Mitarbeiterinformation: Datenschutzgrundregeln an der MVHS

Inhalt

Begriffsklärung

„Personenbezogene Daten sind Einzelangaben über persönliche oder sachliche Verhältnisse bestimmter oder bestimmbarer natürlicher Personen (Betroffene)“ (BayDSG Art. 4, 1), z.B. Name, Adresse, Geburtsdatum etc. Personenbezogene Daten müssen nicht zwangsläufig ein körperliches Merkmal sein, es genügt, wenn ein Bezug zwischen einer Sache (z.B. einer Kursbuchung oder einer Kontonummer) und einer Person hergestellt werden kann.
Besonders sensibel sind personenbezogene Daten, die die ethnische Herkunft, die politische Meinung, religiöse oder philosophische Überzeugungen, die Gewerkschaftszugehörigkeit, die Gesundheit oder das Sexualleben betreffen.

Der Datenschutzbeauftragte der MVHS

Herr Ralf Turban steht für alle datenschutzrelevanten Fragen zur Verfügung und ist Ihr erster Ansprechpartner für Meldungen bei Verletzungen datenschutzrechtlicher Vorgaben.

Kontaktdaten:
Email: datenschutz@mvhs.de

www.Mein-Datenschutzberater.de
Nazibühl 3
86668 Karlshuld

Hinweis: Die Emailadresse datenschutz@mvhs.de wird vom Datenschutzbeauftragten bearbeitet. Die Geschäftsführung hat ebenfalls Zugang zu dem Postfach.

Mitarbeiterinformation: Datenschutzgrundregeln an der MVHS

Meldung von Verstößen

Wenn Sie feststellen,

- dass im Betrieb gegen datenschutzrechtliche Vorgaben verstoßen wird,
- dass durch bestimmte Verhaltensweisen die Datensicherheit für personenbezogene Daten bedroht ist,
- dass besonders sensible oder personenbezogene Informationen gestohlen wurden oder dem Unternehmen auf andere Weise abhandengekommen sind,

dann informieren Sie den Datenschutzbeauftragten, Ihre*n Vorgesetzte*n sowie die Referentin des Managementdirektors umgehend. Eine solche Information hat nichts mit „Anschwärzen" zu tun, vielmehr trägt sie dazu bei, dass im Interesse aller Datenschutz und Datensicherheit gewährleistet bleiben und empfindliche Strafen vermieden werden.

Clean-Desk-Prinzip

1. Aufräumen: Halten Sie Ordnung auf Ihrem Schreibtisch und stellen Sie sich unter Datenschutzaspekten die Frage „Muss das hier liegen?“. So sinkt das Risiko, dass Daten und Informationen in die Hände Unberechtigter gelangen.
2. Wegschließen: Jegliche Datenträger, wie etwa Notebooks, Smartphones, USB-Sticks oder Unterlagen, die personenbezogene Daten enthalten, sollten immer dann weggeschlossen sein, wenn sie nicht im Rahmen der aktuellen Arbeitsaufgabe benutzt werden müssen und insbesondere dann, wenn Sie Ihr Büro oder den Besprechungsraum verlassen.
3. Abschließen: Sobald Sie Ihr Büro für längere Zeit verlassen (Mittagspause, Feierabend, Besprechung), sperren Sie Ihren Bildschirm mit dem „Schloss-Symbol“ auf Ihrer Tastatur und schließen Schränke mit personenbezogenen Daten ab (und ziehen den Schlüssel). Wenn Sie Ihr Büro auch nur für kurze Zeit verlassen, muss zumindest die Bürotür verschlossen sein.

Entsorgen von Unterlagen

Unterlagen mit personenbezogenen Daten oder vertraulichen Informationen dürfen nicht einfach im Papiermüll entsorgt werden. Nutzen Sie einen Aktenvernichter. Für größere Mengen an schützenswerten Unterlagen steht Ihnen eine spezielle Datenschutztonne (sogenannte silberne Tonne) für die sichere und datenschutzkonforme Entsorgung von Papierdokumenten zur Verfügung. Datenträger wie etwa USB-Sticks, Daten-DVDs oder Speicherkarten müssen datenschutzkonform gelöscht oder zerstört werden. Hierfür wenden Sie sich an die IT-Abteilung. Beachten Sie die Archivierungsfristen.

Passwortsicherheit

Die Kennwortvorgaben (vgl. Betriebsvereinbarung IuK, Anlage 1) sind einzuhalten. Wählen Sie eine sichere Aufbewahrung Ihres Passworts (nicht am Arbeitsplatz offen hinterlegen), geben Sie dieses nie an Dritte weiter und aktualisieren sie es in den vorgegebenen Zeiträumen.

Mitarbeiterinformation: Datenschutzgrundregeln an der MVHS

Drucken an zentralen Netzwerkdruckern (Vertrauliches Drucken)

Achten Sie beim Druck von personenbezogenen Daten darauf, dass die Ausgabe der Druckdateien erst nach Eingabe eines Codes erfolgt („Vertrauliches Drucken“). Prüfen Sie generell, ob wirklich alles ausgedruckt werden muss.

Scan

Grundsätzlich müssen personenbezogene Scan-Dateien direkt an die MVHS-interne Adresse versendet werden.

Versand von personenbezogene Daten

Geeignet innerhalb der MVHS:

- **E-Mails**, weil sie innerhalb der MVHS nicht mitgelesen oder verfälscht werden können, da der Transport über einen verschlüsselten Exchangedienst und sicher innerhalb den MVHS-Standorte geschieht.
- **Hauspost**, insofern besonders vertrauliche Unterlagen in einem verschlossenen Umschlag und mit dem Zusatz „vertraulich“ versendet werden.

Geeignet für den Versand nach extern:

- **Postalischer Versand**: Der postalische Versand ist in jedem Fall dem Versand per Fax vorzuziehen, denn der Faxversand erfolgt unverschlüsselt und kann mitgelesen werden. Darüber hinaus können beim Faxversand Informationen durch eine fehlerhafte Anwahl an der falschen Adresse landen oder in die Hände von Unbefugten geraten.
- Das **Dozentenportal** ermöglicht eine gesicherte Datenbereitstellung auf einer verschlüsselten Seite, die der Dozent/die Dozentin über sein persönliches Login erreicht.
- **Passwortgeschützte Dateien per E-Mail versenden**: Das ungeschützte Verschicken einer E-Mail außerhalb des MVHS-Servers ist vergleichbar mit dem Versenden einer Postkarte. D.h. alle Daten und Inhalte können „unterwegs“ mitgelesen, kopiert und gefälscht werden. Selbst der Absender kann manipuliert werden. Einzige Möglichkeit derzeit ist ein Passwortschutz von Dateien. Dieser kann zwar umgangen werden, allerdings ist eine 'schlechte' Verschlüsselung immer noch besser als keine Verschlüsselung. Wählen Sie ein sicheres Passwort analog unserer Kennwortsicherheitsvorgaben (vgl. Betriebsvereinbarung IuK, Anlage 1) und übermitteln Sie dieses auf einem anderen Kommunikationskanal, z.B. Telefon. Eine word-Datei (gilt auch für PDF-Verschlüsselung mit Adobe Acrobat) können Sie mit einem Dokumentenschutz versehen, indem Sie im geöffneten Dokument auf „Datei“ klicken, unter „Informationen“ die Option „Dokument schützen“ auswählen und unter „Mit Kennwort verschlüsseln“ ein Kennwort setzen.
- **Sonstige verschlüsselte Portale** eignen sich, insofern anfordernde Stellen diese anbieten, z.B. BAMF.

Ungeeignet:

- Der Versand von personenbezogenen Daten an die **eigene private E-Mailadresse oder Clouds** ist nicht gestattet. Ebenfalls sollten Sie personenbezogene Daten nicht auf tragbare Geräte (wie z.B. USB-Stick, Laptop, Tablet etc.) kopieren, weil diese verloren gehen können.

Mitarbeiterinformation: Datenschutzgrundregeln an der MVHS

- Im Falle von **genehmigtem Home Office** nehmen Sie bitte Rücksprache mit dem Benutzerservice, falls Ihre Aufgaben mit personenbezogenen Daten zu tun haben. Beachten Sie auch die Regelungen in der Betriebsvereinbarung IuK, Anlage 3.

Beispiele für den Versand von Daten	***Wie***	***Erläuterung***
Anwesenheitslisten mit Teilnehmenden-namen	*Dozentenportal oder postalisch*	*Weitere Daten erhält die Kursleitung i.d.R. nicht. Im Legendentext des Kurses kann die Telefonnummer des Fachgebiets angegeben werden, z.B. für kurzfristige Anfragen. Für Veranstaltungen, für die eine sehr kurzfristige Kontaktierung der Teilnehmenden durch die Kursleitung notwendig ist (z.B. Wetterverhältnisse für das Statt-finden einer Exkursion), muss das schriftliche Einverständnis der Teilnehmenden eingeholt werden, dass die Weitergabe der Telefonnummer an den/die Dozenten/Dozentin in Ordnung ist. Wichtig ist, die Teilnehmen-den zu informieren zu welchem Zweck diese genutzt wird und dass die Kursleitung laut Rahmenvertrag der Verschwiegenheitspflicht unterliegt und die Telefonnummer nicht anderweitig benutzen darf.*
Honorarverträge, -abrechnungen, Bankdaten	*Dozentenportal oder postalisch*	*Das Dozentenportal ist verschlüsselt und nur durch ein Login des Dozenten/der Dozentin zugänglich.*
Bestätigung der Kursbuchung	*ungeschützte E-Mail*	*Wenn die Kursbuchung online erfolgt, findet die Zusendung der Anmeldebestätigung zweckdienlich und mit Einwilligung der buchenden Person über unverschlüsselte E-Mail statt. Die Menge der vermerkten Daten sind verhältnismäßig: Lediglich Name, Adresse und Kurs sind vermerkt. Die Bankdaten werden bis auf die letzten drei Ziffern nicht dargestellt*
*Korrespondenz mit Teilnehmer*in bei Rücktritt, Ermäßigungsnachweis etc.*	*telefonisch o-der unge-schützte E-Mail mit Hin-weis:*	*„Wir bestätigen die Bearbeitung Ihres Rücktritts und werden Ihnen die Kursgebühr, abzüglich der Stornogebühr von 10. – Euro und der Gebühr für eine Unterrichtseinheit, auf Ihr Konto zurücküberweisen. Teilen Sie uns Ihre Bankverbindung (bzw. den Ermäßigungsnachweis oder sonstige personenbezogenen Daten) telefonisch oder postalisch mit, wenn Sie den sichersten Übertragungsweg wählen wollen. Erfolgt der Versand von personenbezogenen Daten dennoch per E-Mail an uns, liegt dies in der Verantwortung des Absenders.“*
*Korrespondenz mit Teilnehmer*in wegen SEPA.*	*telefonisch oder ungeschützte E-Mail mit Hinweis:*	*„Wären Sie so freundlich, uns beigefügtes SEPA-Mandat ausgefüllt und unterschrieben wieder zukommen zu lassen (gerne postalisch mit, wenn Sie den sichersten Übertragungsweg wählen wollen, alternativ eingescannt via E-Mail), so dass wir die Gebühr per Lastschrift abbuchen können.“*

Mitarbeiterinformation: Datenschutzgrundregeln an der MVHS

Korrespondenz mit Ämtern und Kooperationspartnern über besonders schützenswerte personen-bezogene Daten.	*ausschließlich per Telefon oder postalischen Versand*	*(z.B. in der sozialpädagogischen Arbeit mit Psychologen, Pädagogen, Ärzten… und Erziehungsberechtigten- und Sorgeberechtigten)*

Nutzung von personenbezogenen Daten

- Es gilt das Gebot der „Datensparsamkeit“: Es dürfen nur solche Informationen verarbeitet und genutzt werden, die zur betrieblichen Aufgabenerfüllung erforderlich sind und in unmittelbarem Zusammenhang mit dem Verarbeitungszweck stehen. D.h. Personenbezogene Daten werden nur für die interne Verwendung zum Zwecke der Kursbuchung und -abrechung und für die Information des Kunden über Änderungen verwandt.
- Die Erhebung und Verarbeitung personenbezogener Daten muss zulässig sein. Bei sensiblen Daten, z.B. Gesundheitsdaten, gelten gesonderte Anforderungen.
- Personenbezogene Daten werden niemals an Dritte weitergegeben. Falls andere Stellen Informationen über Betroffene anfordern, dürfen diese ohne Einwilligung des Betroffenen nur gegeben werden, wenn hierfür eine gesetzliche Verpflichtung besteht. Zudem muss die Identität des Anfragenden zweifelsfrei feststehen. Im Zweifel ist der Datenschutzbeauftragte zu kontaktieren.
- Ohne dokumentierte Einwilligung der Betroffenen dürfen personenbezogenen Daten nicht für Zwecke der Werbung oder Meinungsforschung genutzt werden (z.B. Umfragen, Newsletter, sonstige Kurswerbung aus den Fachgebieten).
- Teilnehmerlisten für den Nachweis der Anwesenheit enthalten lediglich die Namen.
- Beim Versand von Anmeldekarten werden Kontodaten bis auf die letzten drei Zahlen durch x ersetzt.