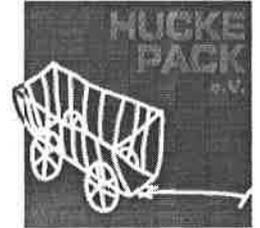


Anlage 1

Merkblatt zum Datenschutz im Huckepack e.V.



Im Rahmen Ihrer dienstlichen Tätigkeit werden Sie zwangsläufig auch Umgang mit personenbezogenen Daten haben, weil Sie bei der Verarbeitung (z.B. in Form des Erfassens, Speicherns, Veränderns, Weitergebens, Löschens oder Vernichtens) oder bei der Nutzung (z.B. Auswertung) solcher Daten mitwirken oder weil Ihnen solche Angaben während Ihrer Tätigkeit zur Kenntnis gelangen.

Rechtsgrundlagen:

EU-Datenschutz-Grundverordnung (EU-DSGVO) und Bundesdatenschutzgesetz (BDSG)

Personenbezogene Daten sind Angaben zum Sein (z.B. Name, Geburtstag, Anschrift, Beruf, Familienstand) oder Haben (z.B. Grundbesitz, Rechtsbeziehungen zu Dritten, Steuermerkmale, Schulden, Vorstrafen) natürlicher Personen (bestimmter oder durch Referenzen bestimmbarer Betroffener, z.B. Klient, Angehöriger, Mitarbeiter). Sozialdaten und Angaben über die rassische und ethnische Herkunft, politische Meinungen, religiöse und weltanschauliche Überzeugungen, Gewerkschaftszugehörigkeit, Gesundheit oder das Sexualleben sind **besondere Arten personenbezogener Daten**, bei deren Erhebung, Verarbeitung und Nutzung **besondere Sorgfalt** zu üben ist.

Datenschutz hat den Einzelnen vor Verletzung seiner Persönlichkeitsrechte beim Umgang mit seinen personenbezogenen Daten zu schützen. Der Datenschutz ist zu beachten, unabhängig davon, ob die Daten maschinell oder auf herkömmliche Art (auf Papier z.B. in Karteien, Akten) verarbeitet oder genutzt werden.

Bereits die Unterzeichnung des Arbeitsvertrages verpflichtet zur Verschwiegenheit über die bei der Ausübung der Tätigkeit bekannt gewordenen Angelegenheiten, soweit dies ihrer Natur nach erforderlich oder durch Rechtsvorschrift oder durch dienstliche Weisung angeordnet ist. Das Datenschutzrecht geht weiter. Jeder, der Umgang mit personenbezogenen Daten hat, ist zum datenschutzgerechten Verhalten verpflichtet, d.h. zur Einhaltung des Datengeheimnisses. Deshalb dürfen die Daten nicht unbefugt (d.h. nicht ohne gesetzliche Legitimation bzw. Einwilligung des Betroffenen oder dessen gesetzlichen Vertreter) erhoben, verarbeitet oder genutzt werden (**Datengeheimnis/Sozialgeheimnis**). Damit ist jedes Beschaffen von Daten auf unrechtmäßige Weise (z.B. ohne Einbeziehung des Betroffenen oder auf Vorrat eine Verletzung des Datengeheimnisses; ebenso jede Weitergabe von Daten, die nicht gesetzlich oder durch Einwilligung abgedeckt ist, sowie das Zerstören von Daten vor Ablauf der Aufbewahrungsfrist. Verletzungen des Datengeheimnisses, also ein Verstoß gegen die Vertraulichkeit, Integrität (Richtigkeit) und Verfügbarkeit der Daten können – je nach Abhängigkeit vom Verschulden - Schadenersatzansprüche des Arbeitgebers oder Dritter begründen und disziplinarische Maßnahmen (bis zur fristlosen Kündigung) oder sogar strafrechtliche Verantwortung zur Folge haben.

Die Verpflichtung zur Wahrung des Datengeheimnisses bleibt auch nach Beendigung der Tätigkeit bestehen.

Die Wahrung des Datengeheimnisses erfordert ein verantwortliches Handeln beim Umgang mit personenbezogenen Daten und die risikobewusste Nutzung der Informations- und Kommunikationstechnik. Fehlverhalten kann zu materiellen und ideellen Schäden mit teilweise beträchtlichen negativen Effekten für den Huckepack e.V. führen.

Die zur Einhaltung des Datenschutzes und zur Sicherung der Daten gegen Verlust oder vor unbefugtem Zugriff erlassenen technischen und organisatorischen Maßnahmen und Dienstanweisungen sind von jedem Mitarbeiter zu beachten. Informieren Sie sich über die Regelungen und machen Sie sich damit vertraut.

Die Teilnahme an den regelmäßig angebotenen Datenschutzs Schulungen ist verpflichtend.

Sie sind verantwortlich,

- dass die in Ihrer Zuständigkeit befindlichen Daten keinem Unbefugten zugänglich sind. Unbefugt ist jede Person, die Ihre mit einer Sicherheitsmaßnahme (Schlüssel, Passwort, Schreib- und Leserecht) gesicherten Daten nicht zur Kenntnis nehmen darf, weil sie die Daten zur Aufgabenerfüllung nicht benötigt.

Deshalb sind

- die Ihnen anvertrauten Daten, Datenträger und Ausdrücke bei Abwesenheit unter Verschluss zu halten (Zugangskontrolle). Das schließt das Sperren des PCs bei Abwesenheit vom Arbeitsplatz ein (z.B. kennwortgeschützter Bildschirmschoner). Auch offene - von allen verlassene - Räume sind ein Verstoß gegen die Zugangskontrolle.
- Passworte sind absolut geheim zu halten nach Vorgabe IT regelmäßig zu wechseln.
Eine Weitergabe auch im Vertretungsfall ist streng untersagt.
- Daten und Datenträger, die zur Erfüllung der zugewiesenen Aufgabe und für gesetzlich vorgeschriebene Nachweise nicht mehr erforderlich sind, sind so zu vernichten, dass eine weitere oder missbräuchliche Verwendung nicht möglich ist (z.B. Papier schreddern bzw. in die dafür vorgesehene Aktenvernichtung entsorgen; Datenträger sind an den Bereich EDV abzugeben, werden dort ordnungsgemäß gelöscht und dann über ein entsprechendes zertifiziertes Unternehmen zerstört und entsorgt). Möglich ist auch die Übernahme in ein den entsprechenden Vorschriften genügendes Archiv.
- Laptops und andere bewegliche datenverarbeitende Geräte bei Außer-Haus-Tätigkeit sorgfältig zu sichern, besonders im Auto, in Verkehrsmitteln, auf Veranstaltungen sowie im Hotel. Es gilt die Nutzungsvereinbarung Telearbeit/Homeoffice. Das Sicherungsgebot gilt auch für Datenträger und Papierunterlagen/Akten.
- dass vertrauliche Informationen nicht ungesichert per Fax verschickt werden. Ist in Ausnahmefällen ein Fax-Versand aufgrund der Eilbedürftigkeit erforderlich, müssen besondere Vorkehrungen (z.B. telefonische Absprache, Doppelkontrolle der Richtigkeit der eingegebenen Fax-Nummer) getroffen werden.
- dass per ungesicherter E-Mail (ohne Verschlüsselungsverfahren) nur versandt wird, was auch auf einer herkömmlichen (offenen) Postkarte mitgeteilt werden darf. Es sei denn, es steht kein alternativer Kommunikationsweg zur Verfügung oder der Betreffende erklärt dazu sein Einverständnis.
- dass vertrauliche Telefonate (insbesondere vom Handy) nicht in der Öffentlichkeit (z.B. im Zug) oder im Beisein Dritter geführt werden.

- dass die Nutzung dienstlicher IT-Einrichtungen und Mobilgeräte zu privaten Zwecken untersagt ist. Es gelten die Nutzungsvereinbarung E.-Mail/Internet und die Nutzungsvereinbarung Smartphones.
- dass Auskünfte aus Datensammlungen (Akten, Dateien, etc.) nur erteilt sowie Vervielfältigungen angefertigt bzw. weitergegeben werden, wenn eine Rechtsvorschrift das erlaubt oder die betroffene Person eingewilligt hat.

Datenschutz beinhaltet auch den Schutz vor vorsätzlichem oder ungewolltem Verändern und/oder Löschen der Daten, z.B. durch Missbrauch sowie durch Bedienfehler oder technische Veränderungen (was auch durch nichtkompatible Software geschehen kann). Es ist daher untersagt, private Software und Datenträger unkontrolliert in die Dienststelle einzubringen. Ebenso ist - soweit nicht ausdrücklich erlaubt - untersagt, Geräte der Dienststelle privat zu nutzen.

Falls Sie sich als Betroffener in Ihren Datenschutzrechten verletzt sehen oder sonstige Fragen bei der Anwendung der Datenschutzvorschriften haben, können Sie sich jederzeit - ohne Benachteiligungen zu fürchten - an den zuständigen Datenschutzbeauftragten wenden.

Ihr zuständiger betrieblicher Datenschutzbeauftragter ist: Hermann J. Janz
Der Datenschutzbeauftragte ist unter jc@jcdatenschutz.de per E-Mail zu erreichen.

Datenschutz-Koordinatorin im Huckepack ist Viktoria Zumpe: viktoria.zumpe@huckepack-ev.de.