Kreishandwerkerschaft Nordfriesland-Nord
VERSTEHEN | BÜNDELN | HANDELN

ANLAGE 1

Stand: 27.06.2018

Datenschutzleitlinie

Ziel der Datenschutzleitlinie

Die Kreishandwerkerschaft Nordfriesland Nord (im folgenden kurz KH) verpflichtet sich im Rahmen seiner gesellschaftlichen Verantwortung zur Einhaltung von Datenschutzrechten. Diese Datenschutzleitlinie gilt für die KH in Bezug auf die Grundprinzipien zum Datenschutz. Die Wahrung des Datenschutzes ist eine Basis für vertrauensvolle Geschäftsbeziehungen und für die KH als Arbeitgeber.
Die Datenschutzleitlinie schafft eine der notwendigen Rahmenbedingungen für die Datenübermittlung zwischen der KH und Mitgliedern sowie sonstigen Geschäftspartner. Sie gewährleistet das von der Europäischen Datenschutz-Grundverordnung und den nationalen Gesetzten verlangte angemessene Datenschutzniveau.

Geltungsbereich dieser Datenschutzleitlinie

Diese Datenschutzrichtlinie gilt für die Kreishandwerkerschaft Nordfriesland Nord und die ihr angeschlossenen Innungen und Vereine. Diese vorliegende Datenschutzrichtlinie erstreckt sich auf sämtliche Verarbeitungen personenbezogener Daten. Anonymisierte Daten, wie z.B. für statistische Auswertungen unterliegen nicht dieser Datenschutzrichtlinie. Die aktuellste Version dieser Datenschutzrichtlinie kann unter den Datenschutzhinweisen auf der Internetseite der KH, www.handwerknordfriesland.de abgerufen / eingesehen werden.

Geltung staatlichen Rechts

Diese Datenschutzrichtlinie beinhaltet die aktuelle EU – Datenschutz – Grundverordnung, ohne das bestehendes nationales Recht (BDSG –neu-) ersetzt wird. Sie ergänzt das jeweilige nationale Datenschutzrecht.

Prinzipien für die Verarbeitung personenbezogener Daten

1. Rechtmäßigkeit
   Bei der Verarbeitung personenbezogener Daten müssen die Persönlichkeitsrechte des Betroffenen gewahrt werden. Personenbezogene Daten müssen auf rechtmäßig Weise erhoben und verarbeitet werden.
2. Zweckbindung
   Die Verarbeitung der Daten darf lediglich für die Zwecke (eindeutig und legitim) erfolgen, die vor der Erhebung der Daten festgelegt wurde. Nachträgliche Änderung der Zwecke sind nur eingeschränkt möglich und bedürfen einer Rechtfertigung.
3. Transparenz
   Der Betroffene muss über den Umgang mit seinen Daten informiert werden. Grundsätzlich sind personenbezogene Daten bei dem Betroffenen selbst zu erheben. Bei der Erhebung der Daten muss der Betroffene mindestens folgendes erkennen können oder entsprechend informiert werden über:
   - Die Identität der erhobenen Stelle
   - Den Zweck der Datenverarbeitung

- Dritte, an die die Daten ggf. übermittelt werden

4. Datenvermeidung und Datenminimierung
   Vor einer Verarbeitung personenbezogener Daten muss überprüft werden, ob und in welchem Umfang diese notwendig sind, um den mit der Verarbeitung angestrebten Zweck zu erreichen. Personenbezogene Daten dürfen nicht auf Vorrat für potentielle zukünftige Zwecke gespeichert werden, es sein denn, dieses ist durch staatliches Recht vorgeschrieben oder erlaubt.
5. Löschung
   Personenbezogene Daten, die nach Ablauf von gesetzlichen oder Meisterkurs-bezogenen Aufbewahrungsfristen nicht mehr erforderlich sind, müssen gelöscht werden. Bestehen im Einzelfall Anhaltspunkte für schutzwürdige Interessen dieser Dritten, müssen die Daten gespeichert bleiben, bis das schutzwürdige Interesse rechtlich geklärt durch die KH geprüft werden konnte.
6. Sachliche Richtigkeit und Datenaktualität
   Personenbezogene Daten sind richtig, vollständig und - soweit erforderlich – auf dem aktuellen Stand zu speichern. Es sind angemessene Maßnahmen zu treffen, um sicherzustellen, dass nicht zutreffende oder veraltete Daten gelöscht, berichtigt, ergänzt oder aktualisiert werden.
7. Vertraulichkeit und Datensicherheit
   Für personenbezogene Daten gilt das Datengeheimnis. Sie müssen im persönlichen Umgang vertraulich behandelt werden und durch angemessene organisatorische und technische Maßnahmen gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie versehentlichen Verlust, Veränderung oder Zerstörung gesichert werden.

Zuverlässigkeit der Datenverarbeitung

Die Erhebung, Verarbeitung und Nutzung personenbezogener Daten ist nur zulässig, wenn einer der nachfolgenden Erlaubnistatbestände vorliegt. Ein solcher Erlaubnistatbestand ist auch dann erforderlich, wenn der Zweck für die Erhebung, Verarbeitung und Nutzung der personenbezogener Daten gegenüber der ursprünglichen Zweckbestimmung geändert werden soll.

1. Mitglieder-, Interessenten- und Geschäftspartnerdaten
   a. Datenverarbeitung bei Anbahnung, Abschluss und Vertragsende / Kündigung
      Personenbezogene Daten des betroffenen Interessenten, Mitgliedes oder Partners dürfen zur Begründung, zur Durchführung und zum Beendigen eines Vertrages verarbeitet werden. Dieses umfasst auch die Betreuung, sofern dies im Zusammenhang mit dem Vertragszweck steht. Im Vorfeld eines Vertrages ist die Verarbeitung von personenbezogenen Daten zur Erstellung von Angeboten erlaubt. Interessenten dürfen im Vorfeld (Anbahnung) unter Verwendung der Daten Kontaktiert werden, die Sie mitgeteilt haben. Eventuell geäußerte Einschränkungen sind hierbei zu beachten.

   b. Einwilligung in die Datenverarbeitung
      Eine Datenverarbeitung kann aufgrund einer Einwilligung des Betroffenen stattfinden. Vor der Einwilligung muss der Betroffene gemäß IV.3 dieser Datenschutzleitlinie informiert werden. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Unter Umständen, z.B. bei telefonischer Beratung, kann die Einwilligung auch mündlich erteilt werden. Ihre Erteilung muss dokumentiert werden.

c. Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Daten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung erforderlich sein und richten sich nach diesen Rechtsvorschriften.

d. Datenverarbeitung aufgrund berechtigter Interessen
Die Verarbeitung personenbezogener Daten kann auch erfolgen wenn dies zur Verwirklichung eines berechtigten Interesses der KH erforderlich ist. Berechtigte Interessen sind in der Regel rechtliche (z.B. Durchsetzung offener Forderungen) oder wirtschaftliche (z.B. Vermeidung von Vertragsstörungen) Tatbestände. Eine Verarbeitung personenbezogener Daten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Betroffenen an der Verarbeitung überwiegt. Die schutzwürdigen Interessen sind für jeden Einzelfall zu prüfen.

e. Verarbeitung besonders schutzwürdiger Daten
Die Verarbeitung besonders schutzwürdiger personenbezogener Daten darf nur erfolgen, wenn dieses gesetzlich erforderlich ist oder der Betroffene ausdrücklich eingewilligt hat. Die Verarbeitung dieser Daten ist auch dann zulässig, wenn sie zwingend notwendig ist, um rechtliche Ansprüche gegenüber dem Betroffenen geltend zu machen, auszuüben oder zu verteidigen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

f. Nutzerdaten und Internet
Wenn auf Internetseiten personenbezogene Daten erhoben, verarbeitet und genutzt werden, sind die Betroffenen hierüber in Datenschutzhinweisen und ggf. durch Cookie – Hinweisen zu informieren. Die Datenschutzhinweisen und ggf. Cookie – Hinweisen sind so zu integrieren, dass diese durch die Betroffenen leicht erkennbar, unmittelbar erreichbar und ständig verfügbar sind.

2. Mitarbeiterdaten
   a. Datenverarbeitung für das Arbeitsverhältnis
   Für das Arbeitsverhältnis dürfen die personenbezogenen Daten verarbeitet werden, die für eine Begründung , Durchführung und Beendigung des Arbeitsvertrages erforderlich sind. Bei der Anbahnung eines Arbeitsverhältnisses dürfen personenbezogene Daten von Bewerbern verarbeitet werden. Nach Ablehnung sind die Daten des Bewerbers unter Berücksichtigung beweisrechtlicher Fristen zu löschen, es sei denn, der Bewerber hat in einer weiteren Speicherung für ein späteren Auswahlprozess eingewilligt. Eine Einwilligung ist auch für eine Verwendung der Daten für weitere Bewerbungsverfahren erforderlich.
   Im bestehenden Arbeitsverhältnis muss die Datenverarbeitung immer auf den Zweck des Arbeitsvertrages bezogen sein. Für Verarbeitungen von personenbezogenen Daten, die im Kontext des Arbeitsverhältnisses stehen, jedoch nicht di-

rekt der Erfüllung des Arbeitsvertrages dienen, muss jeweils eine rechtliche Legitimation vorliegen. Dieses können gesetzliche Anforderungen oder eine Einwilligung des Mitarbeiters oder die berechtigten Interessen des Unternehmens sein.

b. Datenverarbeitung aufgrund gesetzlicher Erlaubnis
Die Verarbeitung personenbezogener Mitarbeiterdaten ist auch dann zulässig, wenn staatliche Rechtsvorschriften die Datenverarbeitung verlangen, voraussetzen oder gestatten. Die Art und der Umfang der Datenverarbeitung müssen für die gesetzlich zulässige Datenverarbeitung zulässig sein und richten sich nach diesen Rechtsvorschriften. Besteht ein gesetzlicher Handlungsspielraum, müssen schutzwürdigen Interessen des Mitarbeiters berücksichtigt werden.

c. Einwilligung in die Datenverarbeitung
Eine Verarbeitung von Mitarbeiterdaten kann aufgrund einer Einwilligung des Betroffenen stattfinden. Einwilligungserklärungen müssen freiwillig abgegeben werden. Unfreiwillige Erklärungen sind unwirksam. Die Einwilligungserklärung ist aus Beweisgründen grundsätzlich schriftlich oder elektronisch einzuholen. Erlauben es die Umstände diese ausnahmeweise nicht, kann die Einwilligung mündlich erteilt werden. Ihre Erteilung ist auf alle Fälle sorgfältig zu dokumentieren. Bei einer informierten freiwilligen Angabe von Daten durch den Betroffenen kann eine Einwilligung angenommen werden, wenn nationales Recht keine explizite Einwilligung vorschreibt. Vor der Einwilligung muss der Betroffene gemäß IV.3 dieser Datenschutzlinie informiert werden.

d. Datenverarbeitung aufgrund berechtigten Interesses
Die Verarbeitung von personenbezogenen Mitarbeiterdaten kann auch erfolgen, wenn diese zur Verwirklichung eines berechtigten Interesses der KH erforderlich ist. Berechtigte Interessen sind in der Regel rechtlich (Geltend machen, Ausüben oder Verteidigen von rechtlichen Ansprüchen) oder wirtschaftlich (z.B. Bewerten eines Mitarbeiters) begründet. Eine Verarbeitung von personenbezogenen Mitarbeiterdaten aufgrund eines berechtigten Interesses darf nicht erfolgen, wenn es im Einzelfall einen Anhaltspunkt dafür gibt, dass schutzwürdige Interessen des Mitarbeiters das Interesse an der Verarbeitung überwiegen. Das Vorliegen schutzwürdiger Interessen ist für jede Verarbeitung zu prüfen.
Kontrollmaßnahmen, die eine Verarbeitung von Mitarbeiterdaten erfordern, dürfen nur durchgeführt werden, wenn eine gesetzliche Verpflichtung besteht oder ein begründeter Anlass gegeben ist. Auch beim Vorliegen eines begründeten Anlasses muss die Verhältnismäßigkeit der Kontrollmaßnahme geprüft werden. Die berechtigten Interessen des Unternehmens an der Durchführung der Kontrollmaßnahmen müssen gegen ein mögliches schutzwürdiges Interesses des von der Maßnahme betroffenen Mitarbeiters am Ausschluss der Maßnahme abgewogen werden und dürfen nur durchgeführt werden, wenn sie angemessen sind. Das berechtigte Interesse des Unternehmens und die möglichen schutzwürdigen Interessen des Mitarbeiters müssen vor jeder Maßnahme festgestellt und dokumentiert werden. Zudem dürfen ggf. nach staatlichen Recht bestehende weiter Anforderungen (z.B. Informationsrechte des Betroffenen) berücksichtigt werden.

e. Verarbeitung besonders schutzwürdiger Daten

Besonders schutzwürdige personenbezogene Daten dürfen nur unter bestimmten Voraussetzungen verarbeitet werden. Besonders schutzwürdige Daten sind Daten über rassische und ethnische Herkunft, über politische Meinungen, über religiöse und philosophische Überzeugungen, über Gewerkschaftszugehörigkeit oder über die Gesundheit oder das Sexualleben des Betroffenen. Aufgrund staatlichen Rechts können weitere Datenkategorien als besonders schutzwürdig eingestuft werden und der Inhalt dieser Datenkategorien unterschiedlich ausgefüllt sein. Ebenso dürfen Daten, die Straftaten betreffen, häufig nur unter besonderen, von staatlichen Recht aufgestellten Voraussetzungen verarbeitet werden. Die Verarbeitung muss aufgrund staatlichen Rechts ausdrücklich erlaubt oder vorgeschrieben sein. Zusätzlich kann eine Verarbeitung erlaubt sein, wenn sie notwendig ist, damit die Verantwortlichen Stelle ihren Rechten und Pflichten auf dem Gebiet des Arbeitsrecht nachkommen kann. Der Mitarbeiter kann freiwillig auch ausdrücklich in der Verarbeitung einwilligen. Wird die Verarbeitung besonders schutzwürdiger Daten geplant, ist der Datenschutzbeauftragte im Vorfeld zu informieren.

f. Telekommunikation und Internet
Telefonanlagen, Email-Adressen, Intranet und Internet sowie soziale Netzwerke (wenn genutzt) werden in erster Linie im Rahmen der betrieblichen Aufgabenstellung durch das Unternehmen zur Verfügung gestellt. Sie sind Arbeitsmittel und Unternehmensressource. Sie dürfen im Rahmen der jeweils geltenden Rechtsvorschriften und der unternehmensinternen Richtlinien genutzt werden. Eine generelle Überwachung der Telefon- und Email-Kommunikation, bzw. der Internetnutzung findet nicht statt. Zur Abwehr von Angriffen auf die IT-Infrastruktur können Schutzmaßnahmen implementiert werden, die schadhafte Inhalte blockieren.

3. Übermittlung personenbezogener Daten
Eine Übermittlung personenbezogener Daten an Empfänger außerhalb des Unternehmens unterliegt den Zulässigkeitsvoraussetzungen der Verarbeitung personenbezogener Daten unter Abschnitt 2. Der Empfänger der Daten muss darauf verpflichtet werden, diese nur zu den festgelegten Zwecken zu verwenden.
Im Falle einer Datenübermittlung von Dritten an die KH muss ebenfalls sichergestellt sein, dass die Daten für die vorgesehenen Zwecke verwendet werden dürfen.

4. Auftragsdatenverarbeitung
Eine Auftragsdatenverarbeitung liegt vor, wenn ein Auftragsnehmer mit der Verarbeitung personenbezogener Daten beauftragt wird, ohne das ihm die Verantwortung für die den zugehörigen Geschäftsprozess übertragen wird. In diesen Fällen ist mit externen Auftragnehmern eine Vereinbarung über eine Auftragsdatenverarbeitung abzuschließen. Dabei behält das beauftragende Unternehmen die Verantwortung für die korrekte Durchführung der Datenverarbeitung.
Der Auftragnehmer darf personenbezogene Daten nur im Rahmen der Weisungen des Auftraggebers verarbeiten. Bei der Erteilung des Auftrages sind die nachfolgenden Vorgaben einzuhalten – der beauftragende Fachbereich muss ihre Umsetzung sicherstellen.

1. Der Auftragnehmer ist nach seiner Eignung zur Gewährleistung der erforderlichen technischen und organisatorischen Schutzmaßnahmen auszuwählen. Der Auftragnehmer hat die Sicherheit gem. Art. 28 Abs.3 c, sowie Art. 32 DS-GVO insbesondere in Verbindung mit Art. 5 Abs. 1 , Abs. 2 DS-GVO herzustellen.

2. Der Auftrag ist in Textform zu erteilen. Dabei sind die Weisungen zur Datenverarbeitung und die Verantwortlichkeiten des Auftraggebers und des Auftragnehmers zu dokumentieren.
3. Der Auftraggeber muss sich vor Beginn der Datenverarbeitung von der Einhaltung der Pflicht des Auftragnehmers überzeugen. Die Einhaltung der Anforderungen an die Datensicherheit kann ein Auftragnehmer insbesondere durch Vorlage einer geeigneten Zertifizierung nachweisen. Je nach Risiko der Datenverarbeitung ist die Kontrolle ggf. während der Vertragslaufzeit regelmäßig zu wiederholen.
4. An zahlreichen Stellen der DS-GVO finden sich Hinweise auf eine „Selbstständige datenschutzrechtliche Pflicht“, welche sich ebenfalls an den Auftragsnehmer richten. (Art. 30 Abs. 2/ Art. 31 / Art. 32 Abs. 1 / Art. 44 DS-GVO

Rechte des Betroffenen

Jeder Betroffene kann die folgenden Rechte wahrnehmen. Ihre Geltendmachung ist umgehend durch den verantwortlichen Bereich zu Bearbeiten und darf für den Betroffenen zu keinerlei Nachteilen führen. Folgendes ist zu beachten:

1. Informationsrecht – Offenlegung
   a. Name und Kontaktdaten des Verantwortlichen (ggf. Vertreters)
   b. Kontaktdaten des Datenschutzbeauftragten
   c. Zweck und Rechtsgrundlage der Verarbeitung
   d. Berechtigtes Interesse (bei Verarbeitung nach Art. 6 DS-GVO [*Rechtmäßigkeit*])
   e. Empfänger bzw. Kategorien von Empfängern
   f. Übermittlung in Drittland oder an internationalen Organisationen
   g. Dauer der Speicherung
   h. Bestehen eines Rechtes auf Auskunft, Berichtigung, Löschung, Wiederspruch
   i. Bestehen eines Rechts auf Wiederspruch der Einwilligung
   j. Bestehen eines Beschwerderechts bei der Aufsichtsbehörde
   k. Information, ob die Bereitstellung der Daten gesetzlich oder vertraglich vorgeschrieben oder für ein Vertragsabschluss erforderlich ist
   l. Bestehen einer automatisierten Entscheidungsfindung einschließlich *profiling*
   m. Information über eine mögliche Zweckänderung der Datenverarbeitung

2. Auskunftsrecht
   a. Zwecke der Datenverarbeitung
   b. Kategorien der Daten
   c. Empfänger oder Kategorien von Empfängern
   d. Dauer der Speicherung
   e. Recht auf Berichtigung, Löschung und Wiederspruch
   f. Beschwerderecht bei einer Aufsichtsbehörde
   g. Herkunft der Daten, wenn nicht beim Betroffenen erhoben
   h. Bestehen einer automatisierten Entscheidungsfindung einschließlich *profiling*
   i. Übermittlung in Drittland oder an internationale Organisationen

3. Vertraulichkeit der Verarbeitung
   Personenbezogene Daten unterliegen dem Datengeheimnis. Eine unbefugte Erhebung , Verarbeitung oder Nutzung ist den Mitarbeitern untersagt. Unbefugt ist jede

Verarbeitung, die ein Mitarbeiter vornimmt, ohne damit im Rahmen der Erfüllung seiner Aufgaben betraut oder entsprechend berechtigt zu sein. Mitarbeiter dürfen nur Zugang zu personenbezogenen Daten erhalten, wenn und soweit dies für ihre jeweilige Aufgaben erforderlich ist. Dies erfordert die sorgfältige Aufteilung und Trennung von Rollen und Zuständigkeiten, sowie deren Umsetzung und Pflege im Rahmen der Berechtigungskonzepte.
Mitarbeiter dürfen personenbezogene Daten nicht für eigene private Zwecke oder wirtschaftliche Zwecke nutzen, an Unbefugte übermitteln oder diese auf andere Weise zugänglich machen. Die Geschäftsleitung hat die Mitarbeiter bei Beginn des Beschäftigungsverhältnisses über die Pflicht zur Wahrnehmung des Datengeheimnisses unterrichtet. Diese Verpflichtung besteht auch nach Beendigung des Beschäftigungsverhältnisses fort.

4. Sicherheit der Verarbeitung
   Personenbezogene Daten sind jederzeit gegen unberechtigten Zugriff, unrechtmäßige Verarbeitung oder Weitergabe, sowie gegen den Verlust, Verfälschung oder Zerstörung zu schützen. Dies gilt unabhängig davon ob die Datenverarbeitung elektronisch oder in Papierform erfolgt. Vor der Einführung neuer Verfahren der Datenverarbeitung, insbesondere neuer IT – Systeme, sind technische und organisatorische Maßnahmen zum Schutz personenbezogener Daten festzulegen und umzusetzen. Diese Maßnahmen haben sich am Stand der Technik, den von der Verarbeitung ausgehenden Risiken und dem Schutzbedarf zu orientieren. Die technisch – organisatorischen Maßnahmen zum Schutz personenbezogener Daten sind Teil des Informationssicherheitsmanagement und müssen kontinuierlich an den technischen Entwicklungen angepasst werden.

5. Datenschutzkontrolle
   Die Einhaltung der Richtlinien zum Datenschutz und der geltenden Datenschutzgesetze muss regelmäßig durch Datenschutzaudits und weitere Kontrollen überprüft werden. Die Durchführung obliegt dem Datenschutzbeauftragten und weitere mit Auditrechten ausgestattete Bereich im Unternehmen.
   Die Ergebnisse der Datenschutzkontrollen sind dem Datenschutzbeauftragten mitzuteilen. Der Geschäftsführer ist über wesentliche Ergebnisse zu informieren. Die zuständige Datenschutzbehörde kann im Rahmen der ihr nach dem staatlichen Recht zustehenden Befugnisse auch eigene Kontrollen der Einhaltung der Vorschriften dieser Leitlinie durchführen.

6. Datenschutzvorfälle
   Jeder Mitarbeiter soll dem Datenschutzbeauftragten unverzüglich Fälle von Verstößen gegen diese Datenschutzrichtlinie oder anderen Vorschriften zum Schutz personenbezogener Daten melden. Die verantwortliche Führungskraft ist verpflichtet, den zuständigen Datenschutzbeauftragten umgehend über Datenschutzvorfälle zu unterrichten.
   In Fällen von
   a. Unrechtmäßiger Übermittlung von personenbezogener Daten an Dritte
   b. Unrechtmäßigem Zugriff durch Dritte auf personenbezogene Daten, oder
   c. bei Verlust personenbezogener Daten

7. Verantwortlichkeiten

Die Geschäftsleitung der KH ist verantwortlich für die Datenverarbeitung. Damit ist sie verpflichtet sicherzustellen, dass die gesetzlichen und die in der Datenschutzlinie enthaltenen Anforderungen des Datenschutzes berücksichtigt werden (z.B. nationale Meldepflichten). Es ist eine Management Aufgabe der Führungskraft, durch organisatorische, personelle und technische Maßnahmen eine ordnungsgemäße Datenverarbeitung unter Beachtung des Datenschutzes umzusetzen und sicherzustellen. Die Umsetzung dieser Vorgaben liegt in der Verantwortung der zuständigen Mitarbeiter. Bei Datenschutzkontrollen durch Behörden ist der Datenschutzbeauftragte umgehend zu informieren.
Die Geschäftsleitung ist verpflichtet, den Datenschutzbeauftragten in seiner Tätigkeit zu unterstützen. Die für Geschäftsprozesse und Projekte fachliche Verantwortlichen (Fachbereichsleiter) müssen den Datenschutzbeauftragten rechtzeitig über neue Verarbeitung personenbezogener Daten informieren. Bei Datenschutzverarbeitungsvorhaben, aus denen sich besondere Risiken für Persönlichkeitsrechte der Betroffenen ergeben können, ist der Datenschutzbeauftragte schon vor Beginn der Verarbeitung zu beteiligen. Dies gilt insbesondere für besonders schutzwürdige personenbezogene Daten. Der Geschäftsführer muss sicherstellen, dass die Mitarbeiter im erforderlichen Umfang zum Datenschutz geschult werden. Eine missbräuchliche Verarbeitung personenbezogener Daten oder anderer Verstöße gegen das Datenschutzrecht werden in vielen Staaten auch strafrechtlich verfolgt und können Schadensersatzansprüche nach sich ziehen Zuwiderhandlungen, für die einzelne Mitarbeiter verantwortlich sind, können zu arbeitsrechtliche Sanktionen führen.

8. Der Datenschutzbeauftragte

Der Datenschutzbeauftragte als internes, fachliches weisungsunabhängiges Organ wirkt auf die Einhaltung der nationalen und internationalen Datenschutzvorschriften hin. Er ist verantwortlich für die Richtlinien zum Datenschutz und überwacht Deren Einhaltung. Der Datenschutzbeauftragte wurde von der Geschäftsleitung der Kreishandwerkerschaft Nordfriesland Nord bestellt.
Jeder Betroffene kann sich mit Anregungen, Anfragen, Auskunftsersuchen oder Beschwerden im Zusammenhang mit Fragen des Datenschutzes oder der Datensicherheit an den Datenschutzbeauftragten wenden. Anfragen und Beschwerden werden vertraulich behandelt.
Kann der Datenschutzbeauftragte einer Beschwerde nicht abhelfen oder einen Verstoß gegen die Datenschutzleitlinie nicht abstellen, muss zur Abhilfe der Datenschutzverletzung die Aufsichtsbehörde eingeschaltet werden. Anfragen an die zuständige Aufsichtsbehörde sind immer dem Datenschutzbeauftragten zur Kenntnis zu bringen. Der Datenschutzbeauftragte kann wie folgt erreicht werden:

Herr
Jens Kardel
Op’n Holm 2
25764 Reinsbüttel

datenschutz@kh-nf.de