

Technische und organisatorische Maßnahmen i.S.d. § 9 BDSG

der

Hochschule Kempten
Bahnhofstr. 61
87435 Kempten

Daten des Projekts 3connect:

Pro Fahrzeug:

- Positionsdaten
- Energiedaten (z.B. Batterieladezustand)
- Fahrzeug-ID

KEINE personenbezogene Daten!

1. Zutrittskontrolle

Maßnahmen, die geeignet sind, Unbefugten den Zutritt zu Datenverarbeitungsanlagen, mit denen personenbezogene Daten verarbeitet oder genutzt werden, zu verwehren.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Alarmanlage | <input type="checkbox"/> Absicherung von Gebäudeschächten |
| <input type="checkbox"/> Automatisches Zugangskontrollsystem | <input checked="" type="checkbox"/> Chipkarten-/Transponder-Schließsystem |
| <input type="checkbox"/> Schließsystem mit Codesperre | <input checked="" type="checkbox"/> Manuelles Schließsystem |
| <input type="checkbox"/> Biometrische Zugangssperren | <input checked="" type="checkbox"/> Videoüberwachung der Zugänge |
| <input checked="" type="checkbox"/> Lichtschranken / Bewegungsmelder | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

2. Zugangskontrolle

Maßnahmen, die geeignet sind zu verhindern, dass Datenverarbeitungssysteme von Unbefugten genutzt werden können.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Zuordnung von Benutzerrechten | <input type="checkbox"/> Erstellen von Benutzerprofilen |
| <input checked="" type="checkbox"/> Passwortvergabe | <input type="checkbox"/> Authentifikation mit biometrischen Verfahren |
| <input checked="" type="checkbox"/> Authentifikation mit Benutzername / Passwort | <input type="checkbox"/> Zuordnung von Benutzerprofilen zu IT-Systemen |
| <input checked="" type="checkbox"/> Gehäuseverriegelungen | <input checked="" type="checkbox"/> Einsatz von VPN-Technologie |
| <input type="checkbox"/> Sperren von externen Schnittstellen (USB etc.) | <input checked="" type="checkbox"/> Sicherheitsschlösser |
| <input checked="" type="checkbox"/> Schlüsselregelung (Schlüsselausgabe etc.) | <input type="checkbox"/> Personenkontrolle beim Pförtner / Empfang |
| <input type="checkbox"/> Protokollierung der Besucher | <input type="checkbox"/> Sorgfältige Auswahl von Reinigungspersonal |
| <input checked="" type="checkbox"/> Sorgfältige Auswahl von Wachpersonal | <input type="checkbox"/> Tragepflicht von Berechtigungsausweisen |

- | | |
|--|--|
| <input checked="" type="checkbox"/> Einsatz von Intrusion-Detection-Systemen | <input type="checkbox"/> Verschlüsselung von mobilen Datenträgern |
| <input type="checkbox"/> Verschlüsselung von Smartphone-Inhalten | <input type="checkbox"/> Einsatz von zentraler Smartphone-Administrations-Software (z.B. zum externen Löschen von Daten) |
| <input checked="" type="checkbox"/> Einsatz von Anti-Viren-Software | <input type="checkbox"/> Verschlüsselung von Datenträgern in Laptops / Notebooks |
| <input checked="" type="checkbox"/> Einsatz einer Hardware-Firewall | <input type="checkbox"/> Einsatz einer Software-Firewall |

3. Zugriffskontrolle

Maßnahmen, die gewährleisten, dass die zur Benutzung eines Datenverarbeitungssystems Berechtigten ausschließlich auf die ihrer Zugriffsberechtigung unterliegenden Daten zugreifen können, und dass personenbezogene Daten bei der Verarbeitung, Nutzung und nach der Speicherung nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können.

- | | |
|--|---|
| <input checked="" type="checkbox"/> Erstellen eines Berechtigungskonzepts | <input checked="" type="checkbox"/> Verwaltung der Rechte durch Systemadministrator |
| <input checked="" type="checkbox"/> Anzahl der Administratoren auf das „Notwendigste“ reduziert | <input type="checkbox"/> Passwortrichtlinie inkl. Passwortlänge, Passwortwechsel |
| <input checked="" type="checkbox"/> Protokollierung von Zugriffen auf Anwendungen, insbesondere bei der Eingabe, Änderung und Löschung von Daten | <input type="checkbox"/> Sichere Aufbewahrung von Datenträgern |
| <input type="checkbox"/> physische Löschung von Datenträgern vor Wiederverwendung | <input type="checkbox"/> ordnungsgemäße Vernichtung von Datenträgern (DIN 32757) |
| <input checked="" type="checkbox"/> Einsatz von Aktenvernichtern bzw. Dienstleistern (nach Möglichkeit mit Datenschutz-Gütesiegel) | <input type="checkbox"/> Protokollierung der Vernichtung |
| <input type="checkbox"/> Verschlüsselung von Datenträgern | |

4. Weitergabekontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten bei der elektronischen Übertragung oder während ihres Transports oder ihrer Speicherung auf Datenträger nicht unbefugt gelesen, kopiert, verändert oder entfernt werden können, und dass überprüft und festgestellt werden kann, an welche Stellen eine Übermittlung personenbezogener Daten durch Einrichtungen zur Datenübertragung vorgesehen ist.

- | | |
|---|--|
| <input checked="" type="checkbox"/> Einrichtungen von Standleitungen bzw. VPN-Tunneln | <input type="checkbox"/> Weitergabe von Daten in anonymisierter oder pseudonymisierter Form |
| <input type="checkbox"/> E-Mail-Verschlüsselung | <input checked="" type="checkbox"/> Erstellen einer Übersicht von regelmäßigen-Abruf- und Übermittlungsvorgängen |
| <input type="checkbox"/> Dokumentation der Empfänger von Daten und der Zeitspannen der geplanten Überlassung bzw. vereinbarter Löschfristen | <input type="checkbox"/> Beim physischen Transport: sichere Transportbehälter/-verpackungen |
| <input type="checkbox"/> Beim physischen Transport: sorgfältige Auswahl von Transportpersonal und -fahrzeugen | |

Kein Personenbezug der Daten an der HS Kempten

5. Eingabekontrolle

Maßnahmen, die gewährleisten, dass nachträglich überprüft und festgestellt werden kann, ob und von wem personenbezogene Daten in Datenverarbeitungssysteme eingegeben, verändert oder entfernt worden sind.

- | | |
|---|---|
| <input checked="" type="checkbox"/> Protokollierung der Eingabe, Änderung und Löschung von Daten | <input checked="" type="checkbox"/> Erstellen einer Übersicht, aus der sich ergibt, mit welchen Applikationen welche Daten eingegeben, geändert und gelöscht werden können. |
| <input checked="" type="checkbox"/> Nachvollziehbarkeit von Eingabe, Änderung und Löschung von Daten durch individuelle Benutzernamen (nicht Benutzergruppen) | <input checked="" type="checkbox"/> Aufbewahrung von Formularen, von denen Daten in automatisierte Verarbeitungen übernommen worden sind |
| <input checked="" type="checkbox"/> Vergabe von Rechten zur Eingabe, Änderung und Löschung von Daten auf Basis eines Berechtigungskonzepts | |

6. Auftragskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten, die im Auftrag verarbeitet werden, nur entsprechend den Weisungen des Auftraggebers verarbeitet werden können.

- | | |
|---|--|
| <input type="checkbox"/> Auswahl des Auftragnehmers unter Sorgfaltsgesichtspunkten (insbesondere hinsichtlich Datensicherheit) | <input type="checkbox"/> vorherige Prüfung der und Dokumentation der beim Auftragnehmer getroffenen Sicherheitsmaßnahmen |
| <input type="checkbox"/> schriftliche Weisungen an den Auftragnehmer (z.B. durch Auftragsdatenverarbeitungsvertrag) i.S.d. § 11 Abs. 2 BDSG | <input type="checkbox"/> Verpflichtung der Mitarbeiter des Auftragnehmers auf das Datengeheimnis (§ 5 BDSG) |
| <input type="checkbox"/> Auftragnehmer hat Datenschutzbeauftragten bestellt | <input type="checkbox"/> Sicherstellung der Vernichtung von Daten nach Beendigung des Auftrags |
| <input type="checkbox"/> Wirksame Kontrollrechte gegenüber dem Auftragnehmer vereinbart | <input type="checkbox"/> laufende Überprüfung des Auftragnehmers und seiner Tätigkeiten |
| <input type="checkbox"/> Vertragsstrafen bei Verstößen | |

*keine Auftragsverarbeitung
personenbezogene Daten!*

7. Verfügbarkeitskontrolle

Maßnahmen, die gewährleisten, dass personenbezogene Daten gegen zufällige Zerstörung oder Verlust geschützt sind.

- | | |
|--|--|
| <input checked="" type="checkbox"/> Unterbrechungsfreie Stromversorgung (USV) | <input type="checkbox"/> Klimaanlage in Serverräumen |
| <input checked="" type="checkbox"/> Geräte zur Überwachung von Temperatur und Feuchtigkeit in Serverräumen | <input checked="" type="checkbox"/> Schutzsteckdosenleisten in Serverräumen |
| <input checked="" type="checkbox"/> Feuer- und Rauchmeldeanlagen | <input checked="" type="checkbox"/> Feuerlöschgeräte in Serverräumen |
| <input checked="" type="checkbox"/> Alarmmeldung bei unberechtigten Zutritten zu Serverräumen | <input checked="" type="checkbox"/> Erstellen eines Backup- & Recoverykonzepts |
| <input checked="" type="checkbox"/> Testen von Datenwiederherstellung | <input checked="" type="checkbox"/> Erstellen eines Notfallplans |
| <input type="checkbox"/> Aufbewahrung von Datensicherung an einem sicheren, ausgelagerten Ort | <input type="checkbox"/> Serverräume nicht unter sanitären Anlagen |
| <input type="checkbox"/> <u>In Hochwassergebieten: Serverräume über der Wassergrenze</u> | |

nicht gegeben

8. Trennungsgebot

Maßnahmen, die gewährleisten, dass zu unterschiedlichen Zwecken erhobene Daten getrennt verarbeitet werden können.

- | | |
|--|--|
| <input type="checkbox"/> physikalisch getrennte Speicherung auf gesonderten Systemen oder Datenträgern | <input checked="" type="checkbox"/> Logische Mandantentrennung (softwareseitig) |
| <input checked="" type="checkbox"/> Erstellung eines Berechtigungskonzepts | <input type="checkbox"/> Verschlüsselung von Datensätzen, die zu demselben Zweck verarbeitet werden |
| <input type="checkbox"/> Versehen der Datensätze mit Zweckattributen/Datenfeldern | <input checked="" type="checkbox"/> Bei pseudonymisierten Daten: Trennung der Zuordnungsdatei und der Aufbewahrung auf einem getrennten, abgesicherten IT-System |
| <input checked="" type="checkbox"/> Festlegung von Datenbankrechten | <input checked="" type="checkbox"/> Trennung von Produktiv- und Testsystem |

Keinen Personenbezug
bei HS Konten

20.09.2016
Datum

Maximilian Stahl

Prof. Dr. rer. nat. Arnulf Deinzer

Verantwortlicher für die Erstellung (in Druckbuchstaben)



Unterschrift des Verantwortlichen



Deinzer, Arnulf, Prof. Dr.

Von: Keppeler Stefan <Stefan.Keppeler@auew.de>
Gesendet: Mittwoch, 14. September 2016 08:45
An: Deinzer, Arnulf, Prof. Dr.
Cc: Fischer Florian; Ziegler Christian
Betreff: AW: personenbezogene Daten ja / nein
Signiert von: stefan.keppeler@auew.de

Lieber Arnulf,

vielen Dank für deine Antwort. Diese Frage wurde von mir schon vor langer Zeit geklärt und ich habe in einer "gemeinsamen Erklärung der Konferenz der unabhängigen Datenschutzbehörden des Bundes und der Länder und des Verbandes der Automobilindustrie (VDA)" die datenschutzrechtlichen Aspekte bei der Nutzung vernetzter und nicht vernetzter Kraftfahrzeuge" bei der Landesdatenschutzaufsichtsbehörde gefunden.

„Die bei der Kfz-Nutzung anfallenden Daten sind jedenfalls dann personenbezogen im Sinne des Bundesdatenschutzgesetzes (BDSG), wenn eine Verknüpfung mit der Fahrzeugidentifikationsnummer oder dem Kfz-Kennzeichen vorliegt. Bei „Online“-Autos (Übermittlung per Datenkommunikation) findet bereits im Zeitpunkt der Datenkommunikation aus dem Fahrzeug heraus eine Erhebung durch die "Verantwortliche Stelle" im Sinne des § 3 Abs. 3 BDSG statt. Als Verantwortliche Stellen ist diesem Fall anzusehen, wer die personenbezogene Daten erhält, d. h. in der Regel die Hersteller und gegebenenfalls dritte Dienste-Anbieter“ (in unserem Fall die Hochschule Kempten).

Da die Hochschule als verantwortliche Stelle eine wissenschaftliche Forschungseinrichtung ist, kann der § 40 BDSG zur Anwendung kommen.

§ 40 Verarbeitung und Nutzung personenbezogener Daten durch Forschungseinrichtungen

(1) Für Zwecke der wissenschaftlichen Forschung erhobene oder gespeicherte personenbezogene Daten dürfen nur für Zwecke der wissenschaftlichen Forschung verarbeitet oder genutzt werden.

(2) Die personenbezogenen Daten sind zu anonymisieren, sobald dies nach dem Forschungszweck möglich ist. Bis dahin sind die Merkmale gesondert zu speichern, mit denen Einzelangaben über persönliche oder sachliche Verhältnisse einer bestimmten oder bestimmbarer Person zugeordnet werden können. Sie dürfen mit den Einzelangaben nur zusammengeführt werden, soweit der Forschungszweck dies erfordert.

Von meiner Seite muss ausgeschlossen sein, dass wir als AÜW oder auch andere öffentliche Personenkreise auf die erhobenen, anonymisierten Fahrzeugdaten der Hochschule zugreifen können. Dementsprechend möchte ich von dir als Datenschutzbeauftragter der Hochschule wissen, wie sicher diese Daten gespeichert sind. Das Standardwerk dazu ist einfach die Dokumentation der technischen und organisatorischen Maßnahmen nach §9 BDSG. Bitte schick mir diese für meine Kontrolle und Dokumentation zu.

Aus deinem angehängten Dokument kann ich leider keine Erkenntnisse entnehmen.

Für Fragen stehe ich Ihnen sehr gerne zur Verfügung.

Mit freundlichen Grüßen

ALLGÄUER ÜBERLANDWERK GmbH

Abteilung Energiemarkt Vertrieb

i.A. Stefan Keppeler

Stefan Keppeler

Datenschutzbeauftragter



Viele Grüße,

Telefon: +49 831 2521-426

E-Mail: stefan.keppeler@auew.de

Fax: +49 831 2521-790 426

Internet: www.auew.de

Mobil: +49 172 8601807

Sitz der Gesellschaft: Kempten (Allgäu), Registergericht: Amtsgericht Kempten, HRB 435

Vorsitzender des Verwaltungsrates: Oberbürgermeister Thomas Kiechle, Geschäftsführer: Michael Lucke

 Bitte denken Sie über Ihre Verantwortung gegenüber der Umwelt nach, bevor Sie diese E-Mail ausdrucken.

Von: Deinzer, Arnulf, Prof. Dr. [<mailto:arnulf.deinzer@hs-kempten.de>]

Gesendet: Montag, 5. September 2016 12:48

An: Keppeler Stefan

Cc: Fischer Florian

Betreff: WG: personenbezogene Daten ja / nein

Lieber Stefan,

die von den Loggern aufgezeichneten Daten in Euren e-Cars sind keine personenbezogenen Daten – genauso wenig wie die Daten der Motorsteuerung Deines PKWs (die zyklisch gespeichert werden – vgl. Folie 6 meiner Vorlesung vom Sommersemester).

Natürlich sind andererseits die bei Euch gepflegten Daten, z.B. welcher Eurer Mitarbeiter wann welches Fahrzeug ausleiht/benutzt personenbezogen – aber da habe ich volles Vertrauen in Euren DSB, dass damit korrekt umgegangen wird.

Alles Gute

Arnulf

Hochschule Kempten
Datenschutzbeauftragter
Prof. Dr. Arnulf Deinzer
87435 Kempten

Von: Stahl, Maximilian

Gesendet: Mittwoch, 31. August 2016 15:14

An: Deinzer, Arnulf, Prof. Dr.

Cc: andreas@rupp-hegge.de

Betreff: WG: personenbezogene Daten ja / nein

Guten Tag Herr Prof. Deinzer,

wie eben telefonisch besprochen die Email vom AÜW in Bezug auf die Erfassung personenbezogener Daten. Bitte setzen Sie bei der Email an die unten genannten Herrn Prof. Rupp in cc.

Datenschutzbeauftragter des Allgäuer Überlandwerks:

Stefan.Keppeler@auew.de

Projektverantwortlicher beim AÜW:

Florian.Fischer@auew.de

Viele Grüße,
Maximilian Stahl

Dipl.-Ing. (FH)
Forschungszentrum Allgäu

Hochschule für angewandte Wissenschaften Kempten

Leonhardstraße 19
87437 Kempten (Allgäu)
Tel.: +49 831 2523 327
Fax: +49 831 2523 540
www.hochschule-kempten.de

Von: Ziegler Christian

Gesendet: Mittwoch, 1. Juni 2016 10:58

An: Keppeler Stefan; 'maximilian.stahl@hs-kempten.de'

Cc: Fischer Florian

Betreff: personenbezogene Daten ja / nein

Guten Tag die Herren,

da ja eine Einigung ob personenbezogene Daten ja oder nein in unserem Fall nicht herbeigeführt werden konnte, wollte ich mich zumindest mal noch kurz damit beschäftigen. Folgendes hab ich speziell auf Geodaten (GPS) gefunden.

Schon hier ist darauf hinzuweisen, dass bei Sachangaben ein *Personenbezug* direkt gegeben, aber auch indirekt und damit vermittelt sein kann. So ist die Antwort auf die Frage nach dem Inhaber einer von einer Person regelmäßig und ausschließlich genutzten Sache wie etwa das private Auto direkt personenbezogen. Wird das Auto aber von vielen Personen genutzt, dann sind die Angaben über die Nutzung schon nicht mehr unmittelbar personenbezogen, sondern lediglich die Haltereigenschaft. Weiter entfernt ist die Person von einer Sache, wenn eine Beziehung bestanden hat, diese aber aufgegeben wurde: Wenn ein Auto von einer Person verkauft worden ist, hat diese Person zu sämtlichen aktuellen Angaben über das Auto keinen Bezug mehr.

Hier trifft zwar auf uns eigentlich die Nutzung des Autos von vielen Personen zu. Doch leider ist natürlich durch die Aufzeichnung mittels Fahrtenbüchern ein Personenzug in unserem Hause erst einmal gegeben. Was dann im Punkt 2.2 zu folgender Problematik führt.

2.2 Bestimmbarkeit

Für die *Bestimmbarkeit* eines Datums zu einer Person kommt es darauf an, ob eine Zuordnung zu einer natürlichen Person mit

einem „unverhältnismäßig großen Aufwand“ möglich ist oder nicht (vgl. § 3 Abs. 7 BDSG). Unerheblich ist, ob die Zuordnung zulässig wäre oder nicht.²² Auch auf den subjektiven Willen einer Zuordnung durch die verarbeitende Stelle kommt es nicht an, sondern ausschließlich auf die objektive Zuordenbarkeit im konkreten Fall.²³

Entgegen einer weit verbreiteten Ansicht kommt es für die Bestimmbarkeit nicht darauf an, ob die verarbeitende Stelle real eine Zuordnung vornehmen könnte. Ist eine dritte Person hierzu grundsätzlich durch Drittwissen in der Lage und ist nicht völlig auszuschließen, dass dieses Drittwissen dem Verarbeiter bekannt wird, [REDACTED]

Gesamter Artikel im Anhang.

Es führt laut den oben genannten Information somit meiner Meinung nach kein Weg an einer Vereinbarung zur Auftragsdatenverarbeitung vorbei.

Max lass uns doch wissen, sobald du eine Rückmeldung aus deinem Haus hierüber hast.

Viele Grüße

Christian

Mit freundlichen Grüßen

ALLGÄUER ÜBERLANDWERK GmbH

Marketing und Vertrieb

i.A. Christian Ziegler

Christian Ziegler
Dipl.-Ing. (FH)



Allgäuer Überlandwerk GmbH

Illerstraße 18

D - 87435 Kempten

Telefon +49 831 2521-182

E-Mail: christian.ziegler@auew.de

Fax: +49 831 2521-790 -182

Internet: www.auew.de

Sitz der Gesellschaft: Kempten (Allgäu), Registergericht: Amtsgericht Kempten, HRB 435

Vorsitzender des Verwaltungsrates: Oberbürgermeister Thomas Kiechle, Geschäftsführer: Michael Lucke

 Bitte denken Sie über Ihre Verantwortung gegenüber der Umwelt nach, bevor Sie diese E-Mail ausdrucken.