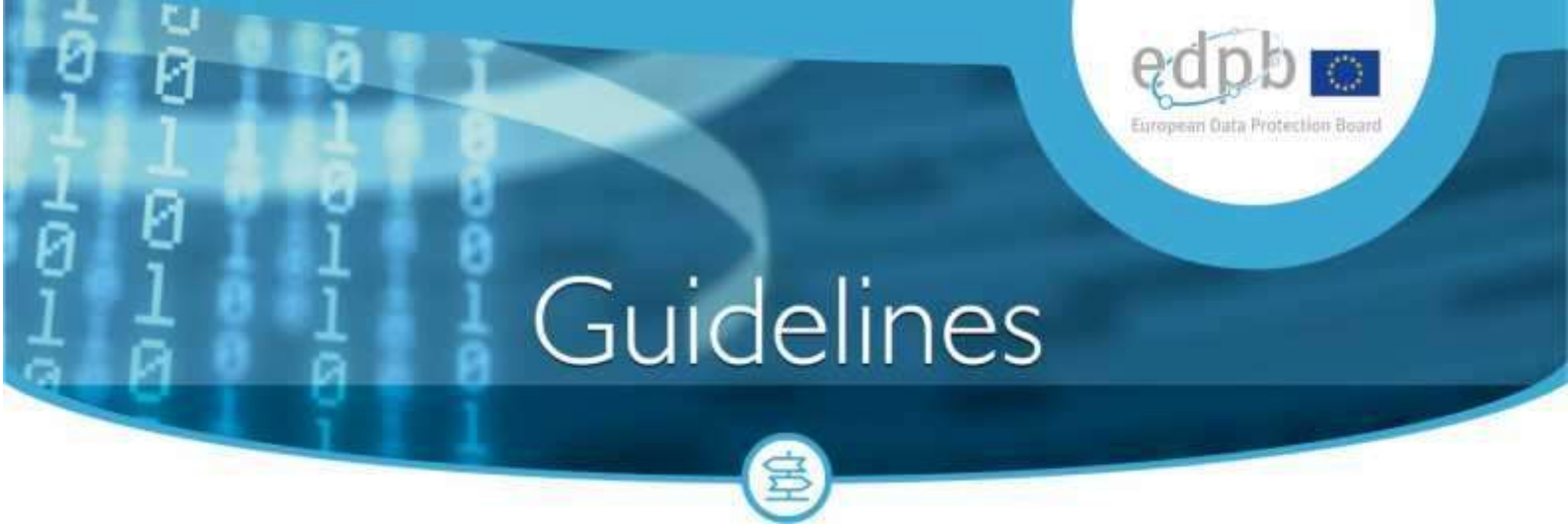

Richtlinien 01/2021

on Beispiele zur Data Breach Notification

Verabschiedet am 14. Januar 2021

Version 1.0

[Nicholas Vollmer: Dies ist noch eine ENTWURFS-Version!
Die Fußnoten wurden entfernt, um eine automatische Übersetzung zu erleichtern.
Diese Übersetzung ist NICHT offiziell.]

Inhaltsübersicht

DER EUROPÄISCHE DATENSCHUTZAUSSCHUSS

gestützt auf Artikel 70 (1e) der Verordnung (EU) 2016/679 des Europäischen Parlaments und des Rates vom 27. April 2016 zum Schutz natürlicher Personen bei der Verarbeitung personenbezogener Daten, zum freien Datenverkehr und zur Aufhebung der Richtlinie 95/46/EG, (nachfolgend "DSGVO"),

gestützt auf das EWR-Abkommen, insbesondere auf Anhang XI und Protokoll 37, geändert durch den Beschluss des Gemeinsamen EWR-Ausschusses Nr. 154/2018 vom 6. Juli 20181,

gestützt auf Artikel 12 und Artikel 22 seiner Geschäftsordnung,

gestützt auf die Mitteilung der Kommission an das Europäische Parlament und den Rat mit dem Titel "Der Datenschutz als Säule der Bürgerbeteiligung und das Konzept der EU für den digitalen Wandel - zwei Jahre Anwendung der Datenschutz-Grundverordnung "2,

HAT DIE FOLGENDEN RICHTLINIEN VERABSCHIEDET

1 EINLEITUNG

1. Die DSGVO führt die Anforderung ein, dass eine Verletzung des Schutzes personenbezogener Daten der zuständigen nationalen Aufsichtsbehörde (im Folgenden "SA") gemeldet werden muss und in bestimmten Fällen den Personen, deren personenbezogene Daten von der Verletzung betroffen sind, mitgeteilt werden muss (Artikel 33 und 34).

2. Die Artikel-29-Datenschutzgruppe hat bereits im Oktober 2017 einen *allgemeinen* Leitfaden zur Meldung von Datenschutzverletzungen erstellt, in dem die einschlägigen Abschnitte der DSGVO analysiert werden (Leitlinien zur Meldung von Datenschutzverletzungen nach der Verordnung (EU) 2016/679, WP 250) (im Folgenden "Leitlinien WP250")[3]. Aufgrund ihrer Art und ihres Zeitpunkts wurden in dieser Leitlinie jedoch nicht alle praktischen Fragen hinreichend detailliert behandelt. Daher ist der Bedarf an einem *praxisorientierten, fallbasierten* Leitfaden entstanden, der die Erfahrungen nutzt, die die ORKB seit der Anwendbarkeit der DSGVO gesammelt haben.

3. Dieses Dokument soll die Leitlinien WP 250 ergänzen und spiegelt die gemeinsamen Erfahrungen der ORKB des EWR seit dem Inkrafttreten der DSGVO wider. Sein Ziel ist es, den für die Datenverarbeitung Verantwortlichen bei der Entscheidung zu helfen, wie sie mit Datenschutzverletzungen umgehen und welche Faktoren bei der Risikobewertung zu berücksichtigen sind.

---

4. Als Teil jedes Versuchs, eine Datenschutzverletzung zu beheben, sollte der für die Verarbeitung Verantwortliche zunächst in der Lage sein, eine solche zu erkennen. Die DSGVO definiert eine "Verletzung des Schutzes personenbezogener Daten" in Artikel 4(12) als "eine Verletzung der Sicherheit, die zur zufälligen oder unrechtmäßigen Zerstörung, zum Verlust, zur Veränderung, zur unbefugten Weitergabe oder zum unbefugten Zugang zu übermittelten, gespeicherten oder anderweitig verarbeiteten personenbezogenen Daten führt".

5. In ihrer Stellungnahme 03/2014 zur Meldung von Sicherheitsverletzungen4 und in ihren Leitlinien WP

250 erklärte die WP29, dass Sicherheitsverletzungen nach den folgenden drei bekannten Grundsätzen der Informationssicherheit kategorisiert werden können:

- "Vertraulichkeitsverletzung" - wenn es zu einer unbefugten oder versehentlichen Offenlegung von oder einem Zugriff auf persönliche Daten kommt.
- "Integritätsverletzung" - wenn es zu einer unbefugten oder versehentlichen Änderung von personenbezogenen Daten kommt.
- "Verfügbarkeitsverletzung" - wenn ein versehentlicher oder unbefugter Verlust des Zugriffs auf oder die Zerstörung von personenbezogenen Daten vorliegt5.

6. Eine Datenschutzverletzung kann potenziell eine Reihe von erheblichen nachteiligen Auswirkungen auf Einzelpersonen haben, die zu physischem, materiellem oder immateriellem Schaden führen können. Die DSGVO erklärt, dass dies den Verlust der Kontrolle über ihre personenbezogenen Daten, die Einschränkung ihrer Rechte, Diskriminierung, Identitätsdiebstahl oder Betrug, finanzielle Verluste, die unbefugte Aufhebung der Pseudonymisierung, Rufschädigung und den Verlust der Vertraulichkeit personenbezogener Daten, die durch das Berufsgeheimnis geschützt sind, umfassen kann. Sie kann auch jeden anderen erheblichen wirtschaftlichen oder sozialen Nachteil für diese Personen umfassen. Eine der wichtigsten Pflichten des Datenverantwortlichen ist es, diese Risiken für die Rechte und Freiheiten der betroffenen Personen zu bewerten und geeignete technische und organisatorische Maßnahmen zu ergreifen, um ihnen zu begegnen.
7. Dementsprechend verlangt die GDPR von dem für die Verarbeitung Verantwortlichen:
    - jede Verletzung des Schutzes personenbezogener Daten zu dokumentieren, einschließlich der Fakten in Bezug auf die Verletzung des Schutzes personenbezogener Daten, ihre Auswirkungen und die ergriffenen Abhilfemaßnahmen6;
    - die Verletzung des Schutzes personenbezogener Daten der Aufsichtsbehörde melden, es sei denn, es ist unwahrscheinlich, dass die Verletzung der Daten ein Risiko für die Rechte und Freiheiten natürlicher Personen darstellt7;

- die betroffene Person über die Verletzung des Schutzes personenbezogener Daten zu informieren, wenn die Verletzung des Schutzes personenbezogener Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führen wird8.

8. Datenschutzverletzungen sind an und für sich ein Problem, aber sie sind auch ein Symptom für ein anfälliges, möglicherweise veraltetes Datensicherheitssystem und weisen somit auf Systemschwächen hin, die behoben werden müssen. Generell gilt, dass es immer besser ist, Datenschutzverletzungen zu verhindern, indem man sich im Voraus darauf vorbereitet, da einige ihrer Folgen von Natur aus unumkehrbar sind. Bevor ein für die Verarbeitung Verantwortlicher das Risiko, das sich aus einer durch eine Form des Angriffs verursachten Verletzung ergibt, *vollständig einschätzen* kann, sollte die Ursache des Problems ermittelt werden, um festzustellen, ob die Schwachstellen, die zu dem Vorfall geführt haben, immer noch vorhanden und somit ausnutzbar sind. In vielen Fällen ist der Controller in der Lage zu erkennen, dass der Vorfall wahrscheinlich zu einem Risiko führt und daher zu melden ist. In anderen Fällen muss die Benachrichtigung nicht aufgeschoben werden, bis das Risiko und die Auswirkungen im Zusammenhang mit der Sicherheitsverletzung vollständig bewertet wurden, da die vollständige Risikobewertung parallel zur Benachrichtigung erfolgen kann und die so gewonnenen Informationen ohne unangemessene weitere Verzögerung schrittweise an die SA weitergeleitet werden können9.

9. Die Verletzung sollte gemeldet werden, wenn der für die Verarbeitung Verantwortliche der Meinung ist, dass sie wahrscheinlich zu einem Risiko für die Rechte und Freiheiten der betroffenen Person führt. Die für die Verarbeitung Verantwortlichen sollten diese Einschätzung zu dem Zeitpunkt vornehmen, zu dem sie von der Verletzung Kenntnis erlangen. Der für die Verarbeitung Verantwortliche sollte nicht auf eine ausführliche forensische Untersuchung und (frühzeitige) Abhilfemaßnahmen warten, bevor er beurteilt, ob die Datenschutzverletzung wahrscheinlich zu einem Risiko führt und daher gemeldet werden sollte oder nicht.

10. Wenn ein Kontrolleur das Risiko selbst als unwahrscheinlich einschätzt, es sich aber herausstellt, dass das Risiko eintritt, kann die zuständige ORKB von ihren Korrekturbefugnissen Gebrauch machen und ggf. Sanktionen beschließen.

11. Jeder für die Verarbeitung Verantwortliche sollte Pläne und Verfahren für den Umgang mit eventuellen Datenverletzungen haben. Organisationen sollten klare Berichtslinien und Personen haben, die für bestimmte Aspekte des Wiederherstellungsprozesses verantwortlich sind.

12. Schulungen und Sensibilisierung des Personals des für die Verarbeitung Verantwortlichen für Datenschutzfragen mit Schwerpunkt auf dem Umgang mit Verletzungen des Schutzes personenbezogener Daten (Erkennung eines Vorfalls einer Verletzung des Schutzes personenbezogener Daten und weitere zu ergreifende Maßnahmen usw.) sind für die für die Verarbeitung Verantwortlichen ebenfalls von wesentlicher Bedeutung. Diese Schulungen sollten je nach Art der Verarbeitungstätigkeit und Größe des für die Verarbeitung Verantwortlichen regelmäßig wiederholt werden, wobei die neuesten Trends und Warnungen aus Cyberangriffen oder anderen Sicherheitsvorfällen behandelt werden sollten.

13. Der Grundsatz der Rechenschaftspflicht und das Konzept des "eingebauten Datenschutzes" könnten eine Analyse beinhalten, die in ein eigenes "Handbuch für den Umgang mit Verletzungen des Schutzes personenbezogener Daten" eines für die Verarbeitung Verantwortlichen einfließt, das darauf abzielt, Fakten für jede Facette der Verarbeitung in jeder wichtigen Phase des Vorgangs zu schaffen. Ein solches, im Voraus erstelltes Handbuch würde eine viel schnellere Informationsquelle darstellen, die es den für die Datenverarbeitung Verantwortlichen ermöglicht, die Risiken zu mindern

und die Verpflichtungen ohne unangemessene Verzögerung zu erfüllen. Dies würde sicherstellen, dass im Falle einer Verletzung des Schutzes personenbezogener Daten die Mitarbeiter der Organisation wissen, was zu tun ist, und dass der Vorfall mit großer Wahrscheinlichkeit schneller abgewickelt wird, als wenn keine Abhilfemaßnahmen oder Pläne vorhanden sind.

14. Obwohl die im Folgenden dargestellten Fälle fiktiv sind, basieren sie auf typischen Fällen aus der kollektiven Erfahrung der SA mit Meldungen von Datenschutzverletzungen. Die angebotenen Analysen beziehen sich explizit auf die Fälle

unter die Lupe genommen, sondern mit dem Ziel, den für die Datenverarbeitung Verantwortlichen eine Hilfestellung bei der Bewertung ihrer eigenen Datenverletzungen zu geben. Jede Änderung der Umstände der nachfolgend beschriebenen Fälle kann zu unterschiedlichen oder bedeutenderen Risikostufen führen und somit andere oder zusätzliche Maßnahmen erfordern. Diese Leitlinien strukturieren die Fälle nach bestimmten Kategorien von Datenschutzverletzungen (z. B. Ransomware-Angriffe). Bestimmte Maßnahmen zur Risikominderung sind in jedem Fall erforderlich, wenn es um eine bestimmte Kategorie von Sicherheitsverletzungen geht. Diese Maßnahmen werden nicht notwendigerweise in jeder Fallanalyse wiederholt, die zur gleichen Kategorie von Sicherheitsverletzungen gehört. Bei den Fällen, die zur gleichen Kategorie gehören, werden nur die Unterschiede dargelegt. Daher sollte der Leser alle Fälle lesen, die zu einer bestimmten Kategorie von Verstößen gehören, um alle richtigen Maßnahmen zu erkennen und zu unterscheiden, die ergriffen werden müssen.

15. Die interne Dokumentation eines Verstoßes ist eine von den mit dem Verstoß verbundenen Risiken unabhängige Pflicht, die in jedem Fall erfüllt werden muss. Die im Folgenden vorgestellten Fälle versuchen, etwas Licht in die Frage zu bringen, ob die Verletzung bei der SA gemeldet und den betroffenen Personen mitgeteilt werden muss oder nicht.

2 RANSOMWARE

16. Ein häufiger Grund für eine Benachrichtigung über eine Datenschutzverletzung ist ein Ransomware-Angriff, den der für die Datenverarbeitung Verantwortliche erlitten hat. In diesen Fällen verschlüsselt ein bösartiger Code die personenbezogenen Daten, und anschließend verlangt der Angreifer von der verantwortlichen Stelle ein Lösegeld im Austausch für den Entschlüsselungscode. Diese Art von Angriff kann in der Regel als eine Verletzung der Verfügbarkeit eingestuft werden, aber oft kann auch eine Verletzung der Vertraulichkeit auftreten.

2.1 FALL Nr. 01: Ransomware mit ordentlichem Backup und ohne Exfiltration

Die Computersysteme eines kleinen Fertigungsunternehmens waren einem Ransomware-Angriff ausgesetzt, und die in diesen Systemen gespeicherten Daten wurden verschlüsselt. Der Datenverantwortliche verwendete Encryption at Rest, d. h. alle Daten, auf die die Ransomware zugriff, wurden mit einem modernen Verschlüsselungsalgorithmus verschlüsselt gespeichert. Der Entschlüsselungsschlüssel wurde bei dem Angriff nicht kompromittiert, d. h. der Angreifer konnte weder auf ihn zugreifen noch ihn indirekt verwenden. Folglich hatte der Angreifer nur Zugriff auf verschlüsselte persönliche Daten. Insbesondere waren weder das E-Mail-System des Unternehmens noch die Client-Systeme, die darauf zugreifen, betroffen. Das Unternehmen nutzt die Expertise eines externen Cybersecurity-Unternehmens, um den Vorfall zu untersuchen. Es liegen Protokolle vor, die alle Datenströme, die das Unternehmen verlassen haben (einschließlich ausgehender E-Mails), nachvollziehen. Nach der Analyse der Protokolle und der Daten, die von den im Unternehmen eingesetzten Erkennungssystemen gesammelt wurden, hat eine interne Untersuchung mit Unterstützung des externen Cybersecurity-Unternehmens *mit Sicherheit* festgestellt, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Die Protokolle zeigen keinen Datenfluss nach außen im Zeitraum des Angriffs. Die von der Verletzung betroffenen personenbezogenen Daten betreffen Kunden und Mitarbeiter des Unternehmens,

17. In diesem Fall wurden die folgenden Elemente aus der Definition einer "Verletzung des Schutzes personenbezogener Daten" realisiert: a
Die Verletzung der Sicherheit führte zu unrechtmäßiger Veränderung und unbefugtem Zugriff auf die

gespeicherten personenbezogenen Daten.

2.1.1 FALL Nr. 01 - Vorherige Maßnahmen und Risikobewertung

18. Wie bei allen Risiken, die von externen Akteuren ausgehen, kann die Wahrscheinlichkeit, dass ein Ransomware-Angriff erfolgreich ist, drastisch reduziert werden, indem die Sicherheit der Datenkontrollumgebung verschärft wird. Die meisten dieser Verstöße können verhindert werden, indem sichergestellt wird, dass angemessene organisatorische, physische und technologische Sicherheitsmaßnahmen ergriffen wurden. Beispiele für solche Maßnahmen sind ein ordnungsgemäßes Patch-Management und der Einsatz eines geeigneten Anti-Malware-Erkennungssystems. Eine ordnungsgemäße und separate Datensicherung hilft dabei

die Folgen eines erfolgreichen Angriffs abzumildern, sollte dieser stattfinden. Darüber hinaus hilft ein Programm zur Sicherheitsausbildung, -schulung und -aufklärung (SETA) der Mitarbeiter, diese Art von Angriffen zu verhindern und zu erkennen. (Eine Liste empfehlenswerter Maßnahmen finden Sie in Abschnitt 2.5) Unter diesen Maßnahmen ist ein ordentliches Patch-Management, das sicherstellt, dass die Systeme auf dem neuesten Stand sind und alle bekannten Schwachstellen der eingesetzten Systeme behoben sind, eine der wichtigsten, da die meisten Ransomware-Angriffe bekannte Schwachstellen ausnutzen.

19. Bei der Bewertung der Risiken sollte der Controller die Verletzung untersuchen und die Art des Schadcodes identifizieren, um die möglichen Folgen des Angriffs zu verstehen. Zu den zu berücksichtigenden Risiken gehört das Risiko, dass Daten exfiltriert wurden, ohne eine Spur in den Protokollen der Systeme zu hinterlassen.

20. In diesem Beispiel hatte der Angreifer Zugriff auf personenbezogene Daten und die Vertraulichkeit des Chiffriertextes, der personenbezogene Daten in verschlüsselter Form enthält, wurde beeinträchtigt. Daten, die möglicherweise exfiltriert wurden, können jedoch vom Täter zumindest vorerst nicht gelesen oder verwendet werden. Die vom Datenverantwortlichen verwendete Verschlüsselungstechnik entspricht dem Stand der Technik. Der Entschlüsselungsschlüssel wurde nicht kompromittiert und konnte vermutlich auch nicht auf anderem Wege ermittelt werden. Folglich sind die Vertraulichkeitsrisiken für die Rechte und Freiheiten natürlicher Personen auf ein Minimum reduziert, es sei denn, es gibt kryptoanalytische Fortschritte, die die verschlüsselten Daten in Zukunft verständlich machen.

21. Der für die Verarbeitung Verantwortliche sollte die Auswirkungen und den Schweregrad der Verletzung berücksichtigen. In diesem Fall scheinen die Risiken für die Rechte und Freiheiten der betroffenen Personen aus der mangelnden Verfügbarkeit der personenbezogenen Daten zu resultieren, und die Vertraulichkeit der personenbezogenen Daten ist nicht gefährdet10. In diesem Beispiel wurden die nachteiligen Auswirkungen der Datenschutzverletzung relativ bald nach dem Eintreten der Verletzung gemildert. Das Vorhandensein eines ordnungsgemäßen Sicherungssystems11 mildert die Auswirkungen der Verletzung, und in diesem Fall war der für die Verarbeitung Verantwortliche in der Lage, es effektiv zu nutzen.

22. Hinsichtlich der Schwere der Folgen für die betroffenen Personen konnten nur geringfügige Folgen festgestellt werden, da die betroffenen Daten innerhalb weniger Stunden wiederhergestellt wurden, die Verletzung keine Folgen für den täglichen Betrieb des für die Verarbeitung Verantwortlichen hatte und sich nicht wesentlich auf die betroffenen Personen auswirkte (z. B. Mitarbeiterzahlungen oder die Bearbeitung von Kundenanfragen).

2.1.2 FALL Nr. 01 - Schadensbegrenzung und Verpflichtungen

23. Ohne ein Backup können nur wenige Maßnahmen zur Behebung des Verlusts personenbezogener Daten durch den Controller ergriffen werden, und die Daten müssen erneut erfasst werden. In diesem speziellen Fall konnten die Auswirkungen des Angriffs jedoch effektiv eingedämmt werden, indem alle kompromittierten Systeme auf einen sauberen Zustand zurückgesetzt wurden, von dem bekannt war, dass er frei von schädlichem Code ist, die Schwachstellen behoben und die betroffenen Daten bald nach dem Angriff wiederhergestellt wurden.

[10] Technisch gesehen erfordert die Verschlüsselung von Daten einen "Zugriff" auf die Originaldaten und im Fall

von Ransomware die Löschung des Originals - auf die Daten muss durch den Ransomware-Code zugegriffen werden, um sie zu verschlüsseln und um die Originaldaten zu entfernen. Ein Angreifer kann vor der Löschung eine Kopie des Originals anfertigen, aber die personenbezogenen Daten werden nicht immer extrahiert. Im Laufe der Ermittlungen eines Datenverantwortlichen können neue Informationen ans Licht kommen, die diese Einschätzung ändern. Ein Zugriff, der zu einer unrechtmäßigen Zerstörung, einem Verlust, einer Veränderung, einer unbefugten Weitergabe der personenbezogenen Daten oder zu einem Sicherheitsrisiko für eine betroffene Person führt, kann auch ohne Auswertung der Daten genauso schwerwiegend sein wie ein Zugriff mit Auswertung der personenbezogenen Daten.

[11] Sicherungsverfahren sollten strukturiert, konsistent und wiederholbar sein. Beispiele für Sicherungsverfahren sind die 3-2-1-Methode und die Großvater-Vater-Sohn-Methode. Jede Methode sollte immer auf ihre Wirksamkeit in Bezug auf die Abdeckung und die Wiederherstellung von Daten getestet werden. Die Tests sollten auch in regelmäßigen Abständen und insbesondere dann wiederholt werden, wenn sich der Verarbeitungsprozess oder seine Umstände ändern, um die Integrität des Systems zu gewährleisten.

Ohne ein Backup gehen Daten verloren und die Schwere kann sich erhöhen, da auch Risiken oder Auswirkungen auf Personen entstehen können.

24. Die Rechtzeitigkeit einer effektiven Datenwiederherstellung aus dem sofort verfügbaren Backup ist eine Schlüsselvariable bei der Analyse der Sicherheitsverletzung. Die Festlegung eines angemessenen Zeitrahmens für die Wiederherstellung der kompromittierten Daten hängt von den einzigartigen Umständen der jeweiligen Verletzung ab. Die DSGVO besagt, dass eine Verletzung des Schutzes personenbezogener Daten ohne unangemessene Verzögerung und, wenn möglich, spätestens nach 72 Stunden gemeldet werden muss. Daher könnte festgestellt werden, dass eine Überschreitung der 72-Stunden-Frist in jedem Fall nicht ratsam ist, aber bei Fällen mit hohem Risikoniveau kann sogar die Einhaltung dieser Frist als unbefriedigend angesehen werden.

25. In diesem Fall hat der für die Verarbeitung Verantwortliche nach einer detaillierten Folgenabschätzung und einem Verfahren zur Reaktion auf den Vorfall festgestellt, dass die Verletzung wahrscheinlich nicht zu einem Risiko für die Rechte und Freiheiten natürlicher Personen führt, so dass keine Mitteilung an die betroffenen Personen erforderlich ist und die Verletzung auch nicht der Aufsichtsbehörde gemeldet werden muss. Wie alle Datenschutzverletzungen sollte sie jedoch gemäß Artikel 33 (5) dokumentiert werden. Die Organisation muss möglicherweise auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren (oder wird später von der Aufsichtsbehörde dazu aufgefordert) und nachbessern.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Kein Risiko (internes Register)	Risiko (SA benachrichtigen)	Hohes Risiko (Kommunikation mit betroffenen Personen)
	X	X

2.2 FALL Nr. 02: Ransomware ohne ordnungsgemäßes Backup

Einer der von einem landwirtschaftlichen Unternehmen genutzten Computer war einem Ransomware-Angriff ausgesetzt und seine Daten wurden vom Angreifer verschlüsselt. Das Unternehmen nutzt die Expertise eines externen Cybersecurity-Unternehmens, um sein Netzwerk zu überwachen. Es liegen Protokolle vor, die alle Datenströme verfolgen, die das Unternehmen verlassen (einschließlich ausgehender E-Mails). Nach der Analyse der Protokolle und der Daten, die die anderen Erkennungssysteme gesammelt haben, stellt die interne Untersuchung mit Unterstützung des Cybersecurity-Unternehmens fest, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Die Protokolle zeigen keinen Datenfluss nach außen im Zeitrahmen des Angriffs. Die von der Sicherheitsverletzung betroffenen personenbezogenen Daten beziehen sich auf die Mitarbeiter und Kunden des Unternehmens, insgesamt einige Dutzend Personen. Es waren keine besonderen Kategorien von Daten

2.2.1 FALL Nr. 02 - Vorherige Maßnahmen und Risikobewertung

26. Der für die Verarbeitung Verantwortliche hätte die gleichen vorherigen Maßnahmen ergreifen müssen, wie in Teil 2.1. und in Abschnitt 2.9. erwähnt. Der Hauptunterschied zum vorherigen Fall ist das Fehlen eines elektronischen Backups und das Fehlen einer Verschlüsselung im Ruhezustand. Dies führt zu kritischen Unterschieden bei den folgenden Schritten.

27. Bei der Risikobewertung sollte der für die Verarbeitung Verantwortliche die Methode der Infiltration

untersuchen und den Typ des Schadcodes identifizieren, um die möglichen Folgen des Angriffs zu verstehen. In diesem Beispiel verschlüsselte die Ransomware die personenbezogenen Daten, ohne sie zu exfiltrieren. Daher scheint es, dass die Risiken für die Rechte und Freiheiten der betroffenen Personen aus der mangelnden Verfügbarkeit der personenbezogenen Daten resultieren und die Vertraulichkeit der personenbezogenen Daten nicht gefährdet ist. Eine gründliche Untersuchung der Firewall-Protokolle und ihrer Auswirkungen ist für die Bestimmung des Risikos unerlässlich. Der für die Datenverarbeitung Verantwortliche sollte die sachlichen Ergebnisse dieser Untersuchungen auf Anfrage vorlegen.

28. Der für die Datenverarbeitung Verantwortliche muss bedenken, dass bei einem ausgefeilteren Angriff die Malware über die Funktionalität verfügt, Protokolldateien zu bearbeiten und die Spuren zu entfernen. Da die Protokolle nicht an einen zentralen Protokollserver weitergeleitet oder repliziert werden, kann der für die Datenverarbeitung Verantwortliche selbst nach einer gründlichen Untersuchung, bei der festgestellt wurde, dass die personenbezogenen Daten nicht vom Angreifer exfiltriert wurden, nicht behaupten, dass das Fehlen eines Protokolleintrags das Fehlen einer Exfiltration beweist, weshalb die Wahrscheinlichkeit einer Verletzung der Vertraulichkeit nicht vollständig ausgeschlossen werden kann.

29. Der für die Datenverarbeitung Verantwortliche sollte die Risiken dieser Verletzung bewerten, wenn der Angreifer Zugriff auf die Daten hatte. Bei der Risikobewertung sollte der für die Datenverarbeitung Verantwortliche auch die Art, die Sensibilität, den Umfang und den Kontext der von der Verletzung betroffenen personenbezogenen Daten berücksichtigen. In diesem Fall sind keine besonderen Kategorien personenbezogener Daten betroffen, und die Menge der verletzten Daten und die Anzahl der betroffenen Personen ist gering.

30. Das Sammeln genauer Informationen über den unbefugten Zugriff ist der Schlüssel zur Bestimmung des Risikoniveaus und zur Verhinderung eines neuen oder fortgesetzten Angriffs. Wenn die Daten aus der Datenbank kopiert worden wären, wäre dies natürlich ein risikoerhöhender Faktor. Wenn man sich über die Einzelheiten des unrechtmäßigen Zugriffs nicht sicher ist, sollte man das schlimmere Szenario in Betracht ziehen und das Risiko entsprechend einschätzen.

31. Das Fehlen einer Backup-Datenbank kann als risikoerhöhender Faktor betrachtet werden, je nach Schwere der Folgen für die betroffenen Personen, die sich aus der fehlenden Verfügbarkeit der Daten ergeben.

2.2.2 FALL Nr. 02 - Minderung und Verpflichtungen

32. Ohne ein Backup können vom für die Verarbeitung Verantwortlichen nur wenige Maßnahmen zur Behebung des Verlusts personenbezogener Daten ergriffen werden, und die Daten müssen erneut erfasst werden, sofern keine andere Quelle zur Verfügung steht (z. B. Auftragsbestätigungs-E-Mails). Ohne ein Backup können Daten verloren gehen, und die Schwere hängt von den Auswirkungen für die Personen ab.

33. Die Wiederherstellung der Daten sollte sich nicht als übermäßig problematisch erweisen12 , wenn die Daten noch in Papierform vorliegen, aber angesichts des Fehlens einer elektronischen Sicherungsdatenbank wird eine Meldung an die ORKB als notwendig erachtet, da die Wiederherstellung der Daten einige Zeit in Anspruch genommen hat und einige Verzögerungen bei der Auslieferung der Aufträge an die Kunden verursachen könnte und eine beträchtliche Menge an Metadaten (z. B. Protokolle, Zeitstempel) möglicherweise nicht abrufbar ist.

34. Die Information der betroffenen Personen über die Sicherheitsverletzung kann auch davon abhängen, wie lange die personenbezogenen Daten nicht verfügbar sind und welche Schwierigkeiten sich daraus für den Betrieb des für die Verarbeitung Verantwortlichen ergeben könnten (z. B. Verzögerungen bei der Überweisung von Mitarbeiterzahlungen). Da diese Verzögerungen bei Zahlungen und Lieferungen zu finanziellen Verlusten für die Personen führen können, deren Daten kompromittiert wurden, könnte man auch argumentieren, dass die Verletzung wahrscheinlich zu einem hohen Risiko führt. Außerdem könnte es sich als unumgänglich erweisen, die betroffenen Personen zu informieren, wenn ihr Beitrag zur Wiederherstellung der verschlüsselten Daten erforderlich ist.

35. Dieser Fall dient als Beispiel für einen Ransomware-Angriff mit einem Risiko für die Rechte und

Freiheiten der betroffenen Personen, der jedoch kein hohes Risiko erreicht. Er sollte gemäß Artikel 33 Absatz 5 dokumentiert und der SA gemäß Artikel 33 Absatz 1 gemeldet werden. Die Organisation benötigt möglicherweise auch (oder ist verpflichtet durch

die SA), ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung zu aktualisieren und zu beheben.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Kein Risiko (internes Register)	Risiko (SA benachrichtigen)	Hohes Risiko (Kommunikation mit betroffenen Personen)
		X

2.3 FALL Nr. 03: Ransomware mit Backup und ohne Exfiltration in einem Krankenhaus

Das Informationssystem eines Krankenhauses/Gesundheitszentrums wurde einem Ransomware-Angriff ausgesetzt und ein erheblicher Teil der Daten wurde vom Angreifer verschlüsselt. Das Unternehmen nutzt die Expertise eines externen Cybersecurity-Unternehmens, um sein Netzwerk zu überwachen. Es liegen Protokolle vor, die alle Datenströme verfolgen, die das Unternehmen verlassen (einschließlich ausgehender E-Mails). Nach der Analyse der Protokolle und der Daten, die die anderen Erkennungssysteme gesammelt haben, stellt die interne Untersuchung mit Unterstützung des Cybersecurity-Unternehmens fest, dass der Täter die Daten nur verschlüsselt hat, ohne sie zu exfiltrieren. Die Protokolle zeigen keinen Datenfluss nach außen im Zeitraum des Angriffs. Die von der Sicherheitsverletzung betroffenen persönlichen Daten beziehen sich auf die Mitarbeiter und Patienten, die Tausende von Personen darstellten. Backups waren in elektronischer Form vorhanden. Der größte Teil der Daten wurde wiederhergestellt, aber dieser Vorgang dauerte 2 Arbeitstage und führte zu erheblichen Verzögerungen bei der Behandlung der

2.3.1 FALL Nr. 03 - Vorherige Maßnahmen und Risikobewertung

36. Der für die Verarbeitung Verantwortliche hätte die gleichen vorherigen Maßnahmen ergreifen müssen, wie in Teil 2.1. und in Abschnitt 2.5. erwähnt. Der Hauptunterschied zum vorherigen Fall ist die hohe Schwere der Folgen für einen wesentlichen Teil der betroffenen Personen.

37. Die Menge der verletzten Daten und die Anzahl der betroffenen Personen sind hoch, da Krankenhäuser in der Regel große Datenmengen verarbeiten. Die Nichtverfügbarkeit der Daten hat eine hohe Auswirkung auf einen erheblichen Teil der betroffenen Personen. Außerdem besteht ein Restrisiko von hohem Schweregrad für die Vertraulichkeit der Patientendaten.

38. Die Art der Sicherheitsverletzung, die Art, die Sensibilität und das Volumen der betroffenen personenbezogenen Daten sind wichtig. Auch wenn ein Backup der Daten vorhanden war und diese innerhalb weniger Tage wiederhergestellt werden konnten, besteht aufgrund der Schwere der Folgen für die betroffenen Personen, die sich aus der mangelnden Verfügbarkeit der Daten zum Zeitpunkt des Angriffs und in den folgenden Tagen ergeben, ein hohes Risiko.

2.3.2 FALL Nr. 03 - Schadensminderung und Verpflichtungen

39. Eine Benachrichtigung der SA wird als notwendig erachtet, da besondere Kategorien personenbezogener Daten betroffen sind und die Wiederherstellung der Daten lange dauern könnte, was zu erheblichen Verzögerungen bei der Patientenversorgung führen würde. Die Information der betroffenen Personen über die Sicherheitsverletzung ist aufgrund der Auswirkungen für die Patienten notwendig, auch nach der Wiederherstellung der verschlüsselten Daten. Während die Daten aller Patienten, die in den letzten Jahren im Krankenhaus behandelt wurden, verschlüsselt wurden, waren nur die Patienten betroffen, die während der Zeit, in der das Computersystem nicht verfügbar war, für eine Behandlung im Krankenhaus vorgesehen waren. Der Controller sollte diese Patienten direkt über

die Datenverletzung informieren. Eine direkte Mitteilung an die anderen Patienten, von denen einige möglicherweise seit mehr als zwanzig Jahren nicht mehr im Krankenhaus behandelt wurden, ist aufgrund der Ausnahme in Artikel 34 (3) c) möglicherweise nicht erforderlich. In einem solchen Fall muss stattdessen eine öffentliche Mitteilung oder eine ähnliche Maßnahme erfolgen, durch die die betroffenen Personen auf ebenso wirksame Weise informiert werden. In diesem Fall sollte das Krankenhaus den Ransomware-Angriff und seine Auswirkungen öffentlich machen.

40. Dieser Fall dient als Beispiel für einen Ransomware-Angriff mit hohem Risiko für die Rechte und Freiheiten der betroffenen Personen. Er ist gemäß Artikel 33 Absatz 5 zu dokumentieren, der Aufsichtsbehörde gemäß Artikel 33 Absatz 1 zu melden und den betroffenen Personen gemäß Artikel 34 Absatz 1 mitzuteilen. Die Organisation muss auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und nachbessern.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Kein Risiko (internes Register)	Risiko (SA benachrichtigen)	Hohes Risiko (Kommunikation mit betroffenen Personen)

2.4 FALL Nr. 04: Ransomware ohne Backup und mit Exfiltration

Der Server eines öffentlichen Verkehrsunternehmens war einem Ransomware-Angriff ausgesetzt und seine Daten wurden verschlüsselt. Nach den Ergebnissen der internen Untersuchung hat der Täter die Daten nicht nur verschlüsselt, sondern auch exfiltriert. Bei den verletzten Daten handelte es sich um personenbezogene Daten von Kunden und Mitarbeitern sowie von mehreren tausend Personen, die die Dienste des Unternehmens nutzen (z.B. Online-Ticketkauf). Über die grundlegenden Identitätsdaten hinaus sind auch Ausweisnummern und Finanzdaten wie Kreditkartendetails von dem Verstoß betroffen. Es existierte eine Backup-Datenbank, die jedoch ebenfalls vom Angreifer verschlüsselt wurde.

2.4.1 FALL Nr. 04 - Vorherige Maßnahmen und Risikobewertung

41. Der für die Datenverarbeitung Verantwortliche hätte die gleichen Vorabmaßnahmen ergreifen müssen, wie in Teil 2.1. und in Abschnitt 2.5. erwähnt. Obwohl ein Backup vorhanden war, war auch dieses von dem Angriff betroffen. Allein diese Vorkehrung wirft Fragen zur Qualität der vorherigen IT-Sicherheitsmaßnahmen des für die Verarbeitung Verantwortlichen auf und sollte während der Untersuchung weiter untersucht werden, da in einem gut konzipierten Backup-System das Backup sicher und ohne Zugriff vom Hauptsystem gespeichert werden muss, da es sonst bei demselben Angriff kompromittiert werden könnte.

42. Diese Verletzung betrifft nicht nur die Datenverfügbarkeit, sondern auch die Vertraulichkeit, da der Angreifer möglicherweise Daten auf dem Server verändert und / oder kopiert hat. Daher ergibt sich aus der Art der Verletzung ein hohes Risiko.

43. Die Art, die Sensibilität und das Volumen der personenbezogenen Daten erhöhen die Risiken weiter, da die Anzahl der betroffenen Personen hoch ist, ebenso wie die Gesamtmenge der betroffenen personenbezogenen Daten. Neben grundlegenden Identitätsdaten sind auch Ausweisdokumente und Finanzdaten wie Kreditkartendetails betroffen. Eine Datenverletzung in Bezug auf diese Arten von Daten stellt für sich genommen ein hohes Risiko dar, und wenn sie zusammen verarbeitet werden, könnten sie unter anderem für Identitätsdiebstahl oder Betrug verwendet werden.

44. Entweder aufgrund fehlerhafter Serverlogik oder organisatorischer Kontrollen waren die Backup-Dateien von der Ransomware betroffen, wodurch die Wiederherstellung der Daten verhindert und das Risiko erhöht wurde.

45. Diese Datenschutzverletzung stellt ein hohes Risiko für die Rechte und Freiheiten von Personen dar, da

sie wahrscheinlich sowohl zu materiellem (z. B. finanziellem Verlust, da Kreditkartendaten betroffen waren) als auch zu immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug, da Ausweisdaten betroffen waren) führen könnte.

2.4.2 FALL Nr. 04 - Schadensminderung und Verpflichtungen

46. Die Kommunikation mit den betroffenen Personen ist unerlässlich, damit diese die notwendigen Schritte zur Vermeidung von materiellem Schaden unternehmen können (z. B. ihre Kreditkarten sperren).

47. Neben der Dokumentation der Verletzung gemäß Artikel 33 Absatz 5 ist in diesem Fall auch eine Benachrichtigung der Aufsichtsbehörde obligatorisch (Artikel 33 Absatz 1), und der für die Verarbeitung Verantwortliche ist außerdem verpflichtet, den betroffenen Personen die Verletzung mitzuteilen (Artikel 34 Absatz 1). Letzteres könnte auf individueller Basis erfolgen, aber bei Personen, für die keine Kontaktdaten verfügbar sind, sollte der für die Verarbeitung Verantwortliche dies öffentlich tun, z. B. durch eine Mitteilung auf seiner Website. Im letzteren Fall ist eine präzise und klare Mitteilung erforderlich, gut sichtbar auf der Homepage des für die Verarbeitung Verantwortlichen, mit genauen Verweisen auf die relevanten GDPR-Bestimmungen. Die Organisation muss möglicherweise auch ihre organisatorischen und technischen Maßnahmen und Verfahren zur Handhabung der Sicherheit personenbezogener Daten und zur Risikominderung aktualisieren und nachbessern.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

2.5 Organisatorische und technische Maßnahmen zur Verhinderung / Minderung der Auswirkungen von Ransomware-Angriffen

48. Die Tatsache, dass ein Ransomware-Angriff stattgefunden haben könnte, ist in der Regel ein Anzeichen für eine oder mehrere Sicherheitslücken im System des für die Verarbeitung Verantwortlichen. Dies gilt auch in Ransomware-Fällen, in denen die personenbezogenen Daten zwar verschlüsselt, aber nicht exfiltriert wurden. Unabhängig vom Ausgang und den Folgen des Angriffs kann die Bedeutung einer umfassenden Evaluierung des Datensicherheitssystems - mit besonderem Schwerpunkt auf der IT-Sicherheit - nicht genug betont werden. Die festgestellten Schwachstellen und Sicherheitslücken sind unverzüglich zu dokumentieren und zu beheben.

49. Empfehlenswerte Maßnahmen:

(*Die Auflistung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Das Ziel ist vielmehr, Präventionsideen und mögliche Lösungen zu liefern. Jede Verarbeitungstätigkeit ist anders, daher sollte der Controller die Entscheidung treffen, welche Maßnahmen für die gegebene Situation am besten geeignet sind.*)

- Die Firmware, das Betriebssystem und die Anwendungssoftware auf den Servern, Client-Rechnern, aktiven Netzwerkkomponenten und allen anderen Rechnern im selben LAN (einschließlich Wi-Fi-Geräten) auf dem neuesten Stand zu halten. Sicherstellen, dass alle angemessenen IT-Sicherheitsmaßnahmen vorhanden sind, sicherstellen, dass sie wirksam sind und sie regelmäßig aktualisiert werden, wenn sich die Verarbeitung oder die Umstände ändern oder weiterentwickeln. Dazu gehört das Führen detaillierter Protokolle darüber, welche Patches zu welchem Zeitpunkt angewendet werden.

- Entwurf und Organisation von Verarbeitungssystemen und Infrastruktur zur Segmentierung oder Isolierung von Datensystemen und Netzwerken, um die Ausbreitung von Malware innerhalb der Organisation und auf externe Systeme zu verhindern.

- Das Vorhandensein eines aktuellen, sicheren und getesteten Backup-Verfahrens. Medien für die mittel- und langfristige Sicherung sollten auch im Falle eines erfolgreichen Angriffs von der operativen Datenhaltung getrennt und für Dritte unerreichbar aufbewahrt werden (z. B. tägliche

inkrementelle Sicherung und wöchentliche Vollsicherung).

- Besitz/Beschaffung einer geeigneten, aktuellen, effektiven und integrierten Anti-Malware-Software.
- Vorhandensein einer geeigneten, aktuellen, effektiven und integrierten Firewall und eines Intrusion Detection and Prevention Systems. Leiten des Netzwerkverkehrs durch die Firewall/Intrusion Detection, auch bei Home-Office oder mobilem Arbeiten (z. B. durch VPN-Verbindungen zu organisatorischen Sicherheitsmechanismen beim Zugriff auf das Internet).

- Schulung der Mitarbeiter über die Methoden zur Erkennung und Verhinderung von IT-Angriffen. Der Controller sollte Mittel zur Verfügung stellen, um festzustellen, ob E-Mails und Nachrichten, die über andere Kommunikationsmittel erhalten wurden, authentisch und vertrauenswürdig sind. Die Mitarbeiter sollten darin geschult werden, zu erkennen, wann ein solcher Angriff realisiert wurde, wie der Endpunkt aus dem Netzwerk genommen werden kann und welche Verpflichtung sie haben, dies sofort dem Sicherheitsbeauftragten zu melden.
- Betonen Sie die Notwendigkeit, den Typ des schädlichen Codes zu identifizieren, um die Folgen des Angriffs zu erkennen und die richtigen Maßnahmen zur Risikominderung zu finden. Für den Fall, dass ein Ransomware-Angriff erfolgreich war und kein Backup vorhanden ist, können Tools wie die des Projekts "no more ransom" (nomoreransom.org) eingesetzt werden, um Daten wiederherzustellen. Falls jedoch ein sicheres Backup vorhanden ist, ist es ratsam, die Daten daraus wiederherzustellen.
- Weiterleitung oder Replikation aller Logs an einen zentralen Log-Server (ggf. mit Signierung oder kryptografischer Zeitstempelung der Log-Einträge).
- Starke Verschlüsselung und Authentifizierung, insbesondere für den administrativen Zugriff auf IT-Systeme (2FA), angemessene Schlüssel- und Passwortverwaltung.
- Schwachstellen- und Penetrationstests auf regelmäßiger Basis.
- Richten Sie ein Computer Security Incident Response Team (CSIRT) oder Computer Emergency Response Team (CERT) innerhalb der Organisation ein oder schließen Sie sich einem kollektiven CSIRT/CERT an. Erstellen Sie einen Incident Response Plan, Disaster Recovery Plan und einen Business Continuity Plan und stellen Sie sicher, dass diese gründlich getestet werden.
- Bei der Beurteilung von Gegenmaßnahmen - sollte die Risikoanalyse überprüft werden.

3 ANGRIFFE ZUR DATENEXFILTRATION

50. Angriffe, die Schwachstellen in Diensten ausnutzen, die der Controller Dritten über das Internet anbietet, z. B. durch Injektionsangriffe (z. B. SQL-Injection, Path Traversal), Website-Kompromittierung und ähnliche Methoden begangen werden, mögen insofern Ransomware-Angriffen ähneln, als das Risiko von der Aktion eines unbefugten Dritten ausgeht, aber diese Angriffe zielen typischerweise darauf ab, persönliche Daten zu kopieren, zu exfiltrieren und für einen bösartigen Zweck zu missbrauchen. Daher handelt es sich hauptsächlich um Verletzungen der Vertraulichkeit und möglicherweise auch der Datenintegrität. Wenn sich der für die Verarbeitung Verantwortliche der Merkmale dieser Art von Verstößen bewusst ist, stehen ihm viele Maßnahmen zur Verfügung, die das Risiko einer erfolgreichen Ausführung eines Angriffs erheblich verringern können.

3.1 FALL Nr. 05: Exfiltration von Bewerbungsdaten von einer Website

Ein Arbeitsvermittler wurde Opfer einer Cyber-Attacke, die einen Schadcode auf seiner Website platzierte. Dieser Schadcode machte personenbezogene Daten, die über Online-Bewerbungsformulare eingegeben und auf dem Webserver gespeichert wurden, für nicht autorisierte Personen zugänglich. 213 solche Formulare möglicherweise betroffen sind, wurde nach Analyse der betroffenen Daten festgestellt, dass keine besonderen Datenkategorien von der Verletzung betroffen waren. Das speziell installierte Malware-Toolkit verfügte über Funktionalitäten, die es dem Angreifer ermöglichten, jegliche Historie der Exfiltration zu entfernen und außerdem die Verarbeitung auf dem Server zu überwachen und persönliche Daten zu erfassen. Das Toolkit wurde nur einen Monat nach seiner Installation entdeckt.

3.1.1 FALL Nr. 05 - Vorherige Maßnahmen und Risikobewertung

51. Die Sicherheit der Umgebung des für die Verarbeitung Verantwortlichen ist äußerst wichtig, da die meisten dieser Verstöße verhindert werden können, indem sichergestellt wird, dass alle Systeme ständig aktualisiert werden, sensible Daten verschlüsselt werden und Anwendungen nach hohen Sicherheitsstandards entwickelt werden, wie z. B. starke Authentifizierung, Maßnahmen gegen Brute-Force-Angriffe, "Escaping" oder "Sanitising "[13] von Benutzereingaben usw. Regelmäßige IT-Sicherheitsaudits, Schwachstellenbewertungen und Penetrationstests sind ebenfalls erforderlich, um diese Arten von Schwachstellen im Voraus zu erkennen und zu beheben. In diesem speziellen Fall hätten Tools zur Überwachung der Dateiintegrität in der Produktionsumgebung helfen können, die Code-Injektion zu erkennen. (Eine Liste mit empfehlenswerten Maßnahmen finden Sie in Abschnitt 3.7).

52. Der für die Verarbeitung Verantwortliche sollte immer damit beginnen, die Verletzung zu untersuchen, indem er die Art des Angriffs und seine Methoden identifiziert, um zu beurteilen, welche Maßnahmen zu ergreifen sind. Damit dies schnell und effizient geschieht, sollte der für die Datenverarbeitung Verantwortliche über einen Plan zur Reaktion auf einen Vorfall verfügen, in dem die schnellen und notwendigen Schritte zur Kontrolle des Vorfalls festgelegt sind. In diesem speziellen Fall war die Art der Verletzung ein risikoerhöhender Faktor, da nicht nur die Vertraulichkeit der Daten beschnitten wurde, sondern der Eindringling auch die Möglichkeit hatte, Änderungen im System vorzunehmen, so dass auch die Datenintegrität in Frage gestellt wurde.

53. Die Art, die Sensibilität und der Umfang der von der Sicherheitsverletzung betroffenen personenbezogenen Daten sollten bewertet werden, um festzustellen, in welchem Umfang die betroffenen Personen von der Sicherheitsverletzung betroffen sind. Obwohl keine besonderen Kategorien personenbezogener Daten betroffen waren, enthalten die abgerufenen Daten beträchtliche Informationen über die Personen aus den Online-Formularen, und solche Daten könnten auf verschiedene Weise missbraucht werden (Targeting mit unerwünschtem Marketing, Identitätsdiebstahl usw.), sodass die Schwere der Folgen das Risiko für die Rechte und Freiheiten der betroffenen Personen erhöhen sollte.

3.1.2 FALL Nr. 05 - Schadensminderung und Verpflichtungen

54. Wenn möglich, sollte nach Behebung des Problems die Datenbank mit der in einem sicheren Backup gespeicherten verglichen werden. Die aus der Sicherheitsverletzung gewonnenen Erfahrungen sollten bei der Aktualisierung der IT-Infrastruktur genutzt werden. Der für die Datenverarbeitung Verantwortliche sollte alle betroffenen IT-Systeme in einen bekanntermaßen sauberen Zustand versetzen, die Schwachstelle beheben und neue Sicherheitsmaßnahmen implementieren, um ähnliche Datenverletzungen in Zukunft zu vermeiden, z. B. Dateiintegritätsprüfungen und Sicherheitsaudits. Wenn personenbezogene Daten nicht nur exfiltriert, sondern auch gelöscht wurden, muss der für die Verarbeitung Verantwortliche systematische Maßnahmen ergreifen, um die personenbezogenen Daten in dem Zustand wiederherzustellen, in dem sie sich vor der Verletzung befanden. Es kann notwendig sein, vollständige Backups, inkrementelle Änderungen und dann möglicherweise die Verarbeitung seit dem letzten inkrementellen Backup erneut durchzuführen - was voraussetzt, dass der Controller in der Lage ist, die seit dem letzten Backup vorgenommenen Änderungen zu replizieren. Dies könnte erfordern, dass die Steuerung das System so ausgelegt hat, dass es die täglichen Eingabedateien für den Fall aufbewahrt, dass sie erneut verarbeitet werden müssen, und erfordert eine robuste Speichermethode und eine geeignete Aufbewahrungsrichtlinie.

55. Da die Verletzung wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, sollten die betroffenen Personen auf jeden Fall darüber informiert werden (Artikel 34 (1)), was natürlich bedeutet, dass auch die zuständige(n) ORKB in Form einer Benachrichtigung über die

Datenschutzverletzung einbezogen werden sollten. Die Dokumentation der Verletzung ist gemäß Artikel 33 (5) DSGVO obligatorisch und erleichtert die Beurteilung der Situation.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

3.2 FALL Nr. 06: Exfiltration eines gehashten Passworts von einer Website

Eine SQL-Injection-Schwachstelle wurde ausgenutzt, um Zugriff auf eine Datenbank des Servers einer Koch-Website zu erhalten. Benutzer durften nur beliebige Pseudonyme als Benutzernamen wählen. Von der Verwendung von E-Mail-Adressen für diesen Zweck wurde abgeraten. Die in der Datenbank gespeicherten Passwörter wurden mit einem starken Algorithmus gehasht und das Salt wurde nicht kompromittiert. Betroffene Daten: gehashte Passwörter von 1.200 Benutzern. Der für die Verarbeitung Verantwortliche informierte die betroffenen Personen sicherheitshalber per E-

3.2.1 FALL Nr. 06 - Vorherige Maßnahmen und Risikobewertung

56. In diesem speziellen Fall ist die Vertraulichkeit der Daten kompromittiert, aber die Passwörter in der Datenbank wurden mit einer aktuellen Methode gehasht, was das Risiko im Hinblick auf die Art, die Sensibilität und den Umfang der personenbezogenen Daten verringern würde. Dieser Fall birgt keine Risiken für die Rechte und Freiheiten der betroffenen Personen.

57. Darüber hinaus wurden keine Kontaktinformationen (z. B. E-Mail-Adressen oder Telefonnummern) von betroffenen Personen kompromittiert, so dass für die betroffenen Personen kein erhebliches Risiko besteht, Ziel von Betrugsversuchen zu werden (z. B. Erhalt von Phishing-E-Mails oder betrügerischen Textnachrichten und Anrufen). Es waren keine besonderen Kategorien von personenbezogenen Daten betroffen.

58. Einige Benutzernamen könnten als personenbezogene Daten angesehen werden, aber das Thema der Website lässt keine negativen Assoziationen zu. Es ist jedoch zu beachten, dass sich die Risikobewertung ändern kann, wenn die Art der Website und die Daten, auf die zugegriffen wird, besondere Kategorien personenbezogener Daten offenbaren könnten (z. B. Website einer politischen Partei oder Gewerkschaft). Die Verwendung einer dem Stand der Technik entsprechenden Verschlüsselung könnte die nachteiligen Auswirkungen der Sicherheitsverletzung abmildern. Die Sicherstellung, dass nur eine begrenzte Anzahl von Anmeldeversuchen erlaubt ist, verhindert, dass Brute-Force-Angriffe auf die Anmeldung erfolgreich sind, und reduziert damit weitgehend die Risiken, die Angreifern durch die Kenntnis der Benutzernamen entstehen.

3.2.2 FALL Nr. 06 - Schadensminderung und Verpflichtungen

59. Die Mitteilung an die betroffenen Personen könnte in einigen Fällen als mildernder Umstand angesehen werden, da die betroffenen Personen auch in der Lage sind, die notwendigen Schritte zu unternehmen, um weitere Schäden durch die Verletzung zu vermeiden, z. B. indem sie ihr Passwort ändern. In diesem Fall war die Benachrichtigung nicht obligatorisch, kann aber in vielen Fällen als gute Praxis angesehen werden.

60. Der für die Datenverarbeitung Verantwortliche sollte die Schwachstelle beheben und neue Sicherheitsmaßnahmen ergreifen, um ähnliche Datenschutzverletzungen in Zukunft zu vermeiden, wie z. B. systematische Sicherheitsaudits der Website.

61. Der Verstoß sollte gemäß Artikel 33 (5) dokumentiert werden, eine Benachrichtigung oder Mitteilung ist jedoch nicht erforderlich.

62. Außerdem ist es in jedem Fall ratsam, die betroffenen Personen über eine Verletzung von Passwörtern zu informieren, auch wenn die Passwörter unter Verwendung eines gesalzenen Hashes mit einem Algorithmus gespeichert wurden, der dem Stand der Technik entspricht. Die Verwendung von Authentifizierungsmethoden, die eine serverseitige Verarbeitung von Passwörtern überflüssig machen, ist zu bevorzugen. Die betroffenen Personen sollten die Möglichkeit haben, geeignete Maßnahmen bezüglich ihrer eigenen Passwörter zu ergreifen.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
	X	X

3.3 FALL Nr. 07: Credential-Stuffing-Angriff auf eine Banken-Website

Eine Bank wurde Opfer eines Cyber-Angriffs auf eine ihrer Online-Banking-Webseiten. Der Angriff zielte darauf ab, alle möglichen Login-Benutzer-IDs mit einem festen trivialen Passwort aufzuzählen. Die Passwörter bestehen aus 8 Ziffern. Aufgrund einer Schwachstelle der Website wurden in einigen Fällen Informationen über betroffene Personen (Name, Vorname, Geschlecht, Geburtsdatum und -ort, Steuernummer, Benutzerkennungen) an den Angreifer weitergegeben, auch wenn das verwendete Passwort nicht korrekt war oder das Bankkonto nicht mehr aktiv war. Dies betraf rund 100.000 betroffene Personen. Von diesen loggte sich der Angreifer erfolgreich in ca. 2.000 Konten ein, die das vom Angreifer versuchte Trivialpasswort benutzten. Im Nachhinein war der Controller in der Lage, alle unrechtmäßigen Anmeldeversuche zu identifizieren. Der für die Datenverarbeitung Verantwortliche konnte bestätigen, dass laut Betrugsbekämpfungsprüfungen keine Transaktionen von diesen Konten während des Angriffs durchgeführt wurden. Die Bank war sich der Datenverletzung bewusst, da ihre Sicherheitszentrale eine hohe Anzahl von Anmeldeanfragen feststellte, die auf die Website gerichtet waren. Als Reaktion darauf deaktivierte der für die Verarbeitung Verantwortliche die Möglichkeit, sich auf der Website anzumelden, indem er sie ausschaltete, und erzwang das Zurücksetzen der Passwörter der kompromittierten Konten. Der für die Verarbeitung

3.3.1 FALL Nr. 07 - Vorherige Maßnahmen und Risikobewertung

63. Es ist wichtig zu erwähnen, dass Controller, die mit sensiblen Daten, Finanzinformationen usw. umgehen, eine größere Verantwortung in Bezug auf die Bereitstellung einer angemessenen Datensicherheit haben, z. B. durch das Vorhandensein einer Sicherheitszentrale und anderer Maßnahmen zur Prävention, Erkennung und Reaktion auf Vorfälle. Die Nichteinhaltung dieser höheren Standards wird mit Sicherheit zu ernsthafteren Maßnahmen bei der Untersuchung durch eine SA führen.

64. Die Sicherheitsverletzung betrifft neben den Identitäts- und Benutzer-ID-Informationen auch Finanzdaten, was sie besonders schwerwiegend macht. Die Anzahl der betroffenen Personen ist hoch.

65. Die Tatsache, dass eine Verletzung in einem so sensiblen Umfeld geschehen konnte, deutet auf erhebliche Datensicherheitslücken im System des für die Verarbeitung Verantwortlichen hin und kann ein Indikator für einen Zeitpunkt sein, an dem die Überprüfung und Aktualisierung der betroffenen Maßnahmen gemäß Artikel 24 (1), 25 (1) und 32 (1) der DSGVO "erforderlich" ist. Die verletzten Daten ermöglichen die eindeutige Identifizierung der betroffenen Personen und enthalten weitere Informationen über sie (einschließlich Geschlecht, Geburtsdatum und -ort), außerdem können sie vom Angreifer verwendet werden, um die Passwörter der Kunden zu erraten oder eine an die Bankkunden gerichtete Spear-Phishing-Kampagne durchzuführen.

66. Aus diesen Gründen wurde es als wahrscheinlich erachtet, dass die Datenschutzverletzung zu einem hohen Risiko für die Rechte und Freiheiten aller betroffenen Personen führt. Daher ist der Eintritt von materiellem (z. B. finanziellem Verlust) und nicht materiellem Schaden (z. B. Identitätsdiebstahl oder Betrug) ein denkbares Ergebnis.

3.3.2 FALL Nr. 07 - Schadensminderung und Verpflichtungen

67. Die in der Fallbeschreibung genannten Maßnahmen des für die Verarbeitung Verantwortlichen sind angemessen. Nach der Sicherheitsverletzung hat er auch die Sicherheitslücke auf der Website behoben und weitere Schritte unternommen, um ähnliche künftige Datenschutzverletzungen zu verhindern, wie z. B. die Hinzufügung einer Zwei-Faktor-Authentifizierung auf der betroffenen Website und die Umstellung auf eine starke Kundenauthentifizierung.

68. Die Dokumentation des Verstoßes gemäß Artikel 33 (5) DSGVO und die Benachrichtigung der Aufsichtsbehörde darüber sind in diesem Szenario nicht optional. Außerdem sollte der für die Verarbeitung Verantwortliche alle 100.000 betroffenen Personen (einschließlich der betroffenen Personen, deren Konten nicht kompromittiert wurden) gemäß Artikel 34 DSGVO benachrichtigen.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

3.4 Organisatorische und technische Maßnahmen zur Verhinderung / Minderung der Auswirkungen von Hackerangriffen

69. Wie bei Ransomware-Attacken, unabhängig vom Ausgang und den Folgen des Angriffs, ist eine Neubewertung der IT-Sicherheit für Controller in ähnlichen Fällen Pflicht.

70. Empfehlenswerte Maßnahmen:[14]

(*Die Auflistung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Das Ziel ist vielmehr, Präventionsideen und mögliche Lösungen zu liefern. Jede Verarbeitungstätigkeit ist anders, daher sollte der Controller die Entscheidung treffen, welche Maßnahmen für die gegebene Situation am besten geeignet sind.*)

- Verschlüsselung und Schlüsselverwaltung auf dem neuesten Stand der Technik, insbesondere wenn Passwörter, sensible oder finanzielle Daten verarbeitet werden. Kryptografisches Hashing und Salting für geheime Informationen (Passwörter) ist immer der Verschlüsselung von Passwörtern vorzuziehen. Die Verwendung von Authentifizierungsmethoden, die die Verarbeitung von Passwörtern auf der Serverseite überflüssig machen, ist vorzuziehen.

- Halten Sie das System auf dem neuesten Stand (Software und Firmware). Sicherstellen, dass alle IT-Sicherheitsmaßnahmen vorhanden sind, sicherstellen, dass sie wirksam sind und sie regelmäßig aktualisiert werden, wenn sich die Verarbeitung oder die Umstände ändern oder weiterentwickeln. Um die Einhaltung von Artikel 5 Absatz 1 Buchstabe f gemäß Artikel 5 Absatz 2 DSGVO nachweisen zu können, sollte der für die Verarbeitung Verantwortliche eine Aufzeichnung aller durchgeführten Aktualisierungen aufbewahren, einschließlich des Zeitpunkts, zu dem sie durchgeführt wurden.

- Verwendung von starken Authentifizierungsmethoden wie Zwei-Faktor-Authentifizierung und Authentifizierungsserver, ergänzt durch eine aktuelle Passwortrichtlinie.

- Zu den Standards für eine sichere Entwicklung gehören das Filtern von Benutzereingaben (unter Verwendung von Whitelisting, soweit dies praktikabel ist), das Verbergen von Benutzereingaben und Maßnahmen zur Verhinderung von Brute Force (z. B. Begrenzung der maximalen Anzahl von Wiederholungsversuchen). "Web Application Firewalls" können bei der effektiven Anwendung dieser Technik helfen.

- Strenge Richtlinien für die Verwaltung von Benutzerrechten und Zugriffskontrolle sind vorhanden.

- Einsatz geeigneter, aktueller, effektiver und integrierter Firewall-, Intrusion-Detection- und anderer Perimeter-Defense-Systeme.

- Systematische IT-Sicherheitsaudits und Schwachstellenbewertungen (Penetrationstests).

- Regelmäßige Überprüfungen und Tests, um sicherzustellen, dass Backups verwendet werden können, um alle Daten wiederherzustellen, deren Integrität oder Verfügbarkeit betroffen war.
- Keine Session-ID in der URL im Klartext.

4 INTERNE MENSCHLICHE RISIKOQUELLE

71. Die Rolle des menschlichen Versagens bei Verstößen gegen den Schutz personenbezogener Daten muss aufgrund ihres häufigen Auftretens hervorgehoben werden. Da diese Arten von Verstößen sowohl beabsichtigt als auch unbeabsichtigt sein können, ist es für die für die Datenverarbeitung Verantwortlichen sehr schwierig, die Schwachstellen zu erkennen und Maßnahmen zu deren Vermeidung zu ergreifen. Die Internationale Konferenz der Datenschutzbeauftragten hat erkannt, wie wichtig es ist, solche menschlichen Faktoren zu berücksichtigen, und hat im Oktober 2019 eine Resolution verabschiedet, die sich mit der Rolle des menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten befasst15. In dieser Resolution wird betont, dass geeignete Schutzmaßnahmen ergriffen werden sollten, um menschliche Fehler zu vermeiden, und sie enthält eine nicht erschöpfende Liste solcher Schutzmaßnahmen und Ansätze.

4.1 FALL Nr. 08: Exfiltration von Geschäftsdaten durch einen ehemaligen Mitarbeiter

Der Mitarbeiter eines Unternehmens kopiert während seiner Kündigungsfrist Geschäftsdaten aus der Datenbank des Unternehmens, auf die er zugreifen darf und die er zur Erfüllung seiner Aufgabe benötigt. Monate später, nachdem er gekündigt hat, nutzt er die so gewonnenen Daten (hauptsächlich grundlegende Kontaktdaten), um die Kunden des Unternehmens zu kontaktieren, um sie für sein neues Geschäft zu gewinnen.

4.1.1 FALL Nr. 08 - Vorherige Maßnahmen und Risikobewertung

72. In diesem speziellen Fall wurden keine vorherigen Maßnahmen ergriffen, um den Mitarbeiter daran zu hindern, Kontaktinformationen der Kundschaft des Unternehmens zu kopieren, da er legitimen Zugang zu diesen Informationen benötigte - und hatte. Da die Erfüllung der meisten Aufgaben im Bereich der Kundenbeziehungen irgendeine Art von Mitarbeiterzugriff auf personenbezogene Daten erfordert, sind diese Datenverletzungen möglicherweise am schwierigsten zu verhindern. Beschränkungen des Zugriffsumfangs können die Arbeit des jeweiligen Mitarbeiters einschränken. Allerdings können gut durchdachte Zugriffsrichtlinien und eine ständige Kontrolle helfen, solche Verstöße zu verhindern.

73. Wie üblich sind bei der Risikobewertung die Art der Verletzung sowie die Art, die Sensibilität und der Umfang der betroffenen personenbezogenen Daten zu berücksichtigen. Bei dieser Art von Verstößen handelt es sich typischerweise um Verstöße gegen die Vertraulichkeit, da die Datenbank in der Regel unversehrt bleibt und ihr Inhalt "lediglich" zur weiteren Verwendung kopiert wird. Auch die Menge der betroffenen Daten ist meist gering oder mittel. In diesem speziellen Fall waren keine besonderen Kategorien personenbezogener Daten betroffen, der Mitarbeiter benötigte lediglich die Kontaktdaten von Kunden, um nach seinem Ausscheiden aus dem Unternehmen mit diesen in Kontakt treten zu können. Daher sind die betroffenen Daten nicht sensibel.

74. Auch wenn sich das einzige Ziel des ehemaligen Mitarbeiters, der die Daten böswillig kopiert hat, darauf beschränken mag, die Kontaktinformationen des Kundenstamms des Unternehmens für seine eigenen kommerziellen Zwecke zu erlangen, kann der für die Verarbeitung Verantwortliche das Risiko für die betroffenen Personen nicht als gering einstufen, da er keinerlei Gewissheit über die Absichten des Mitarbeiters hat. Während also die Folgen des Verstoßes

auf die Entlarvung einer unangemessenen Selbstvermarktung des Ex-Mitarbeiters beschränkt sein könnte, ist ein weiterer und schwerwiegenderer Missbrauch der gestohlenen Daten nicht ausgeschlossen.

4.1.2 FALL Nr. 08 - Schadensminderung und Verpflichtungen

75. Die Abmilderung der negativen Auswirkungen des Verstoßes im obigen Fall ist schwierig. Möglicherweise müssen sofortige rechtliche Schritte eingeleitet werden, um den ehemaligen Mitarbeiter daran zu hindern, die Daten weiter zu missbrauchen und zu verbreiten. In einem nächsten Schritt sollte die Vermeidung ähnlicher zukünftiger Situationen das Ziel sein. Der für die Verarbeitung Verantwortliche könnte versuchen, den Ex-Mitarbeiter anzuweisen, die Verwendung der Daten einzustellen, aber der Erfolg dieser Maßnahme ist bestenfalls zweifelhaft.

76. Es gibt keine "Einheitslösung" für diese Art von Fällen, aber ein systematischer Ansatz kann helfen, sie zu verhindern. Beispielsweise kann das Unternehmen - wenn möglich - in Erwägung ziehen, Mitarbeitern, die ihre Absicht zu kündigen signalisiert haben, bestimmte Formen des Zugriffs zu entziehen oder Zugriffsprotokolle zu implementieren, damit unerwünschte Zugriffe protokolliert und gekennzeichnet werden können. Der mit den Mitarbeitern unterzeichnete Vertrag sollte Klauseln enthalten, die solche Handlungen untersagen.

77. Alles in allem wird, da die gegebene Verletzung nicht zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen führt, eine Benachrichtigung an die SA ausreichen. Die Information der betroffenen Personen könnte jedoch auch für den für die Datenverarbeitung Verantwortlichen von Vorteil sein, da es besser sein könnte, dass sie vom Unternehmen über das Datenleck erfahren und nicht von dem ehemaligen Mitarbeiter, der versucht, sie zu kontaktieren. Die Dokumentation von Datenschutzverletzungen gemäß Artikel 33 (5) ist eine gesetzliche Verpflichtung.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
		X

4.2 FALL Nr. 09: Versehentliche Übermittlung von Daten an eine vertrauenswürdige dritte Person

Ein Versicherungsvertreter stellte fest, dass er - ermöglicht durch die fehlerhaften Einstellungen einer per E-Mail empfangenen Excel-Datei - auf Informationen zu zwei Dutzend Kunden zugreifen konnte, die nicht zu seinem Wirkungskreis gehörten. Er ist an das Berufsgeheimnis gebunden und war der einzige Empfänger der E-Mail. Die Vereinbarung zwischen dem für die Datenverarbeitung Verantwortlichen und dem Versicherungsvertreter verpflichtet den Vertreter, dem für die Datenverarbeitung Verantwortlichen eine Verletzung des Schutzes personenbezogener Daten unverzüglich zu melden. Daher meldete der Agent den Fehler sofort an den für die Verarbeitung Verantwortlichen, der die Datei korrigierte und sie erneut verschickte und den Agenten aufforderte, die frühere Nachricht zu löschen. Nach der oben genannten Regelung muss der Agent die Löschung in einer schriftlichen Erklärung bestätigen, was er auch tat. Die gewonnenen Informationen enthalten keine besonderen Kategorien personenbezogener Daten, sondern nur Kontaktdaten und Daten über die Versicherung selbst (Versicherungsart, Betrag). Nach der Analyse der von der Verletzung betroffenen

4.2.1 FALL Nr. 09 - Vorherige Maßnahmen und Risikobewertung

78. Im Gegensatz zum vorherigen Fall ist die Verletzung hier nicht auf eine absichtliche Handlung eines

Mitarbeiters zurückzuführen, sondern auf einen unbeabsichtigten menschlichen Fehler, der durch Unachtsamkeit verursacht wurde. Diese Art von Verstößen kann vermieden werden durch a) die Durchsetzung von Schulungs-, Ausbildungs- und Sensibilisierungsprogrammen, bei denen die Mitarbeiter ein besseres Verständnis für die Bedeutung des Schutzes personenbezogener Daten erlangen, b) die Reduzierung des Dateiaustauschs per E-Mail und stattdessen die Verwendung dedizierter Systeme z. B. für die Verarbeitung von Kundendaten, c) die doppelte Überprüfung von Dateien vor dem Versand, d) die Trennung von Erstellung und Versand von Dateien.

79. Diese Datenverletzung betrifft nur die Vertraulichkeit der Daten, die Integrität und die Zugänglichkeit der Daten bleiben unangetastet. Die Datenverletzung betraf nur etwa zwei Dutzend Kunden, daher kann die Menge der betroffenen Daten als gering angesehen werden. Außerdem enthalten die betroffenen personenbezogenen Daten keine sensiblen Daten. Die Tatsache, dass sich der Datenverarbeiter nach Bekanntwerden der Datenschutzverletzung unverzüglich mit dem für die Datenverarbeitung Verantwortlichen in Verbindung gesetzt hat, kann als risikomindernder Faktor angesehen werden. (Die Möglichkeit, dass Daten an andere Versicherungsvertreter gesendet wurden, sollte ebenfalls bewertet werden, und falls dies bestätigt wird, sollten entsprechende Maßnahmen ergriffen werden). Aufgrund der angemessenen Schritte, die nach der Datenverletzung unternommen wurden, wird diese wahrscheinlich keine Auswirkungen auf die Rechte und Freiheiten der betroffenen Personen haben.

80. Die Kombination aus der geringen Anzahl der betroffenen Personen, der sofortigen Entdeckung des Verstoßes und den Maßnahmen, die ergriffen wurden, um die Auswirkungen zu minimieren, machen diesen speziellen Fall zu keinem Risiko.

4.2.2 FALL Nr. 09 - Schadensminderung und Verpflichtungen

81. Darüber hinaus sind auch andere risikomindernde Umstände im Spiel: Der Beauftragte ist an das Berufsgeheimnis gebunden; er selbst hat das Problem dem für die Verarbeitung Verantwortlichen gemeldet und die Datei auf Aufforderung gelöscht. Die Schärfung des Bewusstseins und möglicherweise die Einbeziehung zusätzlicher Schritte bei der Prüfung von Dokumenten mit personenbezogenen Daten werden wahrscheinlich dazu beitragen, ähnliche Fälle in Zukunft zu vermeiden.

82. Neben der Dokumentation des Verstoßes gemäß Artikel 33 (5) besteht kein weiterer Handlungsbedarf.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
	X	X

4.3 Organisatorische und technische Maßnahmen zur Vermeidung / Minderung der Auswirkungen interner menschlicher Risikoquellen

83. Eine Kombination der unten genannten Maßnahmen - angewandt in Abhängigkeit von den Besonderheiten des Falles
- sollte dazu beitragen, die Wahrscheinlichkeit einer ähnlichen Verletzung zu verringern.

84. Empfehlenswerte Maßnahmen:

(*Die Auflistung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Das Ziel ist vielmehr, Präventionsideen und mögliche Lösungen zu liefern. Jede Verarbeitungstätigkeit ist anders, daher sollte der Controller die Entscheidung treffen, welche Maßnahmen für die gegebene Situation am besten geeignet sind.*)

- Regelmäßige Durchführung von Schulungs-, Aufklärungs- und Sensibilisierungsprogrammen für Mitarbeiter zu ihren Datenschutz- und Sicherheitspflichten sowie zur Erkennung und Meldung von Bedrohungen für die Sicherheit personenbezogener Daten16. Entwickeln Sie ein Awareness-Programm, um Mitarbeiter an die häufigsten Fehler zu erinnern, die zu Verletzungen des Schutzes personenbezogener Daten führen, und wie sie diese vermeiden können.

[16] Abschnitt 2) Unterabschnitt (i) der Entschließung, um die Rolle menschlichen Versagens bei Verletzungen des Schutzes personenbezogener Daten anzusprechen.

- Einrichtung robuster und effektiver Praktiken, Verfahren und Systeme zum Schutz von Daten und Privatsphäre17.
- Bewertung der Datenschutzpraktiken, -verfahren und -systeme, um eine kontinuierliche Wirksamkeit sicherzustellen18.
- Angemessene Richtlinien für die Zugriffskontrolle erstellen und die Benutzer zwingen, die Regeln zu befolgen.
- Implementierung von Techniken, die eine Benutzerauthentifizierung beim Zugriff auf sensible persönliche Daten erzwingen.
- Deaktivierung des firmenbezogenen Kontos des Benutzers, sobald die Person das Unternehmen verlässt.
- Prüfung auf ungewöhnlichen Datenfluss zwischen dem Dateiserver und den Arbeitsstationen der Mitarbeiter.
- Einrichten der I/O-Schnittstellensicherheit im BIOS oder durch den Einsatz von Software, die die Nutzung von Computerschnittstellen steuert (sperren oder entsperren z. B. USB/CD/DVD etc.).
- Überprüfung der Zugriffsrichtlinien der Mitarbeiter (z. B. Protokollierung des Zugriffs auf sensible Daten und Anforderung an den Benutzer, einen geschäftlichen Grund einzugeben, damit dieser für Audits verfügbar ist).
- Deaktivieren von offenen Cloud-Diensten.
- Verbieten und Verhindern des Zugriffs auf bekannte offene Mail-Dienste.
- Deaktivieren der Druckbildfunktion in OS.
- Durchsetzung einer Clean Desk Policy.
- Automatisches Sperren aller Computer nach einer bestimmten Zeit der Inaktivität.
- Verwenden Sie Mechanismen (z. B. (Funk-)Token zur Anmeldung/zum Öffnen gesperrter Konten) für schnelle Benutzerwechsel in gemeinsam genutzten Umgebungen.
- Verwendung dedizierter Systeme zur Verwaltung personenbezogener Daten, die geeignete Zugriffskontrollmechanismen anwenden und menschliche Fehler, wie z. B. das Senden von Mitteilungen an die falsche Person, verhindern. Die Verwendung von Tabellenkalkulationen und anderen Office-Dokumenten ist kein geeignetes Mittel zur Verwaltung von Kundendaten.

5 VERLORENE ODER GESTOHLENE GERÄTE UND PAPIERDOKUMENTE

85. Eine häufige Fallart ist der Verlust oder Diebstahl von tragbaren Geräten. In diesen Fällen muss der für die Verarbeitung Verantwortliche die Umstände des Verarbeitungsvorgangs berücksichtigen, z. B. die Art der auf dem Gerät gespeicherten Daten sowie die unterstützenden Anlagen und die vor der Verletzung ergriffenen Maßnahmen zur Gewährleistung eines angemessenen Sicherheitsniveaus. All diese Elemente beeinflussen die potenziellen Auswirkungen der Datenverletzung. Die Risikobewertung könnte sich als schwierig erweisen, da das Gerät nicht mehr verfügbar ist.

86. Diese Art von Verstößen kann immer als Verletzung der Vertraulichkeit eingestuft werden. Wenn es jedoch kein Backup für die gestohlene Datenbank gibt, kann die Art der Verletzung auch eine Verletzung der Verfügbarkeit und der Integrität sein.

87. Die folgenden Szenarien zeigen, wie die oben genannten Umstände die Wahrscheinlichkeit und Schwere der Datenverletzung beeinflussen.

5.1 FALL Nr. 10: Gestohlenes Material mit verschlüsselten persönlichen Daten

Bei einem Einbruch in eine Kindertagesstätte wurden zwei Tablets gestohlen. Auf den Tablets befand sich eine App, die persönliche Daten über die Kinder, die die Kindertagesstätte besuchen, enthielt. Betroffen waren Name, Geburtsdatum, persönliche Daten über die Ausbildung der Kinder. Sowohl die verschlüsselten Tablets, die zum Zeitpunkt des Einbruchs ausgeschaltet waren, als auch die App waren durch ein starkes Passwort geschützt. Back-up-Daten waren effektiv und leicht zugänglich für den Controller. Nachdem sie von dem Einbruch erfahren hatte, gab die Kindertagesstätte kurz nach der Entdeckung des Einbruchs aus der Ferne den Befehl, die Tablets

5.1.1 FALL Nr. 10 - Vorherige Maßnahmen und Risikobewertung

88. In diesem speziellen Fall hat der für die Datenverarbeitung Verantwortliche angemessene Maßnahmen ergriffen, um die Auswirkungen einer potenziellen Datenverletzung zu verhindern und abzumildern, indem er eine Geräteverschlüsselung verwendete, einen angemessenen Passwortschutz einführte und ein Backup der auf den Tablets gespeicherten Daten sicherstellte. (Eine Liste empfehlenswerter Maßnahmen ist in Abschnitt 5.7 zu finden).

89. Nach Bekanntwerden einer Verletzung sollte der für die Datenverarbeitung Verantwortliche die Risikoquelle, die Systeme, die die Datenverarbeitung unterstützen, die Art der betroffenen personenbezogenen Daten und die möglichen Auswirkungen der Datenverletzung auf die betroffenen Personen bewerten. Die oben beschriebene Datenschutzverletzung hätte die Vertraulichkeit, die Verfügbarkeit und die Integrität der betroffenen Daten betroffen, aber aufgrund der angemessenen Verfahren des für die Datenverarbeitung Verantwortlichen vor und nach der Datenschutzverletzung ist keines dieser Probleme aufgetreten.

5.1.2 FALL Nr. 10 - Schadensminderung und Verpflichtungen

90. Die Vertraulichkeit der persönlichen Daten auf den Geräten wurde aufgrund des starken Passwortschutzes sowohl auf den Tablets als auch auf den Apps nicht beeinträchtigt. Die Tablets waren so eingerichtet, dass das Setzen eines Passworts auch bedeutet, dass die Daten auf dem Gerät verschlüsselt sind. Dies wurde durch die Aktion des Controllers, der versuchte, alles von den gestohlenen Geräten aus der Ferne zu löschen, noch verstärkt.

91. Durch die getroffenen Maßnahmen blieb auch die Vertraulichkeit der Daten gewahrt. Darüber hinaus wurde durch das Backup die kontinuierliche Verfügbarkeit der personenbezogenen Daten sichergestellt, so dass keine potenziellen negativen Auswirkungen hätten auftreten können.

92. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass die oben beschriebene Datenverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt, daher war keine Benachrichtigung der ORKB oder der betroffenen Personen erforderlich. Allerdings muss auch diese Datenverletzung gemäß Artikel 33 (5) dokumentiert werden.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen

		Personen
	X	X

5.2 FALL Nr. 11: Gestohlenes Material, das nicht verschlüsselte persönliche Daten speichert

Das elektronische Notebook-Gerät eines Mitarbeiters eines Dienstleistungsunternehmens wurde gestohlen. Das gestohlene Notebook enthielt Namen, Vornamen, Geschlecht, Adressen und Geburtsdaten von mehr als 100000 Kunden. Aufgrund der Nichtverfügbarkeit des gestohlenen Gerätes konnte nicht festgestellt werden, ob auch andere Kategorien personenbezogener Daten betroffen waren. Der Zugriff auf die Festplatte des Notebooks war nicht durch ein Passwort

5.2.1 FALL Nr. 11 - Vorherige Maßnahmen und Risikobewertung

93. Der für die Datenverarbeitung Verantwortliche hat keine vorherigen Sicherheitsmaßnahmen getroffen, so dass die auf dem gestohlenen Notebook gespeicherten personenbezogenen Daten für den Dieb oder jede andere Person, die danach in den Besitz des Geräts kam, leicht zugänglich waren.

94. Diese Datenschutzverletzung betrifft die Vertraulichkeit der Daten, die auf dem gestohlenen Gerät gespeichert sind.

95. Das Notebook mit den personenbezogenen Daten war in diesem Fall angreifbar, da es keinen Passwortschutz und keine Verschlüsselung besaß. Das Fehlen grundlegender Sicherheitsmaßnahmen erhöht das Risikoniveau für die betroffenen betroffenen Personen. Darüber hinaus ist auch die Identifizierung der betroffenen Personen problematisch, was ebenfalls die Schwere der Verletzung erhöht. Die beträchtliche Anzahl der betroffenen Personen erhöht das Risiko, dennoch waren keine besonderen Kategorien personenbezogener Daten von der Datenverletzung betroffen.

96. Bei der Risikobewertung sollte der für die Verarbeitung Verantwortliche die möglichen Folgen und nachteiligen Auswirkungen der Verletzung der Vertraulichkeit berücksichtigen. Infolge der Verletzung können die betroffenen Personen einem Identitätsbetrug zum Opfer fallen, der sich auf die auf dem gestohlenen Gerät verfügbaren Daten stützt, daher wird das Risiko als hoch eingestuft.

5.2.2 FALL Nr. 11 - Abmilderung und Verpflichtungen

97. Das Einschalten der Geräteverschlüsselung und die Verwendung eines starken Passwortschutzes der gespeicherten Datenbank hätten verhindern können, dass die Datenverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt.

98. Aufgrund dieser Umstände ist die Benachrichtigung der SA erforderlich, die Benachrichtigung der betroffenen Personen ist ebenfalls erforderlich.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

5.3 FALL Nr. 12: Gestohlene Papierakten mit sensiblen Daten

Aus einer Reha-Einrichtung für Drogenabhängige wurde ein Papier-Logbuch gestohlen. Das Buch enthielt grundlegende Identitäts- und Gesundheitsdaten der Patienten, die in die Reha-Einrichtung aufgenommen wurden. Die Daten waren nur auf Papier gespeichert und den behandelnden Ärzten stand kein Backup zur Verfügung. Das Buch wurde nicht in einer verschlossenen Schublade oder einem Raum aufbewahrt, der Datenverantwortliche hatte weder

5.3.1 FALL Nr. 12 - Vorherige Maßnahmen und Risikobewertung

99. Der für die Datenverarbeitung Verantwortliche hat keine vorherigen Sicherheitsmaßnahmen ergriffen, daher waren die in diesem Buch gespeicherten personenbezogenen Daten für die Person, die es gefunden hat, leicht zugänglich. Außerdem macht die Art der in dem Buch gespeicherten personenbezogenen Daten das Fehlen von Sicherungsdaten zu einem sehr ernsten Risikofaktor.

100. Dieser Fall dient als Beispiel für eine hochriskante Datenverletzung. Aufgrund des Versagens angemessener Sicherheitsvorkehrungen gingen sensible Gesundheitsdaten gemäß Artikel 9 (1) GDPR verloren. Da in diesem Fall eine besondere Kategorie personenbezogener Daten betroffen war, wurde das potenzielle Risiko für die betroffenen Personen erhöht, was von dem für die Verarbeitung Verantwortlichen bei der Risikobewertung ebenfalls berücksichtigt werden sollte.

101. Diese Verletzung betrifft die Vertraulichkeit, Verfügbarkeit und Integrität der betroffenen persönlichen Daten. Durch die Verletzung der Vertraulichkeit wird die ärztliche Schweigepflicht gebrochen und unbefugte Dritte können Zugang zu den privaten medizinischen Daten der Patienten erhalten, was schwerwiegende Auswirkungen auf das persönliche Leben der Patienten haben kann. Die Verletzung der Verfügbarkeit kann auch die Kontinuität der Behandlung des Patienten stören. Da die Änderung/Löschung von Teilen des Buchinhalts nicht ausgeschlossen werden kann, ist auch die Integrität der persönlichen Daten gefährdet.

5.3.2 FALL Nr. 12 - Schadensminderung und Verpflichtungen

102. Bei der Bewertung der Sicherungsmaßnahmen sollte auch die Art des unterstützenden Wirtschaftsguts berücksichtigt werden. Da das Patiententagebuch ein physisches Dokument war, hätte seine Sicherung anders organisiert werden müssen als die eines elektronischen Geräts. Die Pseudonymisierung der Patientennamen, die Aufbewahrung des Buches in einer gesicherten Räumlichkeit und in einer verschlossenen Schublade oder einem Raum sowie eine ordnungsgemäße Zugangskontrolle mit Authentifizierung beim Zugriff darauf hätten die Datenverletzung verhindern können.

103. Die oben beschriebene Datenverletzung kann schwerwiegende Auswirkungen auf die betroffenen Personen haben; daher ist die Benachrichtigung der SA und die Mitteilung der Verletzung an die betroffenen Personen obligatorisch.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

5.4 Organisatorische und technische Maßnahmen zur Verhinderung / Minderung der Auswirkungen von Verlust oder Diebstahl von Geräten

104. Eine Kombination der unten genannten Maßnahmen - angewandt je nach den Besonderheiten des Falles - sollte dazu beitragen, die Wahrscheinlichkeit zu verringern, dass sich eine ähnliche Verletzung wiederholt.

105. Empfehlenswerte Maßnahmen:

(*Die Auflistung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Das Ziel ist vielmehr, Präventionsideen und mögliche Lösungen zu liefern. Jede Verarbeitungstätigkeit ist anders, daher sollte der Controller die Entscheidung treffen, welche Maßnahmen für die gegebene Situation am besten geeignet sind.*)

- Schalten Sie die Verschlüsselung des Geräts ein (z. B. Bitlocker, Veracrypt oder DM-Crypt).
- Verwenden Sie Passcode/Passwort auf allen Geräten. Verschlüsseln Sie alle mobilen elektronischen Geräte so, dass zur Entschlüsselung die Eingabe eines komplexen Passworts erforderlich ist.

- Verwenden Sie eine Multi-Faktor-Authentifizierung.
- Schalten Sie die Funktionalitäten hochmobiler Geräte ein, die es erlauben, diese bei Verlust oder Verlegung zu orten.
- Verwenden Sie MDM (Mobile Devices Management) Software/App und Lokalisierung. Verwenden Sie Blendschutzfilter. Schließen Sie alle unbeaufsichtigten Geräte.

- Wenn möglich und der jeweiligen Datenverarbeitung angemessen, speichern Sie personenbezogene Daten nicht auf einem mobilen Gerät, sondern auf einem zentralen Backend-Server.
- Wenn die Arbeitsstation mit dem Firmen-LAN verbunden ist, führen Sie ein automatisches Backup von den Arbeitsordnern durch, sofern es unvermeidbar ist, dass dort persönliche Daten gespeichert sind
- Verwenden Sie ein sicheres VPN (das z. B. einen separaten Zweitfaktor-Authentifizierungsschlüssel für den Aufbau einer sicheren Verbindung erfordert), um mobile Geräte mit Backend-Servern zu verbinden.
- Stellen Sie den Mitarbeitern physische Schlösser zur Verfügung, damit sie die von ihnen verwendeten mobilen Geräte physisch sichern können, während sie unbeaufsichtigt sind.
- Ordnungsgemäße Regelung der Gerätenutzung außerhalb des Unternehmens.
- Ordnungsgemäße Regelung der Gerätenutzung innerhalb des Unternehmens.
- Verwenden Sie eine MDM-Software/App (Mobile Devices Management) und aktivieren Sie die Remote-Wipe-Funktion.
- Verwenden Sie eine zentralisierte Geräteverwaltung mit minimalen Rechten für die Endbenutzer zur Installation von Software.
- Installieren Sie physische Zugangskontrollen.
- Vermeiden Sie die Speicherung sensibler Informationen auf mobilen Geräten oder Festplatten. Wenn es notwendig ist, auf das interne System des Unternehmens zuzugreifen, sollten sichere Kanäle verwendet werden, wie bereits erwähnt.

6 MISPOSTAL

106. Die Risikoquelle ist auch in diesem Fall ein interner menschlicher Fehler, aber hier führte keine böswillige Handlung zu der Verletzung. Sie ist das Ergebnis von Unachtsamkeit. Der Controller kann im Nachhinein wenig unternehmen, daher ist die Prävention in diesen Fällen noch wichtiger als bei anderen Arten von Sicherheitsverletzungen.

6.1 FALL Nr. 13: Fehler bei der Schneckenpost

Zwei Bestellungen für Schuhe wurden von einem Einzelhandelsunternehmen verpackt. Durch menschliches Versagen wurden zwei Packscheine vertauscht mit der Folge, dass beide Produkte und die dazugehörigen Packscheine an die falsche Person geschickt wurden. Das bedeutet, dass die beiden Kunden die Bestellungen des jeweils anderen erhalten haben, einschließlich der Packzettel mit den personenbezogenen Daten. Nach Bekanntwerden des Verstoßes rief der

6.1.1 FALL Nr. 13 - Vorherige Maßnahmen und Risikobewertung

107. Die Rechnungen enthielten die für eine erfolgreiche Lieferung erforderlichen persönlichen Daten (Name, Adresse sowie den gekauften Artikel und dessen Preis). Es ist wichtig zu ermitteln, wie der menschliche Fehler überhaupt passieren konnte und ob er in irgendeiner Weise hätte verhindert werden können. In dem beschriebenen Fall ist das Risiko gering, da keine besonderen Kategorien

personenbezogener Daten oder andere Daten, deren Missbrauch zu erheblichen negativen Auswirkungen führen könnte, betroffen waren, die Verletzung nicht auf einen systemischen Fehler des für die Verarbeitung Verantwortlichen zurückzuführen ist und nur zwei Personen betroffen sind. Es konnte keine negative Auswirkung auf die Personen festgestellt werden.

6.1.2 FALL Nr. 13 - Abmilderung und Verpflichtungen

108. Der für die Verarbeitung Verantwortliche sollte eine kostenlose Rücksendung der Sendungen und der dazugehörigen Rechnungen vorsehen und die falschen Empfänger auffordern, alle eventuellen Kopien der Rechnungen, die die personenbezogenen Daten der anderen Person enthalten, zu vernichten / zu löschen.

109. Auch wenn die Sicherheitsverletzung selbst kein hohes Risiko für die Rechte und Freiheiten der betroffenen Personen darstellt und daher die Benachrichtigung der betroffenen Personen gemäß Artikel 34 DSGVO nicht zwingend vorgeschrieben ist, kann die Benachrichtigung der betroffenen Personen nicht vermieden werden, da ihre Mitarbeit erforderlich ist, um das Risiko zu mindern.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
	X	X

6.2 FALL Nr. 14: Sensible persönliche Daten versehentlich per Post verschickt

Die Beschäftigungsabteilung einer öffentlichen Verwaltung schickte eine E-Mail-Nachricht - über bevorstehende Schulungen - an die Personen, die in ihrem System als Arbeitssuchende registriert waren. Versehentlich wurde an diese E-Mail ein Dokument angehängt, das die persönlichen Daten all dieser Arbeitssuchenden enthielt (Name, E-Mail-Adresse, Postanschrift, Sozialversicherungsnummer). Die Zahl der betroffenen Personen beläuft sich auf mehr als 60000. Daraufhin hat das Amt alle Empfänger kontaktiert und sie gebeten, die vorherige Nachricht zu löschen und die darin enthaltenen Informationen nicht zu verwenden.

6.2.1 FALL Nr. 14 - Vorherige Maßnahmen und Risikobewertung

110. Für den Versand solcher Meldungen hätten strengere Regeln eingeführt werden müssen. Die Einführung zusätzlicher Kontrollmechanismen muss in Betracht gezogen werden.

111. Die Anzahl der betroffenen Personen ist beträchtlich, und die Einbeziehung ihrer Sozialversicherungsnummer zusammen mit anderen, grundlegenderen personenbezogenen Daten erhöht das als hoch einzustufende Risiko weiter. Die eventuelle Weitergabe der Daten durch einen der Empfänger kann von dem für die Verarbeitung Verantwortlichen nicht eingedämmt werden.

6.2.2 FALL Nr. 14 - Schadensminderung und Verpflichtungen

112. Wie bereits erwähnt, sind die Möglichkeiten, die Risiken eines ähnlichen Verstoßes wirksam zu mindern, begrenzt. Obwohl der für die Verarbeitung Verantwortliche um die Löschung der Nachricht gebeten hat, kann er die Empfänger nicht dazu zwingen, und folglich kann er auch nicht sicher sein, dass sie der Bitte nachkommen.

113. Die Ausführung aller drei unten angegebenen Aktionen sollte in einem solchen Fall selbstverständlich sein.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

6.3 FALL Nr. 15: Personenbezogene Daten versehentlich per Post verschickt

Eine Teilnehmerliste für einen Kurs in Rechtsenglisch, der 5 Tage lang in einem Hotel stattfindet, wird versehentlich an 15 ehemalige Teilnehmer des Kurses statt an das Hotel geschickt. Die Liste enthält Namen, E-Mail-Adressen und Essensvorlieben der 15 Teilnehmer. Nur zwei Teilnehmer haben ihre Essensvorlieben ausgefüllt und angegeben, dass sie eine Laktoseintoleranz haben. Keiner der Teilnehmer hat eine geschützte Identität. Der für die Verarbeitung Verantwortliche entdeckt den Fehler unmittelbar nach dem Versenden der Liste und informiert die Empfänger über den Fehler und bittet sie, die Liste zu löschen.

6.3.1 FALL Nr. 15 - Vorherige Maßnahmen und Risikobewertung

114. Für den Versand solcher Meldungen hätten strengere Regeln eingeführt werden müssen. Die Einführung zusätzlicher Kontrollmechanismen muss in Betracht gezogen werden.

115. Die Risiken, die sich aus der Art, der Sensibilität, dem Umfang und dem Kontext der personenbezogenen Daten ergeben, sind gering. Die personenbezogenen Daten umfassen sensible Daten zu den Ernährungsvorlieben von zwei der Teilnehmer. Auch wenn es sich bei der Information, dass jemand laktoseintolerant ist, um Gesundheitsdaten handelt, ist das Risiko, dass diese Daten in nachteiliger Weise verwendet werden, als relativ gering einzustufen. Während bei Gesundheitsdaten in der Regel davon ausgegangen wird, dass die Verletzung wahrscheinlich zu einem hohen Risiko für die betroffene Person führt19 , ist in diesem speziellen Fall kein Risiko zu erkennen, dass die Verletzung zu physischen, materiellen oder immateriellen Schäden der betroffenen Person aufgrund der unbefugten Offenlegung der Informationen zur Laktoseintoleranz führt. Im Gegensatz zu einigen anderen Lebensmittelpräferenzen kann Laktoseintoleranz normalerweise nicht mit religiösen oder philosophischen Überzeugungen in Verbindung gebracht werden. Auch die Menge der verletzten Daten und die Anzahl der betroffenen Personen ist sehr gering.

6.3.2 FALL Nr. 15 - Schadensminderung und Verpflichtungen

116. Zusammenfassend lässt sich feststellen, dass der Verstoß keine wesentlichen Auswirkungen auf die betroffenen Personen hatte. Die Tatsache, dass der für die Verarbeitung Verantwortliche die Empfänger sofort nach Bekanntwerden des Fehlers kontaktiert hat, kann als mildernder Umstand betrachtet werden.

117. Wenn eine E-Mail an einen falschen/unberechtigten Empfänger gesendet wird, wird empfohlen, dass der für die Datenverarbeitung Verantwortliche eine Bcc-Folge-E-Mail an die unbeabsichtigten Empfänger sendet, in der er sich entschuldigt, anweist, dass die beanstandete E-Mail gelöscht werden soll, und die Empfänger darauf hinweist, dass sie nicht berechtigt sind, die ihnen bekannten E-Mail-Adressen weiter zu verwenden.

118. Aufgrund dieser Tatsachen war es unwahrscheinlich, dass diese Datenverletzung zu einem Risiko für die Rechte und Freiheiten der betroffenen Personen führt, daher war keine Benachrichtigung der ORKB oder der betroffenen Personen erforderlich. Allerdings muss auch diese Datenverletzung gemäß Artikel 33 (5) dokumentiert werden.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
	X	**X**

6.4 FALL Nr. 16: Schneckenpostfehler

Ein Versicherungskonzern bietet Kfz-Versicherungen an. Dazu verschickt sie regelmäßig angepasste Beitragspolicen per Schneckenpost. Der Brief enthält neben dem Namen und der Adresse des Versicherungsnehmers das Kfz-Kennzeichen, die Versicherungstarife des aktuellen und des nächsten Versicherungsjahres, die ungefähre Jahresfahrleistung und das Geburtsdatum des Versicherungsnehmers. Gesundheitsdaten gemäß Artikel 9 GDPR, Zahlungsdaten (Bankverbindung), Wirtschafts- und Finanzdaten sind nicht enthalten.

Briefe werden von automatischen Kuvertiermaschinen verpackt. Aufgrund eines mechanischen Fehlers werden zwei Briefe für unterschiedliche Versicherungsnehmer in einen Umschlag gesteckt und per Briefpost an einen Versicherungsnehmer verschickt. Der Versicherungsnehmer öffnet den Brief zu Hause und wirft einen Blick auf seinen korrekt zugestellten Brief sowie auf den

6.4.1 FALL Nr. 16 - Vorherige Maßnahmen und Risikobewertung

119. Der fehlerhaft zugestellte Brief enthält Name, Adresse, Geburtsdatum, Kennzeichen und die Einstufung des Versicherungstarifs des laufenden und des nächsten Jahres. Erhöht sich der Versicherungstarif im Folgejahr, deutet dies auf einen bei der Versicherung eingereichten Kfz-Schaden hin. Die Auswirkungen auf den Betroffenen sind als mittel einzustufen, da nicht öffentlich zugängliche Informationen wie Geburtsdatum oder Kfz-Kennzeichen und bei einer Erhöhung des Versicherungstarifs ein nicht unerheblicher Schadensfall, der auch ein Unfall gewesen sein könnte, dem unberechtigten Empfänger bekannt wurde. Die Wahrscheinlichkeit eines Missbrauchs dieser Daten wird als gering bis mittel eingeschätzt. Während viele Empfänger den falsch erhaltenen Brief wahrscheinlich im Müll entsorgen werden, kann im Einzelfall jedoch nicht gänzlich ausgeschlossen werden, dass der Brief in sozialen Netzwerken gepostet wird oder der Versicherungsnehmer kontaktiert wird.

6.4.2 FALL Nr. 16 - Abmilderung und Verpflichtungen

120. Der Controller sollte sich das Originaldokument auf eigene Kosten zurücksenden lassen. Der falsche Empfänger sollte außerdem darüber informiert werden, dass er die gelesenen Informationen nicht missbrauchen darf.

121. Es wird wahrscheinlich nie möglich sein, einen Postzustellungsfehler bei einer Massensendung mit vollautomatischen Maschinen vollständig zu verhindern. Im Falle einer erhöhten Häufigkeit ist jedoch zu prüfen, ob die Kuvertiermaschinen ausreichend korrekt eingestellt und gewartet sind oder ob ein anderes systemisches Problem zu einem solchen Verstoß führt.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen
		X

6.5 Organisatorische und technische Maßnahmen zur Verhinderung / Minderung der Auswirkungen von Falschparkern

122. Eine Kombination der unten genannten Maßnahmen - angewandt je nach den Besonderheiten des Falles - sollte dazu beitragen, die Wahrscheinlichkeit zu verringern, dass sich eine ähnliche Verletzung wiederholt.

123. Empfehlenswerte Maßnahmen:

(*Die Auflistung der folgenden Maßnahmen ist keineswegs ausschließlich oder umfassend. Das Ziel ist vielmehr, Präventionsideen und mögliche Lösungen zu liefern. Jede Verarbeitungstätigkeit ist anders, daher sollte der Controller die Entscheidung treffen, welche Maßnahmen für die gegebene Situation am besten geeignet sind*).

- Exakte Vorgaben - ohne Interpretationsspielraum - für den Versand von Briefen/E-Mails.
- Adäquate Schulung des Personals für den Versand von Briefen/E-Mails.
- Wenn Sie E-Mails an mehrere Empfänger senden, werden diese standardmäßig im Feld "bcc" aufgeführt.
- Beim Senden von E-Mails an mehrere Empfänger ist eine zusätzliche Bestätigung erforderlich, und sie werden nicht im Feld "bcc" aufgeführt.

- Anwendung des Vier-Augen-Prinzips.
- Automatische Adressierung statt manueller, wobei die Daten aus einer verfügbaren und aktuellen Datenbank entnommen werden; das automatische Adressierungssystem sollte regelmäßig auf versteckte Fehler und falsche Einstellungen überprüft werden.

- Anwendung der Nachrichtenverzögerung (z. B. kann die Nachricht innerhalb einer bestimmten Zeitspanne nach Anklicken der Schaltfläche "Drücken" gelöscht / bearbeitet werden).
- Deaktivieren der automatischen Vervollständigung beim Eingeben von E-Mail-Adressen.
- Awareness-Sitzungen zu den häufigsten Fehlern, die zu einer Verletzung persönlicher Daten führen.
- Schulungen und Handbücher über den Umgang mit Vorfällen, die zu einer Verletzung des Schutzes personenbezogener Daten führen, und darüber, wer zu informieren ist (Einbeziehung des DSB).

7 ANDERE FÄLLE - SOCIAL ENGINEERING

7.1 FALL Nr. 17: Identitätsdiebstahl

Das Kontaktzentrum eines Telekommunikationsunternehmens erhält einen Telefonanruf von jemandem, der sich als Kunde ausgibt. Der vermeintliche Kunde fordert das Unternehmen auf, die E-Mail-Adresse zu ändern, an die von nun an die Rechnungsinformationen gesendet werden sollen. Der Mitarbeiter des Kontaktzentrums überprüft die Identität des Kunden, indem er nach bestimmten persönlichen Daten fragt, wie sie in den Verfahren des Unternehmens festgelegt sind. Der Anrufer gibt korrekt die Steuernummer und die Postanschrift des angefragten Kunden an (da er Zugang zu diesen Elementen hatte). Nach der Validierung nimmt der Betreiber die gewünschte Änderung vor, und von da an werden die Rechnungsdaten an die neue E-Mail-Adresse gesendet. Das Verfahren sieht keine Benachrichtigung an den früheren E-Mail-Kontakt vor. Im darauffolgenden Monat kontaktiert der rechtmäßige Kunde das Unternehmen und erkundigt sich, warum er keine Rechnungen an seine E-Mail-Adresse erhält, und verneint jeden

7.1.1 FALL Nr. 17 - Risikobewertung, Risikominderung und Verpflichtungen

124. Dieser Fall dient als Beispiel dafür, wie wichtig vorherige Maßnahmen sind. Die Verletzung stellt unter Risikoaspekten ein hohes Risiko dar, da Abrechnungsdaten Auskunft über das Privatleben der betroffenen Person geben können (z. B. Gewohnheiten, Kontakte) und zu materiellem Schaden führen könnten (z. B. Stalking, Gefährdung der körperlichen Unversehrtheit). Die bei diesem Angriff erlangten personenbezogenen Daten können auch dazu verwendet werden, um eine Kontoübernahme in dieser Organisation zu ermöglichen oder weitere Authentifizierungsmaßnahmen in anderen Organisationen auszunutzen. In Anbetracht dieser Risiken sollte die "angemessene" Authentifizierungsmaßnahme eine hohe Messlatte erfüllen, je nachdem, welche personenbezogenen Daten als Ergebnis der Authentifizierung verarbeitet werden können.

125. Infolgedessen sind sowohl eine Meldung an die SA als auch eine Mitteilung an die betroffene Person vom für die Verarbeitung Verantwortlichen erforderlich.

126. Der vorherige Client-Validierungsprozess ist angesichts dieses Falls eindeutig zu verfeinern. Die zur Authentifizierung verwendeten Methoden waren nicht ausreichend. Die böswillige Partei war in der Lage, sich als der beabsichtigte Benutzer auszugeben, indem sie öffentlich verfügbare Informationen und Informationen, auf die sie anderweitig Zugriff hatte, nutzte.

127. Die Verwendung dieser Art von statischer wissensbasierter Authentifizierung (bei der sich die Antwort nicht ändert und die Informationen nicht "geheim" sind, wie es bei einem Passwort der Fall

wäre) wird nicht empfohlen.

128. Stattdessen sollte die Organisation eine Form der Authentifizierung verwenden, die zu einem hohen Maß an Vertrauen führt, dass es sich bei dem authentifizierten Benutzer um die beabsichtigte Person und nicht um eine andere handelt. Die Einführung einer Out-of-Band-Multifaktor-Authentifizierungsmethode würde das Problem lösen, z. B. um die Änderungsanforderung zu verifizieren, indem eine Bestätigungsanforderung an den ehemaligen Kontakt gesendet wird; oder das Hinzufügen zusätzlicher Fragen und die Forderung

Informationen, die nur auf den vorherigen Rechnungen sichtbar sind. Die Entscheidung, welche Maßnahmen eingeleitet werden, liegt in der Verantwortung des Controllers, da er die Details und Anforderungen seines internen Betriebs am besten kennt.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen

7.2 FALL Nr. 18: E-Mail-Exfiltration

Eine SB-Warenhauskette entdeckte drei Monate nach der Konfiguration, dass einige E-Mail-Konten verändert und Regeln erstellt worden waren, sodass jede E-Mail, die bestimmte Ausdrücke (z. B. "Rechnung", "Zahlung", "Banküberweisung", "Kreditkartenauthentifizierung", "Bankverbindung") enthielt, in einen unbenutzten Ordner verschoben und auch an eine externe E-Mail-Adresse weitergeleitet wurde. Außerdem war zu diesem Zeitpunkt bereits ein Social-Engineering-Angriff durchgeführt worden, d. h. der Angreifer, der sich als Lieferant ausgab, hatte die Kontodaten des Lieferanten in seine eigenen geändert. Schließlich waren zu diesem Zeitpunkt bereits mehrere gefälschte Rechnungen versendet worden, die die neue Bankverbindung enthielten. Das Überwachungssystem der E-Mail-Plattform gab schließlich eine Warnung zu den Ordnern aus. Das Unternehmen konnte zwar nicht feststellen, wie der Angreifer überhaupt Zugriff auf die E-Mail-Konten erlangen konnte, vermutete aber, dass eine infizierte E-Mail dafür verantwortlich war, dass die für die Zahlungen zuständige Benutzergruppe Zugriff erhielt.

Aufgrund der stichwortbasierten Weiterleitung von E-Mails erhielt der Angreifer Informationen über 99 Mitarbeiter: Name und Lohn eines bestimmten Monats in Bezug auf 89 betroffene Personen; Name, Familienstand, Anzahl der Kinder, Lohn, Arbeitsstunden und Restinformationen

7.2.1 FALL Nr. 18 - Risikobewertung, Risikominderung und Verpflichtungen

129. Auch wenn der Angreifer wahrscheinlich nicht das Ziel hatte, personenbezogene Daten zu sammeln, da die Verletzung sowohl zu materiellem (z. B. finanziellem Verlust) als auch zu immateriellem Schaden (z. B. Identitätsdiebstahl oder Betrug) führen könnte oder die Daten zur Erleichterung anderer Angriffe (z. B. Phishing) verwendet werden könnten, führt die Verletzung der personenbezogenen Daten wahrscheinlich zu einem hohen Risiko für die Rechte und Freiheiten natürlicher Personen. Daher sollte die Verletzung allen 99 Mitarbeitern mitgeteilt werden und nicht nur den 10 Mitarbeitern, deren Gehaltsinformationen durchgesickert sind.

130. Nach Bekanntwerden des Verstoßes erzwang der Controller eine Passwortänderung für die kompromittierten Konten, blockierte den Versand von E-Mails an das E-Mail-Konto des Angreifers, benachrichtigte den Dienstanbieter der vom Angreifer verwendeten E-Mail über seine Aktionen, entfernte die vom Angreifer gesetzten Regeln und verfeinerte die Warnmeldungen des Überwachungssystems, um eine Warnung auszugeben, sobald eine automatische Regel erstellt wird. Alternativ könnte der Controller den Anwendern das Recht entziehen, Weiterleitungsregeln zu setzen, so dass das IT-Serviceteam dies nur noch auf Anfrage tun muss, oder er könnte eine Richtlinie einführen, dass die Anwender die auf ihren Konten gesetzten Regeln einmal pro Woche oder in Bereichen, in denen mit Finanzdaten gearbeitet wird, häufiger überprüfen und melden müssen.

131. Die Tatsache, dass eine Sicherheitsverletzung so lange unentdeckt bleiben konnte und die Tatsache, dass in einem längeren Zeitraum Social Engineering zur Veränderung weiterer Daten hätte eingesetzt

werden können, hat erhebliche Probleme im IT-Sicherheitssystem des Controllers aufgezeigt. Diese sollten unverzüglich angegangen werden, z. B. durch die Betonung von Automatisierungsprüfungen und Änderungskontrollen sowie Maßnahmen zur Erkennung von Vorfällen und zur Reaktion darauf. Controller, die mit sensiblen Daten, Finanzinformationen usw. umgehen, haben eine größere Verantwortung in Bezug auf die Gewährleistung einer angemessenen Datensicherheit.

Erforderliche Maßnahmen aufgrund der identifizierten Risiken		
Interne Dokumentation	Benachrichtigung an SA	Mitteilung an die betroffenen Personen