SACHSEN-ANHALT

Landesbeauftragter
für den Datenschutz

Häufige Ursachen von Datenschutzverletzungen und Abwehrmaßnahmen

Im Falle der Verletzung des Schutzes personenbezogener Daten müssen Verantwortliche (Unternehmen und Behörden) nach Art. 33 DS-GVO der Aufsichtsbehörde unverzüglich eine Meldung zukommen lassen (Meldeformular auf Homepage des LfD, https://lsaurl.de/DSVerletzung). Jährlich gehen beim Landesbeauftragten hunderte von Meldungen ein. In der folgenden Tabelle sind die häufigsten Ursachen der Datenschutzverletzungen verzeichnet sowie die technischen und organisatorischen Maßnahmen, die bei eingetretener Verletzung des Schutzes personenbezogener Daten der Behebung der Verletzung bzw. der Abmilderung der nachteiligen Auswirkungen dienen sowie die Maßnahmen, die der präventiven Vermeidung der entsprechenden Verletzungen dienen.

Bei den genannten Maßnahmen handelt es sich um nicht abschließende Empfehlungen, die bei den jeweiligen Datenschutzverletzungen geprüft werden sollten. Es sollte auch stets geprüft werden, ob im Einzelfall weitere Maßnahmen erforderlich sind. Im Falle eines hohen Risikos sind die betroffenen Personen nach Art. 34 DS-GVO zu benachrichtigen. Ein hohes Risiko liegt zumindest immer dann nahe, wenn besondere Kategorien personenbezogener Daten – z. B. Gesundheitsdaten – Unberechtigten zur Kenntnis gelangen können.

Weitere Hinweise – insbesondere zur Datensicherheit und zur Meldepflicht – finden Sie auf der Homepage des Landesbeauftragten unter
https://datenschutz.sachsen-anhalt.de

Ursachen der Datenschutzverletzung	**Maßnahmen zur Behebung der Datenschutzverletzung bzw. zur Abmilderung der nachteiligen Auswirkungen**	**Technische und organisatorische Vorsichtsmaßnahmen zur präventiven Vermeidung der Datenschutzverletzung**
Irrtümliche Versendung von Briefpost an Nichtberechtigte	- Hinweis an den Empfänger, dass er Daten nicht verwenden darf - Aufforderung des Empfängers zur Vernichtung und Bestätigung der Vernichtung bzw. Rücksendung z. B. mit Freiumschlag	- Regelungen zum sorgfältigen Umgang mit Adressdaten erlassen - Sorgfältige Übernahme bzw. Eingabe von Adressinformationen und ggf. Prüfung auf Aktualität - Nutzung von automatisierten Adressierungsverfahren - sorgfältige Prüfung des Adressfeldes - Vier-Augen-Prinzip vor Versand
Fehlerhafter Einzug von Schreiben an unterschiedliche Adressaten durch Kuvertiermaschine (z. B. Einzug von mehreren Schreiben)	- Wie oben - Prüfung und ggf. Einstellung der Kuvertiermaschine durch Fachunternehmen	- Regelmäßige fachgerechte Wartung der Kuvertiermaschine
Versendung von E-Mails an Nichtberechtigte durch fehlerhafte Eingabe der E-Mailadresse	- Fehladressat zum Löschen auffordern - Bestätigung der Löschung einholen	- Antwortfunktion nutzen - Elektronisches Adressbuch nutzen - Ggf. Verschlüsselung der Anlagen, idealerweise der gesamten E-Mail - Nachrichtenabwicklung über webbasiertes Kundenportal
Fehlversand von Dokumenten per Fax (fehlerhafte Eingabe der Faxnummer)	- Fehladressat zum Vernichten auffordern - Fehladressat um Bestätigung der Löschung bitten	- Adressspeicher im Faxgerät nutzen - Sorgfältige Überprüfung der Faxnummer vor Versand, ggf. Vier-Augen-Prinzip
E-Mailversand mit offenem Verteiler	- Alle Empfänger zum Löschen der E-Mail auffordern, ggf. Löschung bestätigen lassen - E-Mail erneut verdeckt versenden	- regelmäßige Sensibilisierung der Mitarbeiter durchführen - Versand als Blindkopie bzw. BCC per Voreinstellung (z. B. E-Mail-Vorlagen nutzen)
Abhandenkommen elektronischer Datenträger (z. B. Einbruchdiebstahl, Datenträger verloren gegangen etc.)	- Fernlöschung, soweit möglich - Sensibilisierung der Mitarbeiter durchführen - Anzeige bei der Polizei erstatten, wenn Straftatverdacht besteht	- Verschlusssicherheit herstellen - Datenträgerverschlüsselung - Regelung zum Umgang mit den Datenträgern treffen - Wiederherstellung der Daten aus dem Backup
Abhandenkommen von papierbasierten Datenträgern (Akten)	- Sensibilisierung der Mitarbeiter durchführen - Anzeige bei der Polizei erstatten, wenn Straftatverdacht besteht	- Verschlusssicherheit herstellen - Regelungen zum Umgang mit den Akten treffen
Entsorgung von Unterlagen mit personenbezogenen Daten im (Papier)-Müll	- Sofortige Sicherstellung der Unterlagen (sofern noch möglich)	- Implementierung datenschutzkonformer Entsorgung - Prüfung durch die Beschäftigten, ob Papiere oder andere Datenträger vernichtet werden müssen - Belehrung/Verpflichtung der Reinigungskräfte (auch im Vertretungsfall) über den Ort der Papierentsorgung

Kompromittierung des Unternehmenskontos bei einem Dienstleister (z. B. bei einer Verkaufsplattform)	- Sofortige Sperrung des Kontos und Passwortwechsel	- 2-Faktor-Authentifizierung bevorzugen, wenn möglich
Verschlüsselung von Dateien durch Angreifer	- sofortige Trennung vom Netz - Schwachstellen identifizieren und Konsequenzen ziehen - ggf. Neuinstallation befallener Rechner/Systeme - Wiederherstellung der Daten aus dem Backup	- detaillierte Regelung schaffen zum Umgang mit eingehenden Dateien, E-Mailanlagen etc. - E-Mail Anhänge/Links nur öffnen/anklicken, wenn Absender und Anhang plausibel sind - Rechte- und Rollenmanagement: Zugriffsrechte so gestalten, dass möglichst nur ein beschränkter Datenumfang und nicht die gesamten Unternehmensdaten betroffen sind - aktueller Virenschutz - regelmäßige System- und Anwendungsaktualisierung
Unberechtigte Zugriffe auf personenbezogene Daten durch Beschäftige zu privaten Zwecken	- bei Verdacht: Auswertung der elektronisch gespeicherten Datenzugriffe - Prüfung von arbeitsrechtlichen Maßnahmen	- Verpflichtung auf das Datengeheimnis (siehe https://lsaurl.de/Kurzpapier19) - Protokollierung der Datenzugriffe
Angriff der zentralen IT-Infrastruktur durch Sicherheitslücken (z. B. im Exchangeserver, bei Log4j,)	- betroffene Dienste einschränken - betroffene Systeme vom Netz nehmen - betroffene Systeme neu aufsetzen - Sicherungen zurückspielen - dedizierte Sicherheitspatches einspielen - Hinweise des Bundesamtes für die Sicherheit in der Informationstechnik befolgen https://www.bsi.bund.de	- regelmäßige automatisierte Updates - regelmäßig aktuelle Cybersicherheitsmeldungen (CVS) der einschlägigen Computer Emergency Response Teams (CERT) verfolgen - regelmäßige Sicherheitsaudits
Erlangen von Zugangsdaten durch Täuschung oder Phishing	- sofortiger Passwortwechsel - Ausmaß der Fremdnutzung der Zugangsdaten ermitteln und entsprechend reagieren	- Sensibilisierung der Beschäftigten - regelmäßige Recherche aktuell verbreiteter Täuschungsstrategien - 2-Faktoren-Authentifizierung - regelmäßige Passwortwechsel - Spam-Filter betreiben
Fremdnutzung der eigenen Postfächer für Spammails aufgrund des Emotet-Virus	- sofortiger Passwortwechsel - gründlicher Virenscan - betroffene Endgeräte neu aufsetzen - BSI-Hinweise befolgen	- regelmäßige automatisierte Updates - aktueller Virenschutz - Makroausführung deaktivieren - Spam-Filter betreiben
Anfertigung von Fotografien durch Beschäftigte und unberechtigte Veröffentlichung (in sozialen Netzwerken)	- Versuch die Verbreitung weitestgehend einzudämmen - Sensibilisierung der Mitarbeiter - Prüfung arbeitsrechtlicher Maßnahmen	- Regelungen zum Fotografieren in der Einrichtung und zur Veröffentlichung der Fotografien treffen
Aufzeichnung von Gesprächen	- Sensibilisierung der Mitarbeiter - Hinweis auf das grundsätzliche Verbot der Aufnahme (ohne Einwilligung) - Prüfung arbeitsrechtlicher Maßnahmen	- Sensibilisierung der Mitarbeiter - Regelung der Rahmenbedingungen für Aufnahmen (Einwilligung der Betroffenen) treffen
Veröffentlichung personenbezogener Daten ohne Rechtsgrundlage	- Löschung der Veröffentlichung, falls möglich - Versuch, die Verbreitung weitestgehend einzudämmen	- Regelungen zur Prüfung der Rechtmäßigkeit vor Veröffentlichung treffen - Vier-Augen-Prinzip vor Veröffentlichung - Schwärzung von personenbezogenen Daten aus zu veröffentlichenden Dokumenten
Datenschutzvorfälle beim Auftragsverarbeiter	- Dokumentation der Vorfälle, auch beim Auftragsverarbeiter - Aufklärung zusichern lassen - Abhilfe-Maßnahmen mitteilen lassen und prüfen	- Auftragnehmer nach Eignung hinsichtlich angebotener Sicherheitsmaßnahmen auswählen - Im Vertrag zur Auftragsverarbeitung Benachrichtigungsregeln vereinbaren - Auftragnehmer sensibilisieren
Unbefugte Datenverarbeitung oder Offenlegung durch eigene Mitarbeiter	- Prüfung arbeitsrechtlicher Maßnahmen - Prüfung strafrechtlicher Maßnahmen - Entzug der Zugriffsrechte des Mitarbeiters - Belehrung des Mitarbeiters, dass wahrgenommene Daten nicht zu privaten Zwecken genutzt werden dürfen	- engmaschiges Rechte- und Rollenkonzept umsetzen - individuelle Nutzerkennungen - 2-Faktoren-Authentifizierung - Protokollierung von Datenzugriffen - Sensibilisierung der Beschäftigten über strafrechtliche Folgen und Bußgelder
Versehentlicher öffentlicher Zugang zu internen Datenbeständen	- sofortige Kappung des öffentlichen Zugangs - Ermittlung, ob Datenzugriffe stattgefunden haben - unbefugte Empfänger zur Löschung auffordern	- Beschäftigte der IT sensibilisieren - Konfigurationsrichtlinien festlegen - Veröffentlichung nur im Vier-Augen-Prinzip - gesicherte Fernadministrationszugänge betreiben - erfahrene Dienstleister einsetzen - öffentliche Zugänge regelmäßig überprüfen

Genderhinweis: Aus Gründen der besseren Lesbarkeit wird auf die gleichzeitige Verwendung der Sprachformen männlich, weiblich und divers (m/w/d) verzichtet. Sämtliche Personenbezeichnungen gelten gleichermaßen für alle Geschlechter.