Merkblatt zum Datenschutz

Mit diesem Merkblatt möchten wir Ihnen die wesentlichen Grundsätze des Datenschutzes erläutern, Sie über Ihre Rechte informieren und Sie bei der Einhaltung des Datenschutzes und der Vertraulichkeit unterstützen.

1. Was ist der Zweck des Datenschutzes?

Datenschutz ist ein Grundrecht. Es schützt den Bürger vor der Verletzung seiner Persönlichkeitsrechte. Jeder hat grundsätzlich das Recht, über die Erfassung und Verarbeitung seiner Daten selbst entscheiden zu können.

Datenschutzrechtliche Vorgaben, insbesondere das Kirchengesetz über den Datenschutz der Evangelischen Kirche in Deutschland (nachfolgend DSG-EKD abgekürzt) untersagen es, personenbezogene Daten unbefugt zu verarbeiten. Gesetze können den Umgang mit personenbezogenen Daten aber auch erlauben.

Was personenbezogene Daten sind, ist in § 4 Nr. 1 DSG-EKD definiert. Darunter fallen etwa Namen, Kontaktdaten, Bankverbindung oder Angaben über den Gesundheitszustand einer Person. Daten über juristische Personen (z.B. Firmenadressen) unterfallen nicht dem Datenschutz – hier gelten aber andere Geheimhaltungspflichten, z.B. aus dem Bürgerlichen Gesetzbuch, der Gewerbeordnung, dem Wettbewerbs- und Strafrecht sowie arbeitsvertraglichen Regelungen zum Geschäftsgeheimnis.

2. Wann dürfen personenbezogene Daten verarbeitet werden?

Gemäß § 5 Abs. 1 Nr. 1 DSG-EKD müssen personenbezogene Daten auf **rechtmäßige Weise** und in einer für die betroffene Person **nachvollziehbaren Weise** verarbeitet werden. Nach § 5 Abs. 1 Nr. 1 DSG-EKD müssen personenbezogene Daten zudem in einer Weise verarbeitet werden, die eine angemessene **Sicherheit** der personenbezogenen Daten gewährleistet, einschließlich dem Schutz vor **unbefugter oder unrechtmäßiger Verarbeitung** und vor unbeabsichtigtem **Verlust**, unbeabsichtigter **Zerstörung** oder unbeabsichtigter **Schädigung** durch geeignete technische und organisatorische Maßnahmen („Integrität und Vertraulichkeit“).

Personenbezogene Daten dürfen nach § 6 DSG-EKD nur verarbeitet werden, wenn das DSG-EKD oder eine andere kirchliche oder staatliche Rechtsvorschrift die Datenverarbeitung erlaubt oder anordnet, dies aufgrund einer Einwilligung, zur Erfüllung eines Vertrages, zur Erfüllung einer rechtlichen Verpflichtung, um lebenswichtige Interessen zu schützen, aufgrund einer Aufgabe im kirchlichen Interesse oder in Ausübung der übertragenen öffentlichen Gewalt erfolgt oder wenn die Verarbeitung nach einer Abwägung zur Wahrung berechtigter Interessen erforderlich ist.

Dies ist in der Regel gegeben, wenn Sie die Daten zur Erfüllung der Ihnen übertragenen Aufgaben verarbeiten, beispielsweise Personaldaten in der Personalabteilung oder Daten von Vertragspartnern im Rahmen eines Vertragsverhältnisses. Eine Erlaubnis liegt auch vor, wenn die betroffene Person eine freiwillige, wirksame und (i.d.R.) schriftliche Einwilligung in die konkrete Datenverarbeitung abgegeben hat.

Jede unbefugte Verarbeitung für andere Zwecke ist untersagt.

Sollten Sie unsicher sein, ob ein konkreter Datenverarbeitungsvorgang zulässig ist, sprechen Sie Vorgesetzte oder den örtlich Beauftragten für den Datenschutz (Kontaktdaten am Ende des Merkblattes) an. Diese Verpflichtung besteht nach Beendigung der Tätigkeit fort, d.h. auch wenn Sie unsere Einrichtung verlassen haben, sind Sie nach wie vor verpflichtet, über die verarbeiteten Daten Stillschweigen zu bewahren.

3. Welche Rechte haben betroffene Personen?

Die betroffenen Personen (z.B. Studierende, Mitarbeiter, Ehrenamtliche) haben das Recht auf Auskunft über die zu ihrer Person gespeicherten Daten. In bestimmten Fällen können sie auch eine Berichtigung, Löschung, Einschränkung der Verarbeitung, die Übertragung ihrer Daten verlangen oder einer Datenverarbeitung widersprechen. Eine Berichtigung kommt etwa in Betracht, wenn die Daten unrichtig sind. Daten sind zwingend zu löschen, wenn der Rechtsgrund für die Erhebung bzw. Speicherung nicht (mehr) besteht und keine gesetzliche Aufbewahrungspflicht besteht.

Voraussetzung hierfür ist, dass die betroffene Person weiß, wo, welche und wofür Daten gespeichert und genutzt werden. Deshalb ist die betroffene Person von dem Verantwortlichen (die Einrichtung) bei erstmaliger Speicherung ihrer Daten über die Datenverarbeitung genau zu informieren. Die Datenschutzrechte der betroffenen Personen sind vielfältig und ihnen muss spätestens innerhalb eines Monats nach Eingang des Antrages nachgekommen werden. Ansprechpartner für Fragen zum Datenschutz ist der örtlich Beauftragte für den Datenschutz. Betroffene Personen haben aber auch die Möglichkeit, sich an die Aufsichtsbehörde zu wenden.

Sie sind nicht nur verpflichtet, diese Rechte anderer zu wahren, sondern können sich auch selbst als Beschäftigter auf diese Rechte berufen.

4. Sanktionen bei Datenschutzverstößen

Verstöße gegen den Datenschutz können mit sehr hohen Bußgeldern sowie Geld- oder Freiheitsstrafen geahndet werden. So sieht etwa § 45 Abs. 5 DSG-EKD Sanktionen bis zu 500.000 € für Einrichtungen, die am Wettbewerb teilnehmen, vor. Ferner kann die Aufsichtsbehörde in Fällen von Datenschutzverletzungen auch Bußgelder gegenüber Beschäftigten einer Einrichtung erlassen.

Eine Verletzung des Datenschutzes durch Mitarbeiter stellt in den meisten Fällen einen Verstoß gegen arbeitsvertragliche Pflichten dar und kann arbeitsrechtliche Maßnahmen - von der Abmahnung bis hin zur Kündigung - zur Folge haben. Bei Vorsatz und grober Fahrlässigkeit ist zudem ein Regress möglich. Ebenso kommt eine Strafbarkeit nach den Vorschriften des Strafgesetzbuches (StGB) oder nach § 17 des Gesetzes gegen den unlauteren Wettbewerb (UWG) in Betracht.

Bitte gehen Sie daher mit personenbezogenen Daten sorgsam um.

5. So machen Sie im Datenschutz alles richtig

Hier haben wir Tipps für Sie, wie Sie in Sachen Datenschutz alles richtig machen:

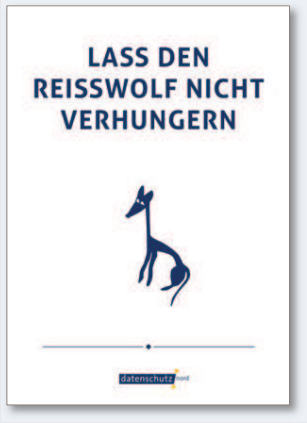
Vertrauliche Unterlagen wegschließen

Sie verlassen das Büro kurz oder haben Pause oder Feierabend? Dann lassen Sie keine vertraulichen Unterlagen mit personenbezogenen Daten auf dem Tisch liegen, sondern schließen Sie sie sicher weg.

Lassen Sie Fenster und Türen nicht geöffnet, wenn der Raum unbeaufsichtigt ist.

Dokumente sicher entsorgen

Immer wieder hört man, dass Unterlagen von Firmen in falsche Hände gelangen, indem sie von fremden Personen aus Mülltonnen oder Papierkörben gefischt werden. Entsorgen Sie daher Unterlagen mit personenbezogenen Daten, die nicht mehr benötigt werden, nur über die besonderen Sammeltonnen oder schreddern Sie die Daten.

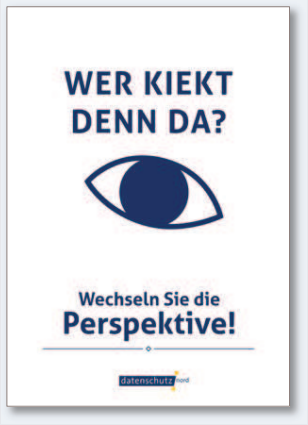


Daten am Kopierer nicht liegen lassen

Holen Sie Ausdrucke am Kopierer umgehend ab.

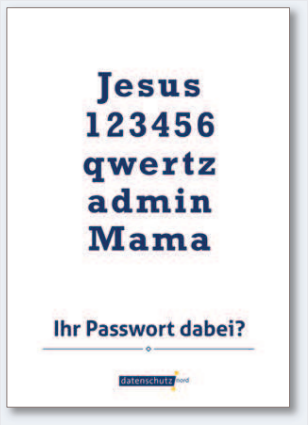
Keinen unbefugten Blick auf den Bildschirm zulassen:

Stellen Sie Ihren Bildschirm möglichst so auf, dass Unbefugte keinen Einblick haben. Machen Sie es sich zur Gewohnheit, Ihren Bildschirm manuell zu sperren (per Strg/Alt/Entf + „Sperren“), wenn Sie Ihren Arbeitsplatz verlassen.



Sichere Passwörter verwenden

Beispiele für unsichere Passwörter sind:



Geben Sie Ihre Passwörter niemals an Unbefugte weiter. Schreiben Sie Passwörter auch niemals auf. Häufiger Fehler ist eine Passwortnotiz unter der Tastatur oder am Bildschirm.

Wählen Sie möglichst komplexe Passwörter aus. In der Regel sicher sind mindestens achtstellige Passwörter aus Klein- und Großbuchstaben, Zahlen und Sonderzeichen. Wählen Sie niemals triviale Passwörter oder Ihren Namen.

Vertrauliche Gespräche schützen

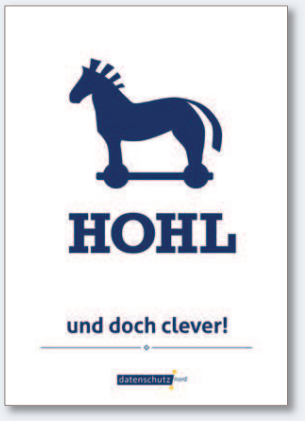
Haben Sie einmal etwas Vertrauliches zu besprechen? Dann suchen Sie einen Bereich auf, in welchem andere Personen das Gespräch nicht mithören können.

Anfragen zu Personendaten? Erst prüfen!

Werden Sie telefonisch oder mündlich nach personenbezogenen Daten gefragt? Dann vergewissern Sie sich, dass der Anfragende seriös ist, z.B. durch Rückruf unter der angegebenden Nummer oder erfragen Sie das Aktenzeichen oder eine Kundennummer. Verweisen Sie dabei gerne auf den Datenschutz in der Einrichtung. Geben Sie vertrauliche Informationen und sensible personenbezogene Daten grundsätzlich nicht mündlich weiter. Beantworten Sie entsprechende Anfragen ggf. schriftlich und ggf. erst nach Rücksprache mit Ihren Vorgesetzten.

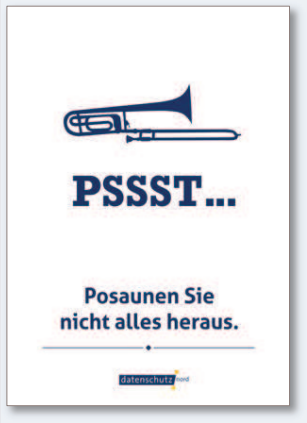
E-Mails kontrollieren, Empfänger schützen

Öffnen Sie keine E-Mails unbekannter Herkunft oder mit „verdächtigen“ Anhängen. Wenn Sie selber eine E-Mail an mehrere Personen versenden, die untereinander nicht die Adressen erkennen sollen, dann setzen Sie die Empfänger „bcc“ (= Empfänger bleiben unerkannt), insbesondere bei der Versendung von Newslettern.



Zurückhaltung im privaten Umfeld

Sie dürfen niemals dienstliche Informationen über Personen im privaten Gespräch oder auf privat genutzten sozialen Medien offenbaren.



6. Kontakt des örtlich Beauftragten für den Datenschutz

Für weitergehende Informationen und in Zweifelsfällen wenden Sie sich bitte an Ihren örtlich Beauftragten für den Datenschutz.

KONTAKTDATEN	
Oliver Stutz datenschutz nord GmbH Konsul-Smidt-Straße 88 28217 Bremen	E-Mail: office@datenschutz-nord.de Web: www.datenschutz-nord-gruppe.de
Ihr direkter Ansprechpartner ist:	
Jan-Christoph Thode datenschutz nord GmbH Niederlassung Berlin Kurfürstendamm 212 10719 Berlin	E-Mail: jthode@datenschutz-nord.de Telefon: 030 3087749-21