezogenen Daten in einen Staat außerhalb des Europäischen Wirtschaftsraumes ist mit dem Datenschutzbeauftragten abzustimmen.

IV. Innerbetriebliche Prozesse

20. Anforderungen an Mitarbeiter

20.1 Alle Mitarbeiter der Verwaltung und Geschäftsleitung des Unternehmens sind besonders auf das Datengeheimnis zu verpflichten. Sie sind darüber zu belehren, dass es untersagt ist, personenbezogene Daten für private Zwecke zu nutzen, an Unbefugte zu übermitteln oder sie Unbefugten zugänglich zu machen. Die Verpflichtung auf das Datengeheimnis soll mit Beginn der Tätigkeit für das Unternehmen erfolgen. Die Mitarbeiter sind darüber zu belehren, dass die Pflicht zur Wahrung der Vertraulichkeit über das Ende der Tätigkeit für das Unternehmen fortgilt.

20.2 Auch innerhalb des Unternehmens ist darauf zu achten, dass nur die Mitarbeiter Zugriff auf personenbezogene Daten erhalten, die sie zur Erledigung ihrer Aufgaben für das Unternehmen benötigen.

20.3 Alle Mitarbeiter der Verwaltung und Geschäftsleitung sollen zu Beginn ihrer Tätigkeit und nachfolgend regelmäßig in Datenschutzthemen geschult werden.

21. Dokumentationspflichten

21.1 Das Unternehmen führt ein Verzeichnis über die Verfahren des Unternehmens zur Verarbeitung personenbezogener Daten (Verzeichnis der Verarbeitungstätigkeiten), das von dem Datenschutzbeauftragten verwaltet wird.

21.2 Um das Verzeichnis der Verarbeitungstätigkeiten vollständig und aktuell zu halten, haben die Mitarbeiter entsprechend den Vorgaben des Datenschutzbeauftragten alle Verfahren unter Nutzung entsprechender Vordrucke zu melden.

21.3 Bestandteil der Dokumentation ist eine Risikobewertung der einzelnen Verfahren. Abhängig von dem Ergebnis der Risikobewertung ist ergänzend zu der standardmäßigen Dokumentation eine umfassende Datenschutz-Folgenabschätzung unter Mitwirkung des Datenschutzbeauftragten zu erstellen.

22. Einführung neuer Systeme zur Datenverarbeitung

Die Einführung neuer Systeme zur Verarbeitung personenbezogener Daten ist dem Datenschutzbeauftragten vorab mitzuteilen, damit dieser die datenschutzrechtliche Zulässigkeit prüfen kann.

V. Rechte der betroffenen Personen

23. Recht auf Auskunft und Datenübertragbarkeit

23.1 Auf Anfrage ist einer betroffenen Person mitzuteilen, ob von dem Unternehmen personenbezogene Daten zu ihrer Person verarbeitet werden. Sofern dies der Fall ist, hat die betroffene Person einen Anspruch auf Auskunft über die entsprechenden personenbezogenen Daten. Die betroffene Person soll dabei die Art der Daten, zu denen sie eine Auskunft wünscht, näher bezeichnen.

23.2 Die Auskunftserteilung soll in einer für die betroffene Person verständlichen Form und Sprache erfolgen. Bei der Auskunftserteilung sind die vorhandenen personenbezogenen Daten und der Zweck der Speicherung mitzuteilen. Weiter soll, soweit

verfügbar, die Herkunft der Daten erläutert werden. Verpflichtend sind außerdem Angaben zu etwaigen Empfänger der Daten, die Dauer der Speicherung, einer etwaigen automatisierten Entscheidungsfindung sowie Hinweise auf die Betroffenenrechte und das Beschwerderecht bei der Aufsichtsbehörde.

23.3 Neben dem Auskunftsrecht steht der betroffenen Person grundsätzlich auch der Anspruch zu, die zu ihrer Person gespeicherten Daten in strukturierter Form zu erhalten, damit diese von einem anderen Verantwortlichen übernommen werden können. Dieses Recht auf Datenübertragbarkeit bezieht sich aber nur auf solche Daten, die auf Basis einer Einwilligung, zur Erfüllung eines Vertrages oder im Rahmen einer automatisierten Verarbeitung verarbeitet wurden.

23.4 Bei der Auskunftserteilung und Erfüllung des Anspruchs auf Datenübertragbarkeit ist sicherzustellen, dass die Identität der betroffenen Person verifiziert wird. Weiter ist zu beachten, dass im Rahmen der Auskunftserteilung keine personenbezogenen Daten Dritter offenbart werden.

23.5 Über alle Anfragen auf Auskunftserteilung oder Ansprüche auf Datenübertragbarkeit ist der Datenschutzbeauftragte zu informieren, damit dieser die weiteren Aktivitäten koordinieren oder übernehmen kann. Soweit der Datenschutzbeauftragte nicht ausdrücklich die Bearbeitung übernimmt, bleibt die jeweilige Fachabteilung für die Beantwortung der Anfrage zuständig.

23.6 Wenn eine Anfrage nicht umgehend beantwortet bzw. ein Anspruch nicht umgehend erfüllt werden kann, ist der betroffenen Person zumindest eine Zwischeninformation zu übermitteln, in der die voraussichtliche Bearbeitungszeit mitgeteilt werden soll.

24. Löschung und Einschränkung der Verarbeitung

24.1 Bei berechtigtem Ersuchen einer betroffenen Person sind die zu ihrer Person gespeicherten personenbezogenen Daten zu löschen. Ein Ersuchen ist insbesondere berechtigt, wenn keine Grundlage für die Datenverarbeitung besteht oder die Grundlage zwischenzeitlich entfallen ist. Sofern keine Grundlage (mehr) für die Speicherung von personenbezogenen Daten besteht, sind diese unabhängig von einem Ersuchen der betroffenen Person zu löschen.

24.2 Soweit eine Löschung nicht in Betracht kommt, ist zu prüfen, inwieweit zumindest eine Einschränkung der Verarbeitung der personenbezogenen Daten erfolgen kann. Eine Einschränkung der Verarbeitung soll insbesondere bis zur Klärung der Zulässigkeit der weiteren Datenverarbeitung erfolgen. Wenn die betroffene Person die weitere Nutzung ihrer Daten nicht mehr wünscht, ist eine Einschränkung der Verarbeitung in Erwägung zu ziehen, damit die Daten der betroffenen Person im Falle einer neuen Datenerhebung nicht (wieder) genutzt werden.

25. Recht auf Berichtigung

25.1 Unvollständige oder unrichtige personenbezogene Daten sind auf Verlangen der betroffenen Person zu korrigieren. Die Korrektur ist dabei auch im Interesse des Unternehmens, da der gesamte Datenbestand möglichst richtig und von hoher Qualität sein soll.

25.2 Soweit ein Mitarbeiter Kenntnis davon hat, dass bei dem Unternehmen gespeicherte Daten unvollständig und unrichtig sind, soll der Mitarbeiter die jeweilige Fachabteilung hierüber informieren, damit eine Korrektur veranlasst werden kann.

26. Recht auf Widerruf, Widerspruch und Beschwerde

26.1 Eine von einer betroffenen Person erteilte Einwilligung in die Verarbeitung ihrer Daten ist jederzeit frei widerruflich. Die betroffene Person ist auf die Möglichkeit des Widerrufs hinzuweisen. Der Widerruf gilt mit Wirkung für die Zukunft.

26.2 Soweit die Verarbeitung von Daten auf Basis einer gesetzlichen Ermächtigungsgrundlage erfolgt, bedarf es keiner Einwilligung der betroffenen Person. Widerspricht die betroffene Person der Datenverarbeitung, ist zu prüfen, inwieweit auf die Datenverarbeitung zukünftig verzichtet werden kann. Ist dies nicht möglich, ist der betroffenen Person dies entsprechend zu erläutern.

26.3 Die betroffene Person hat das Recht, sich über den Umgang mit ihren personenbezogenen Daten im Unternehmen zu beschweren. Die Beschwerde ist unverzüglich an den Datenschutzbeauftragten weiterzuleiten, sofern sie nicht an ihn direkt gerichtet war. Der Datenschutzbeauftragte wird die Beschwerde beantworten und ggf. angemessene Maßnahmen zur Verbesserung des Datenschutzniveaus vorschlagen.

VI. Zuständigkeit

27. Verantwortung

27.1 In erster Linie sind diejenigen Mitarbeiter für die Einhaltung der Vorgaben dieser Unternehmensrichtlinie verantwortlich, die jeweils mit der Datenverarbeitung betraut sind.

27.2 Alle Mitarbeiter des Unternehmens haben auf die Einhaltung dieser Unternehmensrichtlinie zu achten und auf diese Weise dazu beizutragen, dass in dem gesamten Unternehmen einheitlich hohe Datenschutzstandards etabliert werden.

27.3 Die Führungskräfte des Unternehmens haben darauf zu achten, dass die Mitarbeiter über die Unternehmensrichtlinie informiert werden. Zu der Information gehört auch der Hinweis, dass Verstöße gegen die Vorgaben dieser Unternehmensrichtlinie straf-, haftungs- oder arbeitsrechtliche Konsequenzen nach sich ziehen können.

27.4 Das Unternehmen bleibt gegenüber der betroffenen Person der Verantwortliche im datenschutzrechtlichen Sinne. Der einzelne Mitarbeiter handelt daher für das Unternehmen und hat dessen Vorgaben zu beachten.

28. Datenschutzbeauftragter als Ansprechpartner

28.1 Fragen zu dieser Unternehmensrichtlinie oder dem richtigen Umgang mit personenbezogenen Daten können an den Datenschutzbeauftragten gerichtet werden. Die Kontaktdaten des Datenschutzbeauftragten sind auf unserer Homepage hinterlegt.

28.2 Der Datenschutzbeauftragte koordiniert die datenschutzrechtlichen Aktivitäten des Unternehmens. Er ist u.a. Ansprechpartner für die betroffenen Personen, die mit der

Datenverarbeitung betrauten Mitarbeiter und die Geschäftsführung.

28.3 Der Datenschutzbeauftragte ist auch befugt, die Einhaltung dieser Unternehmensrichtlinie zu prüfen und die Beachtung der gesetzlichen Bestimmungen des Datenschutzrechts zu überwachen. Die entsprechende Überwachungsbefugnis entbindet aber nicht den einzelnen Mitarbeiter von seiner Verantwortung.

28.4 Alle Mitarbeiter haben den Datenschutzbeauftragten bei der Erfüllung seiner Aufgaben und Aktivitäten zu unterstützen. Der Datenschutzbeauftragte kann sich in Erfüllung seiner Aufgaben jederzeit an die Geschäftsführung wenden und seine Anliegen vortragen.

28.5 Bei Bedarf kann der Datenschutzbeauftragte in Ergänzung zu dieser Unternehmensrichtlinie Handlungsempfehlungen zu speziellen Themen herausgeben.

29. Meldung von Verstößen und Zusammenarbeit mit Aufsichtsbehörden

29.1 Die Mitarbeiter haben dem Datenschutzbeauftragten unverzüglich Bericht zu erstatten, wenn sie Kenntnis von einem Verstoß gegen diese Unternehmensrichtlinie oder gesetzliche Bestimmungen haben, die sich auf den Schutz personenbezogener Daten beziehen.

29.2 Eine Information hat bereits dann zu erfolgen, wenn erste Anhaltspunkte oder Verdachtsmomente für einen Datenschutzverstoß vorliegen. Auf diese Weise soll der Datenschutzbeauftragte frühzeitig in die Aufklärung der Angelegenheit eingebunden werden. Weitere Details im Hinblick auf das Verhalten bei möglichen Datenschutzverstößen sind in einem gesonderten Konzept für Datenschutzverstöße definiert.

29.3 Auf Basis der erhaltenen Informationen prüft der Datenschutzbeauftragte, inwieweit eine Informationspflicht gegenüber den Aufsichtsbehörden und den betroffenen Personen besteht.

29.4 Das Unternehmen arbeitet mit den zuständigen Aufsichtsbehörden kooperativ und vertrauensvoll zusammen. Im Falle einer gesetzlichen Auskunftsverpflichtung wird das Unternehmen die geforderten Auskünfte unverzüglich erteilen. Maßnahmen und Feststellungen der Aufsichtsbehörden werden von dem Unternehmen uneingeschränkt akzeptiert, soweit sie rechtmäßig sind. Die Kommunikation mit den Aufsichtsbehörden soll über den Datenschutzbeauftragten erfolgen.

VII. Schlussbestimmungen

30. Publizität

30.1 Diese Unternehmensrichtlinie ist allen Mitarbeitern des Unternehmens in geeigneter Weise zugänglich zu machen, insbesondere über unsere Homepage.

30.2 Eine allgemeine Veröffentlichung dieser Unternehmensrichtlinie ist vorgesehen, da es sich zwar um eine interne Richtlinie des Unternehmens handelt, die Richtlinie jedoch als Aushängeschild unseres Unternehmens dienen soll.

31. Änderungen dieser Unternehmensrichtlinie

31.1 Das Unternehmen behält sich das Recht vor, diese Unternehmensrichtlinie bei Bedarf zu ändern. Eine Änderung kann insbesondere erforderlich werden, um gesetzlichen Vorgaben, bindenden Verordnungen, Forderungen der Aufsichtsbehörden oder unternehmensinternen Verfahren zu entsprechen.

31.2 In regelmäßigen Abständen soll auch geprüft werden, inwieweit technologische Veränderungen eine Anpassung dieser Unternehmensrichtlinie erforderlich machen.