Newsletter

Ausgabe Oktober 2022

Liebe Leserin, lieber Leser,

unser neuer Newsletter hält für Sie aktuelle, interessante Themen bereit.

Unsere Themen und Quellen im Überblick:

- **BSI, BfDI und LDI – wer ist zuständig?**
  https://keyed.de/blog/bsi-bfdi-und-ldi-wer-ist-zustaendig/

- **Die Pflicht zur Arbeitszeiterfassung aus datenschutzrechtlicher Sicht**
  https://www.datenschutz-notizen.de/die-pflicht-zur-arbeitszeiterfassung-aus-datenschutzrechtlicher-sicht-5038371/

- **Cloud-Computing im Gesundheitswesen – vereinbar mit der ärztlichen Schweigepflicht?**
  https://www.datenschutz-notizen.de/cloud-computing-im-gesundheitswesen-vereinbar-mit-der-aerztlichen-schweigepflicht-5738749/

- **BSI stellt aktuellen Lagebericht vor**
  https://www.datenschutzticker.de/2022/10/bsi-stellt-aktuellen-lagebericht-vor/

- **Urteile**

- **weitere interessante Links**

Viel Spaß beim Lesen,

freundliche Grüße

Mario Barthel

➢ BSI, BfDI und LDI – wer ist zuständig?

Das Bundesamt für Sicherheit in der Informationstechnik (BSI), der Bundesbeauftragte für den Datenschutz und die Informationsfreiheit (BfDI) und die jeweiligen Landesbeauftragten für den Datenschutz und die Informationsfreiheit (LDI) sind Kontrollorgane für den Schutz und die Sicherheit bei der Verarbeitung personenbezogener Daten. Doch wer übernimmt welche Aufgaben und Zuständigkeiten? Der folgende Überblick hilft weiter:

Bundesamt für Sicherheit in der Informationstechnik (BSI)

- Bundesbehörde, die dem Bundesministerium des Innern und für Heimat untersteht
- Zuständigkeit für die IT-Sicherheit in der öffentlichen Verwaltung, in Unternehmen sowie bei Privatanwendern
- Zentrale Meldestelle für IT-Sicherheit: Sammlung und Auswertung von Informationen über Sicherheitsmängel und Angriffsmuster zur frühen Erkennung von Cyberangriffen sowie sofortige Maßnahmeneinleitung
- Erhebung, Auswertung, Speicherung und Verarbeitung von Protokoll- und Kommunikationsdaten des Bundes
- Festlegung von Mindeststandards und Handlungsempfehlungen
- Schutz der IT-Systeme und Kommunikationsnetze des Bundes vor z.B. Trojaner und Hackerangriffen
- Definition einheitlicher und strenger Sicherheitsstandards für die Bundesverwaltung

Bundesbeauftragter für den Datenschutz und die Informationsfreiheit (BfDI)

- Datenschutzrechtliche Aufsichtsbehörde auf Ebene des Bundes
- Überwachung und Durchsetzung der DSGVO und BDSG
- Sensibilisierung und Aufklärung der Öffentlichkeit, Beratung zu allen Belangen des Datenschutzes und der Informationsfreiheit sowie die Bearbeitung von Beschwerden von betroffenen Personen oder Datenschutzverbänden
- Kooperation mit anderen Aufsichtsbehörden in Deutschland und Europa und die Datenschutzkontrolle aller öffentlichen Stellen, bestimmter Träger der sozialen Sicherung, gesetzlicher Krankenkasse, Unfallkassen, der Deutschen Rentenversicherung, Telekommunikations- und Postdienstunternehmen
- der BfDI kann bei Datenschutzverstoß Stellen warnen, verwarnen, Verbote aussprechen oder Geldbußen verhängen
- jede Bürgerin und jeder Bürger kann in Kontakt mit dem BfDI (derzeit Herr Ulrich Kelber) treten, sobald er oder sie einer Verletzung des Datenschutzrechts unterliegt

Landesbeauftragte für den Datenschutz und die Informationsfreiheit (LDI)

- jedes Bundesland hat einen LDI, der als Aufsichtsbehörde für die Verarbeitung personenbezogener Daten fungiert (die Landesbeauftragte für den Datenschutz Niedersachsen ist derzeit Barbara Thiel)
- im Gegensatz zum BfDI untersteht dem LDI auch die Verarbeitung privater Stellen
- Anlaufstelle für Beschwerden, wenn die eigenen personenbezogenen Daten falsch verarbeitet werden (hier wird die Meldung eines Verstoßes vorgenommen)
- Wachen über die Einhaltung der Vorschriften zum Datenschutz im öffentlichen Bereich und in der Privatwirtschaft
- Beratung öffentlicher und privater Stellen sowie Bürgerinnen und Bürger in datenschutzrechtlichen Fragestellungen, um beispielsweise Verstöße schon im Vorfeld zu verhindern

➢ Die Pflicht zur Arbeitszeiterfassung aus datenschutzrechtlicher Sicht

Nach dem Beschluss Az. 1 ABR 22/21 des Arbeitsgerichts vom 13. September 2022 sind Unternehmen grundsätzlich zur Arbeitszeiterfassung der Beschäftigten verpflichtet. Bei der Verarbeitung dieser Daten gibt es einige datenschutzrechtliche Komponenten zu beachten.

Die Möglichkeiten zur Zeiterfassung sind vielfältig. So werden häufig elektronische Geräte an den Eingängen genutzt, an denen sich die Beschäftigten per Token, Karte oder PIN ausweisen und an- oder abmelden. Im Homeoffice kommen Apps oder Webanwendungen zum Einsatz. Aber auch eine Erfassung in Papierform oder Excel-Listen finden in der Praxis noch Anwendung. Je nach der gewählten Form der Zeiterfassung müssen die entsprechenden datenschutzrechtlichen Aspekte geprüft und umgesetzt werden. Grundsätzlich ist dies datenschutzkonform möglich mit Ausnahme der Zeiterfassung, die biometrische Daten erfasst. Für diese besondere Kategorie personenbezogener Daten gibt es keine einschlägige Rechtsgrundlage.

Für die anderen Möglichkeiten sind folgende Punkte besonders zu beachten:

1. **Datennutzung**
   Die Daten dürfen nur zu dem Zweck verarbeitet werden, zu dem sie erhoben wurden (Zweckbindungsgrundsatz). Bei der Arbeitszeiterfassung soll der Arbeitgeber nachweisen können, dass die Vorschriften zur Arbeitszeit eingehalten werden (Höchstarbeitszeit, Pausen etc.). Darüber hinaus kann die Arbeitszeit für die Lohnabrechnung genutzt werden oder geprüft werden, ob Beschäftigte pünktlich anfangen zu arbeiten. Hierüber müssen die Beschäftigten jedoch informiert werden. Sollen Arbeitszeiten analysiert werden, dient dies nicht mehr dem reinen Zweck der Zeiterfassung und es muss geprüft werden, ob hierfür eine Rechtsgrundlage vorliegt. Ebenfalls wären die Beschäftigten hierüber zu informieren.
2. **Vertraulichkeit**
   Bei der Arbeitszeiterfassung darf nur einem eingeschränkten Personenkreis der Zugriff auf die Daten ermöglicht werden. Hierzu zählen die zuständigen Beschäftigten der Personalabteilung, die zuständigen Führungskräfte sowie der Beschäftigte selbst.
3. **Aufbewahrungsfrist**
   Konkrete Vorgaben finden sich hierzu nur in § 16 Abs. 2 Arbeitszeitgesetz und § 17 Abs. 1 S. 1 Mindestlohngesetz, die die Erfassung der Arbeitszeit für Überstunden und generell für bestimmte Branche vorschreibt. Hiernach sind die Nachweise für zwei Jahre aufzubewahren, was als Richtwert dienen kann.

➢ Cloud-Computing im Gesundheitswesen – vereinbar mit der ärztlichen Schweigepflicht?

Die DSGVO stellt im Zusammenhang mit Cloud-Computing im Gesundheitswesen hohe Anforderungen an die Umsetzung technischer Maßnahmen. Doch auch die strafrechtlichen Regelungen zum Schutz von Geheimnissen durch Berufsgeheimnisträger müssen beachtet werden.

Folgendes ist nach dem § 203 StGB zu berücksichtigen:

- Geheimnisse dürfen nur dann offenbart werden, wenn dies zwingend erforderlich ist, um die Dienstleistung in Anspruch zu nehmen.
- Es ist unbedingt auch die alternative Einbeziehung anderer Dienstleister in Betracht zu ziehen. Ist die Inanspruchnahme eines bestimmten Dienstleisters zwingend mit der Offenbarung von Geheimnissen verbunden ist, ist ein anderer Dienstleister, der die Leistung ohne Offenbarung erbringen kann, vorzuziehen.

- Bei der Einschaltung von Dienstleistern im Ausland hat der Berufsgeheimnisträger zu prüfen, ob das betreffende Land ein vergleichbares Schutzniveau für Berufsgeheimnisse vorsieht und ein Verstoß vergleichbare Sanktionen nach sich ziehen würde. Ergibt die Prüfung des ausländischen Rechts, dass der Schutz von Geheimnissen vergleichbar ist, darf eine Offenbarung an diese Dienstleister erfolgen.
- Bei einem Cloud-Computing-Dienstleister im Ausland ist nach den Vorgaben des § 203 Abs. 4 Ziff. 2 StGB auf die Geheimhaltung zu verpflichten.
- Ist das Schutzniveau bei dem Dienstleister im Ausland nicht gegeben, muss durch Ergreifen entsprechender technischer Maßnahmen sichergestellt sein, dass durch den Einsatz des Dienstleisters kein Offenbaren im Sinne des § 203 StGB vorliegt (z. B. Verschlüsselung von Daten, so dass ausschließlich der Berufsgeheimnisträger in der Lage ist, die Daten zu entschlüsseln. Der Zugriff seitens des Dienstleisters muss durch technische und organisatorische Maßnahmen entsprechend unterbunden werden).

➢ BSI stellt aktuellen Lagebericht vor

Das Bundesamt für Sicherheit in der Informationstechnik (BSI) hat seinen Bericht „Die Lage der IT-Sicherheit in Deutschland 2022“ veröffentlicht und stellt fest: Die Gefährdungslage im Cyber-Raum ist so hoch wie nie. Cyber-Kriminelle nutzen modernste Technologien für ihre Angriffe auf Privatpersonen, Unternehmen und staatliche Institutionen.

Bedrohungen für die Cybersicherheit sind:

- Ransomware

  Mit dieser Schadsoftware verschlüsseln Hacker Daten oder Systeme, so dass der Nutzer keinen Zugang mehr hat. Für die Entschlüsselung der Daten benötigt die betroffene Person ein bestimmtes Tool, wofür sie dem Hacker ein Lösegeld zahlen soll. Es kommt auch vor, dass damit gedroht wird, sensible Daten zu veröffentlichen. Mehrfaktor-Authentisierung, ein Virtuelles Privates Netz (VPN) und strenge Passwortvorgaben sind hilfreich, um Hackern den Zugang zu den Daten zu erschweren.

- Cyberkriminalität im Zusammenhang mit dem Ukrainekrieg

  Hierbei ist es zu einer Vielzahl von Hacker- und Sabotageangriffen gekommen. So wurden Daten von ukrainischen Banken gelöscht, soziale Medien angegriffen oder auch sog. „Distributed Denial of Servies-Angriffe“ (Überlastungsangriffe auf Internetdienste) auf Ziele in Ländern der EU durchgeführt. Auch das pro-ukrainische Hacker-Kollektiv „Anonymous“ hat Unternehmen außerhalb Russlands angegriffen, die geschäftliche Beziehungen zu Russland gepflegt haben.

➢ Urteile

Videoüberwachungsanlage an Firmen-Eingangstor zur Kontrolle geleisteter Arbeitszeiten ungeeignet

Im Rahmen eines arbeitsrechtlichen Kündigungsschutzprozesses ging es u.a. um die Frage, ob der Betrieb einer Videoüberwachung am Eingang des Werksgeländes rechtmäßig ist und somit etwaige Aufzeichnungen im Gerichtsprozess verwertbar sind.

Die Installation einer Videoüberwachungsanlage am Firmen-Eingangstor ist grundsätzlich ungeeignet, um die geleistete Arbeitszeit der Mitarbeiter zu kontrollieren.

Urteil des Landesarbeitsgerichts Hannover vom 6. Juli 2022 - Az.: 8 Sa 1150/20.

Speicherung von Kundendaten auf externem Server nur vorübergehend zulässig

Auch ohne Zustimmung dürfen Kundendaten bei einer Serverstörung vorübergehend in eine externe Datenbank verlagert werden. Die Daten sind jedoch zu löschen, sobald die Störung beseitigt wurde.

In dem Fall hatte ein führender, ungarischer Anbieter von Internet- und Fernsehdiensten nach einer technischen Störung, die den Betrieb ihres Servers beeinträchtigte, eine Testdatenbank auf einem externen Server eingerichtet. Diese enthielt etwa ein Drittel der Daten ihrer Privatkunden. Nach Beseitigung der Störung wurde diese externe Datenbank jedoch nicht gelöscht.

Die ungarische Datenschutzbehörde beanstandete dies. Der EuGH stellte zunächst fest, dass im Falle einer Störung auch ohne Zustimmung Kundendaten in eine externe Datenbank verlagert werden dürfen. Nach Ablauf der Störung muss diese Datenbank dann jedoch gelöscht werden.

Urteil des Europäischen Gerichtshofes vom 20. Oktober 2022 - Az.: C-77/21

- **Weitere interessante Links**

Was sind DDoS-Angriffe? Wie man sie erkennt und sich schützt
Was verbirgt sich hinter dem Akronym DDoS, wie erkennt man einen DDoS-Angriff und wie schützt man sein Unternehmen davor?
https://www.dr-datenschutz.de/was-sind-ddos-angriffe-wie-man-sie-erkennt-und-sich-schuetzt/

Internetnutzung am Arbeitsplatz und der Datenschutz
Der Artikel erläutert, was bei der Internetnutzung am Arbeitsplatz aus Sicht des Datenschutzes zu beachten ist.
https://www.dr-datenschutz.de/internetnutzung-am-arbeitsplatz-und-der-datenschutz/

Bundesregierung bald ohne Facebook?
Der Bundesregierung droht die Abschaltung ihrer Facebook Fanpage durch den Bundesdatenschutzbeauftragten…
https://www.datenschutz-notizen.de/bundesregierung-bald-ohne-facebook-3337819/

Drittland: Einwilligung nur für gelegentliche Datenübermittlung?
Wann die Datenübermittlungen auf Basis einer Einwilligung in unsichere Drittstaaten erfolgen können, stellt dieser Artikel dar.
https://www.dr-datenschutz.de/drittland-einwilligung-nur-fuer-gelegentliche-datenuebermittlung/

Abmahnung wegen Google Fonts erhalten? Ratgeber mit FAQ, Beispielen und Musterantwort
Über das Thema haben wir Sie bereits informiert. Dieser Beitrag gibt Auskunft über die rechtlichen Hintergründe in Form einer FAQ und Sie finden eine Checkliste sowie Beispiele, an deren Hand Sie Ihr Schreiben einschätzen können. Falls Sie das Schreiben erwidern möchten, finden Sie den Vorschlag für ein Musterschreiben anbei.
https://datenschutz-generator.de/abmahnungen-google-fonts/

Achtung, Datenpanne! Tipps und Hinweise zur Meldung einer Datenpanne
Datenpannen passieren tagtäglich und können unterschiedlichsten Ausmaßes sein und unterschiedlichste Risiken für die Rechte und Freiheiten der von dem Vorfall betroffenen Personen haben.
Was ist eigentlich genau zu tun, wenn eine Datenpanne aufgetreten ist?
https://www.datenschutz-notizen.de/achtung-datenpanne-tipps-und-hinweise-zur-meldung-einer-datenpanne-5938488/

Betriebsrat und Datenschutz: Anforderungen der DSGVO
Welche Rolle der Datenschutz bei den Tätigkeiten des Betriebsrates spielt und auf welche Probleme er stößt, wird in diesem Beitrag kurz zusammengefasst.
https://www.dr-datenschutz.de/betriebsrat-und-datenschutz-anforderungen-der-dsgvo/

Bitkom: Umfrage zur DSGVO
Der Digitalverband Bitkom veröffentlichte vor kurzem die Ergebnisse einer Umfrage, bei der deutsche Unternehmen zur Umsetzung der Datenschutz-Grundverordnung (DSGVO) befragt wurden.
https://www.datenschutzticker.de/2022/10/bitkom-umfrage-zur-dsgvo/

Datenschutzkonforme Personaleinsatzplanung
Was ist datenschutzrechtlich zu beachten, wenn die Personaleinsatzplanung digital unterstützt wird und wie können Arbeitgeber gleich vorweg einen datenschutzkonformen Einsatz durch Technikgestaltung gewährleisten.
https://www.datenschutz-notizen.de/datenschutzkonforme-personaleinsatzplanung-4338594/