SACHSEN-ANHALT
Landesbeauftragter
für den Datenschutz

Empfehlungen für KMU zur Verarbeitung personenbezogener Daten in Heimarbeit

Aufgrund der Pandemie durch den Corona-Virus entschließen sich viele kleine und mittlere Unternehmen, ihre Beschäftigten in Heimarbeit tätig werden zu lassen. Werden bei diesen Tätigkeiten personenbezogene Daten verarbeitet, müssen die datenschutzrechtlichen Vorgaben eingehalten werden. Die Verantwortlichkeit liegt bei der Leitung des jeweiligen Unternehmens. Sie muss die Einhaltung der datenschutzrechtlichen Anforderungen gewährleisten und nachweisen können (Art. 5 Abs. 2 Datenschutz-Grundverordnung (DS-GVO)).

Diese Empfehlungen sollen dazu beitragen, Unternehmen vor Datenverlusten, Angriffen auf ihre datenverarbeitenden Systeme durch Schadsoftware sowie vor sonstigen unbefugten Zugriffen auf ihre Daten zu schützen und die gesetzlichen Vorschriften einzuhalten.

1. Prüfung: Heimarbeit ohne personenbezogene Daten?

Das Unternehmen muss als datenschutzrechtlich Verantwortlicher (Art. 4 Nr. 7 DS-GVO) entscheiden, bei welchen Aufgaben es vertretbar ist, diese in Heimarbeit wahrzunehmen (Art. 24 DS-GVO).
Der für die rechtskonforme Verarbeitung personenbezogener Daten erforderliche organisatorische Aufwand lässt sich im Vorfeld ggf. durch eine sorgfältige Prüfung deutlich verringern. Möglicherweise können - zumindest überwiegend - nur Tätigkeiten in den Bereich der Heimarbeit verlagert werden, die ohne oder nur mit einer geringen Verarbeitung personenbezogener Daten auskommen.

2. Verwendung privater Geräte nicht empfehlenswert

Es ist grundsätzlich nicht empfehlenswert, die Verarbeitung personenbezogener Daten auf privaten Geräten bei der Heimarbeit zu erlauben. Das Problem liegt darin, dass der Arbeitgeber nach Art. 32 DS-GVO Maßnahmen zum Schutz personenbezogener Daten ergreifen muss, auf private Geräte aber in der Regel überhaupt keinen Einfluss ausüben kann. Darüber hinaus wären umfangreiche Analysen und Anpassungen notwendig, um die privaten Geräte sicher in das Arbeitsumfeld zu integrieren.
In seinem IX. Tätigkeitsbericht (Nr. 4.9) äußerte sich der Landesbeauftragte zu der vergleichbaren Problematik der Verwendung privater Geräte am Arbeitsplatz („Bring your own device“). Die Ausführungen sind online nachlesbar unter https://lsaurl.de/dsbyod.

3. Nutzung von Cloud-Speichern

Prinzipiell ist es denkbar, auch Cloud-Speicher für die Heimarbeit zu nutzen. Dies könnte z. B. ein Weg sein, auf benötigte Informationen zuzugreifen oder die eigenen Arbeitsergebnisse an das Unternehmen zu übermitteln.
Es spricht nichts dagegen, wenn mit einem dienstlichen Gerät über eine verschlüsselte Verbindung (z. B. VPN oder per HTTPS im Webbrowser oder per transportverschlüsselter App) auf einen datenschutzkonformen dienstlichen Cloud-Speichern zugegriffen wird.

Es sollte unbedingt darauf geachtet werden, dass bei einer spontanen oder kurzfristigen Entscheidung zur Nutzung von Cloud-Speichern nicht in aller Eile versehentlich auf Dienste zurückgegriffen wird, die den datenschutzrechtlichen Anforderungen nicht genügen.
Außerdem sollten keine Daten mit privaten Geräten aus dienstlichen Cloud-Speichern heruntergeladen werden (siehe auch Ziffer 2.).

Weitere Informationen zur Datenschutzkonformität von Cloud-Speichern finden Sie in der Orientierungshilfe „Cloud Computing“ auf der Homepage des Landesbeauftragten unter https://lsaurl.de/cloudcomp.

4. Fernzugriffe („Remotezugriffe“)

Remotezugriffe per VPN mit dienstlichen Geräten auf dienstliche Netze sind nicht ungewöhnlich und durchaus zulässig. Allerdings sollte die Anbindung per VPN lediglich an einen geschützten Teil der IT-Struktur des Arbeitgebers erfolgen und nicht an das komplette Unternehmensnetz. Der von außen zugänglich geschützte Netzteil sollte nur die Dienste bereitstellen, die auch von außen für die Heimarbeit genutzt werden sollen.
Der für den Zugriff erforderliche Identitätsnachweis der Nutzer sollte durch die Kombination zweier unterschiedlicher und insbesondere voneinander unabhängiger Komponenten erfolgen („Zwei-Faktor-Authentisierung“).

5. Umsetzung und Dokumentation von Festlegungen

Soweit Heimarbeit erlaubt wird, sollten allgemeine Verhaltensanweisungen – z. B. in Form einer unternehmensinternen Regelung – erfolgen. Darin sollte geregelt werden, welche personenbezogenen Daten auf welchen Datenträgern (Papier, mobile Datenträger, PCs) in welcher Weise transportiert und außerhalb der Diensträume bearbeitet werden dürfen. Auch sollte festgelegt werden,

welche dienstlichen Kommunikationswege zu nutzen sind (z. B. Telefon, verschlüsselte E-Mails, VPN, Fax oder Rückgabe der mobilen Datenträger, auf denen die Arbeitsergebnisse gespeichert sind).

Besonders wichtig sind Hinweise an die Heimarbeiter, wie durch ihr eigenes Verhalten der Datenschutz gewährleistet und insbesondere die Kenntnisnahme personenbezogener Daten durch Unberechtigte ausgeschlossen werden kann. Einzuhaltende Sicherheitsmaßnahmen sollten genau beschrieben werden. Hilfreich zur Information der Heimarbeiter sind hier die Hinweise des Unabhängigen Landeszentrums für Datenschutz Schleswig-Holstein, welche unter https://lsaurl.de/uldho aufrufbar sind.
Weitere Hinweise zu gegebenenfalls regelungsbedürftigen Punkten finden Sie z. B. beim Bundesamt für Sicherheit in der Informationstechnik unter https://lsaurl.de/bsiho und bei dem Bundesbeauftragten für den Datenschutz unter https://lsaurl.de/bfditelearbeit.

Durch entsprechende unternehmensinterne Regelungen wird die weisungsgemäße Verarbeitung personenbezogener Daten (Art. 29 DS-GVO) und nebenbei auch der Schutz der Betriebsgeheimnisse sichergestellt. Die entsprechende Dokumentation leistet einen Beitrag zur Erfüllung der Rechenschaftspflicht (Art. 5 Abs. 2 DS-GVO).

Neben einer gründlichen Einweisung (siehe oben) sollten die schriftlichen Regelungen den betroffenen Mitarbeiterinnen und Mitarbeitern ausgehändigt werden. Außerdem sollten ihnen leicht und schnell erreichbare Ansprechpartner für Probleme zur Verfügung gestellt werden.

6. Weitere technische und organisatorische Maßnahmen zur Durchführung von Heimarbeit

Das verantwortliche Unternehmen muss auch bei der Durchführung von Heimarbeit insbesondere unter Berücksichtigung der Art, des Umfangs, der Umstände und der Zwecke der Verarbeitung sowie der Schwere des Risikos für betroffene Personen geeignete technische und organisatorische Maßnehmen treffen, um ein angemessenes Schutzniveau zu gewährleisten (Art. 32 Abs. 1 DS-GVO). Vor diesem Hintergrund ist bei der Verwendung dienstlicher Geräte und Speichermedien außerhalb der Geschäftsräume auf eine Verschlüsselung zu achten. Hinweise zur Datenträgerverschlüsselung finden Sie auf meiner Homepage unter
https://lsaurl.de/Datentraegerschutz.

7. Zusammenfassung

Es gibt keine datenschutzrechtliche Vorschrift, durch die die Heimarbeit generell erlaubt oder verboten wird. Vielmehr müssen die Anforderungen nach der DS-GVO insgesamt eingehalten werden. Bei der Festlegung der notwendigen technischen und organisatorischen Maßnahmen sollten zusammengefasst insbesondere folgende Aspekte berücksichtigt werden:

- Welche Daten dürfen in Heimarbeit verarbeitet werden?
- Bestehende Risiken bei der Verarbeitung personenbezogener Daten in Heimarbeit,
- Schutzbedarf / Sensibilität der jeweiligen Daten,
- Sicherheitsanforderungen (Datensicherung, Verschlüsselung, Virenschutz usw.),
- Wege der Datenübermittlung und der Kommunikation (E-Mail, Messenger, VPN, Mobiltelefon, Fax etc.),
- Regeln zum Umgang mit privaten Telefonen (Löschung von (automatisch) gespeicherten Anrufkontakten, keine Übertragung der eigenen Nummer bei Anrufen),
- Aufbewahrung und Vernichtung bzw. Löschung von Papierunterlagen und elektronischen Datenträgern,
- Maßnahmen der Zugriffskontrolle,
- Sicherung des Arbeitsplatzes (verschließbarer Raum, Geräte und Unterlagen nicht unbeaufsichtigt lassen, auch beim kurzfristigen Verlassen Tür verschließen und Bildschirmschoner mit Passwortschutz aktivieren, Telefonate dürfen nicht für andere hörbar sein, Einsehbarkeit durch Fenster verhindern usw.),
- Trennung von dienstlichen und privaten Daten,
- keine private Hardware an dienstliche Geräte anschließen,
- Verfahrensweisen bei Datenpannen (Verlust von Papierunterlagen, Verlust von Datenträgern, Angriffe auf PC-Systeme, unbefugter Zugang zum PC usw.).
- Ansprechpartner

Impressum
Herausgeber:
Landesbeauftragter für den
Datenschutz Sachsen-Anhalt
Leiterstr. 9
39104 Magdeburg

Tel.: (0391) 81803-0
poststelle@lfd.sachsen-anhalt.de
https://datenschutz.sachsen-anhalt.de

Stand: April 2020